

Introduction to Network Security

“शिक्षा मानव को बन्धनों से मुक्त करती है और आज के युग में तो यह लोकतंत्र की भावना का आधार भी है। जन्म तथा अन्य कारणों से उत्पन्न जाति एवं वर्गगत विषमताओं को दूर करते हुए मनुष्य को इन सबसे ऊपर उठाती है।”

— इन्दिरा गांधी

“Education is a liberating force, and in our age it is also a democratising force, cutting across the barriers of caste and class, smoothing out inequalities imposed by birth and other circumstances.”

— Indira Gandhi



MSEI-022

Network Security

Indira Gandhi National Open University
School of Vocational Education and Training

Block

1

INTRODUCTION TO NETWORK SECURITY

UNIT 1

Network Security Concepts

5

UNIT 2

Network Security Techniques

32

UNIT 3

Identity Management

60

UNIT 4

Security Issues in Wireless and Next Generation Networks

83

Programme Expert/Design Committee of Post Graduate Diploma in Information Security (PGDIS)

Prof. K.R. Srivathsan
Pro Vice-Chancellor, IGNOU

Mr. B.J. Srinath, Sr. Director & Scientist 'G', CERT-In, Department of Information Technology, Ministry of Communication and Information Technology, Govt of India

Mr. A.S.A Krishnan, Director, Department of Information Technology, Cyber-Laws and E-Security Group, Ministry of Communication and Information Technology, Govt of India

Mr. S. Balasubramony, Dy. Superintendent of Police, CBI, Cyber Crime Investigation Cell Delhi

Mr. B.V.C. Rao, Technical Director, National Informatics Centre, Ministry of Communication and Information Technology

Prof. M.N. Doja, Professor, Department of Computer Engineering, Jamia Milia Islamia New Delhi

Dr. D.K. Lobiyal, Associate Professor, School of Computer and Systems Sciences, JNU New Delhi

Mr. Omveer Singh, Scientist, CERT-In, Department of Information Technology, Cyber-Laws and E-Security Group, Ministry of Communication and Information Technology Govt of India

Dr. Vivek Mudgil, Director, Eninov Systems Noida

Mr. V.V. Subrahmanyam, Assistant Professor School of Computer and Information Science IGNOU

Mr. Anup Girdhar, CEO, Sedulity Solutions & Technologies, New Delhi

Prof. A.K. Saini, Professor, University School of Management Studies, Guru Gobind Singh Indraprastha University, Delhi

Mr. C.S. Rao, Technical Director in Cyber Security Division, National Informatics Centre Ministry of Communication and Information Technology

Prof. C.G. Naidu, Director, School of Vocational Education & Training, IGNOU

Prof. Manohar Lal, Director, School of Computer and Information Science, IGNOU

Prof. K. Subramanian, Director, ACIL, IGNOU Former Deputy Director General, National Informatics Centre, Ministry of Communication and Information Technology, Govt of India

Prof. K. Elumalai, Director, School of Law IGNOU

Dr. A. Murali M Rao, Joint Director, Computer Division, IGNOU

Mr. P.V. Suresh, Sr. Assistant Professor School of Computer and Information Science IGNOU

Ms. Mansi Sharma, Assistant Professor School of Law, IGNOU

Ms. Urshla Kant
Assistant Professor, School of Vocational Education & Training, IGNOU
Programme Coordinator

Block Preparation

Unit Writers

Dr. K.Kiran Kumar
Reader, Department of
Computer Science
P.G. Center, P.B.S.College
Vijayawada
(Unit 1, 2, 3 & 4)

Block Editor

Mr. Anup Girdhar, CEO
Sedulity Solutions &
Technologies, New Delhi
Ms. Urshla Kant,
Assistant Professor, School
of Vocational Education &
Training, IGNOU

Proof Reading

Ms. Urshla Kant
Assistant Professor
School of Vocational
Education & Training
IGNOU

Production

Mr. B. Natrajan
Dy. Registrar (Pub.)
MPDD, IGNOU, New Delhi

Mr. Jitender Sethi
Asstt. Registrar (Pub.)
MPDD, IGNOU, New Delhi

Mr. Hemant Parida
Proof Reader
MPDD, IGNOU, New Delhi

July, 2011

© Indira Gandhi National Open University, 2011

ISBN-978-81-266-5505-2

All rights reserved. No part of this work may be reproduced in any form, by mimeograph or any other means, without permission in writing from the Indira Gandhi National Open University.

Further information about the School of Vocational Education and Training and the Indira Gandhi National Open University courses may be obtained from the University's office at Maidan Garhi, New Delhi-110068. or the website of IGNOU www.ignou.ac.in

Printed and published on behalf of the Indira Gandhi National Open University, New Delhi, by the Registrar, MPDD

Laser typeset by Mcronics Printographics, 27/3 Ward No. 1, Opp. Mother Dairy, Mehrauli, New Delhi-30

COURSE INTRODUCTION

Generally, the terms privacy, integrity and confidentiality are loosely construed to be synonymous with security. This course deals with Network security. It is required for the protection of data against accidental or intentional destruction, disclosure or modification. Network security refers to the technological safeguards and managerial procedure which can ensure that organizational assets and individual privacy are protected over the network.

Network security is needed to secure the data, to prevent it from hacker and to protect the network. This course introduces many of the methods to secure the network such as authentication, authorization, firewalls, antivirus, cryptography etc.

Authentication is the process of giving a person the permission to access the database or information on network for example— Providing of passwords in order to gain access to a system or some parts of a system. It is used to secure data. It restricts unauthorized access to our system. Only the person who knows the password can gain access to the system.

Firewalls is a special program designed for preventing hackers from breaking into the corporate network stopping users on the internet corporate network from gaining access to any internet resources that may prove harmful to the network. Hackers on the Internet can do harm in a number of ways. They can steal or damage important data and can damage an individual computer on the entire network. The best way to protect a computer against viruses in to use antivirus software. There are several kinds of anti-virus softwares available in the market.

Cryptography is the science and art of secret writing. One of the most powerful and important methods for security in computer systems is to encrypt sensitive records and messages in transit and in storage. Cryptography is the process used to encode (encrypt) an electronic information.

This course emphasize on the importance of network security in order to ensure that only specific authorized users are allowed to access control over information on a computer.

This course includes the following blocks:

Block 1 – Introduction to Network Security

Block 2 – Secure Protocols

Block 3 – Cryptography Techniques

Block 4 – Network Security Technology

BLOCK INTRODUCTION

Computers have become an integral part of our life and network security threats are something that we usually fear and hear about often. Whether it is a personal computer or a computer being used in a huge corporate company, each computer needs to be protected from the computer network security threats. The moment we have a computer ready to be used, we also have it readily exposed to the network security threats such as various virus and bugs which can damage the functionality of the computer. In addition to these network security threats the personal information of the owner which might be stored in the computer is also at risk if the computer has not been protected from the hackers who are ever ready to steal that stored information from your computer. Introduction to Network Security is very essential and it will work as a rescue. This block comprises of four units and is designed in the following way;

The **Unit one** covers all the threats and mechanisms in the Network Security. The common threats in Network Security are Masquerade, Replay, Modification of messages, and Denial of service, Trapdoor and Trojan horses. The mechanisms are Cryptography & Digital Signatures, Authentication, Access Control Lists and others. Cryptography & Digital Signatures consists of Shared Key cryptography, Public Key Cryptography, Hashing/message digest, Applying cryptography. The other availability Mechanisms are Backup & Restore, Environment, Redundancy, Application/Service Redundancy, RAID/Mirroring, System Redundancy, Full Hardware Redundancy.

The **Unit two** covers the detailed descriptions of the digital water marking, Active Directory Controller and digital forensics. The available types of watermarks are public, private, fragile, video, audio, text and image. The structure of the Active Directory Controller includes Forests, trees, domains, Flat-filed, simulated hierarchy and Shadow Groups. The different Structural divisions to improve performance are FSMO Roles, Trust, Adding Users and Computers to the Active Directory Domain and Using Active Directory with Desktop Delivery Controller.

The **Unit three** explains biometrics in the Network Security. The biometrics was implemented by applying different mechanisms. The common biometrics is Finger printing, Login, All physical security, Face recognition and iris recognition. The available biometrics is Fingerprint Recognition, Face Recognition, Iris Recognition, Voice Recognition, Smart Cards, Encryption Systems and Security Tokens and others. Biometrics consists of Summary of biometrics mechanisms and implementation.

Unit four describes different threats posed by malicious fuzzing and how systematic robustness testing can pre-emptively eliminate the threats while using Bluetooth, Wi-Fi and WiMAX. It also covers cellular technologies, which enjoyed immunity in the past, as well as some emerging new wireless technologies.

Hope you benefit from this block.

ACKNOWLEDGEMENT

The material we have used is purely for educational purposes. Every effort has been made to trace the copyright holders of material reproduced in this book. Should any infringement have occurred, the publishers and editors apologize and will be pleased to make the necessary corrections in future editions of this book.

UNIT 1 NETWORK SECURITY CONCEPTS

Structure

- 1.0 Introduction
- 1.1 Objectives
- 1.2 Network Security Threats
 - 1.2.1 Masquerade
 - 1.2.2 Replay
 - 1.2.3 Modification of Messages
 - 1.2.4 Denial of Service
 - 1.2.5 Trapdoor
 - 1.2.6 Trojan Horses
- 1.3 Security Mechanisms
 - 1.3.1 Cryptography & Digital Signatures
 - 1.3.1.1 Shared or Symmetric Key Cryptography
 - 1.3.1.2 Public Key Cryptography
 - 1.3.1.3 Hashing/Message Digest
 - 1.3.1.4 Applying Cryptography
 - 1.3.2 Authentication
 - 1.3.2.1 Summary of Authentication Mechanisms
 - 1.3.2.2 Authentication Products
 - 1.3.3 Access Control Lists (ACLs)
 - 1.3.4 Availability Mechanisms
- 1.4 Let Us Sum Up
- 1.5 Check Your Progress: The Key
- 1.6 Suggested Readings

1.0 INTRODUCTION

In any computing or communication system, there are entities – people, applications, programs, etc. – which are authorized to use the system. Attacks on a system can be categorized as insider or outsider attacks

- 1) **Insider attacks** involve legitimate users of the system behaving in an unintended or unauthorized manner.
- 2) **Outsider attacks** are conducted by non-legitimate users of the system.

Computers have become an integral part of our life and network security threats are something that we usually fear and hear about often. Whether it is a personal computer or a computer being used in a huge corporate company, each computer needs to be protected from the computer network security threats. The moment we have a computer ready to be used, we also have it readily exposed to the network security threats such as various virus and bugs which can damage the functionality of the computer. In addition to these network security threats the personal information of the owner which might be stored in the computer is also at risk if the computer has not been protected from the hackers who are ever ready to steal that stored information from your computer.

Network security involves all activities that organizations, enterprises, and institutions undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations. An effective network security strategy requires identifying threats and then choosing the most effective set of tools to combat them.

In order to protect our computers from the network security threats that it is exposed to, we need to first understand the different types of threats that exist, only then we will be able to safeguard our computer. The most common kind of network security threats that computers are exposed to, are the threat of "Viruses". It is important to know that a virus is usually sent as a downloadable attachment which is in the form of an executable file. Once a person downloads a file and runs it, that's when the problem starts. The moment the executable file is "run" the computer gets affected by the network security threats and a virus has now been downloaded by the user.

1.1 OBJECTIVES

After going through this unit, you will be able to:

- describe the Network Security;
- understand different types of security threats;
- discuss the Security Mechanisms; and
- list of Access Control.

1.2 NETWORK SECURITY THREATS

The most common types of attacks are summarized as follows:

1.2.1 Masquerade

This is when an entity pretends to be a different entity. For instance, authentication sequences can be captured and replayed after a valid authentication sequence has taken place. In this way, the capturing entity assumes the identity of the entity whose authentication was compromised. A masquerade is thus usually used with some other form of active attack. A masquerade is a type of attack where the attacker pretends to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen logon IDs and passwords, through finding security gaps in programs, or through bypassing the authentication mechanism. The attempt may come from within an organization, for example, from an employee; or from an outside user through some connection to the public network. Weak authentication provides one of the easiest points of entry for a masquerade, since it makes it much easier for an attacker to gain access. Once the attacker has been authorized for entry, they may have full access to the organization's critical data and may be able to modify and delete software and data, and make changes to network configuration and routing information.

1.2.2 Replay

This occurs when a message, or part of a message, is repeated to produce an unauthorized effect. For example a valid message containing authentication sequences can be replayed by another entity in order to authenticate itself. A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or

by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution.

Example

Suppose Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Mallory is eavesdropping the conversation and keeps the password. After the interchange is over, Mallory connects to Bob posing as Alice; when asked for a proof of identity, Mallory sends Alice's password read from the last session, which Bob accepts.

Example - Countermeasures

A way to avoid replay attacks is using session tokens:

Bob sends a one-time token to Alice, which Alice uses to transform the password and send the result to Bob (e.g. computing a hash function of the session token appended to the password). On his side Bob performs the same computation; if and only if both values match, the login is successful. Now suppose Mallory has captured this value and tries to use it on another session; Bob sends a different session token, and when Mallory replies with the captured value it will be different from Bob's computation.

Session tokens should be chosen by a (pseudo-) random process. Otherwise Mallory may be able to guess some future token and convince Alice to use that token in her transformation. Mallory can then replay her reply at a later time, which Bob will accept.

Bob can also send nonce's but should then include a Message authentication code (MAC), which Alice should check.

Example - Implementing Time stamping

This is another way of preventing a replay attack. Synchronization should be achieved using a secure protocol. For example Bob periodically broadcasts the time on his clock together with a MAC. When Alice wants to send Bob a message, she includes her best estimate of the time on his clock in her message, which is also authenticated. Bob only accepts messages for which the timestamp is within a reasonable tolerance. The advantage of this scheme is that Bob does not need to generate (pseudo-) random numbers.

1.2.3 Modification of Messages

This occurs when the content of a data transmission is altered without de"Allow Karen Jones to read confidential file 'accounts' "is changed to "Allow Tim Smith to read confidential file 'accounts'".

A system is used to analyze the implementation of a protocol by a device-under-analysis (DUA). The system includes a source endpoint, a destination endpoint (the DUA), and a message generator. The source endpoint generates an original message and attempts to send it to the DUA. The original message is intercepted by the message generator, which generates a replacement message. The replacement message is then sent to the DUA instead of the original message. The structure recognition system determines the underlying structure and/or semantics of a message. After the structure recognition system has determined the structure, it creates a description of the structure. The mutation system modifies the message based on the structure description to generate a replacement message.

For example, a security analyzer sends one or more messages (test messages) to the DUA, and the DUA's response is observed. A response can include, for example,

registering an error or generating a message (response message). The DUA can then send the response message to the security analyzer. Depending on the analysis being performed, the security analyzer might send another test message to the DUA upon receiving the response message from the DUA. The test messages and response messages can be analyzed to determine whether the DUA operated correctly.

1.2.4 Denial of Service

This occurs when an entity fails to perform its proper function or acts in a way that prevents other entities from performing their proper functions. Examples are general, or targeted suppression of messages and/or traffic, or generation of extra traffic or messages intended to disrupt the operation of the network.

A denial of service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. In a distributed denial-of-service, large numbers of compromised systems (sometimes called a botnet) attack a single target.

Although a DoS attack does not usually result in the theft of information or other security loss, it can cost the target person or company a great deal of time and money. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services. A denial of service attack can also destroy programming and files in affected computer systems. In some cases, DoS attacks have forced Web sites accessed by millions of people to temporarily cease operation.

Denial-of-service (or DoS) attacks are usually launched to make a particular service unavailable to someone who is authorized to use it. These attacks may be launched using one single computer or many computers across the world. In the latter scenario, the attack is known as a distributed denial of service attack. Usually these attacks do not necessitate the need to get access into anyone's system.

Denial-of-service attacks have had an impressive history having, in the past, blocked out websites like Amazon, CNN, Yahoo and eBay. The attack is initiated by sending excessive demands to the victim's computer(s), exceeding the limit that the victim's servers can support and making the servers crash. Sometimes, many computers are entrenched in this process by installing a Trojan on them; taking control of them and then making them send numerous demands to the targeted computer.

The other types of DoS attacks are Ping of Death and SYN attacks. A Ping of Death attack involves a very large Internet Control Messaging Protocol (ICMP) packet and the receiving computer gets it in the form of data packets. Then it tries to reassemble it. When reassembled the packet proves to be too large for the buffers and overflows it. The consequences may be anything from reboots to system hangs.

The SYN attack on the other hand involves the three-way handshake of the TCP/IP protocol. First the client sends a SYN packet to the server. Then the server responds with a SYN-ACK. When the client responds to this, only then does the client-server conversation really start. Now in a SYN attack the client does not respond to the SYN-ACK. It waits till just before the service time expires and then sends another request. This way the server machine remains engaged. The above given process keeps on getting repeated till the server machine crashes. What one must remember is that "Denial of Service" is a generic term for a type of attack, which can take many forms. The Melissa virus came to be called a denial of service attack because it clogged networks and servers with the e-mail it generated.

Denial-of-service attacks come in a variety of forms and aim at a variety of services. There are three basic types of attack:

- consumption of scarce, limited, or non-renewable resources
- destruction or alteration of configuration information
- physical destruction or alteration of network components

A) Consumption of Scarce Resources

Computers and networks need certain things to operate: network bandwidth, memory and disk space, CPU time, data structures, access to other computers and networks, and certain environmental resources such as power, cool air, or even water.

1) Network Connectivity

Denial-of-service attacks are most frequently executed against network connectivity. The goal is to prevent hosts or networks from communicating on the network.

In this type of attack, the attacker begins the process of establishing a connection to the victim machine, but does it in such a way as to prevent the ultimate completion of the connection. In the meantime, the victim machine has reserved one of a limited number of data structures required to complete the impending connection. The result is that legitimate connections are denied while the victim machine is waiting to complete bogus "half-open" connections.

You should note that this type of attack does not depend on the attacker being able to consume your network bandwidth. In this case, the intruder is consuming kernel data structures involved in establishing a network connection. The implication is that an intruder can execute this attack from a dial-up connection against a machine on a very fast network.

2) Using Your Own Resources Against You

In this attack, the intruder uses forged UDP packets to connect the echo service on one machine to the chargen service on another machine. The result is that the two services consume all available network bandwidth between them. Thus, the network connectivity for all machines on the same networks as either of the targeted machines may be affected.

3) Bandwidth Consumption

An intruder may also be able to consume all the available bandwidth on your network by generating a large number of packets directed to your network. Typically, these packets are ICMP ECHO packets, but in principle they may be anything. Further, the intruder need not be operating from a single machine; he may be able to coordinate or co-opt several machines on different networks to achieve the same effect.

4) Consumption of Other Resources

In addition to network bandwidth, intruders may be able to consume other resources that your systems need in order to operate. For example, in many systems, a limited number of data structures are available to hold process information (process identifiers, process table entries, process slots, etc.). An intruder may be able to consume these data structures by writing a simple program or script that does nothing but repeatedly create copies

of itself. Many modern operating systems have quota facilities to protect against this problem, but not all do. Further, even if the process table is not filled, the CPU may be consumed by a large number of processes and the associated time spent switching between processes. Consult your operating system vendor or operating system manuals for details on available quota facilities for your system.

An intruder may also attempt to consume disk space in other ways, including:

- generating excessive numbers of mail messages.
- intentionally generating errors that must be logged
- placing files in anonymous ftp areas or network shares.

In general, anything that allows data to be written to disk can be used to execute a denial-of-service attack if there are no bounds on the amount of data that can be written.

There are other things that may be vulnerable to denial of service that you may wish to monitor. These include:

- printers
- tape devices
- network connections
- other limited resources important to the operation of your organization

B) Destruction or Alteration of Configuration Information

An improperly configured computer may not perform well or may not operate at all. An intruder may be able to alter or destroy configuration information that prevents you from using your computer or network.

For example, if an intruder can change the routing information in your routers, your network may be disabled. If an intruder is able to modify the registry on a Windows NT machine, certain functions may be unavailable.

C) Physical Destruction or Alteration of Network Components

The primary concern with this type of attack is physical security. You should guard against unauthorized access to computers, routers, network wiring closets, network backbone segments, power and cooling stations, and any other critical components of your network. Physical security is a prime component in guarding against many types of attacks in addition to denial of service. For information on securing the physical components of your network, we encourage you to consult local or national law enforcement agencies or private security companies.

Common Forms of Denial of Service Attacks are

Buffer Overflow Attacks

The most common kind of DoS attack is simply to send more traffic to a network address than the programmers who planned its data buffers anticipated someone might send. The attacker may be aware that the target system has a weakness that can be exploited or the attacker may simply try the attack in case it might work. A few of the better-known attacks based on the buffer characteristics of a program or system include:

- Sending e-mail messages that have attachments with 256-character file names to Netscape and Microsoft mail programs
- Sending oversized Internet Control Message Protocol (ICMP) packets (this is also known as the Packet Internet or Inter-Network Groper (ping) of death)
- Sending to a user of the Pine e-mail program a message with a "From" address larger than 256 characters

SYN Attack

When a session is initiated between the Transport Control Program (TCP) client and server in a network, a very small buffer space exists to handle the usually rapid "hand-shaking" exchange of messages that sets up the session. The session-establishing packets include a SYN field that identifies the sequence in the message exchange. An attacker can send a number of connection requests very rapidly and then fail to respond to the reply. This leaves the first packet in the buffer so that other, legitimate connection requests can't be accommodated. Although the packet in the buffer is dropped after a certain period of time without a reply, the effect of many of these bogus connection requests is to make it difficult for legitimate requests for a session to get established. In general, this problem depends on the operating system providing correct settings or allowing the network administrator to tune the size of the buffer and the timeout period.

Teardrop Attack

This type of denial of service attack exploits the way that the Internet Protocol (IP) requires a packet that is too large for the next router to handle be divided into fragments. The fragment packet identifies an offset to the beginning of the first packet that enables the entire packet to be reassembled by the receiving system. In the teardrop attack, the attacker's IP puts a confusing offset value in the second or later fragment. If the receiving operating system does not have a plan for this situation, it can cause the system to crash.

Smurf Attack

In this attack, the perpetrator sends an IP ping request to a receiving site. The ping packet specifies that it be broadcast to a number of hosts within the receiving site's local network. The packet also indicates that the request is from another site, the target site that is to receive the denial of service. The result will be lots of ping replies flooding back to the innocent, spoofed host. If the flood is great enough, the spoofed host will no longer be able to receive or distinguish real traffic.

Viruses

Computer viruses, which replicate across a network in various ways, can be viewed as denial-of-service attacks where the victim is not usually specifically targeted but simply a host unlucky enough to get the virus. Depending on the particular virus, the denial of service can be hardly noticeable ranging all the way through disastrous.

Physical Infrastructure Attacks

Here, someone may simply snip a fiber optic cable. This kind of attack is usually mitigated by the fact that traffic can sometimes quickly be rerouted.

1.2.5 Trapdoor

When an entity of a system is altered to allow an attacker to produce an unauthorized effect on command or at a predetermined event or sequence of events, the result is called a trapdoor. An example is modification of the password validation process so that, in addition to its normal effect, it also validates an attacker's password.

Trap door is basically an entry point into a program that allows someone who is aware of trapdoor to gain access, it is basically used for security purposes and used by programmers to debug and test programmes, and to avoid necessary setup and authentication method to activate programme if something is wrong with the authentication procedure.

1.2.6 Trojan Horses

Trojan horse attacks pose one of the most serious threats to computer security. If you were referred here, you may have not only been attacked but may also be attacking others unknowingly. This page will teach you how to avoid falling prey to them, and how to repair the damage if you already did. According to legend, the Greeks won the Trojan war by hiding in a huge, hollow wooden horse to sneak into the fortified city of Troy. In today's computer world, a Trojan horse is defined as a "malicious, security-breaking program that is disguised as something benign". For example, you download what appears to be a movie or music file, but when you click on it, you unleash a dangerous program that erases your disk, sends your credit card numbers and passwords to a stranger, or lets that stranger hijack your computer to commit illegal denial of service attacks like those that have virtually crippled the DALnet IRC network for months on end.

A Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk. In one celebrated case, a Trojan horse was a program that was supposed to find and destroy computer viruses. A Trojan horse may be widely redistributed as part of a computer virus.

Check Your Progress 1

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) Explain masquerade attack?

.....
.....
.....
.....

2) Explain Denial of Service attack.

.....
.....
.....
.....

3) List out various countermeasures for replay attack?

.....
.....
.....
.....

.....

.....

.....

.....

.....

1.3 SECURITY MECHANISMS

Cryptography, Access control lists, Authentication, implementation of rules & policies and availability mechanisms.

1.3.1 Cryptography & Digital Signatures

Cryptography is the translation of information (known as plaintext) into a coded form (known as ciphertext) using a key. Cryptography is mostly used to protect the privacy of information. In a strong cryptosystem, the original information (plaintext) can only be recovered by the use of the decryption key. So the plaintext information is protected from "prying eyes". A strong encryption algorithm is one who cannot be easily inverted on a Supercomputer today (i.e. the PC in 10 years time). There are two principal methods of cryptography, Shared Key and Public Key cryptography.

1.3.1.1 Shared or Symmetric Key Cryptography

Both parties exchanging data have a key; this key is used to encrypt the data before transmission on one side and to decrypt on receipt on the other side. There are two kinds of symmetric ciphers: Block (which encrypt blocks of data at a time) and stream ciphers (which encrypt each bit/byte or word sequentially). Sample algorithms:

- The well known DES (Data Encryption Standard) is a shared key block cipher. DES was developed under contract to NIST (National Institute of Standards and Technology) by IBM. In basic mode it encrypts 64-bit blocks of plaintext, with a 56 bit key, using 16 iterations of an elaborate combination of table lookups and bit rearrangements.
- The US government certified DES in 1977 (it became an ANSI standard in 1981) and continues to re-certify DES every 5 years. With the advances in computing hardware, DES is now breakable by large organisations with significant resources (by brute force: trying all possible combinations of the key). This is mainly due to the relatively small key size of 56 bits used by DES.
- One solution is the so called Triple-DES or 3DES system, in which the data block is encrypted (two or three) times using three different keys (in a time slightly faster than 3 times a normal encryption). 3DES has a key strength roughly equivalent to 112bits. 3DES has not yet been certified by the US government, but it is unlikely that the original DES will be re-certified again.
- There are several "modes of operation" that DES can use, Electronic Codebook (ECB), Cipher Feedback (CFB) and Cipher Block Chaining (CBC). The U.S. government recommends not using the weakest mode ECB. Unfortunately, many commercial encryption packages use ECB mode.

- DESX is a modified version of DES which apparently strengthens it significantly (see the RSA Faq).
- RC2 is a block cipher from RSA Inc., that was a trade secret until anonymously published on the Internet in 1996. It seems quite strong and allows key sizes between 40 and 255 bits (or 2048 bits??).
- RC4, RC5 are (proprietary) variable key size stream ciphers from RSA Inc., developed in 1994. Since key size is variable, they can be more or less secure than DES. USA export approved versions have approx. 40-bit key sizes. Domestic versions can have keys between 40 and 1024 bits. RC4 is the fastest (it was also published as an Internet draft without RSA's approval, called "ARCFOUR" in 1994) and RC5 is considered the "safest".
- IDEA: Developed by the Swiss ETH University in Zurich and Ascom (patented). Published in 1990 and finalised in 1992 by Lai & Massey, it uses a 128 bit key. No weaknesses are currently known in this algorithm and a brute-force attack will not be feasible in the foreseeable future. It is patented by Ascom Tech AG. The licensing terms are basically: personal use is free and integrating IDEA into a sellable product costs money. PGP uses IDEA as it's symmetric algorithm.
- Blowfish: is a public domain algorithm, that is new (1993) but hasn't shown any major weaknesses. It is fast and compact, with variable key sizes (32-448 bits, typically 128 or 256 bit), uses 8 byte blocks and is optimised for 32 and 64bit processors.
- AES: The Advanced Encryption Standard is designed to replace DES. NIST is accepting proposals until June 1998. It should have keys of 128, 192, 256 bits and use 128 bit blocks. The final algorithm probably won't be available until the year 2000. Schneier has proposed Twofish for AES, which is a 128bit block, 16 round block cipher that is in the public domain, faster than Blowfish and requires few resources (can run on smart cards).
- CAST is a block cipher from Carlisle Adams and Stafford Tavares of Northern Telecom (Nortel). It is fast. Nortel has applied for a patent for CAST, but they have made a commitment in writing to make CAST available to anyone on a royalty-free basis. CAST has no weak or semiweak keys. There are strong arguments that CAST is completely immune to both linear and differential cryptanalysis, the two most powerful forms of cryptanalysis in the published literature, both of which have been effective in cracking DES. CAST is too new to have developed a long track record, but its formal design and the good reputations of its designers will undoubtedly attract the attentions and attempted cryptanalytic attacks of the rest of the academic cryptographic community.

Advantages: Shared key algorithms are much faster than their public key counterparts.

Disadvantages: Both side must know the same key and they must find a secure way of exchanging it (via a separate secure channel).

Typical applications: Encryption of information to protect privacy. i.e. local encryption of data files (where no transmission is required), data session encryption, banking systems (PIN encryption).

1.3.1.2 Public Key Cryptography

Both parties have a private key and a public key. The private keys are known only to their owners, but the public keys are available to anyone (like telephone numbers). The sending party encrypts the message with the receivers public key and the

receiver decrypts with his own private key. This is possible due to the discovery by Diffie and Hellman (at Stanford University, autumn 1975) that algorithms can be developed which use one key for encryption and a different key for decryption. The public and private key constitute a key pair.

The following public key crypto-systems are well known:

- the RSA (named after its inventors Rivest, Shamir and Adleman) algorithm was developed at MIT in 1977 and is the most common public key system in use today. A key minimum key length of 768 bits is recommended by RSA Inc. RSAREF is a library from RSA Inc. which is integrated into many commercial products and public domain products (such as the US version of PGP). International, public domain RSA compatible libraries (with large key sizes) do exist and are used in products such as SSH (SSH uses 1024 bit keys by default). RSA key generation is slower than verification. RSA is patented in the U.S. until 20.9.2000.
- The Diffie-Hellman (named also after its inventors) key exchange protocol, published in 1976, produces shared secret keys from publicly known information over unsecured networks. These shared keys can be used to produce session keys. Its strength is based on the "discrete logarithm" problem. Since parties are not authenticated, it is vulnerable to "man in the middle" attacks, which can be prevented by use additional protocols or digital signatures. Sun make extensive use of this algorithm in Secure RPC and SKIP.

This algorithm has the added advantage that its patent expired in 1997.

- The ElGamal Public Key system (invented by Taher ElGamal) consists of both an encryption and signature algorithm. It is similar to the Diffie-Hellman key exchange and its strength is based on the "discrete logarithm" problem. Key length strengths are similar to RSA. It is quite slow, and requires very good random number generation. DSA is based on the signature algorithm.
- DSS is the Digital Signature Standard, that uses the DSA (Digital Signature Algorithm) approved in May 1994 by the U.S. government (NIST & NSA) as the standard for digital authentication. DSA is based on crypto algorithms from ElGamal and Schnorr. Signature generation is faster than verification (which is unusual, there are likely to be more verifications than generations). DSA lacks a key exchange mechanism, is very new and has been criticised because the NSA were heavily involved in its selection and it was not subject to open peer review.

Advantages of PK: Only the private key need be kept secret. No secret channels need exist for key exchange, since only public keys need be exchanged. However the public key must be transferred to the sender in such a way that he is absolutely sure that it is the correct public key! Public key cryptography also provides a method for digital signatures.

Disadvantages: Slow, due to the mathematical complexity of the algorithms.

Typical applications: Ensuring proof of origin, ensuring that only the receiver can decrypt the information, transmission of symmetric session keys.

1.3.1.3 Hashing/Message Digest

A hash function creates a fixed length string from a block of data. If the function is one way, it is also called a message digest function. These (fast) functions analyse a message and produce a fixed length digest which is practically unique i.e. finding

a message with an identical hash very unlikely with very fast computers. There is no known feasible way of producing another message with the same digest. Such algorithms are normally used to create a signature for a message which can be used to verify its integrity.

- MD2, MD4 and MD5 are hash functions developed by Ron Rivest of RSA Inc. They all produce 128-bit digests. MD2 is the slowest, MD4 the fastest. MD5 has a more conservative design than MD4. Both of these are publicly available.
- The MD5 algorithm is the de-facto hashing standard for digests. Public domain versions are available for most platforms on the Internet and it is widely used in integrity checking systems. SHA-1 (Secure hashing algorithm) is a NIST sponsored hashing function has been adopted by the U.S. government as a standard. It produces a 160-bit hash (i.e. larger than MDx) and is roughly 25% slower than MD5. SHA-1 is recommended over MD5.
- Ripe-MD-160 is an algorithm from the European Community.

Advantages: much faster than encryption and output is fixed length (so even a very large file produces the same digest, which is much more efficient for data transmission).

Disadvantages: guarantees integrity only.

- Known weaknesses: The article, by B. Preneel and P.C. van Oorschot, "On the Security of Two MAC Algorithms", Advances in Cryptography-EUROCRYPT '96, Saragosa, Spain, May 1996. It showed some improvements on known forgery attacks on MD5 envelope method (RFC1828) and banking standard MAA (ISO 8731-2).

Typical applications: Many Internet servers provide MD5 digests for important files made available for downloading. Most digital signature systems and secure email system use a digest function to ensure integrity.

An interesting variation of hashes are Message Authentication Codes (MAC), which are hash functions with a key. To create or verify the MAC, one must have the key. This is useful for verifying that hashes have not been tampered with during transmission. Two examples are HMAC (RFC 2104) and NMAC, based on SHA-1.

1.3.1.4 Applying Cryptography

Applications such as PGP, S/MIME, Secure RPC (and hence secure NFS & NIS+) and SKIP use a combination public key cryptography and symmetric cryptography to ensure non repudiation and privacy. Hashing algorithms are used for (fast) generation of signatures.

- The principal problem with most encryption systems is how to distribute and manage keys. Many systems require manual key-ring management. See Certification Authorities below.

Encryption Strength

There are several possible weaknesses in a crypto system, and the strength of the system is the strength of the weakest link.

- The secrecy of the symmetric or private key.
- The difficulty of guessing the key or trying all possible keys. The key length determines the encryption strength of an algorithm. All cryptographic

algorithms are vulnerable to "brute force" attacks (trying all possible key combinations).

- Bad implementation
 - "Pseudo" random number generators used in encryption engines may be (too) predictable. They must be at least as difficult to predict as it is difficult to guess the encryption key.
 - Algorithms can be incorrectly implemented.
 - Backdoors may exist.
- Bad design
 - Certain algorithms are easily inverted (easy to analyse and break), such as WinWord, Pkzip, WordPerfect etc.
 - Algorithms which are not published and subjected to peer review should not be considered as strong, "security through obscurity" is not a defence against the determined, financially powerful attacker.
 - Known plaintext attack: by encrypting many known texts and analysing the output, it may be possible to guess how the algorithm works.
- Mathematics advances each year, so new mathematical ideas can weaken existing cryptosystems (examples are the discovery of differential and linear cryptanalysis in recent years). The strength of current Public key (PK) systems is based on the difficulty of the mathematical factoring and discrete-logarithm problem. It is not impossible that faster mathematical methods to solving these problems be found, making PK guessing easier.

The following discussion concentrates on the issue of key lengths, but strong keys are useless if the above issues are not addressed!

Computers are getting faster (computing power doubles about every 2 years), cheaper and better networked each year. All cryptographic algorithms are vulnerable to "brute force" attacks (trying all possible key combinations).

Symmetric algorithms

In general, the key length determines the encryption strength of an algorithm with the approximate formula of 2 to the power of the key length, so 56 bit keys take 65,536 times longer to crack than 40 bit keys.

Most products come from the U.S. and are subject to U.S. export restrictions, currently either a 40bit limit or escrowing of keys.

- 30 bits can be "brute force" guessed on a powerful PC.
- 40 bits:
 - In 1995, a French student Damien Doligez succeeded in breaking a 40bit Netscape shared encryption key in 8 days using a network of 120 UNIX machines (by brute force: trying all possible combinations of the key).
 - In 1996, an improved algorithm brought this down to 4 hours.
- 56 bits:
 - In 1997, 56 bit DES keys can be broken by dedicated chips (programmable gate arrays) within 3 weeks and by intelligence organisations such as the NSA within seconds.
 - Rumour has it that the NSA has a machine for several years that cracks DES in about 1-2 seconds.

- 64 bits: are probably breakable by governments and very powerful organisations today.
- 80 bits: probably not breakable today?
- 128 bits: probably not breakable in 50 years?

Public (asymmetric) key algorithms:

- Key strength is more important for public keys since they are often use for digital signatures and non repudiation and are rarely changed.
- Public keys are longer than symmetric keys since the problem is guessing the private key, not the public. For the RSA algorithms this equates to factoring a large integer that has two large prime factors.
 - a 256 bit modulus is easily factored by ordinary people
 - 384 bit keys can be broken by university research groups or companies
 - 512 bits is within reach of major governments
 - Keys with 768 bits are probably not secure in the long term.
 - Keys with 1024 bits and more should be safe for now unless major algorithmic advances are made in factoring
 - keys of 2048 bits are considered by many to be secure for decades

The encryption key size should be chosen, based on:

- Who you wish to protect your information from (resources available to the attacker).
- How easy it is for an attacker to get hold of the encrypted information, e.g. how insecure the transport network is (sending information over the Internet certainly requires more protection than on your local subnet).
- how long the information must be protected. It is better to use weak encryption than not to protect data at all, however the danger of a weak encryption system is that it can give users a false sense of security.

Here we define strong encryption as that which uses key sizes greater than or equal to:

Public Key 1568 bits (for RSA, DH and ElGamal)

Shared key 90 bits

“Strong” for new encryption system such as Elliptical curve or Quantum cryptography is not defined here, as yet.

Attacker	Time Span	Recommended key size
Curious hacker	Information must be protected for a few days.	Public Key 512 bits shared key 40 bits
Curious hacker	Information must be protected for minimum 2 years.	Public Key 1024 bits shared key 60 bits
Large organisation	Information must be protected for minimum 20 years.	Public Key 1568 bits shared key 90 bits
Government	Information must be protected for minimum 20 years.	Public Key 2048 bits shared key 128 bits

The U.S. and certain other countries consider encryption to be a weapon and strictly control exports. This is basically crippling the efforts to include encryption in Applications, Internet services such as Email and Operating systems.

In general the U.S. allows export of 40bit shared key systems and 512 bit public key systems.

- Exceptions: There have been some exceptions to this rule, such as export to Canada & Australia and to large financial institutions world-wide.
- Lotus export Notes with a 64bit key, of which 24bits are escrowed with the U.S. Govt., making more difficult for non U.S. agencies to look at your Notes communications!
- Certain products may be used by U.S. companies outside the U.S.
- Vendors have started building Interfaces into which strong encryption products can be plugged, assuming they're available internationally. E.g. Eudora Pro has a Plugin API which could allow seamless integration strong international encryption unit, without break U.S. law. Other examples are Sun (Solaris DES & Diffie Hellman libraries), Microsoft (NT Secure API), Qualcomm (Eudora Pro + PGP), various PGP Plugins and GUI's.

Some countries (e.g. France), forbid encryption except when a key has been deposit in an escrow (so the legal authorities can listen to all communications if they need).

Other countries allied to the U.S. (e.g. Germany, UK, Sweden, etc.) also enforce the U.S. restrictions by allowing strong encryption domestically, but restricting export of cryptographic devices.

Many countries have almost no restrictions, but some (especially European) countries are considering some kind of restriction of the use of cryptography in the future.

The only strong encryption software widely available internationally, known to the author of this document, are from Australia, Finland, Ireland and Russia.

Digital Time-stamping Service (DTS)

A DTS issues a secure timestamp for a digital document.

- A message digest is produced of the document (by the sender) and sent to the DTS. The DTS sends back the timestamp, plus the date & time the timestamp was received with a secure signature from the DTS. This proves that the document existed on the said date. The document contents remain unknown to the DTS (only the digest is known).
- The DTS must use very long keys, since the timestamp may be required for many years.

Certificates, Certification Authorities (CA), PKI and Trusted Third Parties (TTP)

Certificates are digital documents attesting the identity of an individual to his public key. They allow verification that a particular public key does in fact belong to the presumed owner. The ISO certificate standard is X.509 v3 and is comprised of: Subject name, Subject attributes, Subject public key, Validity dates, Issuer name, Certificate serial number and Issuer signature. X.509 names are similar to X.400 mail addresses, but with a field for an Internet email address. The X.509 standard is used in S/MIME, SSL, S-HTTP, PEM, IPsec Key Management.

LDAP (Lightweight Directory Access Protocol) is an X.500 based directory service for certificate management. Certain secure email products such as PGP5 have inbuilt support for querying and updating LDAP servers.

Certificates are issued by the certification authority (CA). The CA is a trusted authority, who confirms the identity of users. The CA must have a trustworthy public key (i.e. very large) and its private key must be kept in a highly secure location. CAs can also exist in a hierarchy, which lower level CAs trust high CAs.

Where sender and receiver must be absolutely sure of who their Peer is, a CA is a possible solution. Another name for a CA is a Trusted Third Party (TTP). If both sides trust a common authority, this authority can be used to validate credentials from each side. E.g. the sender sends his public key, name (and other validifying information) to the CA. The CA verifies this information as far as possible, add its stamp to the packet and sends it to the receiver. The receiver can now be surer than the sender is who he says he is.

- The problem with CAs are that you have to trust them! However, even Banks have overcome that problem with the implementation of SWIFT, a world wide financial transaction network.

Emergency File Access

A frequent requirement when protecting file confidentiality via encryption is Emergency File Access. If the file owner encrypts an important file and forgets the key, what happens? A second key is created, split into five parts such that any two of the five (partial) keys, when combined, could be used as a decryption key. The five (partial) keys could be kept by separate people, only to be used if the original owner was not able to decrypt the important file.

The Windows version of PGP supports these key splitting functions.

Secure Data Transmission using Cryptography

Secure data transmission is the exchange of data in a secure manner over (presumed) insecure networks.

Requirements

Secure data transmission is required for class systems or higher and can be divided into the following categories:

- 1) **Peer entity authentication:** Both sides (users & processes) must identify & authenticate themselves, prior to the exchange of data.
- 2) **Data integrity:** Data must remain complete during transmission. Unauthorised manipulation of user data, audit trail data and replay of transmissions shall be reliably identified as errors.
- 3) **Data confidentiality:** Only authorised persons should be able to access the data. (e.g. end-to-end data encryption).
- 4) **Data origin authentication:** Does the receiving process know who the data is coming from? For class systems, non repudiation of origin may be required: On receipt of data, it shall be possible to uniquely identify and authenticate the sender of the data. Has the receiver proof (e.g. digital signatures) of where information came from?
- 5) **Non repudiation of receipt:** Has the sender proof that the information sent was received by the intended receiver?
- 6) **Access control:** All information previously transmitted which can be used for unauthorised decryption shall be accessible only to authorised persons.

Secure data transmission is achieved by the use of cryptography. There are two principal cryptographic methods, public key and shared key. Normally a mixture of both is used for secure communication.

Using Cryptography for secure transmission, when choosing an authentication system, choose a signature function and encryption method and hash function that require comparable efforts to break. The encryption algorithms described in the previous section can be combined together to produce a system for secure data transmission (refer to the figure below):

- 1) **Data integrity:** MD5 digests are created on the data part of message.
- 2) For performance reasons, normally it is sufficient to encrypt the MD5 digest noted above. The digest encrypted with the sender's private key is called a signature.
- 3) Non repudiation of receipt: not covered here.
- 4) **Data confidentiality:** Confidential parts of the message are encrypted. Shared key encryption is the most efficient method (performance). Normally the shared key is calculated from information known to both sides e.g. the sender uses his private key + receiver's public key and the receiver uses his private key + sender's public key. They can both generate the same unique key due to the mathematical properties of public key algorithms (i.e. multiplying numbers raised to powers). This data encryption key is often called the session key (it is valid only for a particular session).
- 5) **Peer entity authentication:** Where sender and receiver must be absolutely sure of who their peer is, a certification authority is a possible solution. If both sides trust a common authority, this Authority can be used to validate credentials from each side. E.g. the sender sends his public key, name (and other validating information) to the Authority. The Authority verifies this information as far as possible, add its stamp to the packet and sends it to the receiver. The receiver can now be surer than the sender is who he says he is. Similar encryption and hashing to that above would be applied this data.
- 6) Access control depends on implementation.

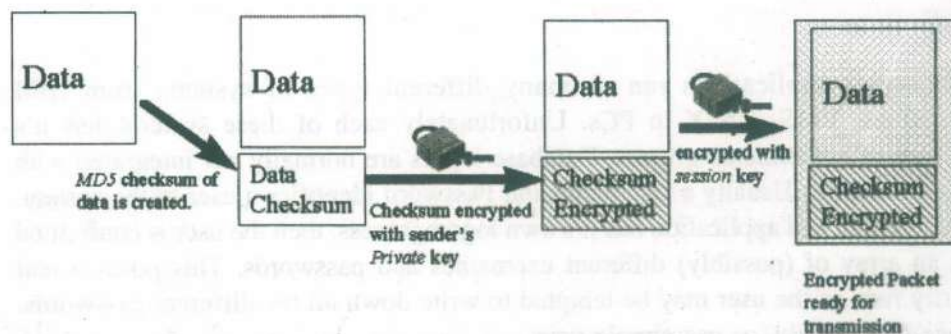


Fig 1: Data is prepared for Transmission

After receipt, the data is decrypted:

Example systems using this approach: Sun's Secure RPC (hence NIS+, NFS), SKIP, S/MIME isn't a million miles away either.

1.3.2 Authentication

Authentication is the process of verifying the identity of a subject. A subject (also called a principal) can be a user, a machine or a process i.e. a "network entity". Authentication uses something which is known to both sides, but not to others i.e. something the subject is, has or knows. Hence this can be biometrics (fingerprints,

retina patterns, hand shape/size, DNA patterns, handwriting, etc.), passphrases, passwords, one-time password lists, identity cards, smart-tokens, challenge-response lists etc. Some systems consist of a combination of the above.

The most common methods of strong authentication today consist of one-time password lists (paper), automatic password generators (smart tokens) and intelligent identity cards.

1.3.2.1 Summary of Authentication Mechanisms

There is no industry standard today. Many different efforts are underway. In particular the Federated Services API, GSS API and RADIUS seem like a logical ways to interconnect the current incompatible systems, without requiring vendors to throw away their existing products. It is hard to imagine such an API offering more than basic functionality however (since advanced functionality is not common to all products). The IETF also have a number of active Authentication groups:

- Authenticated Firewall Traversal (aft)
- Common Authentication Technology (cat)
- One Time Password Authentication (otp)

For enterprise wide authentication and naming services DCE, NIS+ and NODS are the current main runners, with Microsoft's Active Directory service (planned for release with NT5) already generating interest for companies using NT Domains. Support for X.500 directory services will probably appear in most of these, allowing an interoperability gateway to be built. The fact that neither DCE nor NIS+ have been fully adopted in the PC client world is a pity, but perhaps reflects pricing and complexity problems.

SSH is a really impressive product for secure access to UNIX machines. It can use RSA, SecurID or UNIX user/password authentication.

For authentication across unsecured networks, proprietary (incompatible, expensive) encrypting firewalls using certificates or token based authentication are the current solution. Possible future acceptance of proposed standards such as SKIP or IPsec will, hopefully, provide long term interoperability.

Logon

Client/server applications run on many different types of systems from IBM mainframes, VMS, UNIX to PCs. Unfortunately each of these systems has its own way of authenticating users. Database logins are normally not integrated with OS (user) logins. Usually a Username and Password identifies a user to the system. If each system and application has its own logon process, then the user is confronted with an array of (possibly) different usernames and passwords. This poses a real security risk, as the user may be tempted to write down all the different passwords, change them rarely, or use simple ones.

The ideal solution would be to provide a secure single signon. i.e. when a user logs on to a workstation on the network, his identity is established and can be shared with any system or application. Any user can sign from at any system anywhere and have the same name and password. The user needs to remember only one password. An even more secure signon can be achieved by using Personnel ID Cards to validate the user (via a card reader on each workstation) or via hand held Smartcards (with one time passwords).

Achieving single signon is not an easy task in today's heterogeneous environment, but it would seem that Kerberos is the main contender with Sun's NIS+ also an option.

Strong authentication relies (normally) on something the user knows (e.g. a password) and something the user has (e.g. a list, smart card). Applications must support the authentication mechanism (or it must be transparent to the application). The following is a sample of strong firewall authentication methods/products.

Strong authentication mechanisms on Firewalls are very important, if protocols such as Telnet, Rlogin or ftp (writeable) are to be allowed. TCP/IP has inherent security weaknesses (confidentiality, IP spoofing) and these need to be addressed in a strong authentication product. If keys are used, key distribution must be considered.

No standards exist, each product has its own API and interoperability is often very difficult. Some Firewall authentication servers can act as glue, allowing a common database to be used for different authentication products (an example is the Gauntlet authentication server).

HTTP Basic Authentication

A basic authentication method is supported in HTTP.

Algorithm: A WWW client sends a request for a document which is protected by basic authentication. The server refuses access and sends code 401 together with header information indicating that basic authentication is required. The client presents the user with a dialog to input username and password, and passes this to the server. The server checks the user name and password and sends the document back if OK.

Encryption: Very weak. The user name and password are encoded with the base64 method. Documents are sent in clear text.

NT Domains/Lan Manager/SMB & NetBIOS /NetBeui /CIFS

NT's domains are an extension of (IBM/Microsoft) Lan Manager (LM) and are not hierarchical, but domain based - i.e. more suitable for separate LANs.

LM authentication has several dialects: PC NETWORK PROGRAM 1.0, MICROSOFT NETWORKS 3.0, DOS LM1.2X002, DOS LANMAN2.1, Windows for Workgroups 3.1a, NT LM 0.12, CIFS. The last two are the most interesting as they are used in NT4.

- The first few dialects are very old and if supported (and asked for by the client in the SMB protocol), will send passwords in cleartext. The (autumn 1997) patches for NT4 & Win95 mandate the use of encryption by default. The late 1997 version of Samba also supports encryption and more interestingly "pass through" authentication.
- Several weaknesses were published in early 1997 and are partially fixed in NT4.0 SP3 and individual patches. Win95 also has several patches.
- For all dialects except for the last two (i.e. NT4), cracking the encrypted message that passed the network is not that hard: a dictionary attack, coupled with LM's uppercase passwords and division into two 7 byte words makes cracking of words less than 7 characters in a dictionary easy enough.

1.3.2.2 Authentication Products

Kerberos (+ DCE)

Kerberos is a secret-key network authentication service developed at MIT by Project Athena. It is used to authenticate requests for network resources in a distributed, real-time environment. DES (i.e. shared key) encryption and CRC/MD4/MD5

hashing algorithms are used. The source code is freely available (for non-commercial version) and Kerberos runs on many different systems.

Kerberos requires a "security server" or Kerberos server (KDC) which acts as a certification authority, managing keys and tickets. This server maintains a database of secret keys for each principal (user or host), authenticates the identity of a principal who wishes to access secure network resources and generate sessions keys when two users wish to communicate securely.

There are many versions of the Kerberos authentication system: V3 (MIT), V4 (commercial: Transarc, DEC) and V5 (in beta/RFC 1510, DCE, Sesame, NetCheque). BSDI is the only OS to bundle the Kerberos server. Solaris 2 bundles a Kerberos client, which among other things allows NFS to use Kerberos for authentication.

NIS+

NIS+ is a hierarchical enterprise wide naming system, based on Secure RPC. In the default configuration it provides user, group, services naming, automounter and key distribution. NIS+ can be easily extended to define customised tables.

NIS+ is an improved version of the UNIX defacto standard NIS (Network Information System, or yellow pages). NIS & NIS+ were developed by Sun. NIS is available on most UNIX platforms, but has very weak security. NIS+ is much more secure but it only available on Sun's Solaris and recently HP-UX and AIX.

Security is based in the use of Secure RPC, which in turn uses the Diffie/Hellman public key cryptosystem.

- NIS+ is very flexible and can be easily extended to manage customised tables.
- It is stable (Solaris 2.3 or later with the correct patch) enough for production use.
- NIS+ is integrated into the Sun Federated Services (see below) with Solaris 2.5 and higher.

BoKS

BoKS is a full authentication/single signon package for PC and UNIX systems, made by DynaSoft in Sweden. DynaSoft is a 10 year old company employing about 50 people. The BoKS concept has been developed and improved by DynaSoft since 1987. It is a comprehensive security solution covering areas such as access control, strong authentication, encryption, system monitoring, alarms and audit trails. BoKS functions in UNIX and DOS/Windows environments, offers high reliability and is ported to most UNIX platforms. BoKS can also be integrated with enterprise management systems such as Tivoli and database applications such as Oracle and Sybase.

BoKS can use Secure Dynamics SecurID smart tokens. Although the author has little practical experience with BoKS, it seems to be in extensive use where high security is required. Runs on UNIX (SunOS, Solaris and HP-UX) and PCs (Win95 & NT versions should be introduced in late 1996). BoKS uses shared key encryption (40 bit DES outside the U.S., 56bit DES in the U.S.).

OPIE (One-time Passwords in Everything)

OPIE is a public domain release of the U.S. Naval Research Laboratory's. OPIE is an improved version of S/Key Version 1 which runs on POSIX compliant UNIX like systems and has the following additional features to S/Key:

- Simpler (one command installation)
- An OPIE compliant ftp daemon and su, login and passwd utilities are provided.
- MD4 & MD5 are simultaneously supported with MD5 being the default.
- Runs well on Solaris.
- OPIE calculators are available on PCs and MACs too.

ACE Server (SecurID)

The SecurID system from Secure Dynamics is one of the more established names on the market today. It works with most clients (UNIX, NT, VPN clients, terminal servers etc.) and many firewalls provide support for SecurID. The server which manages the user database and allows/refuse access is called ACE and delivered only by Secure Dynamics (whereas clients are delivered by several vendors). The author has used this system for providing secure remote access to hundreds of users on diverse clients.

The tokens are known as SecurID and are basically credit card sized microcomputer, which generate a unique password every minute. In addition each user is attributed a 4 character pin-code (to protect against stolen cards). When a user logs on, he enters his PIN, plus the current pass-code displayed by the SecurID token. The server contains the same algorithm and secret encryption key, allowing both sides to authenticate securely. Software tokens are available for Win95/NT as are SecurID modems from Motorola. The tokens last typically 3 years. This form of authentication is strong, but there is a risk of a session being hijacked (for example if the one time password doesn't change often).

Safeword

Safeword by Secure Computing is direct competition for ACE/SecurID. Its servers run on UNIX. It supports many authentication protocols such as TACACS, TACACS+ and RADIUS.

Many token types are supported: Watchword, Cryptocard, DES Gold & Silver, Safeword Multi-sync and SofToken, AssureNet Pathways SNK (SecureNet Keys).

Watchword

This one time password system from Racal Guardata that are well established competition to the SecurIDs. It works basically as follows:

The server generates a piece of text. The user (on the client) enters this text (called a challenge) into his Watchword calculator. The calculator displays another text, which the users types in. The server verifies that this text was generated by a permitted Watchword calculator and if so, grants access. Attacks could occur in the form of chosen plaintext guessing. Racal Guardata also produce the Access Gateway.

Defender Security System

This system from AssureNet Pathways may be of interest to those using NT servers, since the server runs on NT (not UNIX like most of the above). Features: Authentication via ARA, NT/RAS, TACACS+. Multiple servers are possible via database replication.

The token used are SecureNet Keys (SNK) hardware or software tokens. The challenge/response authentication uses DES, the PIN is never transmitted over the network and sensitive information is encrypted.

Remote Access Control Protocols

RADIUS (Remote Authentication Dial In User Service).

Merit Network and Livingston developed the RADIUS protocol for identification and authentication. There is an IETF working group defining a RADIUS standard.

RADIUS is a vendor independent protocol which should allow multiple dial-in access points to use a centralized user database for authentication. There are however many vendor extensions to the standard and the standard is evolving, meaning that not all implementations are compatible.

RADIUS encrypts password transmitted by a hashing technique using a shared "secret". This secret has to be introduced to both sides by an out of band communication.

XTACACS (Enhanced Terminal Access Controller Access System)

XTACACS is an enhancement on TACACS (Terminal Access Controller Access System), which is a UDP based system from BBN which supports multiple protocols. SLIP/PPP, ARA, Telnet and EXEC protocols are supported.

TACACS+

Also an enhancement on TACACS (from CISCO), but not compatible with XTACACS or TACACS. It allows authentication via S/key, CHAP, PAP in addition to SLIP/PPP and telnet. Authentication and authorisation are separated and may be individually enabled/configured.

TCP is used as opposed to UDP (enhance security).

Information transmitted may be encrypted.

ACLs and password ageing are supported.

Enhanced auditing & billing functions.

Password Authentication protocols: PAP, CHAP

PAP (password authentication protocol) involves the username and password being sent to a server in clear-text. The password database is stored in a weakly encrypted format. CHAP (Challenge Handshake Authentication Protocol) is a challenge/response exchange with a new key being used at each login. However, the password database is not encrypted. Some vendors offer variations of the PAP and CHAP protocols but with enhancements, for example storing passwords in encrypted form in CHAP.

1.3.3 Access Control Lists (ACLs)

An ACL defines who (or what) can access (e.g. use, read, write, execute, delete or create) an object. Access Control Lists (ACL) are the primary mechanism used to ensure data confidentiality and integrity. A system with discretionary access control can discern between users and manages an ACL for each object. If the ACL can be modified by a user (or data owner), it is considered to be discretionary access control. If the ACL must be specified by the system and cannot be changed by the user, mandatory access control is being used. There is no standardised ACLs for access to OS services and applications in UNIX.

- The AIX (optionally), DCE and Windows NT use ACLs to govern access to most objects.
- Solaris 2.5 and later provides ACLs for filesystems (UFS, NFS).
- Normal UNIX also uses ACLs (sort of), but by a different name. For example: protecting files (/etc/groups), protecting sharing of filesystems (/etc/netgroups),

/etc/exports), mounting of filesystems (/etc/fstab), remote access (.rhosts, /etc/hosts.allow), X Windows (xauth, xhost), NIS networks (/etc/securenets), Printers (/etc/hosts.lpd).

1.3.4 Availability Mechanisms

Backup & Restore

- Things to watch out for:
- If possible use heterogeneous products which work on all of your servers.
- On-line indices allow quick retrieval. Backups to disk allow quick restoring.
- Some products allow users to backup and restores their own files without administrator intervention. Jukeboxes (also called tape stackers) reduce the physical work of changing cassettes and can make restore time quicker (more cassettes are available). Some systems automatically label tapes.
- Hardware and software compression can reduce backup times, reduce network load and reduce the number of cassettes needed.
- Network backups load the network significantly, it may not be possible, for example to backup 100 4GB file servers each night over the network. Planning is important.

Environment

The computing environment can be protected with Air Conditioning, locked server rooms and UPS (220V protection).

Redundancy

Redundancy increases availability and may be implemented in hardware (RAID), disk drivers or OS (RAID) or at the application/service level (e.g. Replication, transaction monitors, backup domain controllers).

Application/Service Redundancy

- This is often the cheapest and easiest to implement, where available. The principle problem is that few applications support this type of redundancy. Clients connecting to these servers automatically look for a backup or duplicate server if the primary is not available.
- Naming servers (NIS+, DNS, NIS, WINS, Lan Manager...) often have this capability in-built and it's use is highly recommended. RAID / mirroring is not necessary for these servers, unless the cost of RAID is cheaper.
- Filesystem servers can increase availability by replicating files to another system or to another local disk regularly. If a major crash of the primary file server occurs, users can mount their files from the second system, but changes made since the last replication/ synchronization will be lost.

RAID/Mirroring

- The classical method of increasing system availability is by duplicating one of the weakest part in a computer: the disk. RAID (Redundant Array of Inexpensive Disks) is a de-facto standard for defining how standard disks can be used to increase redundancy. The top RAID systems duplicate disks, disk controllers, power supplies and communication channels. The simplest RAID systems are software-only disk drivers which group together disparate disks in to a redundant set.

There are several RAID levels:

- RAID 1: This is basically mirroring.

- RAID 1+: This is RAID 1 with the addition of parity checking.
- RAID 5: Striping
- RAID 5+: Striping with parity (most commonly used RAID level).
- Things to watch for in RAID systems:
- A black box which is just attached to the scsi port is easier to manage and easier to fix/repair than inbuilt disks & controllers.
- For high availability systems, never buy the latest & hottest. Buy a RAID proven to work for/by others over a period of 6 months/1 year!
- Use a RAID which allows standard disks to be used.
- RAID's rarely work the way you expect with large databases. Run a trial before buying.
- Use the same RAID for all your servers if possible (learn to use one system well, rather than use many different RAID's).
- Special device drivers and kernel patches needed for RAID increase difficulty of maintenance and probably downtime.
- Software only RAID, if used, should be small, easy to install/reinstall and have a very good user interface.

System Redundancy

If applications do not provide built in redundancy, special software (and perhaps hardware) can be installed on two systems to provide Hot Standby functionality. The principle is as follows: Both systems can access shared (high availability, dual ported) disks and have duplicate network connections. The backup machine monitors the primary constantly and if it notices that the primary is no longer functioning, it takes control of the shared disks, reconfigures it self to have the same network address as the primary and starts up the applications that were running on the master. Of course this will only work with certain applications e.g. if the primary crashes and its principal application thrashes its configuration or data files in doing so, the backup server will not be able to start the application.

Full Hardware Redundancy

Specialised computer systems offer complete redundancy in one system i.e. CPU, memory, disks etc.. are fully duplicated. A single point of failure should not exist. These systems often require specially adapted Operating Systems; cost a fortune and are rarely compatible with mainstream systems. Rarely used in the commercial arena, they are most reserved for military or special financial use.

Check Your Progress 2

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

- 1) Differentiate between Symmetric key and public key cryptography?

.....

.....

.....

.....

2) What is a Digital Signature?

.....

.....

.....

.....

.....

3) Explain the role of Message Authentication Code.

.....

.....

.....

.....

.....

4) How Hash function provides message integrity?

.....

.....

.....

.....

.....

.....

1.4 LET US SUM UP

This unit covers the detailed descriptions of all the threats and mechanisms in the Network Security. Here you know how the threats (attacks) and mechanisms are performed. The common threats in Network Security are Masquerade, Replay, Modification of messages, and Denial of service, Trapdoor and Trojan horses. The available mechanisms are Cryptography & Digital Signatures, Authentication, Access Control Lists and others. Cryptography & Digital Signatures consists of Shared Key cryptography, Public Key Cryptography, Hashing/message digest, Applying cryptography. Authentication consists of Summary of authentication mechanisms and Authentication products. The other availability Mechanisms are Backup & Restore, Environment, Redundency, Application/Service Redundency, RAID/Mirroring, System Redundency, Full Hardware Redundency.

1.5 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

- 1) A masquerade is a type of attack where the attacker pretends to be an authorized user of a System in order to gain access to it or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen logon IDs and passwords, through finding security gaps in programs, or through bypassing the authentication mechanism.

- 2) A Denial of Service (DoS) attack is an attack which attempts to prevent the victim from being able to use all or part of their network connection. A denial of service attack may target a user, to prevent them from making outgoing connections on the network. A denial of service may also target an entire organization, to either prevent outgoing traffic or to prevent incoming traffic to certain network services, such as the organizations web page.
- 3) A replay attack is forms of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This attack uses a simple method of exploiting a captured packet or packets, and resends that traffic to cause unexpected results. Countermeasures for replay attacks include session tokens and timestamps.

Session Tokens: A pseudo random token should be issued to the user when the request come from a legitimate user then this session token has to be submitted by the user whenever he sends the subsequent request thus the server can cross check this session token with the token stored at server side.

Timestamps: This is another way of preventing a replay attack, in this synchronization of the time should be achieved using a secure protocol.

- 4) A Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk. Trojan horse may be widely redistributed as part of a computer virus. For example, a Trojan horse might appear to be a computer game, but once you double-click it, the program starts writing over certain parts of your hard drive, corrupting your data.

Check Your Progress 2

- 1) Symmetric cryptography uses the same secret (private) key to encrypt and decrypt its data whereas asymmetric uses both a public and private key. Symmetric requires that the secret key be known by the party encrypting the data and the party decrypting the data. Asymmetric allows for distribution of your public key to anyone with which they can encrypt the data they want to send securely and then it can only be decoded by the person having the private key. This eliminates the need of having to give someone the secret key (as with symmetric encryption) and risk having it compromised.
- 2) A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures facilitate authentication and data integrity verification.
- 3) A message authentication code (MAC) is an authentication tag (also called a checksum) derived by applying an authentication scheme, together with a secret key, to a message. Unlike digital signatures, MACs are computed and verified with the same key, so that they can only be verified by the intended recipient.
- 4) A cryptographic hash function is a hash function with certain additional security properties to make it suitable for use as a primitive in various information security applications, such as authentication and message integrity. A hash function takes a long string (or message) of any length as input and produces a fixed length string as output, sometimes termed a message digest or a digital fingerprint. Cryptographic hash functions are also called one-way functions, because they are designed in such a way that obtaining the original plaintext is nearly impossible and truly computationally unfeasible (in theory, anyway).

1.6 SUGGESTED READINGS

- [ftp.merit.edu/radius/releases](ftp://ftp.merit.edu/radius/releases) and [ftp.livingston.com/pub/radius](ftp://ftp.livingston.com/pub/radius)
- www.entegrity.com www.dynas.se/prod/prod_eng.html
- www.funk.com/new_one/SBR/faq_steel.htm
- www.microsoft.com/workshop/networking/cifs/default.asp
- www.safeword.com/welcome.htm
- www.securecomputing.com

UNIT 2 NETWORK SECURITY TECHNIQUES

Structure

- 2.0 Introduction
- 2.1 Objectives
- 2.2 Digital Watermarking
 - 2.2.1 General Framework for Watermarking
 - 2.2.2 Types of Digital Watermarks
 - 2.2.3 Applications of Digital Watermarks
 - 2.2.4 Attacks on Digital Watermarks
 - 2.2.5 Characteristics of Watermarks
- 2.3 Active Directory Controller (ADC)
 - 2.3.1 Structure of Active Directory Controller
 - 2.3.1.1 Forests, Trees and Domains
 - 2.3.1.2 Flat-filed, Simulated Hierarchy
 - 2.3.1.3 Shadow Groups
 - 2.3.2 Structural divisions to Improve Performance
 - 2.3.2.1 FSMO Roles
 - 2.3.2.2 Trust
 - 2.3.2.3 Adding Users and Computers to the Active Directory Domain
 - 2.3.2.4 Using Active Directory with Desktop Delivery Controller
- 2.4 Digital Forensics
 - 2.4.1 Computer Forensics
 - 2.4.2 Network Forensics
 - 2.4.3 Database Forensics
 - 2.4.4 Mobile Device Forensics
- 2.5 Let Us Sum Up
- 2.6 Check Your Progress: The key
- 2.7 Suggested Readings

2.0 INTRODUCTION

Digital watermarking technology is an emerging field in computer science, cryptography. Digital watermarks are pieces of information added to digital data (audio, video, or still images) that can be detected or extracted later to make an assertion about the data. This information can be textual data about the author, its copyright, etc; or it can be an image itself.

The information to be hidden is embedded by manipulating the contents of the digital data, allowing someone to identify the original owner, or in the case of illicit duplication of purchased material, the buyer involved. These digital watermarks remain intact under transmission/transformation, allowing us to protect our ownership rights in digital form.

Watermarks may be visible, in which case their use is two-fold - to discourage unauthorized usage, and also act as an advertisement. However, the focus is on invisible watermarks, as they do not cause any degradation in the aesthetic quality

or in the usefulness of the data. They can be detected and extracted later to facilitate a claim of ownership, yielding relevant information as well.

Watermarks may also be classified as robust or fragile. Robust watermarks are those which are difficult to remove from the object in which they are embedded, despite various attacks they might be subjected to, discussed later.

Fragile watermarks are those that are easily destroyed by any attempt to tamper with them. Absence of a watermark in a previously watermarked document would lead to the conclusion that the data has been tampered with.

For a digital watermark to be effective for ownership assertion, it must be robust, recoverable from a document, provide the original information embedded reliably, be non-intrusive, and also removable by authorized users.

2.1 OBJECTIVES

After completion of this unit, you will be able to:

- describe the types in digital watermarking and specific issues in watermarking of text, images, and video are discussed along with watermarking examples; and
- describe ADC.

2.2 DIGITAL WATERMARKING

2.2.1 General Framework for Watermarking

Watermarking is the process that embeds data called a watermark or digital signature or tag or label into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. The object may be an image or audio or video. In general, any watermarking scheme consists of three parts: Insertion of a watermark, detection of a watermark, and removal of a watermark.

Important Parameters

The most important properties of digital watermarking techniques are transparency, robustness, security, capacity, invertibility (reversibility) and complexity and possibility of verification. Based on these parameters the algorithms can be evaluated if a specific algorithm has adequate properties and can be used for a certain application area.

From we define the parameter as follows:

- **Transparency** relates to the properties of the human sensory. A transparent watermark causes no artifacts or quality loss.
- **Robustness** describes whether the watermark can be reliably detected after media operations. It is important to note that robustness does not include attacks on the embedding scheme that are based on the knowledge of the embedding algorithm or on the availability of the detector function. Robustness means resistance to "blind", non-targeted modifications, or common media operations.
- **Security** describes whether the embedded watermarking information cannot be removed beyond reliable detection by targeted attacks based on a full knowledge of the embedding algorithm and the detector, except the key, and the knowledge of at least one watermarked data. The concept of security includes procedural attacks, such as the IBM attack, or attacks based on a partial knowledge of the carrier modifications due to message embedding or embedding of templates. The security aspect also includes the false positive detection rates.

- **Capacity** describes how many information bits can be embedded. It addresses also the possibility of embedding multiple watermarks in one document in parallel.
- **Invertibility** describes the possibility to produce the original data during the watermark retrieval.
- **Complexity** describes the effort and time we need to embed and retrieve a watermark. This parameter is essential if we have real time applications. Another aspect addresses whether the original data in the retrieval process or not. We need to distinguish between non-blind and blind watermarking schemes.
- The **verification** procedure describes if we have a private verification like private key functions or a public verification possibility like the public key algorithms in cryptography.

Watermarking life-cycle phases

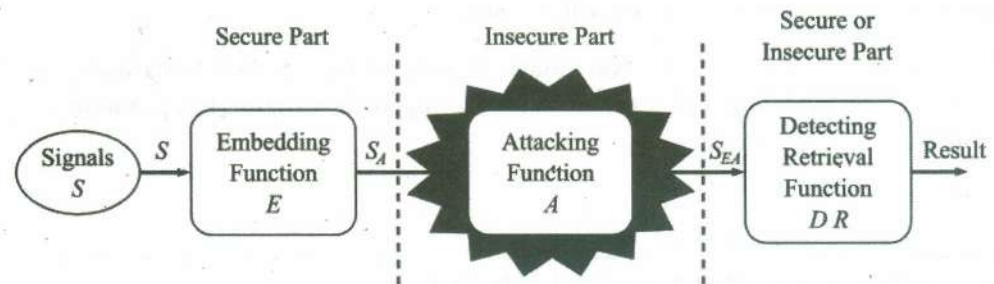


Fig. 1: General watermark life-cycle phases with embedding-, attacking- and detection/ retrieval functions

The information to be embedded is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the host signal. A watermarking system is usually divided into three distinct steps, embedding, attack and detection. In embedding, an algorithm accepts the host and the data to be embedded and produces a watermarked signal.

The watermarked signal is then transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. While the modification may not be malicious, the term attack arises from copyright protection application, where pirates attempt to remove the digital watermark through modification. There are many possible modifications, for example, lossy compression of the data, cropping an image or video, or intentionally adding noise. Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark is still present and it can be extracted. In robust watermarking applications, the extraction algorithm should be able to correctly produce the watermark, even if the modifications were strong. In fragile watermarking, the extraction algorithm should fail if any change is made to the signal.

The optimization of the parameters is mutually competitive and cannot be clearly done at the same time. If we want to embed a large message, we cannot require large robustness simultaneously. A reasonable compromise is always a necessity. On the other hand, if robustness to strong distortion is an issue, the message that can be reliably hidden must not be too long.

There are algorithms which need the original cover signal to retrieve the watermark from the marked cover and also those which can retrieve the watermark without

the original cover. The latter are called blind or oblivious watermarking algorithms, the first are called non-blind or non-oblivious. If the need for the original is acceptable usually depends on the application. In forensic cases the original may be available for comparison. In contrast copy-control environments will not allow access to the original due to the vast overhead and delay caused by such demands. In general blind watermarking algorithms are preferred but more challenging to design and implement. In some applications non-blind algorithms are used due to their potential greater robustness.

Almost all watermarking algorithms use the same secret key for embedding and retrieval. In analogy to cryptography this is called symmetric watermarking. In some algorithms or applications the key is known to the public, which is called public watermarking. The need for the embedding key in the retrieval process induces a serious security challenge in watermarking: Everyone who can retrieve a watermark can also embed a new watermark with the same key as the originator of the first watermark. There are also approaches for asymmetric watermarking, where different keys are used for embedding and retrieval, but a security level comparable with asymmetric watermarking has not been achieved yet and further research is required.

Furthermore, during verification we differ between invertible (reversible) and non-invertible (non-reversible) techniques, where the first one allows the reproduction of the original and the last one provides no possibility to extract the watermark without alterations of the original. Usually robust watermarks should be non-invertible while fragile watermarking has the most interest in invertible schemes to detect bit changes and to allow reproduction of the original.

Watermark Insertion Unit

A general block diagram for the insertion of a watermark is shown which provides a generic approach to watermarking any digital data. It consists of a watermark insertion unit that uses the original image, the watermark, and a user key to obtain the watermarked image.

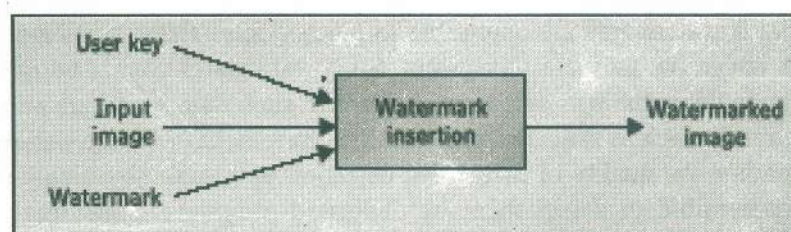


Fig. 2: Watermark Insertion Unit

Similarly, watermark extraction and detection can also be performed using the units shown below as well as the user key.

Watermark Extraction Unit

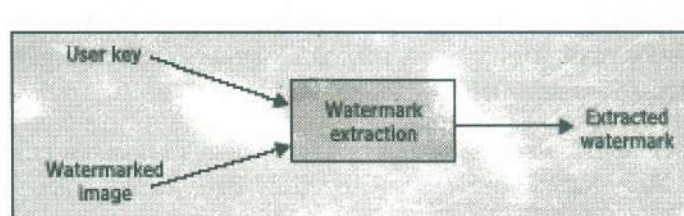


Fig. 3: Watermark Extraction Unit

Extracting the watermark can be divided into two phases, locating the watermark, and recovering the watermark information. Two kinds of extraction are available using the original document and in the absence of the original document.

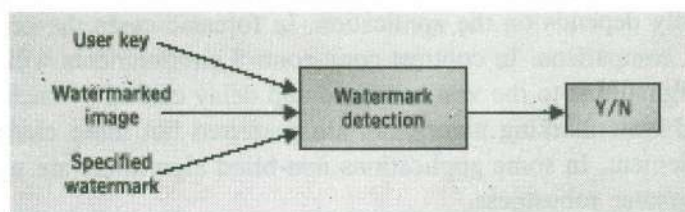


Fig. 4: Watermark Detection

A watermarked detection unit consists of an extraction unit to first extract the watermark, and later compare it with the original watermark inserted. The output is Yes or No depending on whether the watermark is present.

The ease of reproduction, distribution, and manipulation of digital documents creates problems for authorized parties that wish to prevent illegal use of such document. To this end, digital watermarking has been proposed as a last line of defense. A digital watermark is an imperceptible, robust, secure message embedded directly into a document. The watermark is imperceptible both perceptually and statistically. Robustness means that the watermark cannot be removed or modified unless the document is altered to the point of no value. The watermark is secure if unauthorized parties cannot erase or modify it. Current watermarking schemes may be viewed as spread-spectrum communications systems, which transmit a message redundantly using a low-amplitude, pseudo noise carrier signal. An example highlights the basic mechanisms and properties of spread spectrum and their relation to watermarking.

2.2.2 Types of Digital Watermarks

Watermarks and watermarking techniques can be divided into various categories in various ways. Watermarking techniques can be divided into four categories according to the type of document to be watermarked as follows:

- **Visible watermarks:** Visible watermarks are an extension of the concept of logos. Such watermarks are applicable to images only. These logos are inlaid into the image but they are transparent. Such watermarks cannot be removed by cropping the center part of the image. Further, such watermarks are protected against attacks such as statistical analysis. The drawbacks of visible watermarks are degrading the quality of image and detection by visual means only. Thus, it is not possible to detect them by dedicated programs or devices. Such watermarks have applications in maps, graphics and software user interface.
- **Invisible watermark:** Invisible watermark is hidden in the content. It can be detected by an authorized agency only. Such watermarks are used for content and/or author authentication and for detecting unauthorized copier.
- **Public watermark:** Such a watermark can be read or retrieved by anyone using the specialized algorithm. In this sense, public watermarks are not secure. However, public watermarks are useful for carrying IPR information. They are good alternatives to labels.
- **Fragile watermark:** Fragile watermarks are also known as tamper-proof watermarks. Such watermarks are destroyed by data manipulation.
- **Private Watermark:** Private watermarks are also known as secure watermarks. To read or retrieve such a watermark, it is necessary to have the secret key.
- **Perceptual watermarks:** A perceptual watermark exploits the aspects of human sensory system to provide invisible yet robust watermark. Such watermarks are also known as transparent watermarks that provide extremely high quality contents.

- **Bit-stream watermarking:** The term is sometimes used for watermarking of compressed data such as video.

- **Text Watermark**

Many paper documents are more valuable than multimedia like sound clips and images. Digital libraries and archives distribute copyrighted articles, journals, and books in electronic form. Watermarking of text documents provides a means of tracing documents that have been illegally copied, distributed, altered, or forged. Raw text, such as an ASCII text file or computer source code, cannot be watermarked because there is no "perceptual headroom" in which to embed hidden information. However, final versions of documents are typically formatted (e.g., PostScript, PDF, RTF), and it is possible to hide a watermark in the layout information (e.g., word and line spacings) and formatting (e.g., serifs).

- **Image Watermark**

Digital images can be produced from many sources, such as everyday Photographs, satellite pictures, medical scans, or computer graphics. Watermarks for natural images typically modify pixel intensities or transform coefficients, although it is conceivable that a watermark could alter other features such as edges or textures. An image may be viewed for an extended period of time, and it may also be subject to a great deal of manipulation, such as filtering, cropping, geometric transformations, compression, and compositing with other images, and hostile attacks. Thus, imperceptibility, robustness, and security are usually the most important properties of image watermarks; speed and complexity are often secondary. Also, since many images are compressed (e.g., JPEG or GIF), watermarking algorithms that operate in the transform or wavelet domain may be useful. One potential difficulty in image watermarking is the finite bandwidth available. As the image size decreases, the permissible message length decreases unless E is increased (weakening imperceptibility) or N is decreased.

- **Audio Watermark**

Audio watermarks are special signals embedded into digital audio. These signals are extracted by detection mechanisms and decoded. Audio watermarking schemes rely on the imperfection of the human auditory system. However, human ear is much more sensitive than other sensory motors.

Even though the current watermarking techniques are far from perfect, during the last decade audio watermarking schemes have been applied widely. These schemes are sophisticated very much in terms of robustness and imperceptibility. Robustness and imperceptibility are important requirements of watermarking, while they are conflicting each other.

- **Video Watermark**

Digital video is a sequence of still images, and many image watermarking techniques can be extended to video in a straightforward manner. In contrast to single images, the large video bandwidth means that long messages can be embedded in video. Speed is also an important issue because of the huge amounts of data that must be processed. Except for video production (which takes place before distribution), digital video is typically stored and distributed in compressed form (e.g., MPEG). Hence, it is often desired that the marked, compressed video should not require more bandwidth than the unmarked, compressed video. This bit-rate constraint could also be an issue for single images. Compressed-domain video watermarking is especially attractive. Operating on the compressed bit stream obviates the need for compute-

intensive, time-consuming decompression and recompression, such that the watermark can be embedded at the time of distribution or reception.

2.2.3 Applications of Digital Watermarks

Video Watermarking

In this case, most considerations made in previous sections hold. However, now the temporal axis can be exploited to increase the redundancy of the watermark. As in the still images case, watermarks can be created either in the spatial or in the DCT domains. In the latter, the results can be directly extrapolated to MPEG-2 sequences, although different actions must be taken for I, P and B frames. Note that perhaps the set of attacks that can be performed intentionally is not smaller but definitely more expensive than for still images.

Audio Watermarking

Again, previous considerations are valid. In this case, time and frequency masking properties of the human ear are used to conceal the watermark and make it inaudible. The greatest difficulty lies in synchronizing the watermark and the watermarked audio file, but techniques that overcome this problem have been proposed.

Hardware/Software Watermarking

This is a good paradigm that allows us to understand how almost every kind of data can be copyright protected. If one is able to find two different ways of expressing the same information, then one bit of information can be concealed, something that can be easily generalized to any number of bits.

This is why it is generally said that a perfect compression scheme does not leave room for watermarking. In the hardware context, Boolean equivalence can be exploited to yield instances that use different types of gates and that can be addressed by the hidden information bits. Software can be also protected not only by finding equivalences between instructions, variable names, or memory addresses, but also by altering the order of non-critical instructions. All this can be accomplished at compiler level.

Text Watermarking

This problem, which in fact was one of the first that was studied within the information hiding area can be solved at two levels. At the printout level, information can be encoded in the way the text lines or words are separated (this facilitates the survival of the watermark even to photocopying). At the semantic level (necessary when raw text files are provided), equivalences between words or expressions can be used, although special care has to be taken not to destruct the possible intention of the author.

Executable Watermarks

Once the hidden channel has been created it is possible to include even executable contents, provided that the corresponding applet is running on the end user side.

Labeling

The hidden message could also contain labels that allow for example to annotate images or audio. Of course, the annotation may also been included in a separate file, but with watermarking it results more difficult to destroy or loose this label, since it becomes closely tied to the object that annotates. This is especially useful in medical applications since it prevents dangerous errors.

Fingerprinting

This is similar to the previous application and allows acquisition devices (such as video cameras, audio recorders, etc) to insert information about the specific device (e.g., an ID number) and date of creation. This can also be done with conventional digital signature techniques but with watermarking it becomes considerably more difficult to excise or alter the signature. Some digital cameras already include this feature.

Authentication

This is a variant of the previous application, in an area where cryptographic techniques have already made their way. However, there are two significant benefits that arise from using watermarking: first, as in the previous case, the signature becomes embedded in the message, second, it is possible to create 'soft authentication' algorithms that offer a multivalued 'perceptual closeness' measure that accounts for different unintentional transformations that the data may have suffered, instead of the classical yes/no answer given by cryptography-based authentication. Unfortunately, the major drawback of watermarking-based authentication is the lack of public key algorithms that force either to put secret keys in risk or to resort to trusted parties.

Copy and Playback Control

The message carried by the watermark may also contain information regarding copy and display permissions. Then, a secure module can be added in copy or playback equipment to automatically extract this permission information and block further processing if required. In order to be effective, this protection approach requires agreements between content providers and consumer electronics manufacturers to introduce compliant watermark detectors in their video players and recorders. This approach is being taken in Digital Video Disc (DVD).

Signalling

The imperceptibility constraint is helpful when transmitting signalling information in the hidden channel. The advantage of using this channel is that no bandwidth increase is required. An interesting application in broadcasting consists in watermarking commercials with signaling information that permits an automatic counting device to assess the number of times that the commercial has been broadcast during a certain period. An alternative to this would require complex recognition software.

Digital Watermarking Technology for Rights Management

One of the traditional applications of the watermark is copyright protection. The primary reason for using watermarks is to identify the owner of the content by an invisible hidden "mark" that is imprinted into the image. In many cases, the watermark is used in addition to the content encryption, where the encryption provides the secure distribution method from the content owners to the receivers, and the watermark offers the content owners the opportunity to trace the contents and detect the unauthorized use or duplications. Without watermarking, there is no way to extend the control of the content owner once the content leaves the protected digital domain and is released to the user. Digital watermark is used to extend the protection and provide the opportunities for the content owners to protect the rights and properties of the electronic distributed contents. The signature of the owner, content ID and usage limitation can be imprinted into the contents, and stay with the contents as far as it travels. This mechanism extends the opportunity of protecting the contents after the release of the contents to the open environment.

The contents may be changed to the other formats, edited or trimmed by the users or compressed for the storage and transmission, and it is desirable to be able to

detect the watermark from those processed contents. Usually, the watermark signal embedded into the content does not disappear after the editing of the content, but becomes more and more difficult to detect while the content is distorted. In general, higher robustness can be achieved by increasing the strength of the watermark signal, thus improving the detection capability. In other words, the robustness of the watermark is a tradeoff between the amount of watermark signal that applies to the content and the overhead to the detection. Currently, several commercial products and services using watermarking technology are available. They include applications for watermark embedding/detection and services to search the Internet for the contents with certain designated watermarks. These applications are mainly taking place between the large content owners (e.g. electronic publishers/distributors), and their customers (e.g. the content creators). Because the usage is limited within relatively smaller groups, each group tends to use their own proprietary watermark rather than a common one. Among these groups, the standardization is not an urgent issue until their markets shift to public domain consumers.

Digital Watermarking Technology for Authentication and Tamper Proofing

Another application of digital watermark is contents authentication and tamper proofing. The objective is not to protect the contents from being copied or stolen, but is to provide a method to authenticate the image and assure the integrity of the image. Since low-end digital camera arrived to the consumer market, it rapidly expanded to a number of industrial applications as well, because the use of a digital image is far more cost effective and can also save time and cost for the Developing/Printing/Exposing (DPE) compared to the traditional chemical photos.

However, there are some critical issues for some particular applications, where the photos are used as evidence or the material for some kind of business judgment. For instance, automobile insurance companies sometimes use photos of the damaged car sent by the repair shop to estimate the repair cost. A shift to digital photos will save a great amount of time and money for these kinds of processes. However, the digital photos might be altered to exaggerate damage, or even made up from nothing, since the modification of the digital image is getting much easier with some advanced photo-retouching tools be available. This could result in large amounts of extra payment for the insurance company, or more seriously, undermine the credibility of the insurance company itself. A type of digital watermark, called tamper-detect watermark, might resolve this problem, and provide a secure environment for the evidence photos. The way to realize this feature is to embed a layer of the authentication signature into the subject digital image using a digital watermark. This additional layer of watermark is used as a "sensor" to detect the alteration. Our recent implementation can even detect the location of the alteration from the altered image itself. Through a joint study with a major Japanese insurance company, we confirmed the technical feasibility of the technology for the above-mentioned industrial applications.

Visible Reversible Watermarking for Electronic Distribution

Unlike other digital watermarking technologies described above, the visible reversible watermark is visible. It is available as a commercial product. This unique form of watermarking technology by IBM allows the content owners to embed a visible shape or logo mark such as company's logo on top of the image. The mark is removed (the watermark is reversed) only with the application of an appropriate "decryption" key and watermark remover software. This mark is applied by modifying the Discrete Cosine Transformation (DCT) coefficients of the JPEG compressed image following certain pre-defined rule and visual effect analysis result to make it half transparent, but not totally destructive. The key, with the mark removal program, will be used to remove the mark from the image. The removal of the visible mark may be tied up with the embedding of

another invisible mark for the tracking purpose. With this visible watermark on the image, the content becomes self-protective, and content owners can distribute the entire image as a sample to various open media or to the Internet. When a user wants to use a clean copy of the image, all he/she needs to be is to request a "decryption" key and pay some fee for it. This will reduce the security risk and the amount of the data transmission per each buy/sell transaction.

Watermarking Technology for DVD Playback and Record Control

Several watermark applications that are currently in place or very close to being released were discussed. In most of the cases, those applications are targeting at a closed environment or exist between limited number of members, e.g., between image libraries and content creators, insurance companies and repair shops, and so on. In this section, I would like to focus on the watermark application that has much more public impact, namely DVD Copy control.

2.2.4 Attacks on Digital Watermarks

A watermarked image is likely to be subjected to certain manipulations, some intentional such as compression and transmission noise and some intentional such as cropping, filtering, etc. They are summarized below

Lossy Compression: Many compression schemes like JPEG and MPEG can potentially degrade the data's quality through irretrievable loss of data.

Geometric Distortions: Geometric distortions are specific to images and videos and include such operations as rotation, translation, scaling and cropping.

Common Signal Processing Operations

They include the followings:

- D/A conversion
- A/D conversion
- Resampling
- Requantization
- Color reduction
- Addition of a constant offset to the pixel values
- Local exchange of pixels
- Non-linear filtering such as median filtering
- Other intentional attacks:
- Printing and Rescanning
- Watermarking of watermarked image (rewatermarking)

Collusion: A Number of authorized recipients of the image should not be able to come together (collude) and like the differently watermarked copies to generate an un-watermarked copy of the image (by averaging all the watermarked images).

Forgery: A Number of authorized recipients of the image should not be able to collude to form a copy of watermarked image with the valid embedded watermark of a person not in the group with an intention of framing a 3rd party.

IBM attack: It should not be possible to produce a fake original that also performs as well as the original and also results in the extraction of the watermark as claimed by the holder of the fake original.

2.2.5 Characteristics of Watermarks

The desired characteristics of the watermarks are listed below.

Difficult to notice: The invisible watermarks should not be noticeable to the viewers nor should the watermark degrade the quality of the content.

However, if a signal is truly imperceptible, then perceptual based lossy compression algorithm should, in principle, remove such signal. Of course, a just noticeable difference (JND) is usually observed by comparing two signals, e.g. compressed and uncompressed or watermarked and original.

Robustness: In general, a watermark must be robust to transformations that include common signal distortions as well as D/A and A/D conversions and loss compression.

Moreover, for images and video, it is important that the watermark survive geometric distortions such as translation, scaling and cropping etc. It has been argued and that robustness can only be attained if watermark is placed perceptually significant regions of an image. But it has been already mentioned that watermark should be imperceptible, which is possible if watermark is placed in perceptually insignificant regions of an image. They are two conflicting requirements. It should be noted

Robustness actually comprises two separate issues

Whether or not the watermark is still present in the data after distortion and whether the watermark detector can detect it. It should also be noted that ability to embed robust watermarks in digital images does not necessarily imply the ability to establish ownership, unless certain requirements are imposed legally on the watermarking scheme

Tamper-Resistance

As well as requiring the watermark to be robust to legitimate signal distortions, a watermark may also be subjected to signal processing that is solely intended to remove the watermark. It is important that a watermark be resistant to such tampering. There are a number of possible ways this may be achieved:

Private Watermark

A private watermark where either the decoder requires knowledge of the un-watermarked content or the pseudo-random noise sequence that constitutes the watermark is only known to sender and receiver, are inherently more tamper resistant than public watermarks in which everybody is free to decode the watermark

Asymmetric Encoder/Decoder

If removal of a public watermark requires inverting the encoding, then it is highly desirable to make the encoder as complex as possible, especially if the watermark is only to be applied once. However if decoders must run in real time, then it is necessary for the decoding process to be simpler than encoding.

Bit-Rate

The bit rate of a watermark refers to the amount of information a watermark can encode in a signal. This is especially important for public watermarks. Low bit-rate watermarks are more robust

Modification and Multiple Watermarks

In some circumstances, it is desirable to alter the watermark after insertion. For example, in the case of digital video discs, a disc may be watermarked to allow only a single copy. Once this copy has been made, it is then necessary to alter the watermark on the original disc to prohibit further copies. Changing a watermark can be accomplished either:

- a) removing the 1st watermark and then adding a new one or
- b) inserting a 2nd a watermark such that both are readable, but are overrides the other.

Scalability: It is well known that computer speeds are approximately doubling every eighteen months, so that what looks computationally unreasonable today may very quickly become a reality. It is therefore, very desirable to design a watermark whole decoder is scalable with each generation of computers.

Thus for example, the first generation of decoder might be computationally inexpensive but might not be as reliable as next generation decoders that can afford to expend more computation to deal with issues such as geometric distortions.

Unambiguous

Retrieval of watermark should unambiguously identify the owner. The watermark should not need any interpretation as looking into the database of codes to interpret the watermark unless a standard body maintains it internationally.

Universal

The same digital watermark should apply to all three media under consideration. This is potentially helpful in the watermarking of multimedia products. Also this feature is conducive to implementation of audio/image/video watermarking algorithm on common hardware.

Minimum Alternation of Pixels

While watermarking high quality image and art works the amount of pixel modification should be minimum.

Minimum Human Intervention: Insert of watermark should require little human intervention or labor.

Check Your Progress 1

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

- 1) How digital watermarking is used for copyright protection?

.....

.....

.....

.....

- 2) Discuss various phases involved in watermarking.

.....

.....

.....

.....

- 3) What is a robust attack on a watermarked image?

.....

.....

- 4) Discuss about visible and invisible watermarking?
-
-
-
-

2.3 ACTIVE DIRECTORY CONTROLLER (ADC)

2.3.1 Structure of Active Directory Controller

An Active Directory structure is a **hierarchical framework** of objects. The objects fall into two broad categories: resources (e.g., printers) and security principals (user or computer accounts and groups). Security principals are Active Directory objects that are assigned unique security identifiers (SIDs) used to control access and set security.

Each object represents a single entity – whether a user, a computer, a printer, or a group - and its attributes. Certain objects can also be containers of other objects. An object is uniquely identified by its name and has a set of attributes - the characteristics and information that the object can contain - defined by a schema, which also determines the kinds of objects that can be stored in Active Directory.

Each attribute object can be used in several different schema class objects. The schema object exists to allow the schema to be extended or modified when necessary. However, because each schema object is integral to the definition of Active Directory objects, deactivating or changing these objects can have serious consequences because it will fundamentally change the structure of Active Directory itself. A schema object, when altered, will automatically propagate through Active Directory and once it is created it can only be deactivated – not deleted. Changing the schema usually requires a fair amount of planning.

A **Site** object in Active Directory represents a geographic location that hosts networks. Sites contain objects called subnets. Sites can be used to assign Group Policy, facilitate the discovery of resources, manage active directory replication, and manage network link traffic. Sites can be linked to other Sites. Site-linked objects may be assigned a cost value that represents the speed, reliability, availability, or other real property of a physical resource. Site Links may also be assigned a schedule.

2.3.1.1 Forests, Trees and Domains

All objects inside a common directory database are known as a domain. Each domain stores information only about the objects that belong to that domain. A tree consists of a single domain or multiple domains in a contiguous namespace. A forest is a collection of trees and represents the outermost boundary within which users, computers, groups, and other objects exist. The Active Directory framework that holds the objects can be viewed at a number of levels. At the top of the structure is the forest. A forest is a collection of multiple trees that share a common global catalog, directory schema, logical structure, and directory configuration. The forest, tree, and domain are the logical parts in an Active Directory network.

The Active Directory forest contains one or more transitive, trust-linked *trees*. A tree is a collection of one or more *domains* and domain trees in a contiguous namespace, again linked in a transitive trust hierarchy. Domains are identified by their DNS name structure, the namespace.

2.3.1.2 Flat-filed, Simulated Hierarchy

The objects held within a domain can be grouped into containers called Organizational Units (OUs). OUs give a domain a hierarchy, ease its administration, and can give a resemblance of the structure of the organization in organizational or geographical terms. OUs can contain OUs - indeed, domains are containers in this sense - and can hold multiple nested OUs. Microsoft recommends as few domains as possible in Active Directory and a reliance on OUs to produce structure and improve the implementation of policies and administration. The OU is the common level at which to apply group policies, which are Active Directory objects themselves called Group Policy Objects (GPOs), although policies can also be applied to domains or sites. The OU is the level at which administrative powers are commonly delegated, but granular delegation can be performed on individual objects or attributes as well.

However, Organizational Units are just an abstraction for the administrator, and do not function as true containers; the underlying domain operates as if objects were all created in a simple flat-file structure, without any OUs. By contrast, there are other vendor directories such as Novell eDirectory that allow naming attribute duplication across separate OUs. Each user logs in by specifying the context of their account, which is similar to the current working directory of a file system. Context normally operates in relative form: if the login prompt context is "staff-ou.accounts-ou.organization", people with accounts in that specific OU need only type their username "fred". But if the login prompt context were set to be one level higher, at "accounts-ou.organization", people would need to specify the OU within that context: "fred.staff-ou". Context can also be specified in absolute form similar to an absolute directory path by using a leading period: ".fred.staff-ou.accounts-ou.organization", which disregards the current login prompt context.

Novell additionally provides login prompt functionality known as contextless login to permit searching the directory structure via LDAP for all possible matching or similar usernames, making the Novell login process operate similar to Microsoft's flat-file structure that searches the entire domain for accounts regardless of the account's location in the OUs. The concept of account context in the directory does not apply to Active Directory, since object name duplication within a single domain is not permitted to occur in the first place.

Because duplicate usernames cannot exist within separate OUs of a single active directory domain, unique account name generation poses a significant challenge for organizations with hundreds to thousands of users that are part of a generalized mass that can not be easily subdivided into separate domains, such as students in a public school system or university that must be able to login on any computer across the district buildings or campus network.

As the number of users in a domain increases, simple username creation methods such as "first initial, middle initial, last name" will fail due to having so many common names like Smith or Johnson in the collective mass that result in having duplications, such as two JASmith, which requires randomly adding a number to the end (JASmith1) to further differentiate it for one of the two people. At some point of increasingly many users and name duplications, the network IT staff may give up on attempts at making usernames personally memorable, and the username simply becomes a serial number 5 to 10 digits long to provide sufficient naming uniqueness within a single domain.

2.3.1.3 Shadow Groups

In Active Directory, organizational units can not be assigned as owners or trustees. Only groups are selectable, and members of OUs can not be collectively assigned rights to directory objects.

Unlike Active Directory, Novell eDirectory allows organizational units and all users within the OU to be assigned rights to an object, without having to create shadow groups representing the users in each OU.

It is often useful to associate a collection of users to all share access rights to particular file or secured resource, but with Active Directory it is not possible to choose an OU containing all users that need rights. A user group can be selected to accomplish this, but all users within a particular OU are not automatically made members of a group representing that OU.

Groups can be manually created to duplicate the account membership structure within OUs, but it is an extra step of the account creation process by the administrator to remember all the various groups each new user needs to join. If the administrator forgets this manual step, the users will experience problems until the group memberships are corrected.

To make up for this non-automated deficiency, network administrators can write their own custom scripts which periodically run on the server and use LDAP access commands to add or remove users from groups representing the OUs of the users, known as *Shadow Groups*. Microsoft refers to shadow groups in the Server 2008 Reference documentation, but does not explain how to create them.[5] Once created, these shadow groups are selectable in place of the OU in the administrative console tools.

The naming of shadow groups is complicated by the fact that OUs can be nested but groups cannot. Groups can only exist in the root of the domain, and group names are limited in length so matching the naming of a deeply nested string of OUs for a very large domain is difficult.

Novell e-Directory supports the creation of user groups, but OUs can be natively selected as the assigned owner of a secured resource, so shadow groups are unnecessary.

2.3.2 Structural Divisions to Improve Performance

Active Directory also supports the creation of Sites, which are physical, rather than logical, groupings defined by one or more IP subnets. Sites distinguish between locations connected by low-speed (e.g., WAN, VPN) and high-speed (e.g., LAN) connections. Sites are independent of the domain and OU structure and are common across the entire forest. Sites are used to control network traffic generated by replication and also to refer clients to the nearest domain controllers. Exchange 2007 also uses the site topology for mail routing. Policies can also be applied at the site level.

The actual division of an organization's information infrastructure into a hierarchy of one or more domains and top-level OUs is a key decision. Common models are by business unit, by geographical location, by IT Service, or by object type. These models are also often used in combination. OUs should be structured primarily to facilitate administrative delegation, and secondarily, to facilitate group policy application.

Although OUs form an administrative boundary, the only true security boundary is the forest itself and an administrator of any domain in the forest must be trusted across all domains in the forest.

Physically the Active Directory information is held on one or more equal peer domain controllers (DCs), replacing the NT PDC/BDC model. Each DC has a copy of the Active Directory; changes on one computer being synchronized (converged) between all the DC computers by *multi-master replication*. Servers joined to Active Directory that are not domain controllers are called Member Servers.

The Active Directory database is split into different stores or *partitions*. Microsoft often refers to these partitions as 'naming contexts'. The 'Schema' partition contains the definition of object classes and attributes within the Forest. The 'Configuration' partition contains information on the physical structure and configuration of the forest (such as the site topology). The 'Domain' partition holds all objects created in that domain. The first two partitions replicate to all domain controllers in the Forest. The Domain partition replicates only to Domain Controllers within its domain. A subset of objects in the domain partition is also replicated to domain controllers that are configured as global catalogs.

Unlike earlier versions of Windows, which used NetBIOS to communicate, Active Directory is fully integrated with DNS and TCP/IP-DNS is *required*. To be fully functional, the DNS server must support SRV resource records or service records.

Active Directory replication is 'pull' rather than 'push'. The **Knowledge Consistency Checker (KCC)** creates a replication topology of *site links* using the defined *sites* to manage traffic. Intrasite replication is frequent and automatic as a result of change notification, which triggers peers to begin a pull replication cycle. Intersite replication intervals are less frequent and do not use change notification by default, although this is configurable and can be made identical to intrasite replication.

A different 'cost' can be given to each link (e.g., DS3, T1, ISDN etc.) and the site link topology will be altered accordingly by the KCC. Replication between domain controllers may occur transitively through several site links on same-protocol *site link bridges*, if the cost is low, although KCC automatically costs a direct site-to-site link lower than transitive connections. Site-to-site replication can be configured to occur between a *bridgehead server* in each site, which then replicates the changes to other DCs within the site.

In a multi-domain forest the Active Directory database becomes partitioned. That is, each domain maintains a list of only those objects that belong in that domain. So, for example, a user created in Domain A would be listed only in Domain A's domain controllers. Global catalog (GC) servers are used to provide a global listing of all objects in the Forest. The Global catalog is held on domain controllers configured as global catalog servers. Global Catalog servers replicate to themselves all objects from all domains and hence, provide a global listing of objects in the forest. However, in order to minimize replication traffic and to keep the GC's database small, only selected attributes of each object are replicated. This is called the partial attribute set (PAS). The PAS can be modified by modifying the schema and marking attributes for replication to the GC.

Replication of Active Directory uses Remote Procedure Calls (RPC over IP [RPC/IP]). Between Sites you can also choose to use SMTP for replication, but only for changes in the Schema, Configuration, or Partial Attribute Set (Global Catalog) NCs. SMTP cannot be used for replicating the default Domain partition.

The Active Directory database, the *directory store*, in Windows 2000 Server uses the JET Blue-based Extensible Storage Engine (ESE98), limited to 16 terabytes and 1 billion objects in each domain controller's database. Microsoft has created NTDS databases with more than 2 billion objects. (NT4's Security Account Manager could support no more than 40,000 objects). Called NTDS.DIT, it has two main

tables: the *data table* and the *link table*. In Windows Server 2003 a third main table was added for security descriptor single instancing. The features of Active Directory may be accessed programmatically via the COM interfaces provided by **Active Directory Service Interfaces**. Active Directory is a necessary component for many Windows services in an organization such as Exchange, Security.

2.3.2.1 FSMO Roles

Flexible Single Master Operations (FSMO), sometimes pronounced “fizz-mo”) roles are also known as operations master roles. Although the AD domain controllers operate in a multi-master model, i.e. updates can occur in multiple places at once, there are several roles that are necessarily single instance:

Role Name	Scope	Description
Schema Master	1 per forest	Controls and handles updates/modifications to the Active Directory schema.
Domain Naming Master	1 per forest	Controls the addition and removal of domains from the forest if present in root domain
PDC Emulator	1 per domain	Provides backwards compatibility for NT4 clients for PDC operations (like password changes). The PDCs also run domain specific processes such as the Security Descriptor Propagator (SDPROP), and is the master time server within the domain. It also handles external trusts, the DFS consistency check, holds the most current passwords and manages all GPOs as default server.
RID Master	1 per domain	Allocates pools of unique identifier to domain controllers for use when creating objects
Infrastructure Master	1 per domain/partition	Synchronizes cross-domain group membership changes. The infrastructure master cannot run on a global catalog server (GCS)(unless all DCs are also GCs, or environment consists of a single domain)

2.3.2.2 Trust

To allow users in one domain to access resources in another, Active Directory uses trusts. Trusts inside a forest are automatically created when domains are created. The forest sets the default boundaries of trust, not the domain, and implicit, transitive trust is automatic for all domains within a forest. As well as two-way transitive trust, AD trusts can be a *shortcut* (joins two domains in different trees, transitive, one- or two-way), *forest* (transitive, one- or two-way), *realm* (transitive or nontransitive, one- or two-way), or *external* (nontransitive, one- or two-way) in order to connect to other forests or non-AD domains.

Trusts in Windows 2000 (native mode)

- **One-way trust** - One domain allows access to users on another domain, but the other domain does not allow access to users on the first domain.
- **Two-way trust** - Two domains allow access to users on both domains.
- **Trusting domain** - The domain that allows access to users from a trusted domain.

- **Trusted domain** - The domain that is trusted; whose users have access to the trusting domain.
- **Transitive trust** - A trust that can extend beyond two domains to other trusted domains in the forest.
- **Intransitive trust** - A one way trust that does not extend beyond two domains.
- **Explicit trust** - A trust that an admin creates. It is not transitive and is one way only.
- **Cross-link trust** - An explicit trust between domains in different trees or in the same tree when a descendant/ancestor (child/parent) relationship does not exist between the two domains.

Windows 2000 Server – supports the following types of trusts:

- Two-way transitive trusts.
- One-way intransitive trusts.

Additional trusts can be created by administrators. These trusts can be:

- **Shortcut**

Windows Server 2003 offers a new trust type – the forest root trust. This type of trust can be used to connect Windows Server 2003 forests if they are operating at the 2003 forest functional level. Authentication across this type of trust is Kerberos based (as opposed to NTLM). Forest trusts are also transitive for all the domains in the forests that are trusted. Forest trusts, however, are not transitive.

ADAM

Active Directory Application Mode (ADAM) is a light-weight implementation of Active Directory. ADAM is capable of running as a service, on computers running Microsoft Windows Server 2003 or Windows XP Professional. ADAM shares the code base with Active Directory and provides the same functionality as Active Directory, including an identical API, but does not require the creation of domains or domain controllers.

Like Active Directory, ADAM provides a *Data Store*, which is a hierarchical datastore for storage of directory data, a *Directory Service* with an *LDAP Directory Service Interface*. Unlike Active Directory, however, multiple ADAM instances can be run on the same server, with each instance having its own and required by applications making use of the ADAM directory service.

Integrating Unix into Active Directory

Varying levels of interoperability with Active Directory can be achieved on most Unix-like operating systems through standards compliant LDAP clients, but these systems usually lack the automatic interpretation of many attributes associated with Windows components, such as Group Policy and support for one-way trusts.

There are also third-party vendors who offer Active Directory integration for Unix platforms (including UNIX, Linux, Mac OS X, and a number of Java- and UNIX-based applications). Some of these vendors include Centrify (DirectControl), Computer Associates (UNAB), CyberSafe Limited (TrustBroker), Likewise Software (Open or Enterprise), Quest Software (Authentication Services) and Thursby Software Systems (ADmitMac). The open source Samba software provides a way to interface with Active Directory and join the AD domain to provide authentication and authorization: version 4 (in alpha as of October 2009) can act as a peer Active Directory domain controller. Microsoft is also in this market with their free Microsoft Windows Services for UNIX product.

The schema additions shipped with Windows Server 2003 R2 include attributes that map closely enough to RFC 2307 to be generally usable. The reference implementation of RFC 2307, `nss_ldap` and `pam_ldap` provided by PADL.com, contains support for using these attributes directly, provided they have been populated. The default Active Directory schema for group membership complies with the proposed extension, RFC 2307bis. Windows Server 2003 R2 includes a Microsoft Management Console snap-in that creates and edits the attributes.

An alternate option is to use another directory service such as 389 Directory Server (formerly Fedora Directory Server) or Sun Microsystems Sun Java System Directory Server, which can perform a two-way synchronization with Active Directory and thus provide a “deflected” integration with Active Directory as Unix and Linux clients will authenticate to FDS and Windows Clients will authenticate to Active Directory. Another option is to use **OpenLDAP** with its translucent overlay, which can extend entries in any remote LDAP server with additional attributes stored in a local database. Clients pointed at the local database will see entries containing both the remote and local attributes, while the remote database remains completely untouched

2.3.2.3 Adding Users and Computers to the Active Directory Domain

After the new Active Directory domain is established, create a user account in that domain to use as an administrative account. When that user is added to the appropriate security groups, use that account to add computers to the domain.

- 1) To create a new user, follow these steps:
 - a) Click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers** to start the Active Directory Users and Computers console.
 - b) Click the domain name that you created, and then expand the contents.
 - c) Right-click **Users**, point to **New**, and then click **User**.
 - d) Type the first name, last name, and user logon name of the new user, and then click **Next**.
 - e) Type a new password, confirm the password, and then click to select one of the following check boxes:
 - Users must change password at next logon (recommended for most users)
 - User cannot change password
 - Password never expires
 - Account is disabledClick **Next**.
 - f) Review the information that you provided, and if everything is correct, click **Finish**.
- 2) After you create the new user, give this user account membership in a group that permits that user to perform administrative tasks. Because this is a laboratory environment that you are in control of, you can give this user account full administrative access by making it a member of the Schema, Enterprise, and Domain administrators groups. To add the account to the Schema, Enterprise, and Domain administrators groups, follow these steps:

On the Active Directory Users and Computers console, right-click the new account that you created, and then click **Properties**.

- a) Click the **Member Of** tab, and then click **Add**.
 - b) In the **Select Groups** dialog box, specify a group, and then click **OK** to add the groups that you want to the list.
 - c) Repeat the selection process for each group in which the user needs account membership.
 - d) Click **OK** to finish.
- 3) The final step in this process is to add a member server to the domain. This process also applies to workstations. To add a computer to the domain, follow these steps:

Log on to the computer that you want to add to the domain.

- a) Right-click **My Computer**, and then click **Properties**.
- b) Click the **Computer Name** tab, and then click **Change**.
- c) In the **Computer Name Changes** dialog box, click **Domain** under **Member Of**, and then type the domain name. Click **OK**.
- d) When you are prompted, type the user name and password of the account that you previously created, and then click **OK**.

A message that welcomes you to the domain is generated.

- e) Click **OK** to return to the **Computer Name** tab, and then click **OK** to finish.
- f) Restart the computer if you are prompted to do so.

2.3.2.4 Using Active Directory with Desktop Delivery Controller

Desktop Delivery Controller uses the services provided by Active Directory. It requires that all computers in a farm are members of a domain, with mutual trusting relationships between the domain used by Desktop Delivery Controller and the domain(s) used by virtual desktops.

Note: If your organizational structure means that you need a deployment where the Desktop Delivery Controller servers are in a separate Active Directory forest from the desktops for your users. It is important to understand how Desktop Delivery Controller uses Active Directory to appreciate the implications for your Active Directory environment.

Desktop Delivery Controller uses Active Directory for two main purposes:

- Active Directory's inbuilt security infrastructure is used by desktops to verify that communications from controllers come from authorized controllers in the appropriate farm. Active Directory's security infrastructure also ensures that the data exchanged by desktops and controllers is confidential. Desktop Delivery Controller uses Active Directory's inbuilt Kerberos infrastructure to guarantee the authenticity and confidentiality of communication. For more information about Kerberos, refer to Microsoft's product documentation.
- Active Directory is optionally used by desktops to discover the controllers that constitute a farm. This means you can add a new controller to a farm without having to reconfigure all desktops in the farm. Instead, desktops determine which controllers are available by referring to information that controllers publish in Active Directory. This feature is available only if the desktops are in the same Active Directory forest as the controllers.

When you create a farm, a corresponding Organizational Unit (OU) must be created in Active Directory if you want desktops to discover the controllers in the farm through Active Directory. The OU can be created in any domain in the forest that contains your computers. As best practice the OU should also contain the delivery controllers in the farm, but this is not enforced or required. A domain administrator with appropriate privileges can create the OU as an empty container. The domain administrator can then delegate administrative authority over the OU to the Desktop Delivery Controller administrator. If the installing administrator has CreateChild permissions on a parent OU, this administrator can also create the farm OU through the Active Directory Configuration wizard during installation. You can use the standard Active Directory Users and Computers MMC snap-in to configure these permissions.

During the Desktop Delivery Controller installation process, a small number of objects that are essential for the operation of the farm are created in the OU.

Note: Only standard Active Directory objects are created and used by Desktop Delivery Controller. It is not necessary to extend the schema.

The set of objects created includes:

- A Controllers security group. The computer account of all controllers in the farm must be a member of this security group. By default, this is done as part of installing Desktop Delivery Controller on a server. Desktops in a farm accept data from controllers only if they are members of this security group.

Ensure that all controllers have the 'Access this computer from the network' privilege on all virtual desktops running the Virtual Desktop Agent. You can do this by giving the Controllers security group this privilege. If controllers do not have this privilege, virtual desktops will fail to register.

- A Service Connection Point (SCP) object that contains information about the farm, such as the farm's name.

Note: If you use the Active Directory Users and Computers administrative tool to inspect a farm OU, you may have to enable Advanced Features in the View menu to see SCP objects.

- A container called RegistrationServices, which is created within the farm's OU. This contains one SCP object for each controller in the farm. The SCP is created when Desktop Delivery Controller is installed on a server. Each time the controller starts, it validates the contents of its SCP and updates them if necessary.

If multiple administrators are likely to add and remove controllers after the initial installation is complete, they need permissions to create and delete children on the RegistrationServices container and Write properties on the Controllers security group. Either the domain administrator or the original installing administrator can grant these permissions, and Citrix recommends setting up a security group to do this.

The following points are important to bear in mind when you are using a farm OU with Desktop Delivery Controller:

- Information is written to Active Directory only when installing or uninstalling Desktop Delivery Controller, or when a controller starts and needs to update the information in its SCP (for example, because the controller was renamed or because the communication port was changed). By default, the installation routine sets up permissions on the objects in the farm's OU appropriately, giving controllers Write access to their SCP. The contents of the objects in the farm OU are used to establish trust between desktops and controllers. You should ensure that:

- Only authorized Desktop Delivery Controller administrators can add or remove computers from the Controllers security group, using the security group's access control list (ACL)
- Only authorized administrators and the respective controller can change the information in the controller's SCP
- Depending on your Active Directory infrastructure, you should be aware of replication and its impact on a Desktop Delivery Controller implementation. Refer to Microsoft's documentation to understand the concepts of replication and associated delays. This is particularly important if you create the farm's OU in a domain that has domain controllers located in multiple Active Directory sites. Depending on the location of desktops, delivery controllers, and domain controllers, changes that are made to Active Directory when you are initially creating the OU for the farm, installing or uninstalling controllers, or changing controller names or communication ports may not be visible to desktops until that information is replicated to the appropriate domain controller. The symptoms of such replication delay include desktops that cannot establish contact with controllers and are, therefore, not available for user connections.
- Desktop Delivery Controller uses some of the standard computer object attributes in Active Directory to manage desktops. Depending on your setup, the machine object's fully qualified domain name, as stored in the desktop's Active Directory record, can be included as part of the connection settings that are returned to the user to make a connection. It is, therefore, important to ensure that this information is consistent with information held in your DNS environment.

Check Your Progress 2

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) Explain active directory structure.

.....

.....

.....

.....

2) list out the partitions of directory information tree?

.....

.....

.....

.....

3) Explain the role of DNS in Active directory.

.....

.....

.....

.....

- 4) Explain about active directory application mode.

2.4 DIGITAL FORENSICS

Digital forensics is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime. The term digital forensics expanded to cover investigation of all devices capable of storing digital data.

A digital forensic investigation commonly consists of 3 stages: acquisition or imaging of exhibits, analysis, and reporting. Acquisition involves creating an exact sector level duplicate of the media, often using a write blocking device to prevent modification of the original. Both acquired image and original media are hashed and the values compared to verify the copy is accurate.

Investigations can fall into one of four categories. The most common is forensic analysis, in which evidence is recovered to support or refute a hypothesis before a criminal court, closely related to intelligence gathering, in which material is intended to identify other suspects/crimes. eDiscovery is a form of discovery related to civil litigation and intrusion investigation is a specialist investigation into the nature and extent of an unauthorized network intrusion. The technical aspect of an investigation is divided into several sub-branches; computer forensics, network forensics, database forensics and mobile device forensics.

The digital forensic process encompasses the seizure, forensic imaging and analysis of digital media and the production of a report into collected evidence for the benefit of courts or an employer. As well as identifying direct evidence of a crime, digital forensics can be used to attribute evidence to specific suspects, confirm alibis or statements, determine intent, identify sources or authenticate documents. Investigations are much broader in scope than other areas of forensic analysis often involving complex time-lines or hypotheses.

The actual process of analysis can vary between investigations, but common methodologies include conducting keyword searches across the digital media within files as well as unallocated and slack space, recovering deleted files and extraction of registry information.

Investigations can take one of four forms. Firstly as a forensic examination, traditionally associated with criminal law, where evidence is collected to support or oppose a hypothesis. Like other areas of forensics this is often part of a wider investigation spanning a number of disciplines. A related form is "intelligence gathering", functionally identical to a forensic examination the digital evidence is intended to be used as intelligence to locate, identify or halt other crimes. As a result intelligence gathering is sometimes held to a less strict forensic standard. In civil litigation or corporate matters the process is referred to as electronic discovery or eDiscovery. The forensic procedure is similar to that used in criminal investigations but with different legal requirements and limitations. Finally, intrusion investigation is a specialist examination into the nature and extent of an unauthorized network intrusion. Intrusion analysis is usually performed as a damage limitation exercise after an attack, both to establish the extent of any intrusion and

to try and identify the attacker. The main use of digital forensics is to recover objective evidence of a criminal activity.

2.4.1 Computer Forensics

Computer Forensics is a branch of digital forensic science pertaining to legal evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the information.

Although it is most often associated with the investigation of a wide variety of computer crime, computer forensics may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal audit trail. Evidence from computer forensics investigations is usually subjected to the same guidelines and practices of other digital evidence. It has been used in a number of high profile cases and is becoming widely accepted as reliable within US and European court systems.

2.4.2 Network Forensics

Network Forensics is a sub-branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence or intrusion detection. Unlike other areas of digital forensics, network investigations deal with volatile and dynamic information. Network traffic is transmitted and then lost, so network forensics is often a pro-active investigation.

Network forensics generally has two uses. The first, relating to security, involves monitoring a network for anomalous traffic and identifying intrusions. An attacker might be able to erase all log files on a compromised host; network-based evidence might therefore be the only evidence available for forensic analysis. The second form of Network forensics relates to law enforcement. In this case analysis of captured network traffic can include tasks such as reassembling transferred files, searching for keywords and parsing human communication such as emails or chat sessions. Two systems are commonly used to collect network data; a brute force "catch it as you can" and a more intelligent "stop look listen" method.

Applying forensic methods on the Ethernet layer is done by eavesdropping bit streams with tools called monitoring tools or sniffers. The most common tools on this layer is **Wireshark**. It collects all data on this layer and allow the user to filter for different events. With these tools websites, email attachments and more that has been transmitted over the network can be reconstructed. An advantage of collecting this data is that it is directly connected to a host. To collect data on this layer, the network interface card (NIC) of a host can be put into "promiscuous mode". By this, it collects all traffic that comes over the network not only the traffic meant for this special host.

On the network layer the Internet Protocol is responsible for directing the packets generated by TCP through the network by adding source and destination information which can be interpreted by routers all over the network. Cellular digital packet networks, like GPRS, use similar protocols like IP, so the methods described for IP work with them as well.

For the correct routing, every intermediate router must have a routing table to know where to send the packet next. These routing tables are one of the best sources of information if investigating a digital crime and trying to track down an attacker. To do this, it is necessary to follow the packets of the attacker, reverse the sending route and find the computer the packet came from the attacker.

The internet can be a rich source of digital evidence including web browsing, email, newsgroup, synchronous chat and peer-to-peer traffic. For example web

server logs can be used to show when (or if) a suspect accessed information related to criminal activity. Email accounts can often contain useful evidence; but email headers are easily faked and, so, network forensics may be used to prove the exact origin of incriminating material. Network forensics can also be used in order to find out who is using a particular computer by extracting user account information from the network traffic.

Wireless forensics is a sub-discipline of network forensics. The main goal of wireless forensics is to provide the methodology and tools required to collect and analyze wireless network traffic that can be presented as valid digital evidence in a court of law. The evidence collected can correspond to plain data or, with the broad usage of Voice-over-IP technologies, especially over wireless, can include voice conversations. Analysis of wireless network traffic is similar to that on wired networks, however there may be the added consideration of wireless security measures.

2.4.3 Database Forensics

Database Forensics is a branch of digital forensic science relating to the forensic study of databases and their related metadata.

A forensic examination of a database may relate to the timestamps that apply to the update time of a row in a relational table being inspected and tested for validity in order to verify the actions of a database user. Alternatively, a forensic examination may focus on identifying transactions within a database system or application that indicate evidence of wrong doing, such as fraud.

Software tools such as ACL, Idea and Arbutus (which provide a read-only environment) can be used to manipulate and analyze data. These tools also provide audit logging capabilities which provide documented proof of what tasks or analysis a forensic examiner performed on the database.

Currently many database software tools are in general not reliable and precise enough to be used for forensic work as demonstrated in the first paper published on database forensics. There is currently a single book published in this field, though more are destined. Additionally there is a subsequent SQL Server forensics book by Kevvie Fowler named SQL Server Forensics which is well regarded also.

The forensic study of relational databases requires a knowledge of the standard used to encode data on the computer disk. A documentation of standards used to encode information in well known brands of DB such as SQL Server and Oracle has been contributed to the public domain.

2.4.4 Mobile Device Forensics

Mobile Device Forensics is a branch of digital forensics relating to recovery of digital evidence or data from a mobile device under forensically sound conditions. The phrase mobile device usually refers to mobile phones; however, it can also relate to any digital device that has both internal memory and communication ability.

The use of phones in crime was widely recognized for some years, but the forensic study of mobile devices is a relatively new field, dating from the early 2000s. A proliferation of phones on the consumer market caused a demand for forensic examination of the devices, which could not be met by existing computer forensics techniques. The memory type, custom interface and proprietary nature of mobile devices requires a different forensic process compared to computer forensics. Each device often has to have custom extraction techniques used on it. Mobile devices can be used to save several types of personal information such as contacts, photos, calendars and notes.

As mobile device technology advances, the amount and types of data that can be found on a mobile device is constantly increasing. Evidence that can be potentially recovered by law enforcement agents from a mobile phone may come from several different sources, including SIM card, Handset and attached memory cards.

Traditionally mobile phone forensics has been associated with recovering SMS and MMS messaging, as well as call logs, contact lists and phone IMEI/ESN information. Newer generations of smart phones also include wider varieties of information; from web browsing, Wireless network settings, e-mail and other forms of rich internet media, including important data now retained on smartphone applications.

Check Your Progress 3

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

Explain Mobile device forensics.

.....

.....

.....

.....

2.5 LET US SUM UP

This unit covers the detailed descriptions of the digital water marking and Active Directory Controller. Here you know the important parameter in digital watermarking and insertion and extraction units of watermark. The available types of watermarks are public, private, fragile, video, audio, text and image. After completion of these you study the attacks and characteristics of digital watermarking. The structure of the Active Directory Controller includes Forests, trees, domains, Flat-filed, simulated hierarchy and Shadow Groups. The different Structural divisions to improve performance are FSMO Roles, Trust, Adding Users and Computers to the Active Directory Domain and Using Active Directory with Desktop Delivery Controller. It also describes digital forensics.

2.6 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

- 1) Watermarking is the process that embeds data called a watermark, tag or label into a multimedia Object such that watermark can be detected or extracted later to make an assertion about the object. The object may be an image or text or audio or Video. Digital watermarking allows a person to hide copyrights on audio, video or images. This information usually includes the maker, the copyright itself and any other data the owner wants to include copyright protection systems prevent or deter unauthorized copying of digital media. In this use a copy device retrieves the watermark from the signal before making a copy; the device makes a decision to copy or not depending on the contents of the watermark.
- 2) The information to be embedded is called a digital watermark. The signal where the watermark is to be embedded is called the host signal. Embedding and detection are the two steps in watermarking life cycle. In embedding, an

algorithm accepts the host and the data to be embedded and produces a watermarked signal. The watermarked signal is then transmitted or stored. detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it.

- 3) Robustness attacks attempt to diminish or remove the presence of watermarks in a suspect image without rendering the image useless. These attacks can be classified into two types: signal processing attacks, and analytic and algorithmic attacks. A signal processing attack include common processing operations such as compression, filtering, resizing, printing, and scanning. Analytic and algorithmic attacks involve removal or weakening of watermarks in images based on the specific methods of watermark insertion and detection.
- 4) A watermark is a secondary image which is overlaid on the primary image, and provides a means of protecting the image. A visible watermark is a visible translucent image which is overlaid on the primary image. Perhaps consisting of the logo or seal of the organization which holds the rights to the primary image, it allows the primary image to be viewed, but still marks it clearly as the property of the owning organization. An invisible watermark is an overlaid image which cannot be seen, but which can be detected algorithmically.

Check Your Progress 2

- 1) The Active Directory structure and storage architecture consists of four parts:
 - i) **Active Directory domains and forests:** Forests, domains, and organizational units (OUs) make up the core elements of the Active Directory logical structure. A forest defines a single directory and represents a security boundary. Forests contain domains.
 - ii) **Domain Name System (DNS) support for Active Directory:** DNS provides a name resolution service for domain controller location and a hierarchical design that Active Directory can use to provide a naming convention that can reflect organizational structure.
 - iii) **Schema:** The schema provides object definitions that are used to create the objects that are stored in the directory.
 - iv) **Data store:** The data store is the portion of the directory that manages the storage and retrieval of data on each domain controller.
- 2) Directory Information Tree (DIT) is broken into the following partitions:

Schema partition - Defines rules for object creation and modification for all objects in the forest. Replicated to all domain controllers in the forest. Replicated to all domain controllers in the forest, it is known as an enterprise partition.

Configuration partition - Information about the forest directory structure is defined including trees, domains, domain trust relationships, and sites (TCP/IP subnet group). Replicated to all domain controllers in the forest, it is known as an enterprise partition.

Domain partition - Has complete information about all domain objects (Objects that are part of the domain including OUs, groups, users and others). Replicated only to domain controllers in the same domain. Partial domain directory partition - Has a list of all objects in the directory with partial list of attributes for each object.
- 3) Active Directory is integrated with Domain Naming System (DNS) and requires it to be present to function. DNS is the naming system used for the Internet

and on many Intranets. You can use DNS which is built into Windows 2000 and newer, or use a third party DNS infrastructure such as BIND if you have it in the environment. It is recommended you use Windows' DNS service as it is integrated into Windows and provides the easiest functionality. AD uses DNS to name domains, computers, servers, and locate services. A DNS server maps an object's name to its IP address. In an Active Directory network, it is used not only to find domain names, but also objects and their IP address. It also uses service location records (SRV) to locate services.

- 4) Active Directory Application Mode (ADAM) is a new mode of Active Directory that is designed specifically for directory-enabled applications. ADAM is a Lightweight Directory Access Protocol (LDAP) directory service that runs as a user service, rather than as a system service. You can run ADAM on servers and domain controllers running operating systems in the Windows Server 2003 family (except for Windows Server 2003, Web Edition) and also on client computers running Windows XP Professional. ADAM does not require the deployment of domains or domain controllers. You can run multiple instances of ADAM concurrently on a single computer, with an independently managed schema and independently managed data for each ADAM instance.

Check Your Progress 3

Mobile device forensics: It is a branch of digital forensics relating to recovery of digital evidence or data from a mobile device under forensically sound conditions. The phrase mobile device usually refers to mobile phones; however, it can also relate to any digital device that has both internal memory and communication ability.

The use of phones in crime was widely recognized for some years, but the forensic study of mobile devices is a relatively new field, dating from the early 2000s. A proliferation of phones on the consumer market caused a demand for forensic examination of the devices, which could not be met by existing computer forensics techniques. The memory type, custom interface and proprietary nature of mobile devices requires a different forensic process compared to computer forensics. Each device often has to have custom extraction techniques used on it. Mobile devices can be used to save several types of personal information such as contacts, photos, calendars and notes.

As mobile device technology advances, the amount and types of data that can be found on a mobile device is constantly increasing. Evidence that can be potentially recovered by law enforcement agents from a mobile phone may come from several different sources, including SIM card, Handset and attached memory cards.

2.7 SUGGESTED READINGS

- <http://msdn.microsoft.com/en-us/library/ms675160%28VS.85%29.aspx>
- <http://technet.microsoft.com/en-us/library/bb727051.aspx>
- <http://technet.microsoft.com/en-us/library/cc978003.aspx>
- www.safeword.com/welcome.htm
- www.securecomputing.com

UNIT 3 IDENTITY MANAGEMENT

Structure

- 3.0 Introduction
- 3.1 Objectives
- 3.2 Biometrics
 - 3.2.1 Biometric Technologies
 - 3.2.2 Risks of a Biometric System
- 3.3 All Physical Security
- 3.4 Login
- 3.5 Finger Printing
- 3.6 Let Us Sum Up
- 3.7 Check Your Progress: The Key
- 3.8 Suggested Readings

3.0 INTRODUCTION

Identity management is a term related to how humans are identified and authorized across computer networks. It covers issues such as how users are given an identity, the protection of that identity, and the technologies supporting that protection (e.g., network protocols, digital certificates, passwords, etc.).

While the term management requires little explanation, the term identity is a more abstract concept that will always be difficult to define in a way that satisfies everyone. It is a concept that is fluid and contextual depending on a number of factors including culture.

Thus the term management is appended to "identity" to indicate that there is technological and best practices framework around a somewhat intractable philosophical concept. Digital identity can be interpreted as the codification of identity names and attributes of a physical instance in a way that facilitates processing. In each organization there is normally a role or department that is responsible for managing the schema of digital identities of their staff and their own objects, these represented by object identities or object identifiers.

The biometric identifier generation algorithms employ image hashing functions using singular value decomposition and support vector classification techniques. Based on the biometric type and the classification models, as a result of the empirical evaluation we can generate biometric identifiers ranging from 64 bits up to 214 bits. We provide an example use of the biometric identifiers in privacy preserving multi-factor identity verification based on zero knowledge proofs. Therefore several identity verification factors, including various traditional identity attributes, can be used in conjunction with one or more biometrics of the individual to provide strong identity verification. We also ensure security and privacy of the biometric data. More specifically, we analyze several attack scenarios. We assure privacy of the biometric using the one-way hashing property, in that no information about the original biometric image is revealed from the biometric identifier.

3.1 OBJECTIVES

After completion of this unit, you will be able to:

- Understand what Identity Management is all about?

- Describe the types of Identity Management in Digital Watermarking; and
- Describe Biometrics, All Physical Security, Login and Finger Printing.

3.2 BIOMETRICS

Biometric security offers a different method of authentication by using something that is far more unique than a password. A biometric is a physical trait that consists of facial structure, eye color, voice, iris pattern, and fingerprint.

An introduction to authentication technologies and biometrics dealing with privacy issues Biometric technologies, including finger, hand geometry, handwriting, iris, retina, voice, and face Security concerns related to biometrics, including attempts to spoof or fake results Deployment of biometric security systems, including vendor selection and roll out procedures Real-life case studies. For security, system, and network administrators and managers, as well as anyone who is interested in the application of cutting-edge biometric technology, Biometrics for Network Security will prove an indispensable addition to your library!

Biometrics Integrated has extensive hands-on experience with all biometric hardware and software solutions, including fingerprint, AFIS, facial recognition, hand geometry, iris recognition, retina-scan, voice recognition, signature verification, and keystroke dynamics. Biometrics Integrated is completely vendor-independent and technology-neutral, allowing it to objectively and independently assess biometrics companies, biometrics technologies, biometric products, and projects.

The main use of Biometric network security will be to replace the current password system. Maintaining password security can be a major task for even a small organization. Passwords have to be changed every few months and people forget their password or lock themselves out of the system by incorrectly entering their password repeatedly. Very often people write their password down and keep it near their computer. This is of course completely undermines any effort at network security. Biometrics can replace these. For example the city of Glendale in Los Angeles county California replaced its password system with fingerprint scanners that use biometrics. The cities employees had the usual password problems. The passwords had to be changed every 90 days and no dictionary words were allowed, only 8-digit alphanumeric strings. The vast majority of users failed to change their passwords and as a result got locked out of the system. The only way for them to get back in the system was a call to the IT helpdesk, which became swamped with calls. The help desk staff ended up spending a disproportionately large amount of time fixing problems with passwords. This is the hidden cost of using passwords, the helpdesk admin costs that always result when people get locked out of the system. The use of biometric identification stops this problem and while it may be expensive to set up at first, these devices save on administration and user assistance costs.

One way that biometrically verified logons would be implemented is using a centralized system (particularly using voice biometrics). Such a system would be ideal for implementing secure remote logons by mobile users. Remote network access enables tele working, which has been promised by the 'e' community for a long time, especially with the arrival of broadband access from the home. It is also important for field employees who travel all over for the company, yet need access to company resources. Biometric identification used along with a secure connection (a problem that is entirely separate to that of Biometrics) to the network makes this once vulnerable aspect of networking more secure. Biometric technology uses a physical or psychological trait for identification and/or authentication.

Biometrics is the automated method of recognizing a person based on a physiological or behavioral characteristic. Biometric technologies are becoming

the foundation of an extensive array of highly secure identification and personal verification solutions.

Biometric technologies should be considered and evaluated giving full consideration to the following characteristics:

- **Universality:** Every person should have the characteristic. People who are mute or without a fingerprint will need to be accommodated in some way.
- **Uniqueness:** Generally, no two people have identical characteristics. However, identical twins are hard to distinguish.
- **Permanence:** The characteristics should not vary with time. A person's face, for example, may change with age.
- **Collectibility:** The characteristics must be easily collectible and measurable.
- **Performance:** The method must deliver accurate results under varied environmental circumstances.
- **Acceptability:** The general public must accept the sample collection routines. Nonintrusive methods are more acceptable.
- **Circumvention:** The technology should be difficult to deceive.

Biometrics is expected to be incorporated in solutions to provide for Homeland Security including applications for improving airport security, strengthening the United States' national borders, in travel documents, visas and in preventing ID theft. Now, more than ever, there is a wide range of interest in biometrics across federal, state, and local governments. Congressional offices and a large number of organizations involved in many markets are addressing the important role that biometrics will play in identifying and verifying the identity of individuals and protecting national assets.

There are many needs for biometrics beyond Homeland Security. Enterprise-wide network security infrastructures, secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies. A range of new applications can be found in such diverse environments as amusement parks, banks, credit unions, and other financial organizations, Enterprise and Government networks, passport programs and driver licenses, colleges, physical access to multiple facilities (e.g., nightclubs) and school lunch programs.

Biometric-based authentication applications include workstation, network, and domain access, single sign-on, application logon, data protection, remote access to resources, transaction security and Web security. Trust in these electronic transactions is essential to the healthy growth of the global economy. Utilized alone or integrated with other technologies such as smart cards, encryption keys and digital signatures, biometrics are set to pervade nearly all aspects of the economy and our daily lives. Utilizing biometrics for personal authentication is becoming convenient and considerably more accurate than current methods (such as the utilization of passwords or PINs). This is because biometrics links the event to a particular individual (a password or token may be used by someone other than the authorized user), is convenient (nothing to carry or remember), accurate (it provides for positive authentication), can provide an audit trail and is becoming socially acceptable and inexpensive.

Biometric authentication requires comparing a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (for example, a fingerprint captured during a login). During **Enrollment** a sample of the biometric trait is captured, processed by a computer, and stored for later comparison.

Biometric recognition can be used in **Identification** mode, where the biometric system identifies a person from the entire enrolled population by searching a database for a match based solely on the biometric. For example, an entire database can be searched to verify a person has not applied for entitlement benefits under two different names. This is sometimes called “one-to-many” matching. A system can also be used in **Verification** mode, where the biometric system authenticates a person’s claimed identity from their previously enrolled pattern. This is also called “one-to-one” matching. In most computer access or network access environments, verification mode would be used. A user enters an account, user name, or inserts a token such as a smart card, but instead of entering a password, a simple touch with a finger or a glance at a camera is enough to authenticate the user.

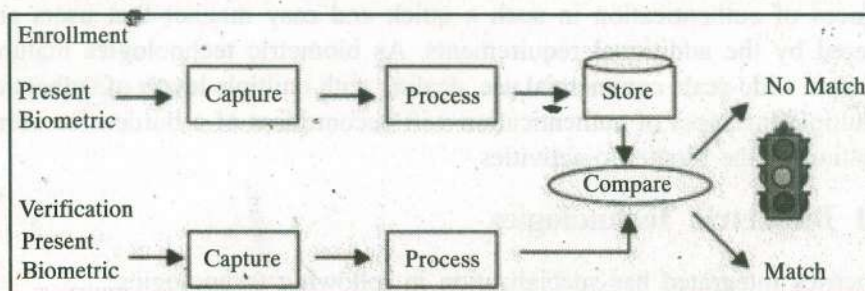


Fig. 1

Biometric-based authentication applications include workstation and network access, single sign-on, application logon, data protection, remote access to resources, transaction security, and Web security. The promises of e-commerce and e-government can be achieved through the utilization of strong personal authentication procedures. Secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies. Biometric technologies are expected to play a key role in personal authentication for large-scale enterprise network authentication environments, Point-of-Sale and for the protection of all types of digital content such as in Digital Rights Management and Health Care applications. Utilized alone or integrated with other technologies such as smart cards, encryption keys and digital signatures, biometrics are anticipated to pervade nearly all aspects of the economy and our daily lives. For example, biometrics is used in various schools such as in lunch programs in Pennsylvania, and a school library in Minnesota. Examples of other current applications include verification of annual pass holders in an amusement park, speaker verification for television home shopping, Internet banking, and users' authentication in a variety of social services.

Using biometrics for identifying human beings offers some unique advantages. Biometrics can be used to identify you as you. Tokens, such as smart cards, magnetic stripe cards, photo ID cards, physical keys and so forth, can be lost, stolen, duplicated, or left at home. Passwords can be forgotten, shared, or observed. Moreover, today's fast-paced electronic world means people are asked to remember a multitude of passwords and personal identification numbers (PINs) for computer accounts, bank ATMs, e-mail accounts, wireless phones, web sites and so forth. Biometrics hold the promise of fast, easy-to-use, accurate, reliable, and less expensive authentication for a variety of applications.

There is no one “perfect” biometric that fits all needs. All biometric systems have their own advantages and disadvantages. There are, however, some common characteristics needed to make a biometric system usable. First, the biometric must be based upon a distinguishable trait. For example, for nearly a century, law enforcement has used fingerprints to identify people. There is a great deal of scientific data supporting the idea that “no two fingerprints are alike.” Technologies such as hand geometry have been used for many years and technologies such as face or iris recognition have come into widespread use. Some newer biometric

methods may be just as accurate, but may require more research to establish their uniqueness.

Another key aspect is how "user-friendly" a system is. The process should be quick and easy, such as having a picture taken by a video camera, speaking into a microphone, or touching a fingerprint scanner. Low cost is important, but most implementers understand that it is not only the initial cost of the sensor or the matching software that is involved. Often, the life-cycle support cost of providing system administration and an enrollment operator can overtake the initial cost of the biometric hardware.

The advantage biometric authentication provides is the ability to require more instances of authentication in such a quick and easy manner that users are not bothered by the additional requirements. As biometric technologies mature and come into wide-scale commercial use, dealing with multiple levels of authentication or multiple instances of authentication will become less of a burden for users. An indication of the biometric activities

3.2.1 Biometric Technologies

Biometrics Integrated has specialization in following technologies:

- Fingerprint Recognition
- Face Recognition
- Iris Recognition
- Voice Recognition
- Smart Cards
- Signature Verification
- Hand and Finger Geometry
- Encryption Systems
- Security Tokens

Fingerprint Recognition is one of the most used and familiar biometric methods. Fingerprint Recognition Technology or Fingerprint Authentication is a technique of verifying a match between two human fingerprints. In biometrics technologies, fingerprints are one of many forms of biometrics used to identify an individual and verify their identity. Fingerprint Recognition Technology has many security application in real world like it can be used in -

- Network/ PC Login Security
- Web Page Security
- Employee Recognition Systems
- Time and Attendance Systems
- Voting Solutions

Face Recognition: The identification of a person by their facial image can be done in a number of different ways such as by capturing an image of the face in the visible spectrum using an inexpensive camera or by using the infrared patterns of facial heat emission. Facial recognition in visible light typically model key features from the central portion of a facial image. Using a wide assortment of cameras, the visible light systems extract features from the captured image(s) that do not change over time while avoiding superficial features such as facial expressions or hair. Several approaches to modeling facial images in the visible

spectrum are Principal Component Analysis, Local Feature Analysis, neural networks, elastic graph theory, and multi-resolution analysis.

Some of the challenges of facial recognition in the visual spectrum include reducing the impact of variable lighting and detecting a mask or photograph. Some facial recognition systems may require a stationary or posed user in order to capture the image, though many systems use a real-time process to detect a person's head and locate the face automatically. Major benefits of facial recognition are that it is non-intrusive, hands-free, continuous and accepted by most users.

Face recognition is a biometric technique for automatic identification or verification of a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a facial database. Face Recognition System is typically used in security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems.

Iris Recognition: This recognition method uses the iris of the eye which is the colored area that surrounds the pupil. Iris patterns are thought unique. The iris patterns are obtained through a video-based image acquisition system. Iris scanning devices have been used in personal authentication applications for several years. Systems based on iris recognition have substantially decreased in price and this trend is expected to continue. The technology works well in both verification and identification modes (in systems performing one-to-many searches in a database). Current systems can be used even in the presence of eyeglasses and contact lenses. The technology is not intrusive. It does not require physical contact with a scanner. Iris recognition has been demonstrated to work with individuals from different ethnic groups and nationalities.

Iris Recognition is a biometric authentication method that uses pattern recognition techniques based on high-resolution images of the irides of an individual's eyes. Converted into digital templates, these images provide mathematical representations of the iris that yield unambiguous positive identification of an individual. Iris recognition technology has become popular in security applications because of its ease of use, accuracy, and safety. Its most common use is controlling access to high-security areas. Iris recognition technology is currently used at physical access points demanding high security, such as airports, government buildings, and research laboratories.

Voice Recognition or Speaker Recognition is a biometric process of validating a user's claimed identity using characteristics extracted from their voices. Thus voice recognition can be an effective technique in user authentication and identification. Speaker recognition has a history dating back some four decades, where the output of several analog filters were averaged over time for matching. Speaker recognition uses the acoustic features of speech that have been found to differ between individuals. These acoustic patterns reflect both anatomy (e.g., size and shape of the throat and mouth) and learned behavioral patterns (e.g., voice pitch, speaking style). This incorporation of learned patterns into the voice templates (the latter called "voiceprints") has earned speaker recognition its classification as a "behavioral biometric." Speaker recognition systems employ three styles of spoken input: text-dependent, text-prompted and text-independent. Most speaker verification applications use text-dependent input, which involves selection and enrollment of one or more voice passwords. Text-prompted input is used whenever there is concern of imposters.

The various technologies used to process and store voiceprints includes hidden Markov models, pattern matching algorithms, neural networks, matrix representation and decision trees. Some systems also use "anti-speaker" techniques, such as cohort models, and world models.

Ambient noise levels can impede both collection of the initial and subsequent voice samples. Performance degradation can result from changes in behavioral attributes of the voice and from enrollment using one telephone and verification on another telephone. Voice changes due to aging also need to be addressed by recognition systems. Many companies market speaker recognition engines, often as part of large voice processing, control and switching systems. Capture of the biometric is seen as non-invasive. The technology needs little additional hardware by using existing microphones and voice-transmission technology allowing recognition over long distances via ordinary telephones (wire line or wireless).

Smart Cards are digital security pocket-sized cards with embedded integrated circuits which can process data. Thus smart cards can be used for identification, authentication, and data storage. It can also be used as a medium to provide a means of effecting business transactions in a flexible, secure, standard way with minimal human intervention. Smart card can provide strong authentication for single sign-on or enterprise single sign-on to computers, laptops, data with encryption, enterprise resource planning platforms such as SAP, etc...

Signature Verification: This technology uses the dynamic analysis of a signature to authenticate a person. The technology is based on measuring speed, pressure and angle used by the person when a signature is produced. One focus for this technology has been e-business applications and other applications where signature is an accepted method of personal authentication.

Hand and Finger Geometry: These methods of personal authentication are well established. Hand recognition has been available for over twenty years. To achieve personal authentication, a system may measure either physical characteristics of the fingers or the hands. These include length, width, thickness and surface area of the hand. One interesting characteristic is that some systems require a small biometric sample (a few bytes). Hand geometry has gained acceptance in a range of applications. It can frequently be found in physical access control in commercial and residential applications, in time and attendance systems and in general personal authentication applications.

A Hand Geometry Example

Corporations such as Time Masters, Inc, out of Los Angeles, California, have specialized in this technology and have marketed hand and finger geometry as a part of a workforce management solution for companies. The Time Masters Hand Punch (Figures E and F) captures a three-dimensional accurate image of an employee's hand each time an employee punches in and out with green and red lights notifying the employee of the status of each punch.

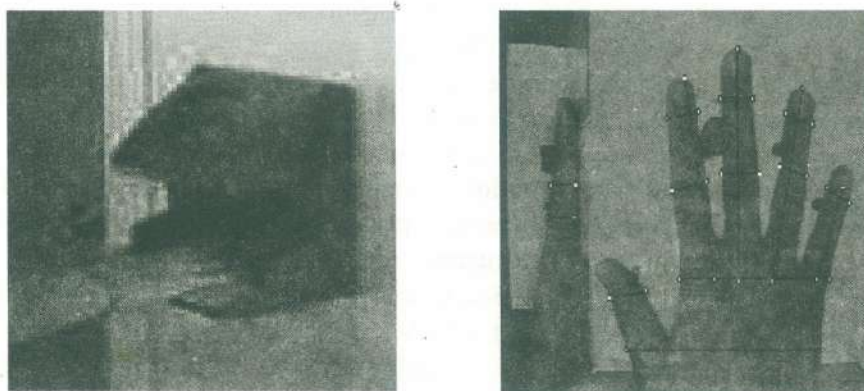


Fig. 2

Encryption Systems on the other hand, use an encryption technique for transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually

referred to as a key. The result of the process is encrypted information (in cryptography, referred to as cipher text). Encryption Systems can be used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines. Encryption has long been used by militaries and governments to facilitate secret communication. Encryption is now commonly used in protecting information within many kinds of civilian systems.

Security Tokens (or sometimes a hardware token, hard token, authentication token, USB token, cryptographic token, or key fob) are biometric devices which ease authentication for authorized user of computer services. These tokens are also known as Software Tokens. Security tokens are used to prove one's identity electronically (as in the case of a customer trying to access their bank account). The token is used in addition to or in place of a password to prove that the customer is who they claim to be. The token acts like an electronic key to access something

3.2.2 Risks of a Biometric System

By using biometric system, we can identify a number of potential points of attack. These attack points vary in function of the operation mode (identification or verification) and the control model. The main risks of a biometric system have been compiled by several IT security and certification organizations. The risk list is presented in the table below.

Risks	Examples	Possible Countermeasures
Spoofing and mimicry attacks	Artificial finger used on fingerprint biometric device	Multimodal biometrics, vitality detection, interactive protocol
Fake reference template risk	Fake reference template stored in server or supplied during enrolment	Encryption, intrusion detection system (IDS), supervised enrolment
Transmission risk	Data intercepted during transmission during enrolment or data acquisition	Interactive recognition, rejection of identical signals, system integration
Component alternation risk	Malicious code, Trojan, etc.	System integration, well implemented security policy
Enrolment, administration and system use risk	Data altered during enrolment, administration or system use	Well-implemented security policy
Similar template/similar characteristics risk	An illegitimate user has a template similar to a legitimate user.	Technology assessment, multimodal access, calibration review
Brute-force attack risk	An intruder uses brute force to deceive the system.	Account lock after number of unsuccessful attempts
Injection risk	Captured digital signal injected into authentication system	Secure transmission; heat sensor activated scanner (warm body present); date/time stamps in digital representation of images

Users' rejection	The invasive nature of biometrics techniques could cause users to reject using the system.	the least intrusive technique possible
Changes in physical characteristics	Some techniques depend on face or hand characteristics, but these human aspects change with the years.	Monitoring of template evolution during use of system
Cost of integration with other legacy systems	Coherence with other techniques used for legacy systems than have to be integrated	Cost-benefit analysis
Risk of loss of data	Hard disk/hardware failure	Data backup and restoration
Risk of biometric data dissemination	Exchange of biometric data between operators without consent of data subjects	No storage of raw data, limit for the lifetime of a biometric template, encapsulated storage of biometric data in the hand of the data subject

Main risks of a biometric system

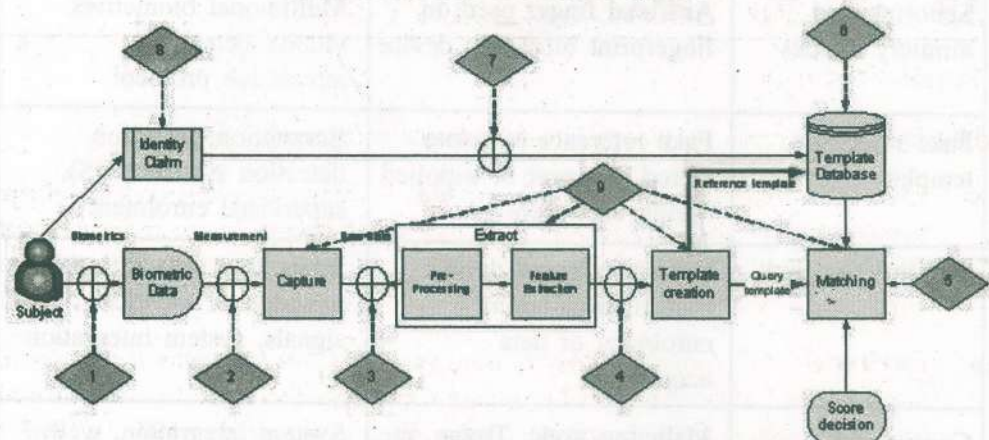


Fig. 3: Fault sensitive points of a biometric system

Check Your Progress 1

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) Define Identity Management.

.....

.....

.....

.....

.....

.....

- 2) Explain how smart cards provide security.

.....

.....

.....

.....

- 3) Explain about Iris recognition process.

.....

.....

.....

.....

- 4) List out various advantages of a Biometric Authentication?

.....

.....

.....

.....

3.3 ALL PHYSICAL SECURITY

Physical Security

Physical Security can be placed into four major categories:

- **Electrical:** Electrical vulnerabilities are seen in things such as spikes in voltage to different devices and hardware systems, or brownouts due to an insufficient voltage supply. Electrical threats also come from the noise of unconditioned power and, in some extreme circumstances, total power loss.
- **Environmental:** Not only do you need to secure your systems from human interference, but you also need to secure them from the interference of natural disasters such as fires, hurricanes, tornados, and flooding, which fall under the realm of environmental threat. Environmental issues also come from extreme temperature or humidity.
- **Hardware:** Hardware threats are simply the threat of physical damage to corporate hardware or its theft.
- **Maintenance:** Maintenance threats are due to poor handling of electronic components, which cause ESD (electrostatic discharge), the lack of spare parts, poor cabling, poor device labeling, etc.

Place your systems (servers, routers, switches, appliances, management stations, etc.) in a controlled environment whenever feasible. Mission-critical equipment must be confined to computer rooms, server rooms, or wiring closets. Here are some recommendations for equipment security:

- Offer limited and locked (physical or electronic) access to authorized personnel only.
- The area should not be accessible through dropped ceilings, raised floors, windows, or ductwork.

- An official, secured access point must be the only point of entry.
- Electronic access control should be implemented, if feasible, with all attempts to access logged by security systems and monitored by security personnel.
- Trained security personnel should monitor security cameras with automatic log recording if possible.

In addition to the physical security mentioned earlier in this section, electrical supply problems should be limited with the following measures:

- Install UPS (uninterruptible power supply) systems for mission-critical hardware.
- Deploy backup generator systems for mission-critical disaster recovery if feasible.
- Test and maintain UPS and/or generators based on the manufacturers' suggested preventative maintenance schedule.
- Monitor and alarm power-related parameters at the supply and device level.
- Use filtered power and install redundant power supplies on mission-critical devices.

The following guidelines should be used to mitigate against hardware and maintenance-related threats:

- Always follow ESD procedures when replacing or working inside hardware devices.
- Label and secure cabling to equipment racks to protect against accidental disconnection or damage. This also helps prevent hardware from walking away with the assistance of thieves.
- Use cable runs and/or raceways to traverse rack-to-ceiling or rack-to-rack links.
- Maintain critical spare parts and modules in case of emergencies.
- Don't leave a console, workstation, or management station logged on with administrative access when you leave the area for any significant amount of time. Be sure these systems are locked down with cables and locks as well.
- Maintain a regularly updated database of all hardware documentation and technical support information in case of emergencies.

One of the most significant reasons for placing physical security as the top security layer is that it can often be implemented with low cost, diligence, and common sense. Remember that an entire fleet of expensive security software tools can quickly be rendered impotent if a malicious user can gain physical access to your corporate servers, networking devices, and management workstations.

Data Security

The second layer of security is data security, which involves a variety of complex mechanisms. This area consists of components to guard against unauthorized access to data in storage as well as data that is transmitted over communications networks, both private and public. This layer involves components such as integrity controls, and authentication, plus additional access controls and/or encryption mechanisms.

Integrity controls are mechanisms that ensure that the data being electronically stored or transmitted is valid. One of the best open standards for implementing data security is IPSec (Internet Protocol Security). This can include additional support for message and user authentication. Message authentication is the process

of ensuring that the sent message exactly matches the received message. User authentication makes sure that the sender of the message is genuinely who they are supposed to be. Businesses can also use these technologies to guarantee accountability and reliability when exchanging electronic documents, such as contracts and agreements.

System access controls involve controlling access to corporate information, system and documentation files, electronic records and assets, and even data about customers or clients. User access management prevents unauthorized access to business information systems and computers as well. These access controls can also involve monitoring and auditing. Network operating systems from a number of vendors provide secure directories and file systems with access security measures and hardening techniques -- Microsoft Windows 2003 with Active Directory is a prominent example.

Encryption is any process or technology that uses cryptography to translate plaintext into cipher text. This is used to keep someone other than the intended recipient from reading the data. Encryption is often provided by third-party components or integrated code on the actual system boards. Digital signatures, certificates, and PKI (Public Key Infrastructure) tools can be used to provide this service.

Application Security

Application security mechanisms include the usage of secure program code, regular updates, patching, and fixing, and security policy software solutions to guarantee secure business application processes. Some programs introduced into the environment can be Trojan horse programs that are actually snippets of nefarious code in disguise. You should use antivirus software and software firewalls in concert with your corporate collaboration and productivity applications to protect against attacks.

Network Security

You absolutely must protect your internal corporate network and perimeter networks from intruders and malware using network firewalls (software and/or appliances), VPNs (virtual private networks), IDSs (intrusion detection systems), as well as web and content filtering for your enterprise. Network security is a constantly continuing and dynamic process.

Network security includes the following four steps:

- **Secure:** Lock your networks with a combination of authentication, encryption, firewalls, and continuous patching of system vulnerabilities.
- **Examine:** To maintain a secure network, you have to regularly monitor the state of security mechanisms, readiness, and incident handling procedures. Network vulnerability scanners from a number of reputable vendors will proactively locate areas of weakness, and IDSs can alert and respond to security events when they occur. Your organization can get high visibility of the network data stream and the security condition of the network using emerging security solutions.
- **Test:** Equally as vital as network examination and assessment is testing. Without adequate testing of the security solutions, it's tough to know about new threats and attacks. The hacker community is an ever-changing continuum with menacing designs on your systems and data. You can perform this testing yourself or you can outsource it to a third party.
- **Enhance:** Use the information gathered from the Examine and Test phases to constantly enhance and improve the corporate security implementation and modify the security policy as new vulnerabilities and risks are identified and the business model changes.

It's much more effective to address security with a sound proactive strategy as opposed to a reactive and uncoordinated approach. A strategic methodology allows you to control security at the business level and at every area of vulnerability. This layers of security implementation provides a technique for each area of security in your business. Your security team can pick and choose which layers to concentrate on for your particular business needs. You can effectively prioritize specific areas for immediate action, and then easily add security mechanisms at any layer at any time as your business changes and your security assessment dictates.

3.4 LOGIN

Fingerprint Recognition Technology

Human fingerprints are unique to each person and can be regarded as a sort of signature, certifying the person's identity. Because no two fingerprints are exactly alike, the process of identifying a fingerprint involves comparing the ridges and impressions on one fingerprint to those of another.

This first involves capturing the likeness of the fingerprint, either through use of a fingerprint scanner (which takes a digital picture of a live fingerprint), scanning a pre-existing paper-based fingerprint image or by pulling what is known as a "latent fingerprint" from a crime scene or other place of investigation, from which a digital image is created.

Once the fingerprint image is captured, the process of identification involves the use of complex algorithms (mathematical equations) to compare the specific features of that fingerprint to the specific features of one or more fingerprint images that have been previously stored in a database.

The most famous application of fingerprint recognition technology is in criminology. However, nowadays, automatic fingerprint matching is becoming increasingly popular in systems which control access to physical locations (such as doors and entry gates), computer/network resources or bank accounts, or which register employee attendance time in enterprises.

Straightforward matching of the to-be-identified fingerprint pattern against many already known fingerprint patterns would not serve well, due to the high sensitivity to errors in capturing fingerprints (e.g. due to rough fingers, damaged fingerprint areas or the way a finger is placed on different areas of a fingerprint scanner window that can result in different orientation or deformation of the fingerprint during the scanning procedure). A more advanced solution to this problem is to extract features of so called minutiae points (points where the tiny ridges and capillary lines in a fingerprint have branches or ends) from the fingerprint image, and check matching between these sets of very specific fingerprint features.

The extraction and comparison of minutiae points requires sophisticated algorithms for reliable processing of the fingerprint image, which includes eliminating visual noise from the image, extracting minutiae and determining, rotation and translation of the fingerprint. At the same time, the algorithms must be as fast as possible for comfortable use in applications with a large number of users.

Many of these applications can run on a PC; however some applications require that the system be implemented on low cost, compact and/or mobile embedded devices such as doors, gates, handheld computers, cell phones etc.). For developers who intend to implement the fingerprint recognition algorithm into a microchip, compactness of algorithm and small size of required memory may also be important.

Mega Matcher technology is intended for large-scale AFIS and multi-biometric systems developers. The technology ensures high reliability and speed of biometric identification even when using large databases.

Mega Matcher is available as a software development kit that allows development of large-scale fingerprint, face or multi-biometric face-fingerprint and optionally iris identification products for Microsoft Windows and Linux platforms. Iris and palm print template extraction and matching engines are available as add-ons for the SDK.

- Proven in national-scale projects, including passport issuance and border control.
- NIST MINEX-compliant fingerprint engine.
- 200,000,000 irises or 100,000,000 fingerprints per second can be matched using MegaMatcher Accelerator.
- Fused face-fingerprint and optionally iris and/or palm print matching algorithm can be used for higher reliability.
- Rolled, flat and latent fingerprint matching.
- BioAPI 2.0 and other ANSI and ISO biometric standards support.
- Multiplatform, scalable cluster architecture for parallel matching.
- Effective price/performance ratio, flexible licensing and free customer support

Face Identification

Currently there are many methods of biometric identification: fingerprint, eye iris, retina, voice, face etc. Each of these methods has certain advantages and disadvantages which must be considered in developing biometric systems, such as: system reliability, price, flexibility, necessity of physical contact with the scanning device and many others. Selecting a certain biometric identification method or using a multi-biometric system can help to support these often discrepant requirements.

Face recognition can be an important alternative for selecting and developing an optimal biometric system. Its advantage is that it does not require physical contact with an image capture device (camera). A face identification system does not require any advanced hardware, as it can be used with existing image capture devices (webcams, security cameras etc.).

Thus, facial recognition should be considered as a serious alternative in the development of biometric or multi-biometric systems.

Facial Recognition Technology

Like fingerprint biometrics, facial recognition technology is widely used various systems, including physical access control and computer user accounts security.

Usually these systems extract certain features from face images and then perform face matching using these features. A face does not have as many uniquely measurable features as fingerprints and eye irises, so facial recognition reliability is slightly lower than these other biometric recognition methods. However, it is still suitable for many applications, especially when taking into account its convenience for user. Facial recognition can also be used together with fingerprint recognition or another biometric method for developing more security-critical applications.


The multi-biometric approach is especially important for identification (1-to-many) systems. In general, identification systems are very convenient to use because they do not require any additional security information (smart cards, passwords etc.). However, using 1-to-many matching routines with only one biometric method, can result in a higher false acceptance probability, which may become unacceptable for applications with large databases. Using face identification as an additional biometric method can dramatically decrease this effect.

This multi-biometric approach also helps in situations where a certain biometric feature is not optimal for certain groups of users. For example, people who do heavy labor with their hands may have rough fingerprints, which can increase the false rejection rate if fingerprint identification was used alone.

VeriEye SDK

VeriEye iris identification technology is intended for biometric systems developers and integrators. The technology includes many proprietary solutions that enable robust eye iris enrollment under various conditions and fast iris matching in 1-to-1 and 1-to-many modes.

VeriEye is available as a software development kit that allows development of PC- and Web-based solutions on Microsoft Windows, Linux and Mac OS X platforms.

- Rapid and accurate iris identification, proven by NIST IREX.
- Robust recognition, even with gazing-away eyes or narrowed eyelids.
- Original proprietary algorithm solves the limitations and drawbacks of existing state-of-the-art algorithms.
- Available as multiplatform  at supports multiple programming languages.
- Reasonable prices, flexible licensing and free customer support.

With **biometric login access security** from Misidentify Enterprise, only users assigned access privileges by system administrators can access corporate data. The resulting identity-based audit trail provides users and company management with secure knowledge of access events and associated system activity.

Return on Security

- Reduce Help Desk Calls Up To 40%
- Recurring Costs From Tokens Are Eliminated
- Longevity of Solution Components Ensures Long Lasting ROI
- Simplified Installation & Implementation
- Automatic Configuration of Input Technology & Communication

Access Control



- Privileges granted based on Absolute Biometric Identity
- Strengthens Audit Trail Via True Identity Access Events

- Risks of Internal Threats Minimized
- External Intrusion Opportunities Significantly Reduced
- High User Acceptance Through Increased Convenience
- Scalable single token solution to 20,000 users (more upon request)

3.5 FINGER PRINTING

The patterns of friction ridges and valleys on an individual's fingertips are unique to that individual. For decades, law enforcement has been classifying and determining identity by matching key points of ridge endings and bifurcations. Fingerprints are unique for each finger of a person including identical twins. One of the most commercially available biometric technologies, fingerprint recognition devices for desktop and laptop access are now widely available from many different vendors at a low cost. With these devices, users no longer need to type passwords – instead, only a touch provides instant access. Fingerprint systems can also be used in identification mode. Several states check fingerprints for new applicants to social services benefits to ensure recipients do not fraudulently obtain benefits under fake names. New York State has over 900,000 people enrolled in such a system.

It is the oldest and most popular physical technique used today. Fingerprinting takes an image (either using ink or a digital scan) of a person's fingertips and records its characteristics. The patterns are matched (ink) or encoded (digital) and then compared with other fingerprint records. Although the popularity of ink is still common, digital scanning is preferred. With digital scanning, a user presses his or her finger gently against a small optical or silicon reader surface where fingerprint information is taken from the digital scan and sent to a database for verification and identification comparison.



Fig. 4

Fingerprint Matching

Among all the biometric techniques, fingerprint-based identification is the oldest method which has been successfully used in numerous applications. Everyone is known to have unique, immutable fingerprints. A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending.

Fingerprint matching techniques can be placed into two categories: minutiae-based and correlation based. Minutiae-based techniques first find minutiae points and then map their relative placement on the finger. However, there are some difficulties when using this approach. It is difficult to extract the minutiae points accurately when the fingerprint is of low quality. Also this method does not take into account the global pattern of ridges and furrows. The correlation-based method is able to overcome some of the difficulties of the minutiae-based approach. However, it has some of its own shortcomings. Correlation-based techniques require the precise location of a registration point and are affected by image translation and rotation.

Fingerprint matching based on minutiae has problems in matching different sized (unregistered) minutiae patterns. Local ridge structures can not be completely characterized by minutiae. We are trying an alternate representation of fingerprints which will capture more local information and yield a fixed length code for the fingerprint. The matching will then hopefully become a relatively simple task of calculating the Euclidean distance will between the two codes.

We are developing algorithms which are more robust to noise in fingerprint images and deliver increased accuracy in real-time. A commercial fingerprint-based authentication system requires a very low False Reject Rate (FAR) for a given False Accept Rate (FAR). This is very difficult to achieve with any one technique. We are investigating methods to pool evidence from various matching techniques to increase the overall accuracy of the system. In a real application, the sensor, the acquisition system and the variation in performance of the system over time is very critical. We are also field testing our system on a limited number of users to evaluate the system performance over a period of time.

Fingerprint Classification

Large volumes of fingerprints are collected and stored everyday in a wide range of applications including forensics, access control, and driver license registration. An automatic recognition of people based on fingerprints requires that the input fingerprint be matched with a large number of fingerprints in a database (FBI database contains approximately 70 million fingerprints!). To reduce the search time and computational complexity, it is desirable to classify these fingerprints in an accurate and consistent manner so that the input fingerprint is required to be matched only with a subset of the fingerprints in the database.

Fingerprint classification is a technique to assign a fingerprint into one of the several pre-specified types already established in the literature which can provide an indexing mechanism. Fingerprint classification can be viewed as a coarse level matching of the fingerprints. An input fingerprint is first matched at a coarse level to one of the pre-specified types and then, at a finer level, it is compared to the subset of the database containing that type of fingerprints only. We have developed an algorithm to classify fingerprints into five classes, namely, whorl, right loop, left loop, arch, and tented arch. The algorithm separates the number of ridges present in four directions (0 degree, 45 degree, 90 degree, and 135 degree) by filtering the central part of a fingerprint with a bank of Gabor filters. This information is quantized to generate a Finger Code which is used for classification. Our classification is based on a two-stage classifier which uses a K-nearest neighbor classifier in the first stage and a set of neural networks in the second stage. The classifier is tested on 4,000 images in the NIST-4 database. For the five-class problem, classification accuracy of 90% is achieved. For the four-class problem (arch and tented arch combined into one class), we are able to achieve a classification accuracy of 94.8%. By incorporating a reject option, the classification accuracy can be increased to 96% for the five-class classification and to 97.8% for the four-class classification when 30.8% of the images are rejected.

Fingerprint Image Enhancement

A critical step in automatic fingerprint matching is to automatically and reliably extract minutiae from the input fingerprint images. However, the performance of a minutiae extraction algorithm relies heavily on the quality of the input fingerprint images. In order to ensure that the performance of an automatic fingerprint identification/verification system will be robust with respect to the quality of the fingerprint images, it is essential to incorporate a fingerprint enhancement algorithm in the minutiae extraction module. We have developed a fast fingerprint enhancement algorithm, which can adaptively improve the clarity of ridge and furrow structures of input fingerprint images based on the estimated local ridge

orientation and frequency. We have evaluated the performance of the image enhancement algorithm using the goodness index of the extracted minutiae and the accuracy of an online fingerprint verification system. Experimental results show that incorporating the enhancement algorithms improves both the goodness index and the verification accuracy.



Fig. 5

The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns. It is also necessary to know the structure and properties of human skin in order to successfully employ some of the imaging technologies.

The three basic patterns of fingerprint ridges are the arch, loop, and whorl. An arch is a pattern where the ridges enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger. The loop is a pattern where the ridges enter from one side of a finger, form a curve, and tend to exit from the same side they enter. In the whorl pattern, ridges form circularly around a central point on the finger. Scientists have found that family members often share the same general fingerprint patterns, leading to the belief that these patterns are inherited.

Minutia features

The major Minutia features of fingerprint ridges are: ridge ending, bifurcation, and short ridge (or dot). The ridge ending is the point at which a ridge terminates. Bifurcations are points at which a single ridge splits into two ridges. Short ridges (or dots) are ridges which are significantly shorter than the average ridge length on the fingerprint. Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical.

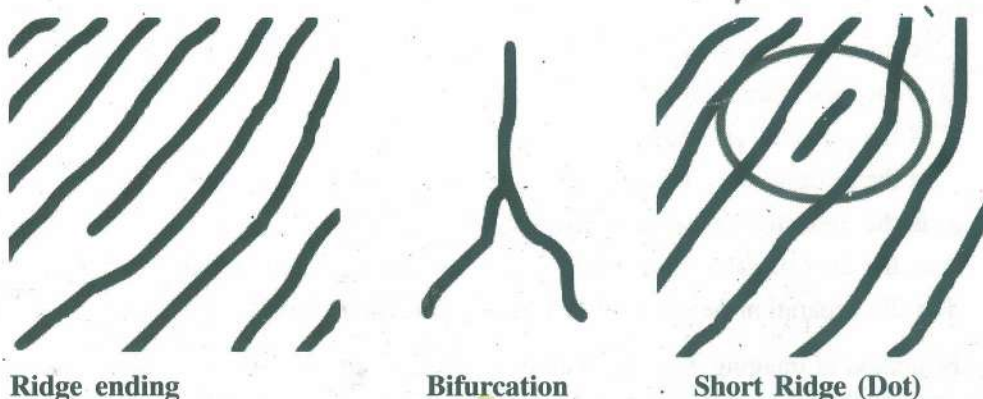


Fig. 6

Fingerprint Sensors

A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan. This live scan is

digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching. This is an overview of some of the more commonly used fingerprint sensor technologies.

Optical

Optical fingerprint imaging involves capturing a digital image of the print using visible light. This type of sensor is, in essence, a specialized digital camera. The top layer of the sensor, where the finger is placed, is known as the touch surface. Beneath this layer is a light-emitting phosphor layer which illuminates the surface of the finger. The light reflected from the finger passes through the phosphor layer to an array of solid state pixels (a charge-coupled device) which captures a visual image of the fingerprint. A scratched or dirty touch surface can cause a bad image of the fingerprint. A disadvantage of this type of sensor is the fact that the imaging capabilities are affected by the quality of skin on the finger. For instance, a dirty or marked finger is difficult to image properly. Also, it is possible for an individual to erode the outer layer of skin on the fingertips to the point where the fingerprint is no longer visible. It can also be easily fooled by an image of a fingerprint if not coupled with a "live finger" detector. However, unlike capacitive sensors, this sensor technology is not susceptible to electrostatic discharge damage.

Ultrasonic

Ultrasonic sensors make use of the principles of medical ultrasonography in order to create visual images of the fingerprint. Unlike optical imaging, ultrasonic sensors use very high frequency sound waves to penetrate the epidermal layer of skin. The sound waves are generated using piezoelectric transducers and reflected energy is also measured using piezoelectric materials. Since the dermal skin layer exhibits the same characteristic pattern of the fingerprint, the reflected wave measurements can be used to form an image of the fingerprint. This eliminates the need for clean, undamaged epidermal skin and a clean sensing surface.

Capacitance

Capacitance sensors utilize the principles associated with capacitance in order to form fingerprint images. The two equations used in this type of imaging are:

$$C = \frac{Q}{V}$$

$$C = \epsilon_0 \epsilon_r \frac{A}{d}$$

where

C is the capacitance in farads

Q is the charge in coulombs

V is the potential in volts

ϵ_0 is the permittivity of free space, measured in farads per metre

ϵ_r is the dielectric constant of the insulator used

A is the area of each plane electrode, measured in square metres

d is the separation between the electrodes, measured in metres

In this method of imaging, the sensor array pixels each act as one plate of a parallel-plate capacitor, the dermal layer (which is electrically conductive) acts as the other plate, and the non-conductive epidermal layer acts as a dielectric.

Passive Capacitance

A passive capacitance sensor uses the principle outlined above to form an image of the fingerprint patterns on the dermal layer of skin. Each sensor pixel is used to

measure the capacitance at that point of the array. The capacitance varies between the ridges and valleys of the fingerprint due to the fact that the volume between the dermal layer and sensing element in valleys contains an air gap. The dielectric constant of the epidermis and the area of the sensing element are known values. The measured capacitance values are then used to distinguish between fingerprint ridges and valleys.

Active Capacitance

Active capacitance sensors use a charging cycle to apply a voltage to the skin before measurement takes place. The application of voltage charges the effective capacitor. The electric field between the finger and sensor follows the pattern of the ridges in the dermal skin layer. On the discharge cycle, the voltage across the dermal layer and sensing element is compared against a reference voltage in order to calculate the capacitance. The distance values are then calculated mathematically, using the above equations, and used to form an image of the fingerprint. Active capacitance sensors measure the ridge patterns of the dermal layer like the ultrasonic method. Again, this eliminates the need for clean, undamaged epidermal skin and a clean sensing surface.

Algorithms

Matching algorithms are used to compare previously stored templates of fingerprints against candidate fingerprints for authentication purposes. In order to do this either the original image must be directly compared with the candidate image or certain features must be compared.

Pattern-based (or image-based) Algorithms

Pattern based algorithms compare the basic fingerprint pattern (loop, whorl, or arch) between a previously stored template and a candidate image. The images are aligned in the same orientation. To do this, a central point in the fingerprint image is found and centered on the template.

In a pattern-based algorithm, the template contains the basic pattern of patterns within the aligned fingerprint image. The candidate image is graphically compared with the template to determine a match.



Fingerprinting Examples

Casio Computer and Alps Electric have developed a small fingerprint scanner (Figure 7(a)) built into a short, thin cylinder for use in cellular telephones and other portable devices for use in Fall 2003. The cylinder, 0.2 inches in diameter and 0.6 inches long, contains a sensor, light, and lens. When users roll their fingers over the device, it can produce an 8-level monochrome fingerprint image at 600 dots per inch resolution.



(a)

(b)

Fig. 7

Hewlett-Packard (Figure 7 (b)) became the first manufacturer to add biometric identity checking to a mass-market consumer portable electronics device last year, when it built a small fingerprint scanner into its HP IPAQ H5450 PDA(Williams p1)

Check Your Progress 2

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) Explain Fingerprint authentication.

.....

.....

.....

.....

.....

2) How Biometric Login Procedures protect your system?

.....

.....

.....

.....

.....

3) Explain the role of Facial recognition in providing security.

.....

.....

.....

.....

.....

4) What are the disadvantages of Biometric Authentication procedures?

.....

.....

.....

.....

.....

3.6 LET US SUM UP

This unit covers the detailed descriptions of the biometrics in the Network Security. Here you know how the biometrics was implemented by applying different mechanisms. The common biometrics is Finger printing, Login, All physical security, Face recognition and iris recognition. The available biometrics is Fingerprint Recognition, Face Recognition, Iris Recognition, Voice Recognition, Smart Cards, Encryption Systems and Security Tokens and others. Biometrics consists of Summary of biometrics mechanisms and implementation.

3.7 CHECK YOUR PROGRESS: THE KEY

• Check Your Progress 1

- 1) Identity management is a discipline which encompasses all of the tasks required to create, manage, and delete user identities in a computing environment. Identity management begins with the creation of the user account and the assignment of appropriate attributes to the account. The user account is then provisioned into all of the systems to which that user is to be given access. Identity management tasks during the lifetime of the user account include: Adding or removing access to specific systems Password resets for lost passwords enforcing periodic password changes to increase network security.
- 2) A smart card usually contains an embedded microprocessor. The microprocessor is under a gold contact pad on one side of the card. The microprocessor on the smart card is there for security. The host computer and card reader actually "talk" to the microprocessor. The microprocessor enforces access to the data on the card. Smart cards can be used with a smart-card reader attachment to a personal computer to authenticate a user. Web browsers also can use smart card technology to supplement Secure Sockets Layer (SSL) for improved security of Internet transactions.
- 3) Iris recognition technology is used to identify individuals by photographing the iris of their eye. It falls under a category of technology known as biometric-based authentication, also called biometric security. Iris recognition technology works by combining computer vision, pattern recognition, and optics. First, a black-and-white video camera zooms in on the iris and records a sharp image of it. The iris is lit by a low-level light to aid the camera in focusing. A frame from this video is then digitized into a 512 byte file and stored on a computer database.

An individual's identity can then be confirmed by taking another picture of their iris and comparing it to the database. Iris recognition technology can confirm someone's identity within a few seconds

- 4) There are a number of advantages to biometric authentication. Biometric identification can provide extremely accurate, secured access to information; fingerprints, retinal and iris scans produce absolutely unique data sets when done properly. Current methods like password verification have many problems (people forget them, they make up easy-to-hack passwords). Automated biometric identification can be done very rapidly and uniformly. Another advantage of biometric authentication systems may be their speed. The authentication of a habituated user using an iris-based identification system may take 2 (or 3) seconds while finding your key ring, locating the right key and using it may take some 5 (or 10) seconds.

Check Your Progress 2

- 1) A biometric fingerprint reader records the impressions left by the patterns of the ridges of the finger pads of a human being. A fingerprint is entirely unique to a certain person. Thus it authenticates people and stores the imprints to be matched further whenever required therefore assuring of the safest and most trustworthy method of verification. Fingerprints are the tiny ridges, whorls and valley patterns on the tip of each finger. Digital scanners capture an image of the fingerprint. To create a digital fingerprint, a person places his or her finger on an optical or silicon reader surface and holds it there for a few seconds. The reader converts the information from the scan into digital data patterns. The computer then maps points on the fingerprints and uses those points to search for similar patterns in the database.

- 2) A login, logging in or logging on is the entering of identifier information into a system by a user in order to access that system (e.g., a computer or a website). It is an integral part of computer security procedures. A login generally requires the user to enter two pieces of information, first a user name and then a password. Biometric authentication is the identification of an individual on the basis of his or her unique biological or physiological characteristics such as facial features, fingerprints, hand geometry, retinal patterns and voiceprint.
- 3) A facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a facial database. An algorithm may analyze the relative position, size, and/or shape of the eyes, nose, cheekbones, and jaw. These features are then used to search for other images with matching features.
- 4) The Disadvantages of Biometrics are the following: In Finger print authentication, the finger print of those people working in Chemical industries are often affected. Therefore these companies should not use the finger print mode of authentication. In Speaker recognition technique, with age the voice of a person differs. Also when the person has flu or throat infection the voice changes or if there are too much noise in the environment this method may not authenticate correctly. In iris or retina authentication people affected with diabetes, their eyes get affected resulting in differences.

3.8 SUGGESTED READINGS

- www.biometricsintegrated.com/BiometricsServices
- www.bityard.com
- www.globalsecurity.org/security
- www.sean.co.uk > Articles
- www.springerlink.com/index/72480w3123681303.pdf

UNIT 4 SECURITY ISSUES IN WIRELESS AND NEXT GENERATION NETWORKS

Structure

- 4.0 Introduction
- 4.1 Objectives
- 4.2 Security Issues in Wireless
 - 4.2.1 Robustness
 - 4.2.2 Wireless Vulnerabilities and Incidents
- 4.3 Next Generation Networks
 - 4.3.1 Packet-Based Networks
 - 4.3.2 Human-Aided Networks
 - 4.3.3 Piracy-Driven Networks
 - 4.3.4 Mobile Networks or Cellular Networks
- 4.4 Let Us Sum Up
- 4.5 Check Your Progress: The Key
- 4.6 Suggested Readings

4.0 INTRODUCTION

Wireless networking technology is quickly changing the way networked computers communicate. The convenience offered by the ability to connect to networks using mobile computing devices has also introduced many security issues that do not exist in the wired world. The security measures we have relied on in the past to secure our networks are now obsolete with this new technology.

From a security standpoint, human involvement in a network adds an extra factor of security and complicates attacks since it is harder to attack a human-based point remotely, and physical attacks are harder to execute. Any WLAN client within the service area of an access point can access data being transmitted to or from the access point. Radio waves are not stopped by obstructions such as walls, ceilings or floors, thus the transmitted data may reach unintended recipients even outside the building where the access point is installed. Without stringent security measures in place, installing a WLAN can be equivalent to placing Ethernet ports on the outside of your building, accessible to anyone interested in plugging into your network. Stream ciphers such as WEP operate by expanding a relatively short key into an infinite pseudo-random key stream. This key stream is XORed with the plaintext of the data by the sender to generate the ciphertext. The recipient has a copy of the same key and uses it to generate an identical key stream. XORing this key stream with the ciphertext results in the original plaintext. This mode of operation makes stream ciphers vulnerable to several attacks. If an attacker flips a bit in the ciphertext, then upon decryption, the corresponding bit in the plaintext will be flipped. Also, if an eavesdropper intercepts two ciphertexts encrypted with the same key stream, it is possible to obtain the XOR of the two plaintexts.

Knowledge of this XOR can enable statistical attacks to recover the plaintexts. The statistical attacks become increasingly practical, as more ciphertexts that use the same key stream are known. Once one of the plaintexts becomes known, it is trivial to recover all of the others.

Next generation networks are important because they can provide us the way to expand the traffic of digital or the analog networking and also enhance the networking technologies. It is also important to make the old telecommunication technologies valuable and increase their reliability and also modernize them by increase their mobility

4.1 OBJECTIVES

After completion of this unit, you will be able to:

- know the various security issues in wireless networks; and
- next generation networks.

4.2 SECURITY ISSUES IN WIRELESS

The 802.11b standard includes a provision for encryption called Wired Equivalent Privacy. Depending on the manufacturer and the model of the NIC card and access point, there are two levels of WEP commonly available. one based on a 40-bit encryption key and 24-bit Initialization Vector (IV), also called 64-bit encryption and generally considered insecure, and a 104-bit key plus the 24-bit IV (so called 128 bit encryption).

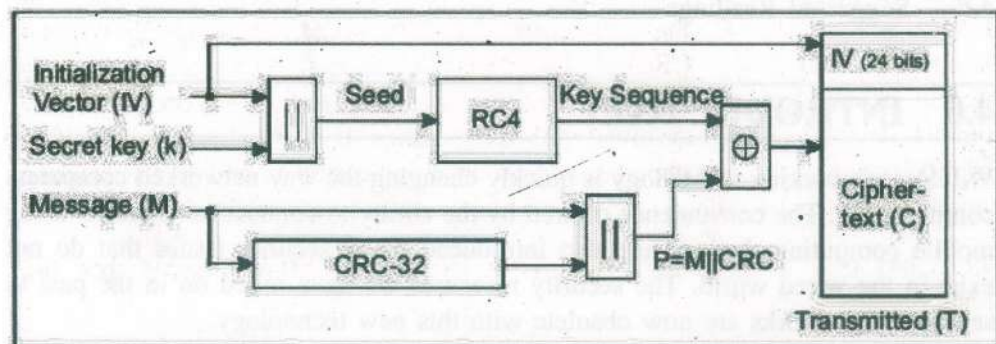


Fig. 1: WEP encryption

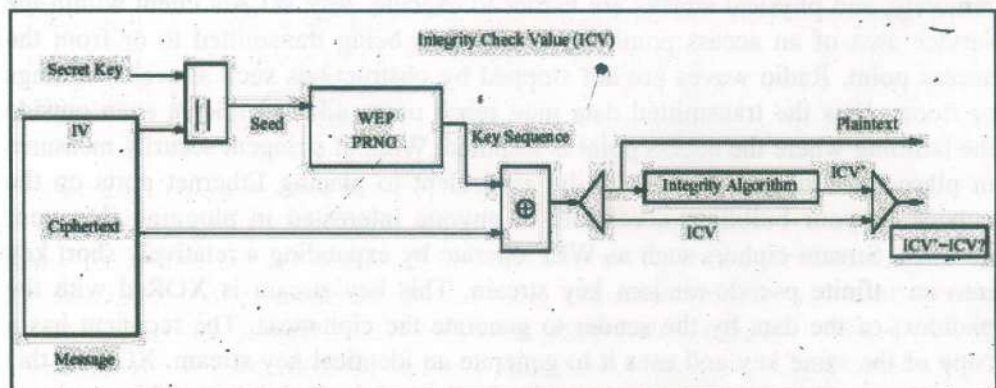


Fig. 2: WEP decryption

Figure 1 shows the encryption process in WEP. Two processes are applied to the plaintext data. One encrypts the plaintext using the RC4 algorithm; the other process protects it against unauthorized data modification using checksum (CRC). If an eavesdropper intercepts two cipher texts encrypted with the same key stream, it is possible to obtain the XOR of the two plaintexts, because the key disappears with the XORing of the cipher text.

If $C1 = P1 \oplus RC4$

and $C2 = P2 \oplus RC4$

then

$$C1 \oplus C2 = (P1 \oplus RC4) \oplus (P2 \oplus RC4) = P1 \oplus P2$$

Knowledge of this XOR can enable statistical attacks to recover the plaintexts. The statistical attacks become increasingly practical as more cipher texts, that use the same key stream, are known. Once one of the plain texts becomes known, it is trivial to recover all the others. WEP has defenses against this attack. To avoid encrypting two cipher texts with the same key stream, an Initialization Vector (IV) is used to augment the shared secret key and produce a different RC4 key for each packet, the IV is also included in the package (Figure 1). So the secret key (40 bits) is concatenated with the initialization vector (24 bits) resulting in a 64 bit total key size.

To ensure that a package has not been modified during transition, it uses an Integrity Check (CRC) field in the package. The integrity check field is implemented as a CRC-32 checksum, which is part of the encrypted payload of the package. This is because the key sequence is used to protect the integrity check value as well as the data. This results in encrypted bytes equal in length to the number of data bytes that are to be transmitted plus 4 bytes. In decryption, the IV of the incoming message is used to generate the key sequence necessary to decrypt the incoming message (Figure 2). The receiver has a copy of the same key, and uses it to generate an identical key stream; XORing the key stream with the cipher text yields the original plaintext and the ICV = CRC-32. The decryption is verified by performing the integrity check algorithm, CRC-32, on the recovered plaintext and comparing the output ICV' to the ICV transmitted with the message. If ICV' is not equal to ICV, the received message is tampered, and an error indication is sent to the sending station. Mobile units with erroneous messages are not authenticated.

There has been some interesting work to develop attacks exploiting the vulnerabilities in WEP.

Even though WEP has been shown to be basically insecure with its current implementation of static keys, the real problem is that the majority of access points are being deployed without WEP even being enabled. That's the equivalent to giving full access to your house to any stranger by keeping your doors open. WEP is vulnerable because of relatively short IVs and keys that remain static. The issues with WEP don't really have much to do with the RC4 encryption algorithm. With only 24 bits, WEP eventually uses the same IV for different data packets.

For a large busy network, this reoccurrence of IVs can happen within an hour or so. This results in the transmission of frames having keystreams that are too similar. If a hacker collects enough frames based on the same IV, the individual can determine the shared values among them, i.e., the keystream or the shared secret key. This leads to the hacker decrypting any of the 802.11 frames. The static nature of the shared secret keys emphasizes this problem. 802.11 doesn't provide any functions that support the exchange of keys among stations. As a result, system administrators and users generally use the same keys for weeks, months, and even years. This gives mischievous culprits plenty of time to monitor and hack into WEP-enabled networks.

WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is designed to work with all wireless network interface cards. WPA2 implements the full standard, but will not work with some older network cards. WPA is designed for use with an 802.1X authentication server, which distributes

different keys to each user; however, it can also be used in a less secure preshared key (PSK) mode, where every user is given the same passphrase. The Wi-Fi Alliance [4] calls the preshared key version WPA-Personal or WPA2-Personal and the 802.1X authentication version WPA-Enterprise or WPA2-Enterprise. Data is encrypted using the RC4 stream cipher, with a 128-bit key and a 48-bit initialization vector (IV). One major improvement in WPA over WEP is the Temporal Key Integrity Protocol (TKIP), which dynamically changes keys as the system is used. When combined with the much larger IV, this defeats the well-known key recovery attacks on WEP. In addition to authentication and encryption, WPA also provides vastly improved payload integrity. The cyclic redundancy check (CRC) used in WEP is inherently insecure; it is possible to alter the payload and update the message CRC without knowing the WEP key. An algorithm named Michael is used to provide more secure message authentication code (a MIC for Message Integrity Code) in WPA. The MIC used in WPA includes a frame counter, which prevents replay attacks being executed; this was another weakness in WEP. By increasing the size of the keys and IVs, reducing the number of packets sent with related keys, and adding a secure message verification system, WPA makes breaking into a Wireless LAN far more difficult. The Michael algorithm was the strongest that WPA designers could come up with that would still work with most older network cards; however it is subject to a packet forgery attack. It is possible to find the Temporal Key (TK) and the MIC key if a few RC4 keys in WPA are known. This is not a practical attack on WPA, but it shows that parts of WPA are weak on their own. To limit this risk, WPA networks shut down for 30 seconds whenever an attempted attack is detected. WPA2 is the certified form of IEEE 802.11i tested by the Wi-Fi Alliance. WPA2 implements the mandatory elements of 802.11i. In particular, the Michael algorithm is replaced by a message authentication code, CCMP, that is considered fully secure and RC4 is replaced by AES. WPA2 is officially supported in Microsoft Windows XP and on all AirPort Extreme-4 enabled Macintoshes.

Today, security problems plague the software products used to access the vast Internet, operating systems, WWW browsers and e-mail programs. These all have had their share of reported problems. Significant portions of these vulnerabilities are robustness problems caused by careless or misguided programming. The Internet's "underground community" searches for these flaws using non-systematic, ad-hoc methods, and then publishes their results for profit. The large number of reported problems from some software packages can be explained by the huge attention they have received, and also by the numerous flaws they contain. Security assessment of software by source code auditing is expensive and laborious. There are only a few methods for security analysis without access to the source code, and they are usually limited in scope. This may be one reason why many major software vendors have been stuck randomly fixing vulnerabilities that have been found and providing countless patches to their clients to keep the systems protected. This is also known as the "patch-and-penetrate race."

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. Wireless networks are very common, both for organizations and individuals. Many laptop computers have wireless cards pre-installed. The ability to enter a network while mobile has great benefits. However, wireless networking has many security issues. Crackers have found wireless networks relatively easy to break into, and even use wireless technology to crack into wired networks. As a result, it's very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources. Wireless Intrusion Prevention Systems (WIPS) or Wireless Intrusion Detection Systems (WIDS) are commonly used to enforce wireless security policies.

The risks to users of wireless technology have increased as the service has become more popular. There were relatively few dangers when wireless technology was first introduced. Crackers had not yet had time to latch on to the new technology

and wireless was not commonly found in the work place. However, there are a great number of security risks associated with the current wireless protocols and encryption methods, and in the carelessness and ignorance that exists at the user and corporate IT level. Cracking methods have become much more sophisticated and innovative with wireless. Cracking has also become much easier and more accessible with easy-to-use Windows or Linux-based tools being made available on the web at no charge.

Some organizations that have no wireless access points installed do not feel that they need to address wireless security concerns. In-Stat MDR and META Group have estimated that 95% of all corporate laptop computers that were planned to be purchased in 2005 were equipped with wireless. Issues can arise in a supposedly non-wireless organization when a wireless laptop is plugged into the corporate network. A cracker could sit out in the parking lot and gather info from it through laptops and/or other devices as handhelds, or even break in through this wireless card-equipped laptop and gain access to the wired network.

4.2.1 Robustness

Negative testing of communication protocols is called robustness testing or fuzzing. The robustness testing is based on the systematic creation of a very large number of protocol messages, from thousands to several million test cases, containing exceptional elements simulating malicious attacks. The method provides a low-cost pre-emptive way of assessing software robustness. Robustness indicates the extent to which software can tolerate exceptional input and stressful environmental conditions. A piece of software that is not robust fails when facing such circumstances. A malicious intruder can easily take advantage of robustness shortcomings and compromise the system running the piece of software. A large portion of information security vulnerabilities reported to the public is caused by robustness weaknesses. All robustness problems can be exploited by causing denial-of-service conditions by feeding the vulnerable component with maliciously formatted input. There are no false positives in robustness testing. A found failure is always a critical failure, such as a crash or a memory leak. Some of the mistakes are exploitable - an attacker can execute malicious code on the target system. An example is a buffer overflow type of robustness flaw that can almost always be exploited to run externally supplied code in the vulnerable component.

Robustness testing is one of the most effective black-box assessment technologies for security and reliability problems. All robustness tests presented in this paper have been conducted with the DEFENSICS product family, and can be repeated by third parties to verify the research results. To protect the reputation of the software companies, A disclose details of individual vulnerabilities, nor the names of any products tested in these assessments.

In this, we are on Bluetooth and Wi-Fi, with some preliminary information on WiMAX and other new wireless technologies. Each case is has an introduction, the test results and the threat evolution section, which includes an examination of the drivers behind the threats and security incidents. The threat evolution section for WiMAX is naturally forward-looking, drawing from the cellular, Wi-Fi and Bluetooth experiences, as little real-word data currently exists.

Based on the experiences with the cellular Bluetooth and Wi-Fi technologies, educated guesses can be made on emerging technologies, such as WiMAX, NFC and others. Some preliminary tests were run against the WiMAX base laboratories in order to compare the security with the more well-known technologies. WiMAX is an emerging wireless technology that was originally intended for solving the "last-mile" problem in the areas where wired connections were not desirable. This was the so-called "Fixed WiMAX". With the emergence of "Mobile WiMAX", carriers are looking at WiMAX as one of the technologies for delivering broadband

content for mobile users. WiMAX security is getting attention in public discussions. Currently, there are two schools of thought: one is expecting to see security issues similar to Wi-Fi and Bluetooth and the other believes that the threats are not severe, as security is built into WiMAX. It is important to note that most of the time when someone claims WiMAX is secure, they are referring to encryption and authentication, which were initially weak with Wi-Fi. Potential for the fuzzing type of attack, however, has received little attention.

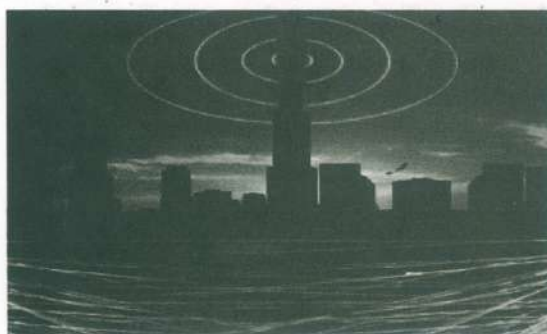


Fig. 3

At the time of testing, the over-the-air attack vector was unavailable, so the testing was conducted against the interfaces that were visible from the fixed network side. The following suspicious problems were found with the Wi-MAX equipment:

- Reboot of IPv4 stack in system under test that repeatedly caused state of denial of service when receiving large amount of abnormal IPv4 packets.
- Crash and reboot of system under test when receiving SunRPC request packet with length anomalies.
- Crash and reboot of system under test when receiving RPC request packet with overflow anomalies.

These defects are such that they could manifest themselves without being explicitly exploited. This means the resulting defects are receiving badly formatted network messages as part of normal operation. Furthermore, it appears that anyone able to access the device would be able to trigger some of the found issues. As a mitigating factor, it is noted that found issues are likely to be exploitable only if the user has the direct IP address to the base station's management interface or IP address. The testing conclusively proved that the software stack employed in Wi-MAX base stations is not free of the implementation-level errors anymore than those of the other wireless technologies.



wimax

Fig. 4

A comparison between Wi-Fi and Bluetooth has indicated that the complexity of the software stack gives indications about the amount of vulnerabilities. Even the very cursory testing of the well-established, higher-layer protocols of WiMAX have uncovered weaknesses. The MAC layer of 802.16e is fairly complex, settling somewhere between Wi-Fi and Bluetooth, but there is no reason to assume it will be free of the implementation-level vulnerabilities. As such, it will be susceptible to the fuzzing type of attacks.

It can be predicted that the MAC access will not be as readily available as it was for Bluetooth, but WiMAX is expected to make its way into laptops as well as mobile handsets. As Wi-Fi has shown, it will be only a matter of time before the open SDKs will be available for the general public. Looking at hacking from the motivation perspective, the mobile station side is likely to be as attractive a target as any consumer device.

Base station hacking might not be as commonplace, but the stakes are much higher. As a reminder, the base station can be a portal for an anonymous long-distance attack.

4.2.2 Wireless Vulnerabilities and Incidents

Wireless technology sometimes allows threats, attacks and vulnerabilities to enter the wireless space. Malicious people will exploit any known weaknesses through service attacks, worms, spam, malware and man-in-the-middle attacks. Wireless networks have three additional aspects that make the security of wireless networks even more challenging than the security of fixed networks as follows;

- Wireless networks are always open
- Attackers can connect into the network from anywhere and from any distance
- Attackers are always anonymous

Wireless networks are always open - Physical media does not protect them. Any device that implements the same radio interface can access a wireless network. One common assumption is that wireless technologies are secure when authentication and encryption are properly deployed. Looking closely at the operation of related protocols, there are many message sequences that take place before the authentication. These message sequences can always be attacked regardless of the deployed security measures. Attacks are not limited by location or distance. The distance from where the attacker can reach the wireless network is only limited by the power of the transmitter. For example, Bluetooth attack tools are known to have several-mile radiuses, although valid usage scenarios would never attempt such range of coverage for Bluetooth. Attackers are always anonymous. Although a valid user can be pinpointed with good accuracy, an attacker can use directed antennas that will only target a selected victim. It is impossible to guarantee detection of malicious users in wireless networks. After the analysis we observe that the threats have realized for these technologies with certain characteristics which as follows;

- Easy, low-cost access to technology
- Programmable environment, such as stack access in PC
- Motivation to hack

Check Your Progress 1

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) What is Wireless?

.....

.....

.....

.....

- 2) What are the different types of Wireless Technology?

.....

.....

.....

.....

.....

- 3) What is a Wi-Fi Security Key?

.....

.....

.....

.....

.....

- 4) What are the Different Types of Wi-Fi Networks?

.....

.....

.....

.....

.....

4.3 NEXT GENERATION NETWORKS

As this technology is the evolution of the different types of communication technologies so it has many important features that are really beneficial of the new technologies. Some of them are as follows;

It can able to transport all type of data such as voice communication, data transfer and also deals with different types of video technologies

- 1) As next generation network is the fusion technology so, it can provide high speed communication services related to networking.
- 2) This technology provide the generalized mobility to the old system and advance its working properties
- 3) As a number of protocols are involved in the working of the next generation networks so it can also provide interoperability where required.
- 4) It can provide different types of security features for the users to avoid the access of the restricted networking areas and prevent the whole networking system from unauthorized access.

● **Next Generation Networks Architecture**

Next generation networks are arranged in a very different manner as compared to other networking technologies. The particular architecture of the next generation networks based on the telephony in different steps such as different types of networking protocols are used to separate the different components of the telephony and all are treated then separately. The whole architecture of the next generation

networks are based on the different components, the main components are as follows; application servers, servers providing the media which are also called as circuits, the gateways of the media and the soft switch. These four components of the architecture deals with the whole next generation network architecture and also used to improvising the signaling properties of the servers.

● Components of Next Generation Networks

There are different components on which the working of the technology based. The most important component on which it is based is the internet. Some of the important components of internet on which next generation networks are based are given below:

- 1) Internet protocols
- 2) Session initiation protocols
- 3) Multi protocol

Other than the internet components it has also some other components such as softswitch, it is that type of component that is required to control or transport the voice calls related to the IP also called as VoIP. It is programmable and can operate easily. Another important component of the next generation networks is the gatekeeper, it is that type of device he is used to convert the analog or the digital signals into the data packets for transmission, it can also manage the working of all the gateways take part in the working.

New wireless technologies such as WiMAX, NFC and ZigBee are rapidly being adopted, along with existing wireless standards such as Bluetooth, Wi-Fi, GSM and other cellular technologies. Bluetooth and Wi-Fi have already become notorious for severe security shortcomings during their relatively brief existence. New vulnerabilities and exploits are reported and demonstrated every week on live public networks. The credibility of these wireless technologies has been damaged by security incidents, stemming from fundamental problems in requirement gathering, implementation quality and protocol design. Despite boasts of hardened security measures, security researchers and black-hat hackers keep humiliating vendors.

On the other hand, GSM and various descendant technologies have been almost 100 percent free of security incidents. What can be done to avoid making the same mistakes all over again with new emerging wireless technologies such as WiMAX? What is the anatomy and evolution behind security problems, and why have some cellular technologies been almost problem-free? This paper draws from the past and current state of existing wireless technologies and reflects experiences with emerging technologies.

It describes how robustness-testing techniques can be used to assess the security of the available implementations and give statistics about the current state of affairs of Bluetooth and Wi-Fi. Quality and reliability improvements in these implementations will lead directly to decreased development and deployment costs, as well as increased public acceptance and faster adoption.

When discussing the security of wireless technologies, there are several possible Perspectives. Different authentication, access control and encryption technologies all fall under the umbrella of security. Although relevant and important building blocks for overall security, these are not the focus of this paper. Instead, it will explore the problems at the implementation level of the current wireless access technologies and their real world implications. The problems are explored through one attack category, namely fuzzing, and the remediation through systematic robustness testing. This is because most security attacks do not exploit features in wireless technologies, but they abuse various implementation mistakes in the products.

4.3.1 Packet-Based Network

A software-controlled means of directing digitally encoded information in a communication network from a source to a destination, in which information messages may be divided into smaller entities called packets. Switching and transmission are the two basic functions that effect communication on demand from one point to another in a communication network, an interconnection of nodes by transmission facilities. Each node functions as a switch in addition to having potentially other nodal functions such as storage or processing.

Switched (or demand) communication can be classified under two main categories: circuit-switched communication and store-and-forward communication. Store-and-forward communication, in turn, has two principal categories: message-switched communication (message switching) and packet-switched communication (packet switching).

In circuit switching, an end-to-end path of a fixed bandwidth (or speed) is set up for the entire duration of a communication or call. The bandwidth in circuit switching may remain unused if no information is being transmitted during a call. In store-and-forward switching, the message, either as a whole or in parts, transits through the nodes of the network one node at a time. The entire message, or a part of it, is stored at each node and then forwarded to the next.

In message switching, the switched message retains its integrity as a whole message at each node during its passage through the network. For very long messages, this requires large buffers (or storage capacity) at each node. Also, the constraint of receiving the very last bit of the entire message before forwarding its first bit to the next node may result in unacceptable delays. Packet switching breaks a large message into fixed-size, small packets and then switches these packets through the network as if they were individual messages. This approach reduces the need for large nodal buffers and "pipelines" the resources of the network so that a number of nodes can be active at the same time in switching a long message, reducing significantly the transit delay. One important characteristic of packet switching is that network resources are consumed only when data are actually sent.

All public packet networks require that terminals and computers connecting to the network use a standard access protocol. Interconnection of one public packet network to others is carried out by using another standardized protocol.

Packet-switched networks using satellite or terrestrial radio as the transmission medium are known as packet satellite or packet radio networks, respectively. Such networks are especially suited for covering large areas for mobile stations, or for applications that benefit from the availability of information at several locations simultaneously.

Asynchronous transfer mode (ATM) is a type of packet switching that uses short, fixed-size packets (called cells) to transfer information. The ATM cell is 53 bytes long, containing a 5-byte header for the address of the destination, followed by a fixed 48-byte information field. The rather short packet size of ATM, compared to conventional packet switching, represents a compromise between the needs of data communication and those of voice and video communication, where small delays and low jitter are critical for most applications.

Data communication (or computer communication) has been the primary application for packet networks. Computer communication traffic characteristics are fundamentally different from those of voice traffic. Data traffic is usually *bursty*, lasting from several milliseconds to several minutes or hours. The holding time for data traffic is also widely different from one application to another. These characteristics of data communication make packet switching an ideal choice for

most applications. The principal motivation for ATM is to devise a unified transport mechanism for voice, still image, video, and data communication.

Next Generation Network refers in essence to the network architectural evolution over the next five to ten years. NGNs will be integrated, packet-based networks over phone, cable, satellite, or mobile networks that communicate converged multimedia information comprising voice, video, text, and other data. The shift from communication over analog telephone lines to a converged internet protocol (IP) backbone comprised of diverse network types means a shift from circuit-based voice to packet-based (multimedia) data. NGNs have support for generalized mobility and will provide for services including multimedia communication and messaging, video content distribution and streaming, interactive gaming, location-based services, mobile internet access and mobile TV. One of the possibilities provided by this seamless integration is the effortless porting between offline and online access to the network to the extent that the user is in fact oblivious to when he is connected. The user's device connects or disconnects from a network transparently, whenever necessary, and without any initiation by the user. This gives an increased sense of ubiquity in terms of the user's connection to the network via his personal devices.

● Cable

Television (TV) networks deliver TV broadcasts from TV stations to cable TV subscriber homes. Digital TV broadcasts using VHF and UHF frequencies between 47 MHz to 862 MHz. Each TV channel occupies 6 MHz bandwidth and modulated using 64/128/256 QAM before combines together with all other channels at the cable TV headend. Coaxial cables are used to deliver the TV RF signals to the subscriber homes.

In order for the cable TV network to delivery high speed data services, a set of cable network communication interface and operation support standards call DOCSIS (Data Over Cable Service Interface Standards) are developed by the cable industry. There are four version of DOCSIS; Versions 1.0, 1.1, 2.0 and 3.0. DOCSIS 1.0 enables cable TV operators to provide internet access up to 36 Mbps downstream over their HFC (Hybrid Fiber Coax) networks. Version 1.1 adds QoS (Quality of Service) capability to enable cable TV networks to deliver voice and streaming services (IP multicast). Version 2.0 enhanced the upstream speed (30 Mbps maximum) using 64 QAM modulation and 6.4 MHz upstream channel bandwidth to accommodate increase in demand of symmetric services (e.g. IP telephony). DOCSIS 3.0 significant increases the downstream speed (to 160 Mbps) and upstream speed (to 120Mbps) by bonding multiple upstream and downstream channels.

PacketCable is another cable industry standards developed to provide packet based voice, video and other high speed multimedia service over HFC cable systems. PacketCable is a set of protocols developed to deliver QoS enhanced communications services using packetized data transmission to a consumer's home over the cable network. PacketCable network architecture support toll quality VOIP (Voice over IP) services and allows connection of a plain analog phone using an Embedded Multimedia Terminal Adapter (EMTA). It supports primary and secondary residential voice line with battery backup capability. Packet Cable leverages QoS capability of DOCSIS 1.1/2.0 and will support SIP (Session Initiation Protocol) in version 2.0. While the initial service offerings for PacketCable product line are Packet Voice and Packet Video, the long term objective encompasses a large family of packet based services such as Virtual Private Network (VPN), real time interactive video sessions, multimedia telephony, interactive gaming and media streaming.

The two main components in DOCSIS are the Cable Modem (CM) in the subscriber premise and the Cable Modem Termination Systems (CMTS) in the cable operator

headend. DOCSIS specifies the physical and MAC layers communications interfaces between CM and CMTS. PacketCable networks use IP as the basis for robust multimedia architecture. PacketCable architecture supports end-to-end functions including signaling for services, media transport at variable QoS levels, security, provisioning of the client device, billing, and other network administration functions. PacketCable VOIP telephone service uses a managed IP network instead of the public internet to carry its voice traffic. PacketCable specifications for Voice over IP (VoIP) describe the basic functions that are typically consolidated onto a single Class 5 central office switch. These functions can be implemented across multiple elements or can be consolidated onto a single element, which leads to a low cost and highly flexible.

With the deployment of DOCSIS and PacketCable network architecture, cable operators can become full service providers of triple play of voice, data and multimedia services. Cable operators can also use their cable network to provide CableHome services such as remote control, management and diagnose of customer's home network (router, firewall, network address translation, secure software download, etc) and other devices

● **Satellite**

Internet access is Internet access provided through satellites. The service can be provided to users world-wide through Low Earth Orbit (LEO) satellites. Geostationary satellites can offer higher data speeds, but their signals can not reach some polar regions of the world. Different types of satellite systems have a wide range of different features and technical limitations, which can greatly affect their usefulness and performance in specific applications. Satellite internet customers range from individual home users with one PC to large remote business sites with several hundred PCs.

Home users tend to make use of shared satellite capacity, to reduce the cost, while still allowing high peak bit rates when congestion is absent. There are usually restrictive time based bandwidth allowances so that each user gets their fair share, according to their payment. When a user exceeds their Mbytes allowances, the company may slow down their access, deprioritise their traffic or charge for the excess bandwidth used. For consumer satellite internet, the allowance can typically range from 200 MB per day to 17,000 MB per month. A shared download carrier may have a bit rate of 1 to 40 Mbit/s and be shared by up to 100 to 4000 end users. Note that the average bit rate per end user PC is only about 10 - 20kbit/s.

The uplink direction for shared user customers is normally TDMA, which involves transmitting occasional short packet bursts in between other users (similar to how a cellphone shares a cell tower). Business users tend to opt for dedicated bandwidth services where any congestion is under their local control. Each remote location may also be equipped with a telephone modem; the connections for this are as with a conventional dial-up ISP. Two-way satellite systems may sometimes use the modem channel in both directions for data where latency is more important than bandwidth, reserving the satellite channel for download data where bandwidth is more important than latency, such as for file transfers.

A network technology that breaks up a message into small packets for transmission. Unlike circuit switching, which requires the establishment of a dedicated point-to-point connection, each packet in a packet-switched network contains a destination address. Thus, all packets in a single message do not have to travel the same path. As traffic conditions change, they can be dynamically routed via different paths in the network, and they can even arrive out of order. The destination computer reassembles the packets into their proper sequence. Network protocols such as IP and IPX were designed for packet-based networks.

Packet switching has always excelled at handling messages of different lengths, as well as different priorities, providing quality of service attributes were included. However, packet switching was designed for data. Today, using the IP protocol, packet networks are becoming the norm for voice and video as well.

X.25, Frame Relay and ATM

The first international standard for wide area packet switching networks was X.25, which was defined when all circuits were analog and very susceptible to noise. Subsequent technologies, such as frame relay, were designed for today's almost-error-free digital lines.

ATM uses a cell-switching technology that provides the bandwidth-sharing efficiency of packet switching with the guaranteed bandwidth of circuit switching

4.3.2 Human-Aided Networks

Human-Aided Computing, an approach that uses an electroencephalograph (EEG) device to measure the presence and outcomes of implicit cognitive processing, processing that users perform automatically and may not even be aware of. We describe a classification system and present results from two experiments as proof-of concept. Results from the first experiment showed that our system could classify whether a user was looking at an image of a face or not, even when the user was not explicitly trying to make this determination. Results from the second experiment extended this to animals and inanimate object categories as well, suggesting generality beyond face recognition. We later improve classification accuracies if we show images multiple times, potentially to multiple people, attaining well above 90% classification accuracies with even just ten presentations.

Computers have taken over the many human tasks due to their higher efficiency, effectiveness and better suitability for mundane procedures. Yet, their interaction with humans has remained, mostly where humans are the end-users, because computers typically replaced humans that were used for information processing. Clearly, this bears resemblance to the interaction between digital and analog counterparts. Indeed, as our physical world is analog and so no matter how much digital the information processing and communication becomes digital, at the other end the information needs to be converted back to analog signal form in order to be used in the "real world" again. Our thesis here is that just as many of nature's processes go in cycles, so too does the information processing world. To elaborate, networks are moving towards having digital entities interact with human users not just at the terminal points but throughout the process at different intermediate points.

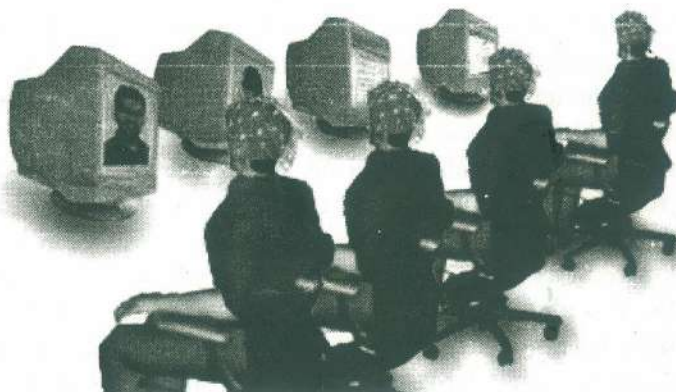


Fig. 5: multiple people connected to electroencephalograph devices, implicitly classifying images they see.

The reason is not that humans are becoming more efficient, but that there are so-called out-of-band tasks for which only humans are capable. The increasing involvement of humans at intermediate points is due to the development of two areas: ubiquity and security.

While ubiquity is a matter of fact, security-as a process- remains a delicate trade-off between privacy, cost, and usability. Human Involvement as a Consequence of Ubiquity. The wireless revolution and the reduction in size for devices has created a world of ubiquity where devices can be used anywhere with great mobility and ease. Because of the size reduction factor, embedded processor chips can be embedded into smart cards and radio frequency identification (RFID) tags, the smallest of which was recently developed by Hitachi that just measures 0.05×0.05 square millimetres. Also, the concept of wearable computer emphasizes the progressive reconciliation between people and machines. Ubiquity also warrants a single multiple-use device (also known as a smart device, e.g. iPhone) since a human user may not want to carry a different device for each separate application. This ubiquity leads to small devices interconnected with each other, and as an individual's collection of interconnected devices accumulates, this gives birth to personal area networks (PANs). The human user is in the middle of the PAN and is expected to interact with each device, sometimes even as simply as relaying information from one device to another. This is in contrast to the more conventional computer networks or the internet where no human intermediaries exist; the digital world is becoming more of a heterogeneous metanetwork. Increased Security Due to Human Intermediaries As more devices are interconnected, more points of remote attack exist for human adversaries who do not have direct physical access. Present day deployed network technologies and protocols, such as Bluetooth and certified wireless USB, now involve more human interaction and communication of authentication information via external human-aided channels that are harder to exploit without physical access; these are also so called out-of-band channels. Recent security results have caused people to start realizing that humans are an inevitable part of any communication protocol. Interaction with humans affects security, and so concepts like "out-of-band channels" and "ceremonies" are gaining popularity; humans now act as intermediaries or actively play a security-based role within networks.

The idea is to formally analyze the security of an entire communication protocol or system by including humans as one of the entities, rather than analyzing non-human components only while leaving out the human interaction as out of scope of the network protocol design. While humans are said to be the weakest link in a network, counter-intuitively we are returning to the humans to add extra factors for security, that is, having security based not just on public key infrastructure or passwords, but also on communicating information through real-world physical humanaided communication channels, such as voice, visual, etc.

The following figure shows an example of the response in one of our users with face and non-face stimuli. The response for face images, a strong N170 face-specific response is seen in the left image, data measured after a user has seen a face, but not in the right, in which they see non-faces. This is the purple line that protrudes out the bottom of the series at about 170 ms after stimulus presentation. In order to exploit this response and others like it, the system uses a time window that is 100-300ms following stimulus presentation from some set of EEG channels. The system utilizes a recently developed spatial projection algorithm designed for processing ERPs. This algorithm projects the response sequences from the multiple channels onto three maximally discriminative time series. We then use Regularized Linear Discriminant Analysis (RLDA), a supervised machine learning method, to classify the resulting features into mutually exclusive and exhaustive groups, namely the categories of interest. While we show in this paper that this technique works relatively well, implementing and testing other machine learning techniques for

such problems remains future work. Also, while we batch processed experimental results, the system is able to classify the signal in real-time once the model is built.

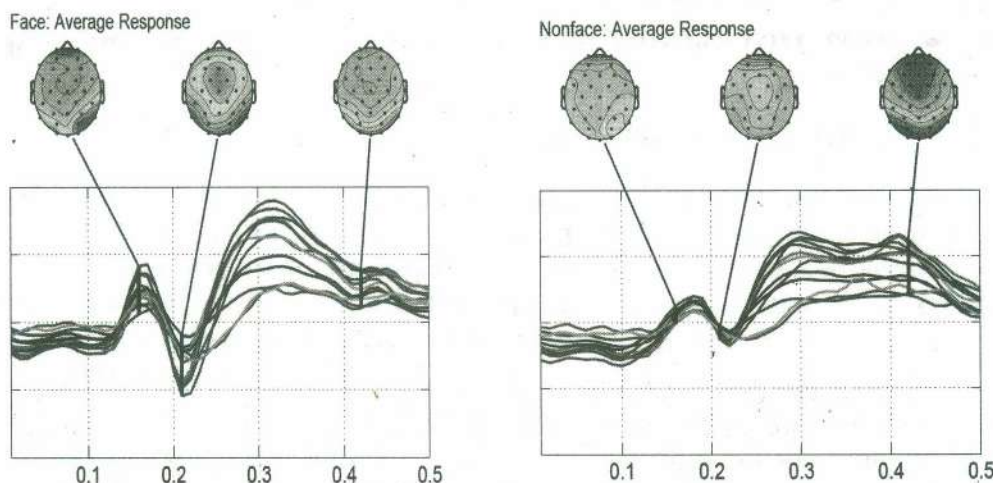


Fig. 6: Average ERP responses to viewing faces (left) and non-faces (right) for one user with the controlled images.

The wireless revolution and the reduction in size for devices has created a world of ubiquity where devices can be used anywhere with great mobility and ease. Because of the size reduction factor, embedded processor chips can be embedded into smart cards and radio frequency identification (RFID) tags, the smallest of which was recently developed by Hitachi that just measures 0.05×0.05 square millimetres. Also, the concept of wearable computer emphasizes the progressive reconciliation between people and machines. Ubiquity also warrants a single multiple-use device (also known as a smart device, e.g. iPhone) since a human user may not want to carry a different device for each separate application. This ubiquity leads to small devices interconnected with each other, and as an individual's collection of interconnected devices accumulates, this gives birth to personal area networks (PANs). The human user is in the middle of the PAN and is expected to interact with each device, sometimes even as simply as relaying information from one device to another. This is in contrast to the more conventional computer networks or the internet where no human intermediaries exist; the digital world is becoming more of a heterogeneous meta network.

Increased Security Due to Human Intermediaries As more devices are interconnected, more points of remote attack exist for human adversaries who do not have direct physical access. Present day deployed network technologies and protocols, such as Bluetooth and certified wireless USB, now involve more human interaction and communication of authentication information via external human-aided channels that are harder to exploit without physical access; these are also so called out-of-band channels. Recent security results have caused people to start realizing that humans are an inevitable part of any communication protocol. Interaction with humans affects security, and so concepts like "out-of-band channels" and "ceremonies" are gaining popularity; humans now act as intermediaries or actively play a security-based role within networks. The idea is to formally analyze the security of an entire communication protocol or system by including humans as one of the entities, rather than analyzing non-human components only while leaving out the human interaction as out of scope of the network protocol design. While humans are said to be the weakest link in a network, counter-intuitively we are returning to the humans to add extra factors for security, that is, having security based not just on public key infrastructure or passwords, but also on communicating information through real-world physical human aided communication channels, such as voice, visual, etc. From a security standpoint, human involvement in a network adds an extra factor of security and complicates attacks since it is harder to attack a human-

based point remotely, and physical attacks are harder to execute. Thus, we now cycle back through the network protocol evolution: starting with the state prior to the digital revolution where humans have major roles to play, through the decades of the digital era where human roles were replaced by machines, and now back to present day networks where we see again increasingly more human involvement as intermediaries.

4.3.3 Privacy-Driven Networks

Security of information has always preceded privacy of the human throughout the ages, even in ancient times when encryption was used by Julius Caesar. As information became easier to access in the digital era, the urgent need was to protect the information secrecy or at least control access to the information. The points along the information communication channel were commonly non-human while humans only existed at the end points. Thus the only important entity to protect along a communication channel was the information itself that was being communicated. Yet in this paper, we assert that the privacy requirement is catching up with, if not bypassing, its security counter part, due to two major developments: increasing human involvement and ubiquity.

Related to the previous subsection, increased human involvement at intermediate network points means that humans now also need to be protected against attacks. While the more conventional notions of information secrecy, integrity, authenticity basically correspond to security properties, privacy is recently also increasingly a concern since humans are now present along the network, at times forming human-intuitive physically-perceptible out-of-band channels. In particular, being involved at different points of a network should not cause the human to be traceable without his consent or knowledge. This leads to the issue of untraceable privacy.

Because the wireless revolution has led to ubiquitous devices, the threat to user's privacy has increased; it is indeed now easier to track his location and activities by tracking his mobile connected devices. Traditionally, devices like computers were non-mobile so that the most serious privacy issue was tied to the secrecy of the human information processed by the computer. Yet, today privacy includes assuring that the human is not being tracked as he uses his mobile devices since these devices are with him wherever he physically goes. Due to ubiquity, the devices are further pervasively connected and interconnected, often in a manner seamless and transparent to the user. The ubiquity of network devices is also partially influenced by the deployment of wireless sensors deployed for national security reasons. The world now has more diverse types of devices connected to networks, each potentially leaking information, that corresponds to a human privacy. Ubiquity is synonymous to omnipresence, thus the fact that connectivity is available anywhere at a certain point in time is in fact in direct contradiction to untraceable privacy. So, for NGNs where ubiquity is inherent, it is vital to analyze the impact on privacy and if possible, how it can still be offered in the face of ubiquity.

Here, We discuss here a general untraceable privacy (Priv) model that can be used to determine whether network protocols can safeguard protocol entities from being tracked. The model defined herein can be seen as in the same vein as the Bellare et al. models for authenticated key exchange (AKE) protocols, which can be regarded as one of the most commonly considered type of network security protocols. In fact, this model defined specifically for radio frequency identification devices (RFIDs) was used recently in to successfully analyze violations of privacy in recent RFID authentication schemes.

A protocol entity interacts in protocol sessions as per the protocol specifications until the end of the session upon which each party outputs Accept if it feels the protocol has been normally executed with the correct entities. Adversary A controls the communications between all protocol entities (U0, U1, etc.) by interacting

with them as defined by the protocol, formally captured by A's ability to issue queries of the following form:

- **Execute(U0,U1, i):** This query models passive attacks, where adversary A gets access to an honest execution of the protocol session i between $U0$ and $U1$ by eavesdropping.
- **Send(U0,U1, i,m):** This query models active attacks by allowing the adversary A to impersonate some entity $U0$ in some protocol session i and send a message m of its choice to an instance of some other entity $U1$.
- **Corrupt(U,K0):** This query allows the adversary A to learn the stored secret K of an entity U , and which further sets the stored secret to $K0$. It captures the notion of forward privacy and the extent of the damage caused by the compromise of U 's stored secret.
- **TestPriv(U, i):** This query is the only query that does not correspond to any of A's abilities or any real-world event. This query allows to define the indistinguishability based notion of untraceable privacy (Priv). If the party U has accepted and receives a TestPriv query, then depending on a randomly chosen bit $b \in \{0, 1\}$, A is given U_b from the set $\{U0,U1\}$. Informally, A succeeds if it can guess the bit b . In order for the notion to be meaningful, a Test session must be fresh in the sense of Definition 2.

4.3.4 Mobile Networks or Cellular Networks

Mobile Networks provides communication with learners beyond their traditional places of learning. It also supports face-to-face learning by reaching out to learners outside the traditional classroom. m-learning technologies deliver education at reduced costs by leveraging the relatively cheap mobile infrastructure. m-learning technology is an aid for the people who are suffering from a lack of interactivity. Many online classes simply provide recorded instructor lectures to which distance students listen after downloading. They have developed a cutting-edge mobile learning system that can deliver live broadcasts of real-time classroom teaching to online students with mobile devices. Their system allows students to customize their means of content-reception, based on when and where the students are tuning into the broadcast. This system also supports short text-messaging and instant polls. Through these features, students can ask questions and make suggestions in real time, and the instructor can respond immediately. Mobile devices have a strong appeal among young adults that helps to provide flexible learning opportunities regardless of the time or the location of learners. In this paper we show how it can be used to support ODL, using technologies such as context and location awareness, mobile learning management systems, and mobile RSS. We show how classroom learning can be supported with m-Learning technologies that deliver concise course notes, summaries, assignments, and tutorials directly to individual learners after each class or topic is covered. The technology supports opinions and other forms of student interaction and communicates information on timetables/schedules, deadlines, news, alerts, etc. to an entire class.

M-learning means learning through the use of mobile devices and is targeted at people who are always on the move. This kind of training can be given through mobile phones, PDA's and digital audio players and even digital cameras. M-learning' is the follow up of E-learning and which originates from D-learning. M-learning is the delivery of education to the students who are not having fixed location or who prefer to use mobile phone technology for learning. The rapid growth in the mobile and communication sector make it possible to develop new forms of education. M-learning means delivery of education by means of the mobile phone devices, PDAs and audio players. M-learners seek the lessons in the small format.

M-Learning or mobile learning is related to e-learning and distance education, learning with mobile devices. This learning is useful when the learner is not at a fixed or predetermined location. Mobile learning decreases limitation of learning location with the mobility of general portable devices. M-learning focuses on the mobility of the learner, interacting with portable technologies, and learning that reflects a focus on how society and its institutions can accommodate and support an increasingly mobile population. In this sharing is almost instantaneous among everyone using the same content, which leads to the reception of instant feedback and tips. M-Learning also brings strong portability by replacing books and notes with small RAMs, filled with prepared learning contents. The mobile phone (through text SMS notices) can be used especially for distance education or with students whose course requires them to be highly mobile and in particular to communicate information regarding availability of assignment results, venue changes and cancellations, etc. It can also be of value to business people. The use of mobile learning in the military is becoming increasingly common due to low cost and high portability.

Using portable computing devices (such as laptops, PDAs, smart phones, and tablet PCs) with wireless networks enables mobility and mobile learning. Mobility allows teaching and learning to extend to spaces beyond the traditional classroom. Within the classroom, mobile learning gives instructors and learners increased flexibility and new opportunities for interaction. Mobile technologies support learning experiences that are collaborative, accessible, and integrated with the world beyond the classroom

Mobile phones and their network vary very significantly from provider to provider and country to country. However the basic communication method of all of them is through the electromagnetic microwaves with a cell base station. The cellular companies have large antennas, which are usually mounted over towers, buildings and poles. The cell phones have low-power transceivers that transmit voice and data to the nearest sites usually within the 5 to 8 miles (8 to 13 kilometers away).

Current Mobile Phones can support many latest services such as SMS, GPRS, MMS, email, packet switching, WAP, Bluetooth and many more. Most of the mobile phones connect to the cellular networks and which are further connected with the PSTN (Public switching telephone network). Besides mobile communications, there is a wide range of mobile products available such mobile scanners, mobile printers and mobile labelers.

A **cellular network** is a radio network distributed over land areas called cells, each served by at least one fixed-location transceiver known as a cell site or base station. When joined together these cells provide radio coverage over a wide geographic area. This enables a large number of portable transceivers (e.g., mobile phones, pagers, etc.) to communicate with each other and with fixed transceivers and telephones anywhere in the network, via base stations, even if some of the transceivers are moving through more than one cell during transmission.

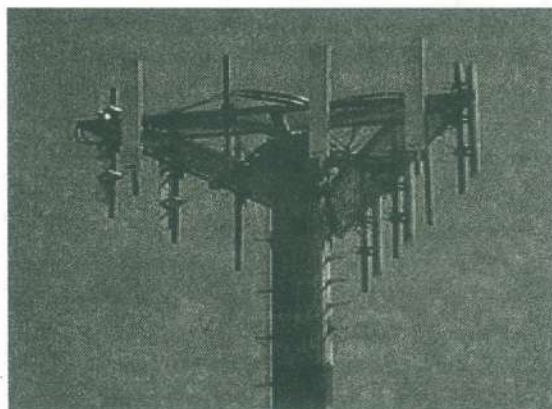


Fig. 7: Top of a cellular radio tower

Cellular networks offer a number of advantages over alternative solutions:

- increased capacity
- reduced power use
- larger coverage area
- reduced interference from other signals

An example of a simple non-telephone cellular system is an old taxi driver's radio system where the taxi company has several transmitters based around a city that can communicate directly with each taxi.

In a cellular radio system, a land area to be supplied with radio service is divided into regular shaped cells, which can be hexagonal, square, circular or some other irregular shapes, although hexagonal cells are conventional. Each of these cells is assigned multiple frequencies ($f_1 - f_6$) which have corresponding radio base stations. The group of frequencies can be reused in other cells, provided that the same frequencies are not reused in adjacent neighboring cells as that would cause co-channel interference.

The increased capacity in a cellular network, compared with a network with a single transmitter, comes from the fact that the same radio frequency can be reused in a different area for a completely different transmission. If there is a single plain transmitter, only one transmission can be used on any given frequency. Unfortunately, there is inevitably some level of interference from the signal from the other cells which use the same frequency. This means that, in a standard FDMA system, there must be at least a one cell gap between cells which reuse the same frequency.

In the simple case of the taxi company, each radio had a manually operated channel selector knob to tune to different frequencies. As the drivers moved around, they would change from channel to channel. The drivers know which frequency covers approximately what area. When they do not receive a signal from the transmitter, they will try other channels until they find one that works. The taxi drivers only speak one at a time, when invited by the base station operator.

Cell Signal Encoding

To distinguish signals from several different transmitters, frequency division multiple access (FDMA) and code division multiple access (CDMA) were developed.

With FDMA, the transmitting and receiving frequencies used in each cell are different from the frequencies used in each neighbouring cell. In a simple taxi system, the taxi driver manually tuned to a frequency of a chosen cell to obtain a strong signal and to avoid interference from signals from other cells.

The principle of CDMA is more complex, but achieves the same result; the distributed transceivers can select one cell and listen to it.

Other available methods of multiplexing such as polarization division multiple access (PDMA) and time division multiple access (TDMA) cannot be used to separate signals from one cell to the next since the effects of both vary with position and this would make signal separation practically impossible. Time division multiple access, however, is used in combination with either FDMA or CDMA in a number of systems to give multiple channels within the coverage area of a single cell.

Frequency Reuse

The key characteristic of a cellular network is the ability to re-use frequencies to increase both coverage and capacity. As described above, adjacent cells must utilize

different frequencies, however there is no problem with two cells sufficiently far apart operating on the same frequency. The elements that determine frequency reuse are the reuse distance and the reuse factor.

The reuse distance, D is calculated as

$$D = R\sqrt{3N},$$

where R is the cell radius and N is the number of cells per cluster. Cells may vary in radius in the ranges (1 km to 30 km). The boundaries of the cells can also overlap between adjacent cells and large cells can be divided into smaller cell.

The frequency reuse factor is the rate at which the same frequency can be used in the network. It is $1/K$ (or K according to some books) where K is the number of cells which cannot use the same frequencies for transmission. Common values for the frequency reuse factor are $1/3$, $1/4$, $1/7$, $1/9$ and $1/12$ (or 3, 4, 7, 9 and 12 depending on notation).

In case of N sector antennas on the same base station site, each with different direction, the base station site can serve N different sectors. N is typically 3. A reuse pattern of N/K denotes a further division in frequency among N sector antennas per site. Some current and historical **reuse patterns** are $3/7$ (North American AMPS), $6/4$ (Motorola NAMPS), and $3/4$ (GSM).

If the total available bandwidth is B , each cell can only utilize a number of frequency channels corresponding to a bandwidth of B/K , and each sector can use a bandwidth of B/NK .

Code Division Multiple Access - based systems use a wider frequency band to achieve the same rate of transmission as FDMA, but this is compensated for by the ability to use a frequency reuse factor of 1, for example using a reuse pattern of $1/1$. In other words, adjacent base station sites use the same frequencies, and the different base stations and users are separated by codes rather than frequencies. While N is shown as 1 in this example, that does not mean the CDMA cell has only one sector, but rather that the entire cell bandwidth is also available to each sector individually.

Directional Antennas

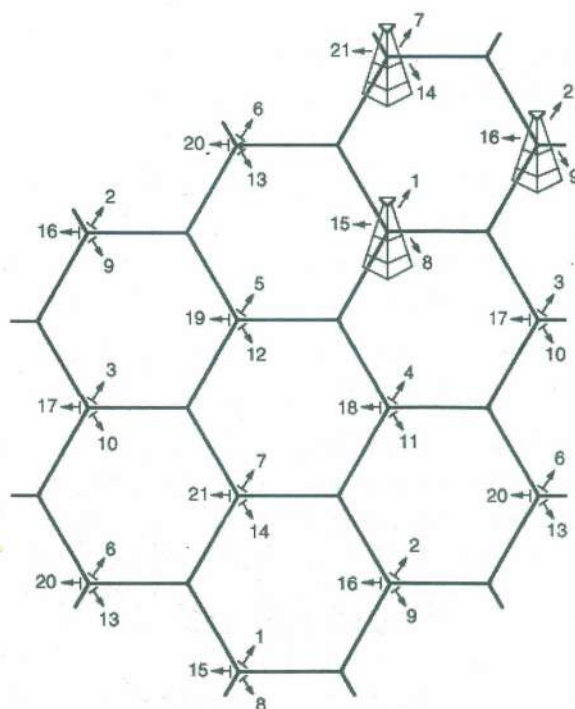


Fig. 8: Cellular telephone frequency reuse pattern.

Depending on the size of the city, a taxi system may not have any frequency-reuse in its own city, but certainly in other nearby cities, the same frequency can be used. In a big city, on the other hand, frequency-reuse could certainly be in use.

Recently also orthogonal frequency-division multiple access based systems such as LTE are being deployed with a frequency reuse of 1. Since such systems do not spread the signal across the frequency band, inter-cell radio resource management is important to coordinate resource allocation between different cell sites and to limit the inter-cell interference. There are various means of Inter-cell Interference Coordination (ICIC) already defined in the standard. Coordinated scheduling, multi-site MIMO or multi-site beam forming are other examples for inter-cell radio resource management that might be standardized in the future.

Although the original 2-way-radio cell towers were at the centers of the cells and were omni-directional, a cellular map can be redrawn with the cellular telephone towers located at the corners of the hexagons where three cells converge. Each tower has three sets of directional antennas aimed in three different directions with 120 degrees for each cell (totaling 360 degrees) and receiving/transmitting into three different cells at different frequencies. This provides a minimum of three channels (from three towers) for each cell. The numbers in the illustration are channel numbers, which repeat every 3 cells. Large cells can be subdivided into smaller cells for high volume area.

Broadcast Messages and Paging

Practically every cellular system has some kind of broadcast mechanism. This can be used directly for distributing information to multiple mobiles, commonly, for example in mobile telephony systems, the most important use of broadcast information is to set up channels for one to one communication between the mobile transceiver and the base station. This is called **paging**.

The details of the process of paging vary somewhat from network to network, but normally we know a limited number of cells where the phone is located. Paging takes place by sending the broadcast message to all of those cells. Paging messages can be used for information transfer. This happens in pagers, in CDMA systems for sending SMS messages, and in the UMTS system where it allows for low downlink latency in packet-based connections.

Movement from Cell to Cell and Handover

In a primitive taxi system, when the taxi moved away from a first tower and closer to a second tower, the taxi driver manually switched from one frequency to another as needed. If a communication was interrupted due to a loss of a signal, the taxi driver asked the base station operator to repeat the message on a different frequency.

In a cellular system, as the distributed mobile transceivers move from cell to cell during an ongoing continuous communication, switching from one cell frequency to a different cell frequency is done electronically without interruption and without a base station operator or manual switching. This is called the handover or handoff. Typically, a new channel is automatically selected for the mobile unit on the new base station which will serve it. The mobile unit then automatically switches from the current channel to the new channel and communication continues.

The exact details of the mobile system's move from one base station to the other varies considerably from system to system (see the example below for how a mobile phone network manages handover).

Example of a Cellular Network: the Mobile Phone Network

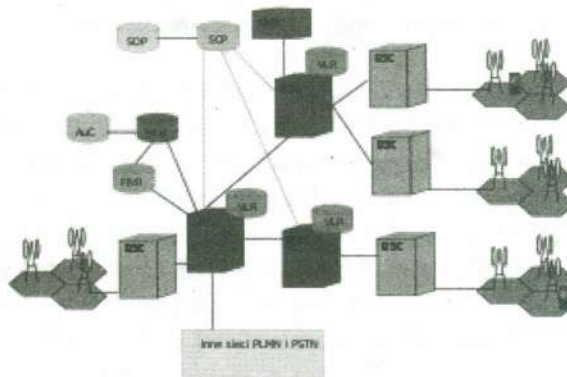


Fig. 9: GSM network architecture

The most common example of a cellular network is a mobile phone (cell phone) network. A mobile phone is a portable telephone which receives or makes calls through a cell site (base station), or transmitting tower. Radio waves are used to transfer signals to and from the cell phone.

Modern mobile phone networks use cells because radio frequencies are a limited, shared resource. Cell-sites and handsets change frequency under computer control and use low power transmitters so that a limited number of radio frequencies can be simultaneously used by many callers with less interference.

A cellular network is used by the mobile phone operator to achieve both coverage and capacity for their subscribers. Large geographic areas are split into smaller cells to avoid line-of-sight signal loss and to support a large number of active phones in that area. All of the cell sites are connected to telephone exchanges (or switches), which in turn connect to the public telephone network.

In cities, each cell site may have a range of up to approximately $\frac{1}{2}$ mile, while in rural areas, the range could be as much as 5 miles. It is possible that in clear open areas, a user may receive signals from a cell site 25 miles away.

Since almost all mobile phones use cellular technology, including GSM, CDMA, and AMPS (analog), the term "cell phone" is in some regions, notably the US, used interchangeably with "mobile phone". However, satellite phones are mobile phones that do not communicate directly with a ground-based cellular tower, but may do so indirectly by way of a satellite.

There are a number of different digital cellular technologies, including: Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), Code Division Multiple Access (CDMA), Evolution-Data Optimized (EV-DO), Enhanced Data Rates for GSM Evolution (EDGE), 3GSM, Digital Enhanced Cordless Telecommunications (DECT), Digital AMPS (IS-136/TDMA), and Integrated Digital Enhanced Network (iDEN).

Structure of the Mobile Phone Cellular Network

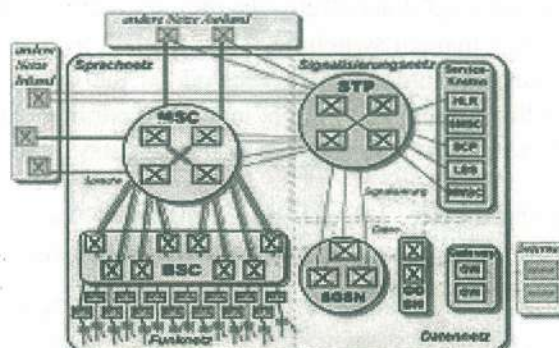


Fig. 10: Structure of the mobile phone cellular network

A simple view of the cellular mobile-radio network consists of the following:

- A network of Radio base stations forming the Base station subsystem.
- The core circuit switched network for handling voice calls and text
- A packet switched network for handling mobile data
- The Public switched telephone network to connect subscribers to the wider telephony network

This network is the foundation of the GSM system network. There are many functions that are performed by this network in order to make sure customers get the desired service including mobility management, registration, call set up, and handover.

Any phone connects to the network via an RBS in the corresponding cell which in turn connects to the MSC. The MSC allows the onward connection to the PSTN. The link from a phone to the RBS is called an uplink while the other way is termed downlink.

Radio channels effectively use the transmission medium through the use of the following multiplexing schemes: frequency division multiplex (FDM), time division multiplex (TDM), code division multiplex (CDM), and space division multiplex (SDM). Corresponding to these multiplexing schemes are the following access techniques: frequency division multiple access (FDMA), time division multiple access (TDMA), code division multiple access (CDMA), and space division multiple access (SDMA).

Cellular Handover in Mobile Phone Networks

As the phone user moves from one cell area to another cell whilst a call is in progress, the mobile station will search for a new channel to attach to in order not to drop the call. Once a new channel is found, the network will command the mobile unit to switch to the new channel and at the same time switch the on to the new channel.

With CDMA, multiple CDMA handsets share a specific radio channel. The signals are separated by using a pseudonoise code (PN code) specific to each phone. As the user moves from one cell to another, the handset sets up radio links with multiple cell sites (or sectors of the same site) simultaneously. This is known as "soft handoff" because, unlike with traditional cellular technology, there is no one defined point where the phone switches to the new cell.

In IS-95 inter-frequency handovers and older analog systems such as NMT it will typically be impossible to test the target channel directly while communicating. In this case other techniques have to be used such as pilot beacons in IS-95. This means that there is almost always a brief break in the communication while searching for the new channel followed by the risk of an unexpected return to the old channel.

If there is no ongoing communication or the communication can be interrupted, it is possible for the mobile unit to spontaneously move from one cell to another and then notify the base station with the strongest signal.

Cellular Frequency Choice in Mobile Phone Networks

The effect of frequency on cell coverage means that different frequencies serve better for different uses. Low frequencies, such as 450 MHz NMT, serve very well for countryside coverage. GSM 900 (900 MHz) is a suitable solution for light

urban coverage. GSM 1800 (1.8 GHz) starts to be limited by structural walls. UMTS, at 2.1 GHz is quite similar in coverage to GSM 1800.

Higher frequencies are a disadvantage when it comes to coverage, but it is a decided advantage when it comes to capacity. Pico cells, covering e.g. one floor of a building, become possible, and the same frequency can be used for cells which are practically neighbours.

Cell service area may also vary due to interference from transmitting systems, both within and around that cell. This is true especially in CDMA based systems. The receiver requires a certain signal-to-noise ratio. As the receiver moves away from the transmitter, the power transmitted is reduced. As the interference (noise) rises above the received power from the transmitter, and the power of the transmitter cannot be increased any more, the signal becomes corrupted and eventually unusable.

In CDMA-based systems, the effect of interference from other mobile transmitters in the same cell on coverage area is very marked and has a special name, cell breathing.

One can see examples of cell coverage by studying some of the coverage maps provided by real operators on their web sites. In certain cases they may mark the site of the transmitter, in others it can be calculated by working out the point of strongest coverage.

Coverage Comparison of Different Frequencies

Following table shows the dependency of frequency on coverage area of one cell of a CDMA2000 network:

Frequency (MHz)	Cell radius (km)	Cell area (km ²)	Relative Cell Count
450	48.9	7521	1
950	26.9	2269	3.3
1800	14.0	618	12.2
2100	12.0	449	16.2

Check Your Progress 2

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) What is a Next Generation Network?

.....

.....

.....

.....

2) What are the Features of Next Generation Networks?

.....

.....

.....

.....

- 3) List the Components of Next Generation Networks.

.....

.....

.....

.....

- 4) List the types of services offered by NGNs.

.....

.....

.....

.....

4.4 LET US SUM UP

To understand the threats posed by malicious fuzzing and how systematic robustness testing can pre-emptively eliminate the threats, we have collected results from three different use cases, namely Bluetooth, Wi-Fi and WiMAX. We have looked at the different characteristics of these technologies and how they affect the threat evolution. We have also briefly mentioned cellular technologies, which enjoyed immunity in the past, as well as some emerging new wireless technologies. We can continue to evaluate the security of the present and future wireless technologies to improve the ability to identify the vulnerable ones. This paper only gives basics for assessing whether the wireless technology an organization is about to deploy would be susceptible to a malicious fuzzing attack. Robustness testing has been found to be extremely cost-effective and a fast security assessment tool. On average, testing found problems in 90 percent of the devices tested. In light of the test results from WiMAX tests, there is no reason to believe that other WiMAX interfaces, including those used on the physical layer, would be any less free of bugs than the tested, classical IP-based interfaces tested in the WiMAX study. Using any available tools to verify and guarantee the robustness of 802.16d, 802.16e and the MAC layer is highly recommended when robustness testers will be available that is similar to what we currently have for Bluetooth and Wi-Fi.

4.5 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

- 1) For the purpose of this document, Wireless is defined as the means to move information from one computer, Person Digital Assistant (PDA) or SmartPhone to another by using radio waves instead of wires. The radio wave is modulated similar to Television and FM signals to carry information along with the wave. For computer, PDA or SmartPhone communication the distances will generally be short. For Mobile Broadband adapters (cellular) the distance will depend on the terrain and the number of cellular towers nearby.
- 2) There are many different types of wireless devices you use every day without giving it a second thought. Cell phones, cordless phones and remote controls for your TV are just a few everyday devices that use wireless technology. Wireless technology for computers, can be just as easy and carefree to use when setup correctly. For the rest of the document when referring to Wireless it's talking about wireless technology for computers.

Wireless technology for computers is divided into different types. Each type of wireless technology is covered in a different section. Each technology has its own uses, processes and standards. Below is a list of the different technologies with a brief explanation that will be covered.

- **Wireless Local Area Networking** - Referred to as WLAN or Wi-Fi. This type of wireless is used to get to the Internet and connect other devices such as computers, PDAs, SmartPhone and printers just to name a few.
 - **Bluetooth®**- Bluetooth technology is a short range wireless technology for connecting devices that are very close (30 feet or 10 meters). This technology is used to connect devices such as Bluetooth keyboards, mice, stereo headsets, PDA's and SmartPhone's. Many people already use this technology to connect wireless headset to cell phones.
 - **Mobile Broadband** - Also called Wireless Wide Area Networking (WWAN). Mobile Broadband uses cellular service to provide access to the Internet. Mobile Broadband technology is used in cell phones that can connect to the Internet. It requires a data enabled cellular service which is not available in all areas.
 - **Wireless USB** - This technology recently became available. It allows a wireless connection from a computer to a Wireless USB hub. USB devices are then connected to the Wireless USB hub and the hub acts as a bridge. The range is very short (10 feet / 3 meters).
- 3) A Wi-Fi security (network) key is very similar to a door key, it protects yourself from unknown people getting on your wireless network. Below is a list of the three types of wireless security offered for home and small business users as well as their strength in relation to the others.

It is recommended that the wireless network be configured with the highest level of security that the wireless devices have in common.

- **Wired Equivalent Privacy (WEP)**

Low protection

WEP is one of the original security types. Every home wireless router supports WEP even the latest models to make it compatible with every wireless network adapter. While WEP is better than no security the network key used to encrypt the wireless data can be broken in as little as a few minutes.

- **Wi-Fi Protected Access (WPA)-Medium protection**

WPA was developed to close the security holes that WEP has. It uses several mechanisms to prevent the network key from being broken but still uses the same encryption method as WEP.

- **Wi-Fi Protected Access 2 (WPA2)-Highest protection**

WPA2 has been implemented has the highest form of security for home and small businesses. It takes the mechanisms used by WPA and uses a more secure encryption method.

- 4) There are two basic types of networks they are called **Infrastructure** and **Ad-hoc**, the differences are discussed below.

- **Infrastructure**

An infrastructure network is one that has a centralized device that controls the network such as a wireless broadband router. The devices connected

to it transmit data to each other through the router. This will allow both wired and wireless devices to communicate with each other at the same time.

- **Ad-Hoc**

An Ad-Hoc network is the opposite of an Infrastructure network where there is no centralized device. The devices on the network communicate with each other directly and due to there being no centralized device can only support up to 10 devices on the network.

Check Your Progress 2

- 1) Networks using different technologies have been developed to carry different types of communication. For example, Public Switched Telephone Network (PSTN) carries voice calls. The PSTN is a traditional 'circuit-switched' network, in which data travels along a single path that is defined at the start of the call and reserved until it ends. By contrast, the Internet is a 'packet-based' network. Messages are split up into many packets that may travel along different routes and are reassembled when they reach their destination. The technology used to do this is known as Internet Protocol (IP). The fundamental idea of NGNs is to carry all types of service on a single packet-based network. This 'network convergence' allows operators to save money by having to maintain only one network platform, and to provide new services that combine different types of data. NGNs are more versatile than traditional networks because they do not have to be physically upgraded to support new types of service. The network simply transports data, while services are controlled by software on computers that can be located anywhere. This means that third parties can easily launch new services, not just the network operators themselves. NGNs are based on IP, like the Internet, but they build in features that the Internet does not have, such as the ability to guarantee a certain quality of service and level of security.
- 2) As this technology is the evolution of the different types of communication technologies so it has many important features that are really beneficial of the new technologies. Some of them are as follows:
 - i) It can able to transport all type of data such as voice communication, data transfer and also deals with different types of video technologies
 - ii) As next generation network is the fusion technology so, it can provide high speed communication services related to networking:
 - iii) This technology provide the generalized mobility to the old system and advance its working properties
 - iv) As a number of protocols are involved in the working of the next generation networks so it can also provide interoperability where required.
- 3) The most important component on which it is based is the internet. Some of the important components of internet on which next generation networks are based are given below
 - 1) internet protocols
 - 2) session initiation protocols
 - 3) Multi protocol

Other than the internet components it has also some other components such as softswitch, it is that type of component that is required to control or transport the voice calls related to the IP also called as VoIP. It is programmable and can operate easily. Another important component of the next generation

networks is the gatekeeper, it is that type of device he is used to covert the analog or the digital signals into the data packets for transmission, it can also manage e working of all the gateways take part in the working.

4) NGNs service types, includes:

- Specialized resource services (e.g., provision and management of transcoders, multimedia multipoint conferencing bridges, media conversion units, voice recognition units, etc.)
- Processing and storage services (e.g., provision and management of information storage units for messaging, file servers, terminal servers, OS platforms, etc.)
- Middleware services (e.g., naming, brokering, security, licensing, transactions, etc.)
- Application-specific services (e.g., business applications, e-Commerce applications, supply-chain management applications, interactive video games, etc.)
- Content provision services that provide or broker information content (e.g., electronic training, information push services, etc.)

4.6 SUGGESTED READINGS

- Arbaugh, William, Narendar Shankar and Justin Wan. "Your 802.11 Wireless Network Has No Clothes." March 30, 2001.
- URL: <http://www.cs.umd.edu/~waa/wireless.pdf> (December 17, 2002).
- Borisov, Nikita, Ian Goldberg and David Wagner. "Security of the WEP Algorithm." N/A
- URL: <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html> (December 17, 2002).
- Convery, Sea and Darrin Miller. "Wireless LAN Security in Depth." July 16, 2002.
- URL: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm (December 17, 2002).
- RSA Security. "What is RC4?." N/A
- URL: <http://www.rsasecurity.com/rsalabs/faq/3-6-3.html> (December 17, 2002).



Student Satisfaction Survey



Student Satisfaction Survey of IGNOU Students

Enrollment No.	
Mobile No.	
Name	
Programme of Study	
Year of Enrolment	
Age Group	<input type="checkbox"/> Below 30 <input type="checkbox"/> 31-40 <input type="checkbox"/> 41-50 <input type="checkbox"/> 51 and above
Gender	<input type="checkbox"/> Male <input type="checkbox"/> Female
Regional Centre	
States	
Study Center Code	

Please indicate how much you are satisfied or dissatisfied with the following statements

Sl. No.	Questions	Very Satisfied	Satisfied	Average	Dissatisfied	Very Dissatisfied
1.	Concepts are clearly explained in the printed learning material	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.	The learning materials were received in time	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.	Supplementary study materials (like video/audio) available	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.	Academic counselors explain the concepts clearly	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.	The counseling sessions were interactive	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.	Changes in the counseling schedule were communicated to you on time	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.	Examination procedures were clearly given to you	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.	Personnel in the study centers are helpful	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.	Academic counseling sessions are well organized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.	Studying the programme/course provide the knowledge of the subject	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.	Assignments are returned in time	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.	Feedbacks on the assignments helped in clarifying the concepts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13.	Project proposals are clearly marked and discussed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14.	Results and grade card of the examination were provided on time	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15.	Overall, I am satisfied with the programme	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
16.	Guidance from the programme coordinator and teachers from the school	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

After filling this questionnaire send it to:
Programme Coordinator, School of Vocational Education and Training,
Room no. 19, Block no. 1, IGNOU, Maidangarhi, New Delhi- 110068

IGNOU-STRIDE © All rights reserved 2009, ACIL

