Cyber Security Safeguards: Overview

Access control,

Audit,

Authentication,

Biometrics,

Cryptography,

Scanning,.

Security policy,

Threat management

Digital Forensics Science:

Need for Computer Cyber forensics and Digital Evidence,

Digital Forensics Life cycle

Forensics of social networking sites,

Handheld devices-mobile phones, smart phones, printers, scanners

basics of IPR with cyber security.

WHAT IS ACCESS CONTROL?

- ACCESS CONTROL – GRANTING OR DENYING APPROVAL TO USE SPECIFIC RESOURCES; IT IS CONTROLLING ACCESS

- *PHYSICAL ACCESS CONTROL* – FENCING, HARDWARE DOOR LOCKS, AND MANTRAPS THAT LIMIT CONTACT WITH *DEVICES*

- *TECHNICAL ACCESS CONTROL* – TECHNOLOGY RESTRICTIONS THAT LIMIT USERS ON COMPUTERS FROM ACCESSING *DATA*

INTRODUCTION

- USERS FIRST MUST BE IDENTIFIED AS AUTHORIZED USER, SUCH AS BY LOGGING IN WITH USER NAME AND PASSWORD TO LAPTOP COMPUTER
- BECAUSE LAPTOP CONNECTS TO CORPORATE NETWORK THAT CONTAINS CRITICAL DATA, IMPORTANT ALSO TO RESTRICT USER ACCESS TO ONLY SOFTWARE, HARDWARE, AND OTHER RESOURCES FOR WHICH USER HAS BEEN APPROVED
- THESE TWO ACTS—AUTHENTICATING ONLY APPROVED USERS AND CONTROLLING THEIR ACCESS TO RESOURCES—ARE IMPORTANT FOUNDATIONS IN INFORMATION SECURITY

ACCESS CONTROL TERMINOLOGY

- *IDENTIFICATION* – PRESENTING CREDENTIALS (EXAMPLE: DELIVERY DRIVER PRESENTING EMPLOYEE BADGE)
- *AUTHENTICATION* – CHECKING CREDENTIALS (EXAMPLE: EXAMINING THE DELIVERY DRIVER'S BADGE)
- *AUTHORIZATION* – GRANTING PERMISSION TO TAKE ACTION (EXAMPLE: ALLOWING DELIVERY DRIVER TO PICK UP PACKAGE)

Action	Description	Scenario example	Computer process
Identification	Review of credentials	Delivery person shows employee badge	User enters user name
Authentication	Validate credentials as genuine	Gabe reads badge to determine it is real	User provides password
Authorization	Permission granted for admittance	Gabe opens door to allow delivery person in	User authorized to log in
Access	Right given to access specific resources	Delivery person can only retrieve box by door	User allowed to access only specific data

TECHNICAL ACCESS CONTROL PROCESS

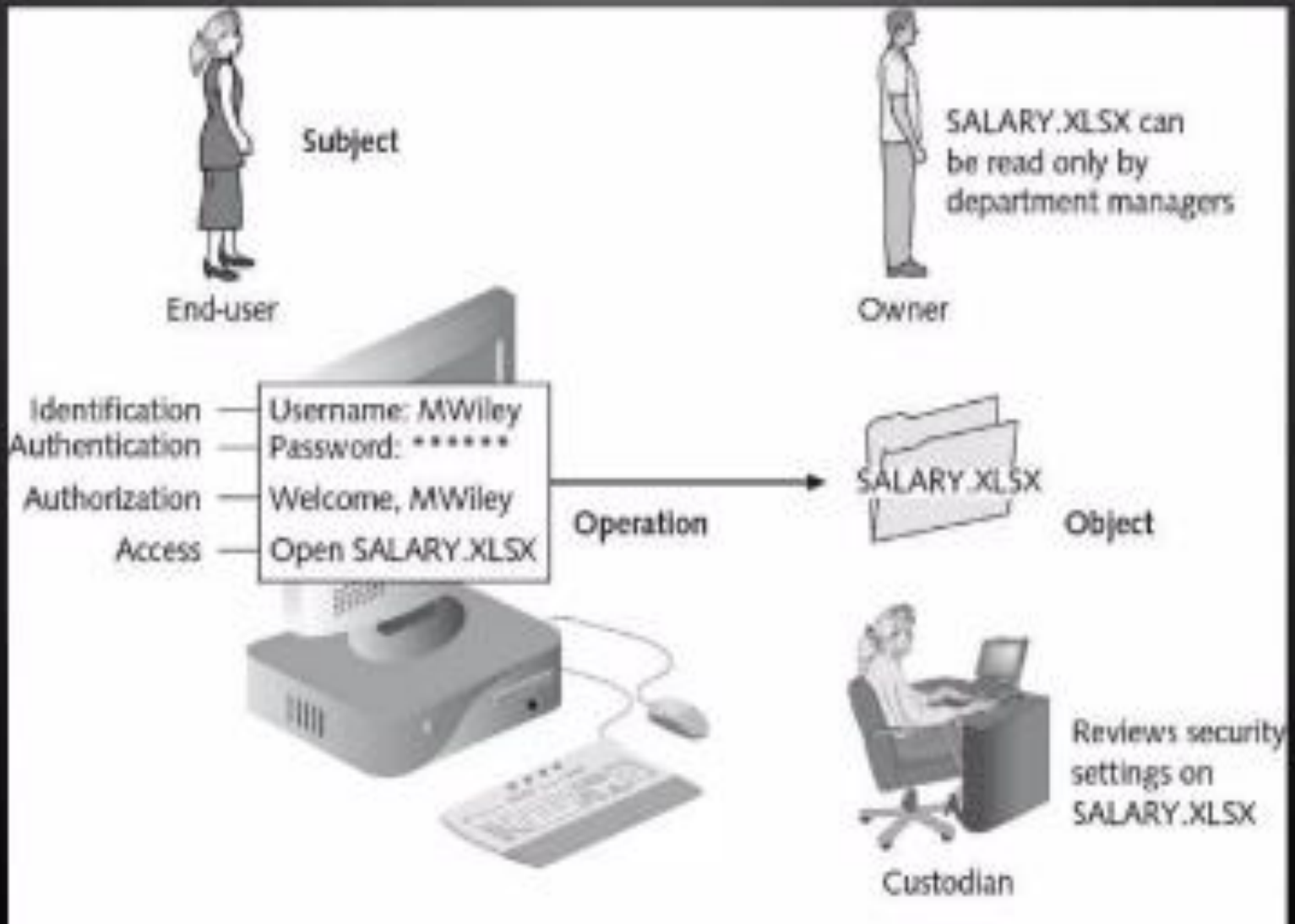


Figure 11-1 Technical access control process and terminology

ACCESS CONTROL MODELS

- ACCESS CONTROL MODEL – HARDWARE AND SOFTWARE PREDEFINED *FRAMEWORK* THAT CUSTODIAN CAN USE FOR CONTROLLING ACCESS
- ACCESS CONTROL MODELS USED BY CUSTODIANS FOR ACCESS CONTROL ARE NEITHER CREATED NOR INSTALLED BY CUSTODIANS OR USERS; INSTEAD, THESE MODELS ARE ALREADY PART OF SOFTWARE AND HARDWARE.
- ACCESS CONTROL MODELS
  - DAC – LEAST RESTRICTIVE MODEL
  - MAC – OPPOSITE OF DAC AND IS MOST RESTRICTIVE ACCESS CONTROL MODEL
  - UAC – USER/ADMIN LEVEL MODEL THAT NOTIFIES OR REQUIRES AUTHENTICATION PRIOR TO GRANTING ACCESS

discretionary access control

mandatory access control

User Account Control

DISCRETIONARY ACCESS CONTROL (DAC)

- DISCRETIONARY ACCESS CONTROL (DAC) – LEAST RESTRICTIVE MODEL
- EVERY OBJECT HAS OWNER, WHO HAS TOTAL CONTROL O THAT OBJECT
- OWNERS CAN CREATE AND ACCESS THEIR OBJECTS FREEL
- OWNER CAN GIVE PERMISSIONS TO OTHER SUBJECTS OVE THESE OBJECTS
- DAC USED ON OPERATING SYSTEMS LIKE UNIX AND MICROSOFT WINDOWS
- DAC HAS TWO SIGNIFICANT WEAKNESSES:
  - DAC RELIES ON DECISIONS BY END-USER TO SET PROPER LEVEL OF SECURITY; INCORR PERMISSIONS MIGHT BE GRANTED TO SUBJECT OR PERMISSIONS MIGHT BE GIVEN TO UNAUTHORIZED SUBJECT
  - SUBJECT'S PERMISSIONS WILL BE "INHERITED" BY ANY PROGRAMS THAT SUBJECT EXECUTES; ATTACKERS OFTEN TAKE ADVANTAGE OF THIS INHERITANCE BECAUSE END-USERS

Figure 11-2 Windows Discretionary Access Control (DAC)

MANDATORY ACCESS CONTROL (MAC)

- MANDATORY ACCESS CONTROL (MAC) – OPPOSITE OF DAC AND IS MOST RESTRICTIVE ACCESS CONTROL MODEL
- MAC ASSIGNS USERS' ACCESS CONTROLS STRICTLY ACCORDING TO CUSTODIAN'S DESIRES AND USER HAS NO FREEDOM TO SET ANY CONTROLS
- TWO KEY ELEMENTS TO MAC:
  - *LABELS* – EVERY ENTITY IS AN OBJECT (LAPTOPS, FILES, PROJECTS, AND SO ON) AND ASSIGNED CLASSIFICATION LABEL (*CONFIDENTIAL*, *SECRET*, AND *TOP SECRET*) WHILE SUBJECTS ASSIGNED PRIVILEGE LABEL (A *CLEARANCE*)
  - *LEVELS* – HIERARCHY BASED ON LABELS IS ALSO USED, BOTH FOR OBJECTS AND SUBJECTS (*TOP SECRET* HIGHER LEVEL THAN *SECRET*)

WINDOWS USER ACCOUNT CONTROL (UAC)

Figure 11-3 Windows User Account Control (UAC) prompt

Source: Microsoft Windows

ROLE BASED ACCESS CONTROL (RBAC)

- ROLE BASED ACCESS CONTROL (RBAC) – CONSIDERED MORE "REAL–WORLD" ACCESS CONTROL THAN OTHER MODELS BECAUSE ACCESS BASED ON USER'S JOB FUNCTION WITHIN ORGANIZATION
- INSTEAD OF SETTING PERMISSIONS FOR EACH USER OR GROUP ASSIGNS PERMISSIONS TO PARTICULAR ROLES IN ORGANIZATION AND THEN ASSIGNS USERS TO THOSE ROLES
- OBJECTS ARE SET TO BE A CERTAIN TYPE, TO WHICH SUBJECTS WITH THAT PARTICULAR ROLE HAVE ACCESS
- SUBJECTS MAY HAVE MULTIPLE ROLES ASSIGNED TO THEM

- RULE BASED ACCESS CONTROL (RBAC) – DYNAMICALLY ASSIGN ROLES TO SUBJECTS BASED ON SET OF RULES DEFINED BY CUSTODIAN
- EACH RESOURCE OBJECT CONTAINS SET OF ACCESS PROPERTIES BASED ON RULES
- WHEN USER ATTEMPTS TO ACCESS THAT RESOURCE, SYSTEM CHECKS RULES CONTAINED IN OBJECT TO DETERMINE IF ACCESS IS PERMISSIBLE

ACCESS CONTROL MODELS

Name	Restrictions	Description
Mandatory Access Control (MAC)	End-user cannot set controls	Most restrictive model
Discretionary Access Control (DAC)	Subject has total control over objects	Least restrictive model
Role Based Access Control (RBAC)	Assigns permissions to particular roles in the organization and then users are assigned to roles	Considered a more "real-world" approach
Rule Based Access Control (RBAC)	Dynamically assigns roles to subjects based on a set of rules defined by a custodian	Used for managing user access to one or more systems

Table 11-3 Access control models

BEST PRACTICES FOR ACCESS CONTROL

- ESTABLISHING BEST PRACTICES FOR LIMITING ACCESS CAN HELP SECURE SYSTEMS AND DATA

- A FEW BEST PRACTICES:
  - SEPARATION OF DUTIES – NOT TO GIVE ONE PERSON TOTAL CONTROL
  - JOB ROTATION – INDIVIDUALS PERIODICALLY MOVED BETWEEN JOB RESPONSIBILITIES
  - LEAST PRIVILEGE – LIMITING ACCESS TO INFORMATION BASED ON WHAT IS NEEDED TO PERFORM A JOB FUNCTION
  - IMPLICIT DENY – IF CONDITION IS NOT EXPLICITLY MET, ACCESS REQUEST IS REJECTED
  - MANDATORY VACATIONS – LIMITS FRAUD, BECAUSE PERPETRATOR MUST BE PRESENT DAILY TO HIDE FRAUDULENT ACTIONS

IMPLEMENTING ACCESS CONTROL

- NOW THAT WE HAVE DISCUSSED THE MODELS THAT CAN BE IMPLEMENTED IT IS TIME TO EXAMINE THE TECHNOLOGIES USED TO IMPLEMENT ACCESS CONTROL:
  - ACCESS CONTROL LISTS
  - GROUP POLICY
  - ACCOUNT RESTRICTIONS

ACCESS CONTROL LISTS (ACLS)

- ACCESS CONTROL LIST (ACL) – SET OF PERMISSIONS ATTACHED TO AN OBJECT
- SPECIFIES WHICH SUBJECTS MAY ACCESS THE OBJECT AN WHAT OPERATIONS THEY CAN PERFORM
- WHEN SUBJECT REQUESTS TO PERFORM AN OPERATION SYSTEM CHECKS ACL FOR AN APPROVED ENTRY
- ACLS USUALLY VIEWED IN RELATION TO OPERATING SYS FILES
- EACH ENTRY IN THE ACL TABLE IS CALLED ACCESS CONTROL ENTRY (ACE)
- ACE STRUCTURE (WINDOWS)
  - SECURITY IDENTIFIER FOR THE USER OR GROUP ACCOUNT OR LOGON SESSION
  - ACCESS MASK THAT SPECIFIES ACCESS RIGHTS CONTROLLED BY ACE
  - FLAG THAT INDICATES TYPE OF ACE

```
$ setfacl -m user:tdk:rw- samplefile
$ getacl samplefile
# file: samplefile
# owner: reo
# group: sysadmin
user::rw-user:
tdk:rw-              #effective:r--
group::r--           #effective:r--
mask:r--
other:r--
```

Figure 11-4 UNIX file permissions

ACCESS CONTROL LIST (ACLS): LIMITATIONS

- ALTHOUGH WIDELY USED, ACLS HAVE LIMITATIONS:
  - USING ACLS IS NOT EFFICIENT – ACL FOR EACH FILE, PROCESS, OR RESOURCE MUST BE CHECKED EVERY TIME THE RESOURCE IS ACCESSED.
  - CAN BE DIFFICULT TO MANAGE IN AN ENTERPRISE SETTING WHERE MANY USERS NEED TO HAVE DIFFERENT LEVELS OF ACCESS TO MANY DIFFERENT RESOURCES; SELECTIVELY ADDING, DELETING, AND CHANGING ACLS ON INDIVIDUAL FILES, OR EVEN GROUPS OF FILES, CAN BE TIME-CONSUMING AND OPEN TO ERRORS, PARTICULARLY IF CHANGES MUST BE MADE FREQUENTLY

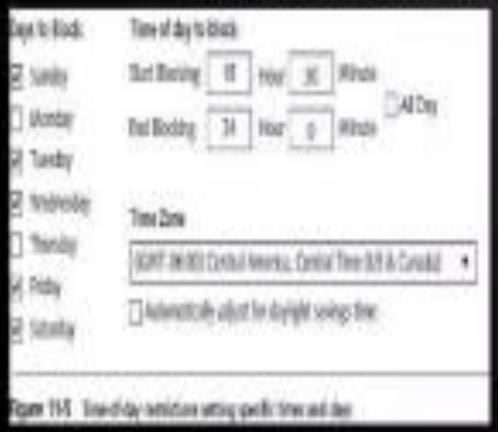
GROUP POLICIES

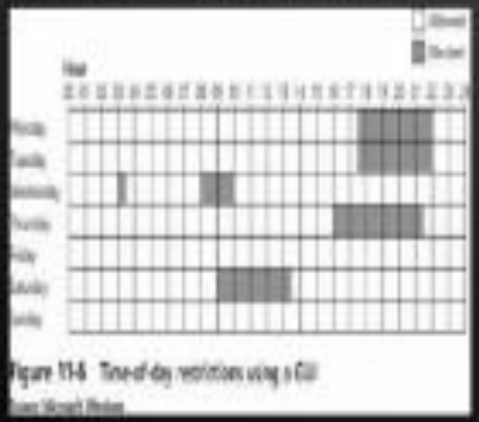
- GROUP POLICY – MICROSOFT WINDOWS FEATURE THAT PROVIDES CENTRALIZED MANAGEMENT AND CONFIGURATION OF COMPUTERS AND REMOTE USERS USING ACTIVE DIRECTORY (AD)
- USUALLY USED IN ENTERPRISE ENVIRONMENTS
- SETTINGS STORED IN *GROUP POLICY OBJECTS (GPOS)*
- *LOCAL GROUP POLICY* HAS FEWER OPTIONS THAN A GROUP POLICY AND USED TO CONFIGURE SETTINGS FOR SYSTEMS NOT PART OF AD

ACCOUNT RESTRICTIONS

TIME OF DAY RESTRICTIONS

- TIME OF DAY RESTRICTIONS – LIMITS THE TIME OF DAY A USER MAY LOG ONTO A SYSTEM
- TIME BLOCKS FOR PERMITTED ACCESS ARE CHOSEN
- CAN BE SET ON INDIVIDUAL SYSTEMS





ACCOUNT EXPIRATION RESTRICTIONS

- *ORPHANED ACCOUNTS* – ACCOUNTS THAT REMAIN ACTIVE AFTER EMPLOYEE HAS LEFT ORGANIZATION
- *DORMANT ACCOUNTS* – ACCOUNTS NOT ACCESSED FOR LENGTHY PERIOD OF TIME
- BOTH CAN BE SECURITY RISKS
- ACCOUNT EXPIRATION – PROCESS OF SETTING A USER'S ACCOUNT TO EXPIRE
- ACCOUNT EXPIRATION CAN BE EXPLICIT (ACCOUNT EXPIRES ON A SET DATE) OR BASED ON SPECIFIC NUMBER OF DAYS OF INACTIVITY

Security Audit

1- Security audit is an audit on the level of information security in an organization. Within the broad scope of auditing information security there are multiple types of audits, multiple objectives for different audits, etc. Most commonly the controls being audited can be categorized to technical, physical and administrative.

2- Auditing information security covers topics from auditing the physical security of data centers to auditing the logical security of databases and highlights key components to look for and different methods for auditing these areas.

Types Of Audits

1- External : These are conducted by a third party

2- Internal : Corporate : By headquarters

or

Personnel from other units of the same company.

3- Self : In –house – by the plant personnel themselves.

Audits Objectives

1- The main objective of the audit is to assess the adequacy and effectiveness of EC's security measures and management controls, through four specific objectives focusing on high-risk areas.

2- To assess the adequacy of the physical security threat identification and risk management process, with a focus on activities performed at the facility level.

3- To determine whether roles and responsibilities of all parties involved in departmental physical security are clearly defined, performed by the appropriate party, and cover the span of security activity, as defined by the TB Policy on Government Security;

Key Audit Questions

- Remember, audits are principally concerned with how security policies are actually implemented
- Key questions to be answered:
  - Are passwords difficult to crack?
    - Are they on post-it notes on the monitor or inside the desk's top drawer?
  - Are there access control lists (ACLs) in place on network devices to control who has access to shared data?
  - Are there audit logs to record who accesses data?
  - Are the audit logs reviewed?

Key Audit Questions (continued)

- Are the security settings for operating systems in accordance with accepted industry security practices?
- Have all unnecessary applications and computer services been eliminated for each system?
- Are these operating systems and commercial applications patched to current levels?
- How is backup media stored? Who has access to it? Is it up-to-date?
- Is there a disaster recovery plan? Have the participants and stakeholders ever rehearsed the disaster recovery plan?

Key Audit Questions (continued)

- Are there adequate cryptographic tools in place to govern data encryption, and have these tools been properly configured?
- Have custom-built applications been written with security in mind?
- How have these custom applications been tested for security flaws?
- How are configuration and code changes documented at every level? How are these records reviewed and who conducts the review?

Audit Checklists

- Audits are conducted by checklist
- Checklists are widely available but should be tailored for each audit by the audit team
- Checklists may be challenge-response (i.e. check-in-the-box or yes-or-no answers) or they may be scale rankings (1-4, 1-5, 1-10, etc.)

Sample Audit Checklist

General IT Controls
Audit Program
Purpose / Scope
Perform a General Controls review of Information Technology (IT). The reviews will include all IT related policies, procedures, data security administration, data center operations, system development / maintenance, the IT Disaster / Recovery plan and its relation to the corporate Business Continuity plan.

Audit steps	Date	Initials	W/P Ref.

IT General Controls

Planning

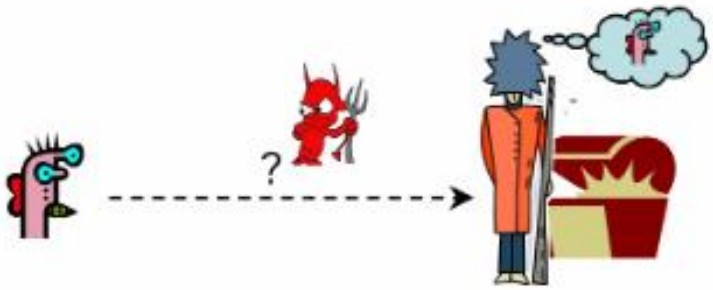
Determine if committees review, approve, and report to the board on:
Short and long term information systems plans
IT operating standards
Data security policies and procedures
Resource allocation (major hardware/software acquisition and project priorities)
Status of major projects
IT budgets and current operating cost

Policies, Standards, and Procedures

Determine whether the board of directors has reviewed and approved IT policies.

Examine how IT management has defined standards and adopted a methodology governing the process of developing, acquiring, implementing, and maintaining information systems and related technology.
Determine if IT management has adequate standards and procedures for:
Systems development
Program change control
Data Center operations
Data Base administration
DASD management
Performance monitoring

Authentication



How do you prove to someone that you are who you claim to be?

Any system with access control must solve this problem

Authentication

- Authentication can be defined as determining an identity to the required level of assurance
- Authentication is the first step in any cryptographic solution
  - Because unless we know who is communicating, there is no point in encryption what is being communicated

•Authentication may be implemented using Credentials, each of which is composed of a User ID and Password. Alternately, Authentication may be implemented with Smart Cards, an Authentication Server or even a Public Key Infrastructure

Many Ways to Prove Who You Are

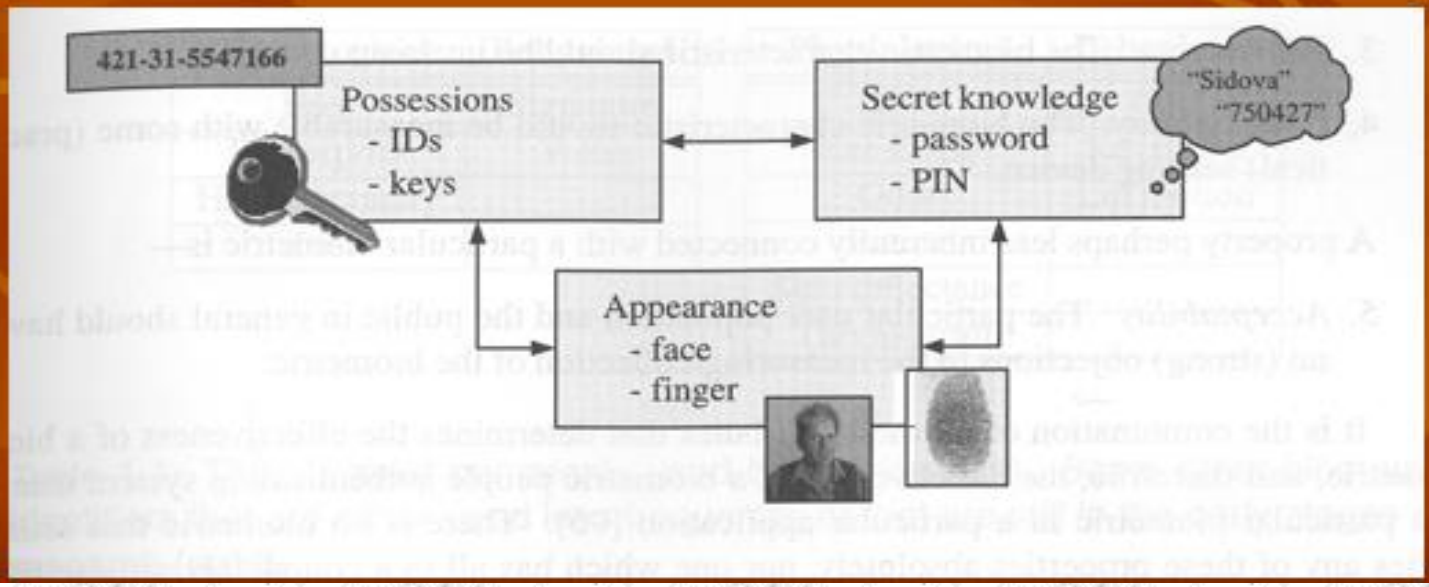
- What you know
  - Passwords/Secret key
- Where you are
  - IP address
- What you are
  - Biometrics (e.g. fingerprint)
- What you have
  - Secure tokens/smart card/ ATM card

Authentication

- There are 3 traditional way of verifying the identity of a person:
  - Possessions (keys, passports, smartcards , …)
  - Knowledge
    - Secret (passwords, pass phrases, …)
    - Non-secret (user Id, mothers maiden name, favorite color)
  - Biometrics
    - Physiological (fingerprints, face, iris, …)
    - Behavioral (walking, keystroke pattern, talking, …)

Authentication

- The 3 modes of authentication are sometimes combined
  - User id + password
  - ATM card + password
  - Passport + face picture and signiture



Biometrics

What is Biometrics?

- Automated method for recognizing individuals based on measurable biological and behavioral characteristics

Finger Print Recognition

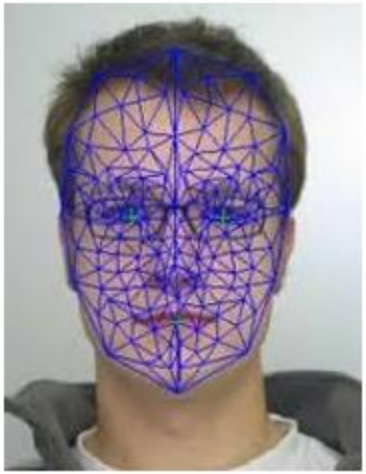
- Minutiae
- Pattern Matching
- Problems: sometimes unusable

Vascular Pattern Matching

- LED infrared light
- Fingers and back of hand
- Not completely viable

Facial Recognition

- Location and position of facial features
- Dependent on background and lighting conditions

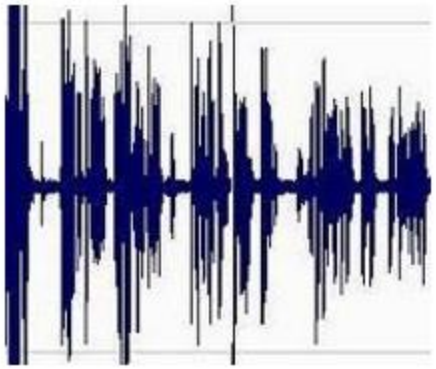


Hand Geometry

- Scan both sides of hand
- Primarily used for verification
- Not as accurate as other methods

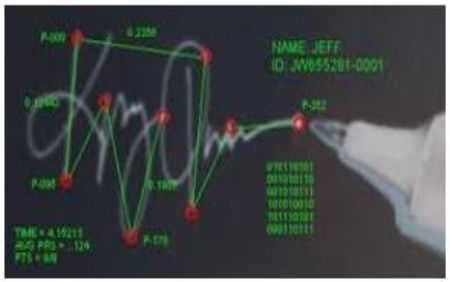
Voice Verification

- Factors: pitch, intensity, quality and duration
- Text dependent
- Text independent
- Problems: include background noise



Dynamic Signature

- Factors: velocity, acceleration and speed
- Mainly used for verification
- Problems: forgers could reproduce



Retina Recognition

- One of the most secure means of biometrics
- Unique to each person
- Unique to each eye
- Problems: require effort on the part of subjects

Other Types

- Keystroke
- Gait
- DNA
- Odor

Commercial Applications

- Computer login
- Electronic Payment
- ATMs
- Record Protection

Government Applications

- Passport control
- Border control
- Access Control

Forensic Applications

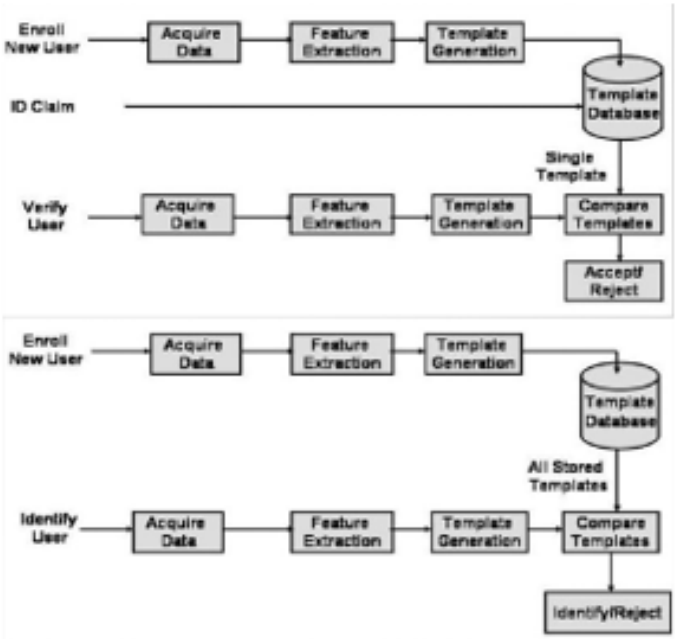
- Missing Persons
- Corpse identification
- Criminal investigations

Constraints on Biometrics

- Typical "Constrained" Image
- Constraints:
  - Lighting
  - Distance
  - Pose
  - Expression
  - Time Lapse
  - Occlusion

Type of Authentication

- Authentication
  - 1:1
- Verification
  - 1:N



Cyber Security and Biometrics

Authentication

There are two different authentication methods in biometrics

- ***Verification***: Is he/she the person who claims he/she is? Works with id + biometrics. Thus it is based on a combination of modes.

- ***Identification***: Who is this person? Uses only the biometrics and searches the entire database.

Overview of Biometric Systems

There are five important properties of biometric identifiers:

1. Universality
2. Uniqueness
3. Permanence
4. Collectability
5. Acceptability

Overview of Biometric Systems

Biometric Identifiers

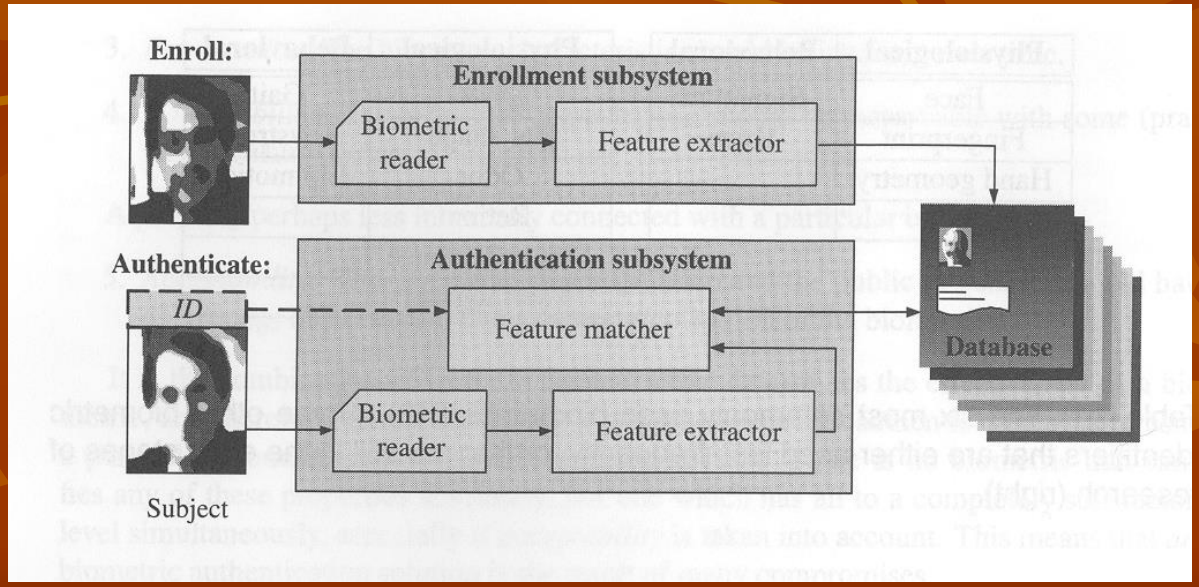
Physiological	Behavioral
Face	Signature
Fingerprint	Voice
Hand geometry	
Iris	

Physiological	Behavioral
DNA	Gait
Ear shape	Keystroke
Odor	Lip motion
Retina	
Skin reflectance	
Thermogram	

Overview of Biometric Systems

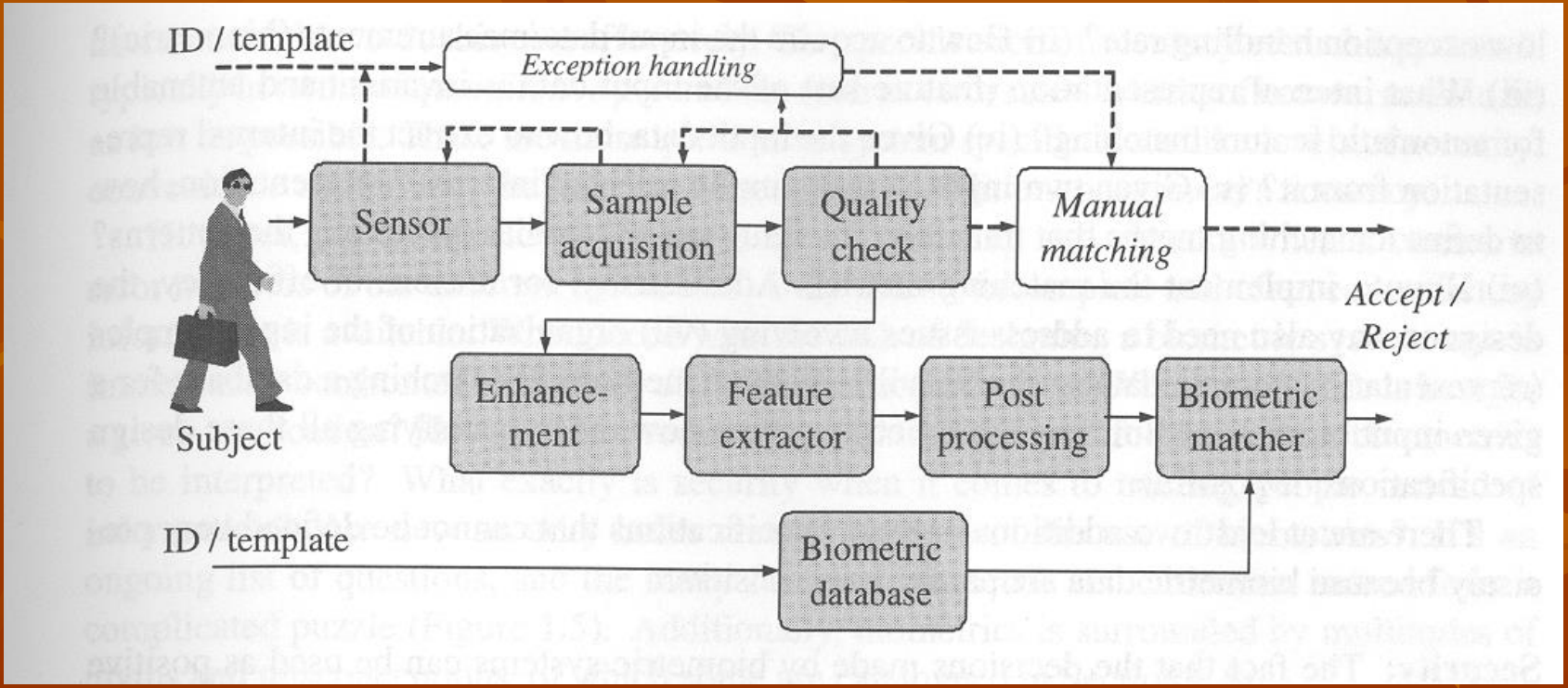
Biometric Subsystems

- Biometric readers (sensors)
- Feature extractors
- Feature Matchers



Overview of Biometric Systems

A generalized diagram of a biometric system is as follows:



Overview of Biometric Systems

Design Issues:

4 basic design specifications of biometric systems are

- System accuracy
  - How often the system accepts an imposter (FAR)
  - How often the system rejects a genuine user (FRR)
- Computational Speed
- Exception Handling
  - Failure to use (FTU)
  - Failure to enroll (FTE)
  - Failure to acquire (FTA)
- System Cost

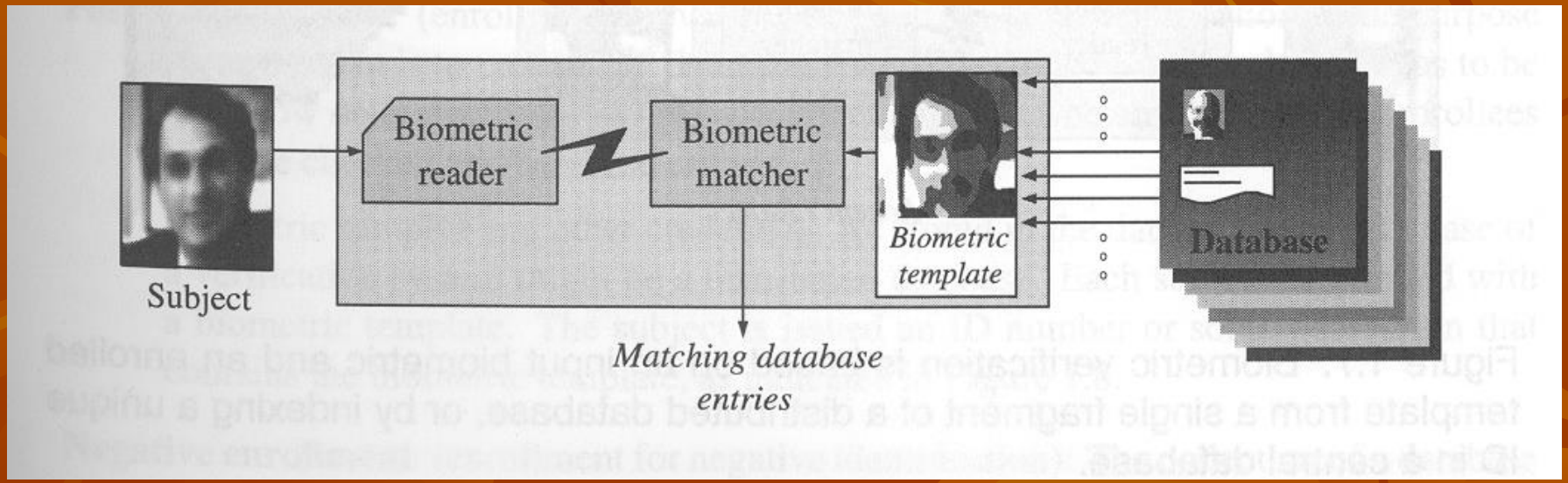
Overview of Biometric Systems

Engineering Questions

- Trusting people/biometrics?
- Which biometrics is best for a given application?
- How are the error numbers that are reported for different biometrics to be interpreted?
- Are new security holes created because of the use of the biometrics?
- How to achieve a low exception rate?
- How to acquire the biometrics and how to do it in a convenient way?
- What feature set is amenable for automatic matching?
- Given the input data how to extract the features from it?
- How to define a matching metric that translates the intuition of "similarity" among the patterns?
- How to implement the matching metric?
- Organization of the database?
- Methods for searching the database?
- Security?
- Privacy?

Biometric Identification

Biometric identification is based only on biometric credentials.



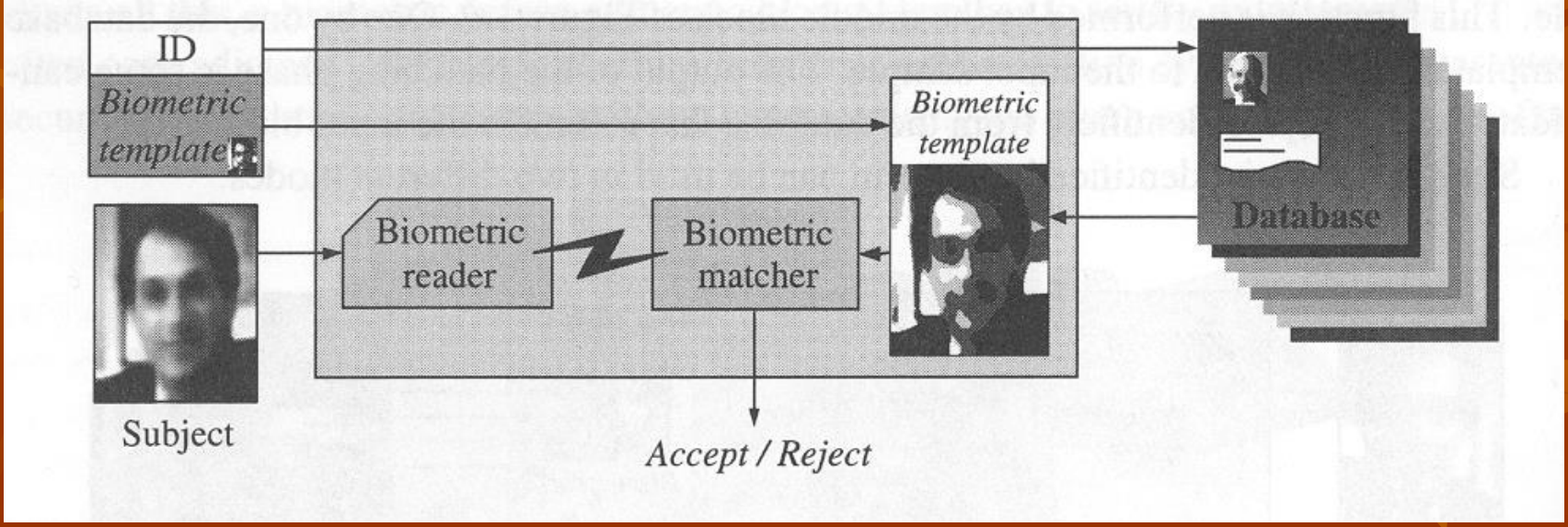
Biometric Identification

Biometric identification system can be used in two different modes

- Positive identification
  - Authorization of a group without id
- Negative identification
  - Most Wanted List

Biometric Verification

Biometric verification differs from biometric identification in that the presented biometric is only compared with a single enrolled biometric entity which matches the input id



Biometric Verification

There are two possible database configurations for the verification systems

Centralized Database: As the name suggests the enrollment information is in a central database. When the token (id/card) is provided, the corresponding biometrics is retrieved and the comparison is made with the newly presented biometric sample. E.g. laptop

Distributed Database: In this case the enrollment template is usually stored in a device that the user carries. The user provides the device and his/her biometrics. Then the comparison is performed between the two. E.g. smart cards

Biometric Enrollment

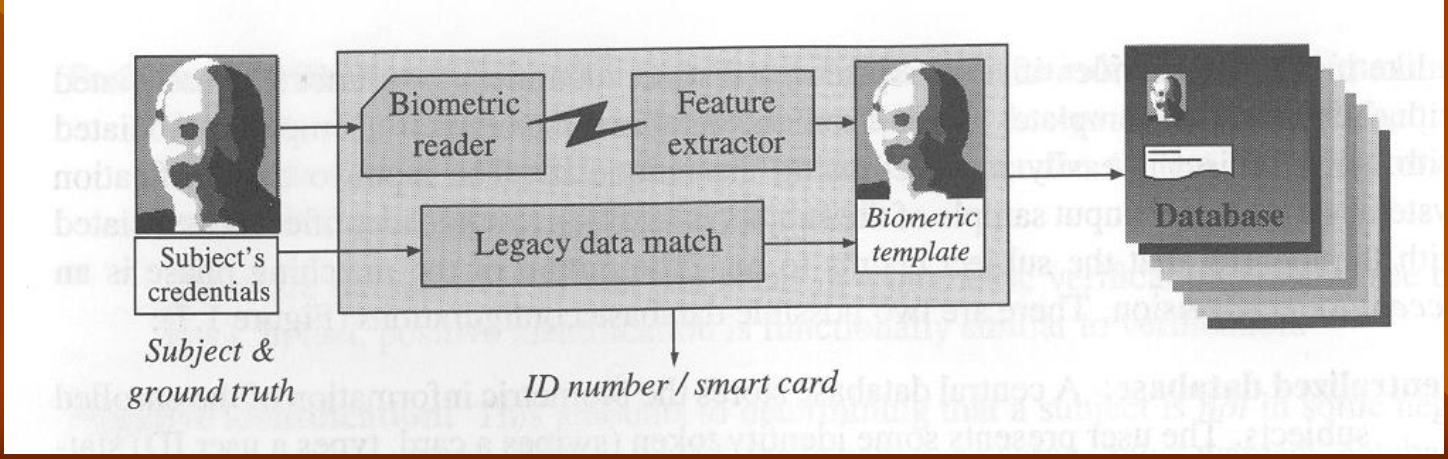
Process of registering subjects in biometric database

Positive Enrollment:

- To create a database of eligible subjects
- Biometric samples and other credentials are stored in the database. An id (or a smart card) is issued to the subject.

Negative Enrollment:

- To create a database of ineligible subjects
- Often without subject cooperation or even knowledge



Biometric System Security

- Possible Security Concerns:
  - Biometric information is presented when the owner is not present.
  - Hacking the scanner, feature extractor, matcher, database, and any other possible module in the system.

Cryptography,

Today, cryptography is used to keep sensitive material, such as private passwords, secure online. Cybersecurity experts use cryptography to design algorithms, ciphers, and other security measures that codify and protect company and customer data.

Difference between Cryptography and Cyber Security

Cyber Security	Cryptography
It is a process of keeping networks, devices, programs, data secret and safe from damage or unauthorized access.	It is a process of keeping information secret and safe simply by converting it into unintelligible information and vice-versa.

2 types of cryptography:

Cryptography is broadly classified into two categories: Symmetric key Cryptography and Asymmetric key Cryptography (popularly known as public key cryptography).

Cryptography can be broken down into three different types:

- Secret Key Cryptography.
- Public Key Cryptography.
- Hash Functions.

Example of cryptography

Examples of public-key cryptography include: **RSA, used widely on the internet**. Elliptic Curve Digital Signature Algorithm (ECDSA) used by Bitcoin. Digital Signature Algorithm (DSA) adopted as a Federal Information Processing Standard for digital signatures by NIST in FIPS 186-4.

Scanning

A vulnerability scanner enables organizations to monitor their networks, systems, and applications for security vulnerabilities. Most security teams utilize vulnerability scanners to bring to light security vulnerabilities in their computer systems, networks, applications and procedures.

Scanning could be basically of three types:

- Port Scanning – Detecting open ports and running services on the target host.
- Network Scanning – Discovering IP addresses, operating systems, topology, etc.
- Vulnerability Scanning – Scanning to gather information about known vulnerabilities in a target.

Tools used for scanning:

Aircrack is a vulnerability detection tool is popularly used to assess Wi-Fi network security. Aircrack tools are used in the network auditing process as well. Aircrack tool supports multiple operating systems such as Solaris, NetBSD, Windows, and more.

Security policy

Definitions

- A policy is

  A plan or course of action, as of a government, political party, or business, intended to influence and determine decisions, actions, and other matters

- Policies are *organizational laws*
- Standards are more detailed statements of what must be done to comply with policy
- Practices, procedures, and guidelines effectively explain how to comply with policy
- For a policy to be effective it must be
  - Properly disseminated
  - Read, understood and agreed to by all to whom it applies

Types of Policy

Management defines three types of security policy:

- General or security program policy
- Issue-specific security policies
- Systems-specific security policies

Security Program Policy

- Security program policy (SPP) also known as
  - A general security policy
  - IT security policy
  - Information security policy
- Sets strategic direction, scope, and tone for all security efforts within the organization
- An executive-level document
  - Usually drafted by or with the CIO of the organization
  - Usually 2 to 10 pages long

ACL Policies

- Both Microsoft Windows servers and Novell Netware translate ACLs into sets of configurations that administrators use to control access to their respective systems
- ACLs allow configuration to restrict access from anyone and anywhere
- ACLs regulate:
  - Who can use the system
  - What authorized users can access
  - When authorized users can access the system
  - Where authorized users can access the system from
  - How authorized users can access the system

Threat management

Categories

Classification of the threats on the basis of threat actor

"External Threats"

A threat originating outside a company, government agency, or institution

"Internal Threats"

A threat originating inside the organization—typically by an employee or "insider."

"0-Day Threats"

A zero-day threat is a threat that exploits an unknown computer security vulnerability

"APT"

APT is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time

CYBER THREAT MANAGEMENT APPROACH

This approach is very high level for assessing the risk in the organization. For better assessing the risk, we need to know about the threat actor, threat vector, threat impact. Analysis & Analytics of threat and threat protection

General Process for better threat management
go ahead and follow the basic 5 steps

1

Identification of assets [Endpoints, Network, Assets]

2

Assessing the risk

3

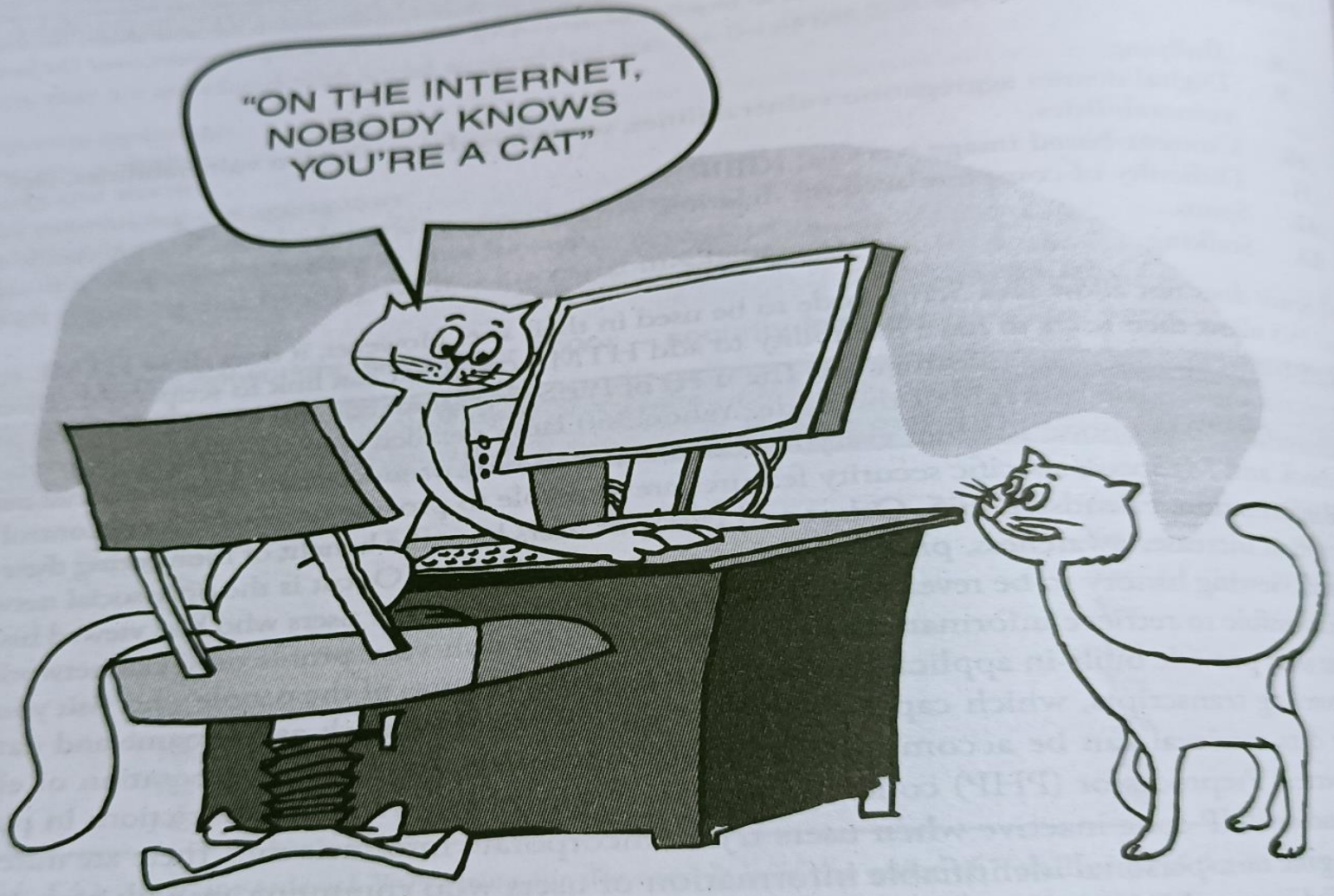
Threat Prediction [Detection & Response]

4

Threat intelligence Analytics & Publish Advisory

5

Threat Protection & Future Measures



"Annonymity breeds crime"
"Stranger is Danger"

Figure 7.25 | On the Internet, it does not matter "who" you are as long as you have "ID"!!

Digital Forensics / Cyber Forensics/ Computer Forensics Science

Digital forensics (sometimes known as **digital forensic science**) is a branch of **forensic science** encompassing the recovery and investigation of material found in **digital** devices, often in relation to **computer** crime. ... **Digital forensics** investigations have a variety of applications.

Cyberforensics plays a key role in investigation of cybercrime. "Evidence" in the case of "cyberoffenses" is extremely important from legal perspective.

NOTE: Only the technically trained and experienced experts should be involved in the forensics activities. (WHY?)

Historical background of Cyberforensics

The earliest recorded computer crimes occurred in 1969 and 1970 when student protestors burned computers at various universities. Around the same time, people were discovering methods for gaining unauthorized access to large-time shared computers. Computer intrusion and fraud committed with the help of computers were the first crimes to be widely recognized as a new type of crime.

The Florida Computer Crimes Act was the first computer crime law to address computer fraud and intrusion. It was enacted in Florida in 1978.

The application of Computer for investigating computer-based crime has led to development of a new field called computer forensics / digital forensics has existed for as long as people have stored data inside computers.

Basically,

Computer forensics experts need digital evidence in cases involving data acquisition, preservation, recovery, analysis and reporting, intellectual property theft, computer misuse, corporate policy violation, mobile device data acquisition and analysis, malicious software / application, system intrusion and compromise, encrypted, deleted and hidden files recovery, pornography, confidential information leakage, etc.

Computer Security Vs Computer forensics

- Computer Security is the prevention of unauthorized access to computer systems as well as maintaining "confidentiality", "Integrity" and "availability" of Computer systems.

- Where as, Computer Forensics is the primarily concerned with the systematic "identification", "acquisition", "preservation" and "analysis" of digital evidence, typically after an unauthorized access to computer or unauthorized use of computer has taken place. Thus, the goal of computer forensics is to perform a structured investigation on a digital system.

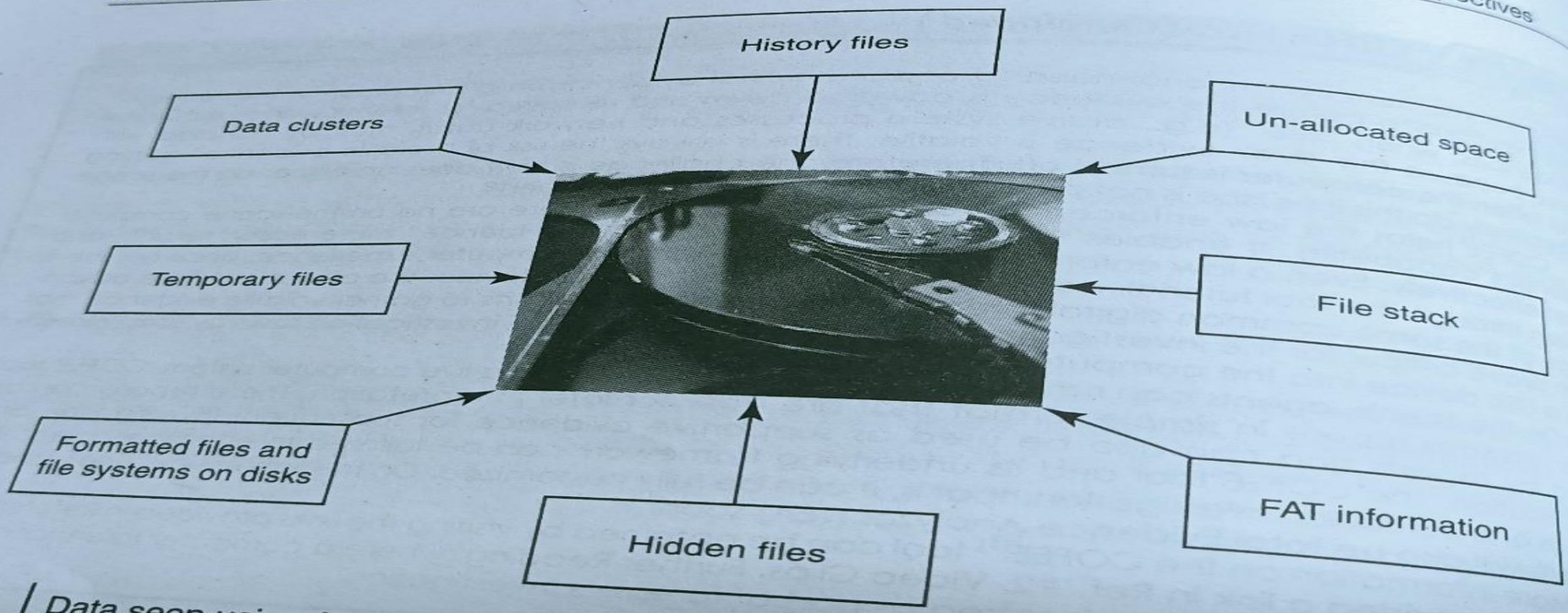
Exercise

- COFEE Time! – Computer Online Forensics Evidence Extractor is a USB thumb-drive gadget
- Tea Time! – Total Evidence Analyzer (TEA)
- Differences between Forensics Policy and Security Policy

Digital forensics Science

Digital forensics is the application of analyses techniques to the reliable and unbiased collection, analysis, interpretation and presentation of digital evidence.

1. **Computer Forensics** – It is the lawful and ethical seizure, acquisition, analysis, reporting and safeguarding of data and metadata derived from digital devices which may contain information that is notable and perhaps of evidentiary value to the trier of fact in managerial, administrative, civil and criminal investigations. In other words, it is the collection of techniques and tools used to find evidence in a computer.
2. **Digital Forensics** – It is the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorized actions shown to be disruptive to planned operations.
3. **Digital Evidence** – The collection and examination of all forms of digital data, including the data found in cell phones, PDAs, iPods and other electronic devices.



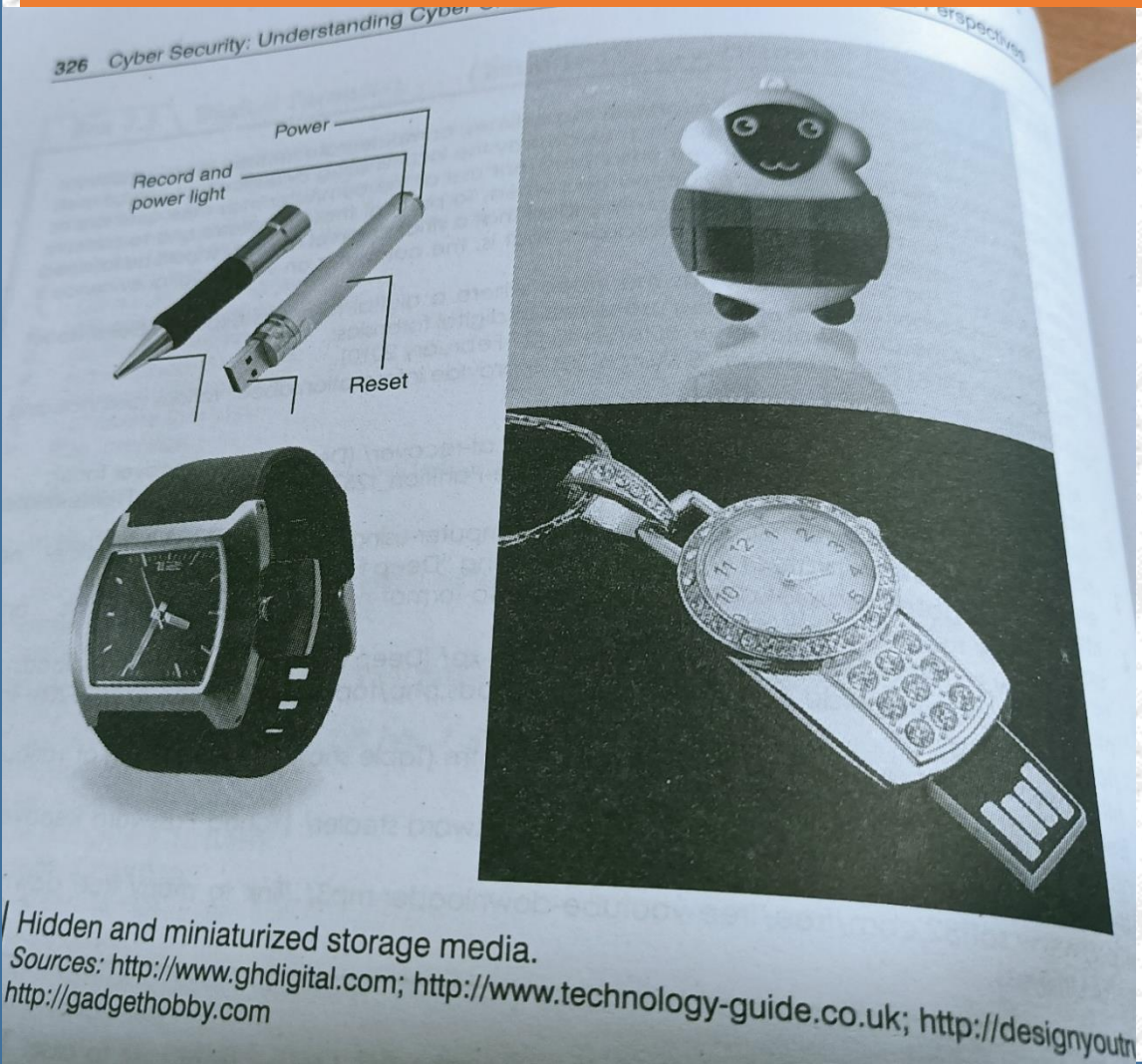
1 / Data seen using forensics tools. FAT means file allocation table.

gital forensics techniques, one can:

oborate

Note: Chain of custody means the chronological documentation trail, etc, that indicates the seizure, custody, control, transfer, analysis and disposition of evidence, physical or electronic.

Need for Computer Cyber forensics and Digital Evidence



Hidden and miniaturized storage media.
Sources: http://www.ghdigital.com; http://www.technology-guide.co.uk; http://designyoutr
http://gadgethobby.com

The media, on which clues related to cybercrime reside, would vary from case to case. There are many challenges for the forensics investigator because storage devices are getting miniaturized due to advances in electronic technology.

Note:

1. **Fungibility** – Means the extent to which the components of an operation or product can be interchanged with similar components without decreasing the value of the operation or product.
2. **Chian of custody** is also used in most evidence situations to maintain the integrity of the evidence by providing documentation of the control, transfer and analysis of evidence.
3. **Network forensics** is the study of network traffic to search for truth in civil, criminal and administrative matters to protect users and resources from exploitation, invasion of privacy and any other crime fostered by the continual expansion of network security.
4. **Paper evidence**, the process is clear and intuitively obvious. Digital evidence by its very nature is invisible to the eye. Therefore, the evidence must be developed using tools other than the human eye.

Cyber forensics and Digital Evidence

Cyber forensics can be divided into two domains:

1. Computer forensics
2. Network forensics

As compared to the "physical" evidence, "digital evidence" is different in nature. First of all, digital evidence is **much easier to change / manipulate**! Second, **"perfect" digital copies can be made without harming original**. At the same time the integrity of digital evidence can be proven. Another subtle aspect is that it is usually in the form of the "image" – this means that it is convenient and possible to create a defensible "clone" of storage device. Different information (clues) can be found at different levels of abstraction.

Understanding the uniqueness of digital evidence is important for appreciating the phases involved in a digital forensics investigation and maintaining the "chain of custody"

Computer forensics experts know the techniques to retrieve the data from files listed in standard directory search, hidden files, deleted files, deleted E-mail and passwords, login IDs, encrypted files, hidden partitions, etc. Typically the evidences reside on computer systems, user created files, user protected files, computer created files and on computer networks. Computer systems have the following:

1. Logical file system that consists of
   - File System: It includes files, volumes, directories and folders, file allocation tables (FAT) as in the older version of Windows operating system, clusters, partitions, sectors.
   - Random access memory.
   - Physical storage media: It has magnetic force microscopy that can be used to recover data from overwriting area.
     - Slack space: It is a space allocated to the file but is not actually used due to internal fragmentation and
     - Unallocated space
2. User created files: It consists of address books, audio/video files, calendars, database files, spreadsheets, E-mails, Internet bookmarks, documents and text files.
3. Computer created files: It consists of backups, cookies, configuration files, history files, log files, swap files, system files, temporary files etc.
4. Computer networks: It consists of the application layer, the transportation Layer, the Network layer, the data link layer.

Path of evidence

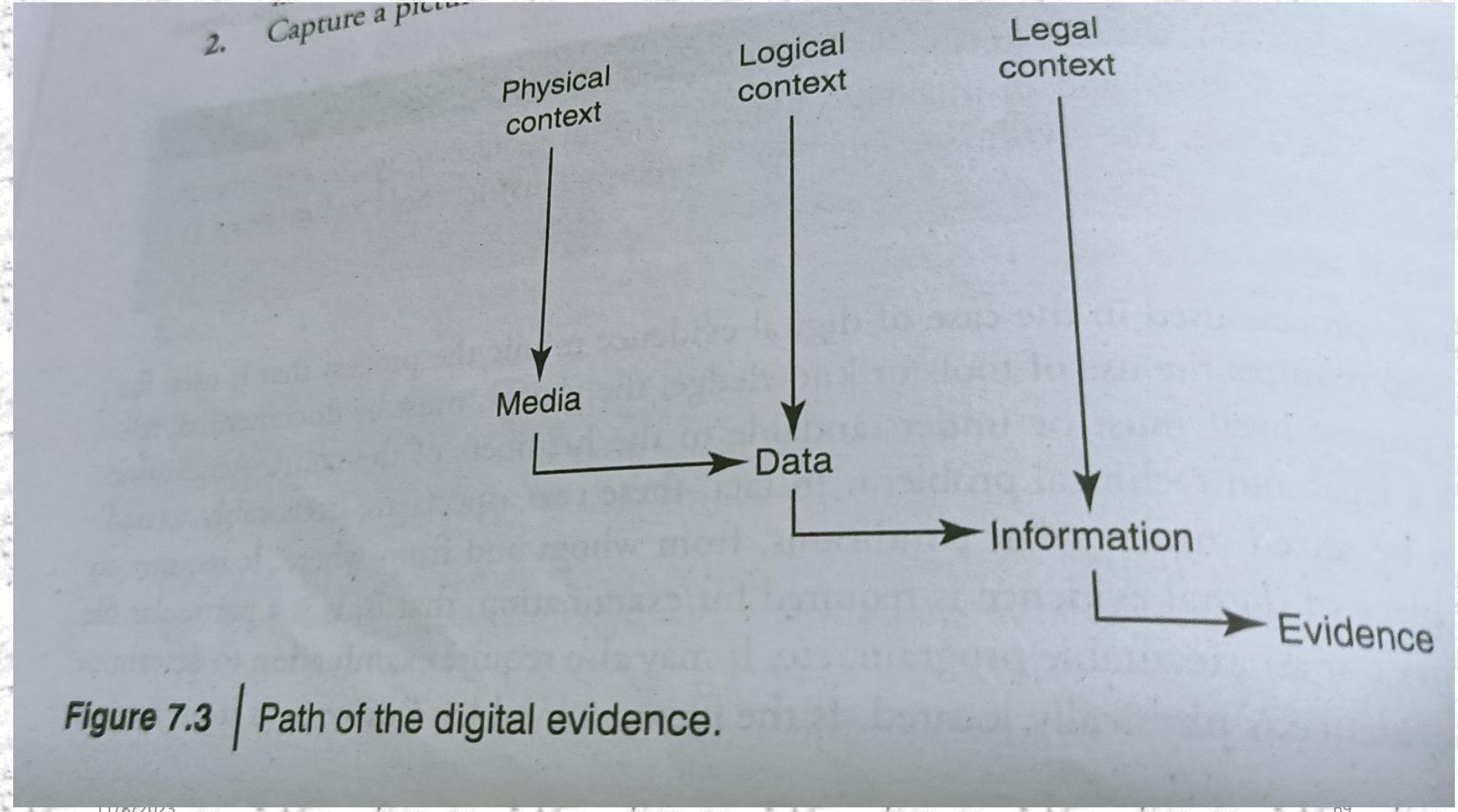


Figure 7.3 | Path of the digital evidence.

Digital Forensics Life Cycle.

As per FBI's (Federal bureau of Investigation) view, digital evidence is present in nearly every crime scene.

That is why law enforcement must know how to recognize, seize, transport and store original digital evidence to preserve it for forensics examination.

The process model for understanding a seizure and handling of forensics evidence legal framework. The cardinal rules to remember are that evidence.

1. Is admissible;
2. Is authentic;
3. Is complete;
4. Is reliable;
5. Is understandable and believable.

Digital Forensics process:

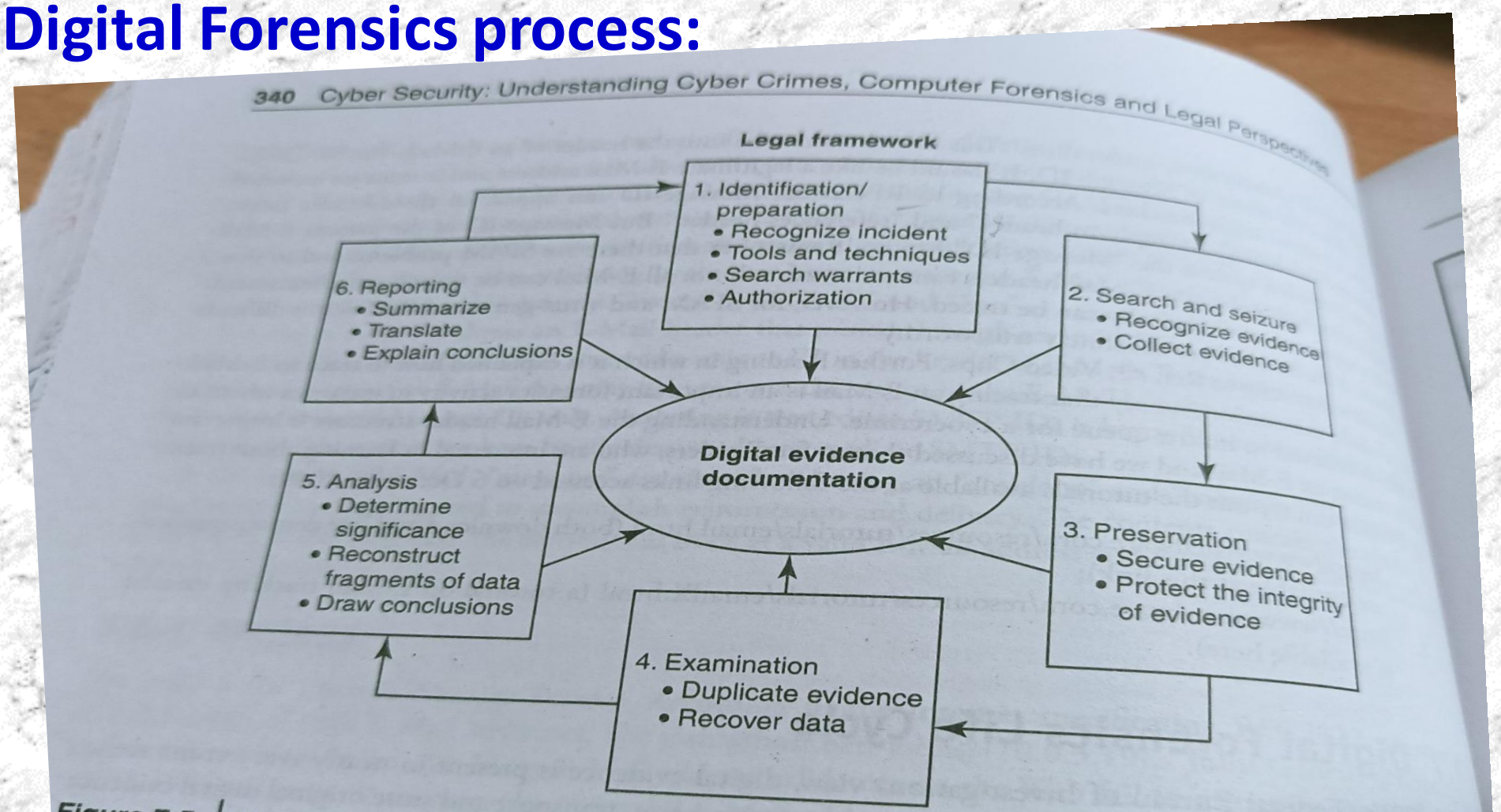


Figure 7.5 | Process model for understanding a seizure and handling of forensics evidence legal framework.

levant, authentic and that the evidence presented is not the result of h
uivalent thereof, and more probative than prejudi
Usually the assumption i

Phases in Computer Forensics / Digital Forensics:

1. Preparation and Identification;
2. Collection and recording
3. Storing and transporting
4. Examination / investigation;
5. Analysis, interpretation and attribution;
6. Reporting;
7. testifying

Collecting and recording digital evidence

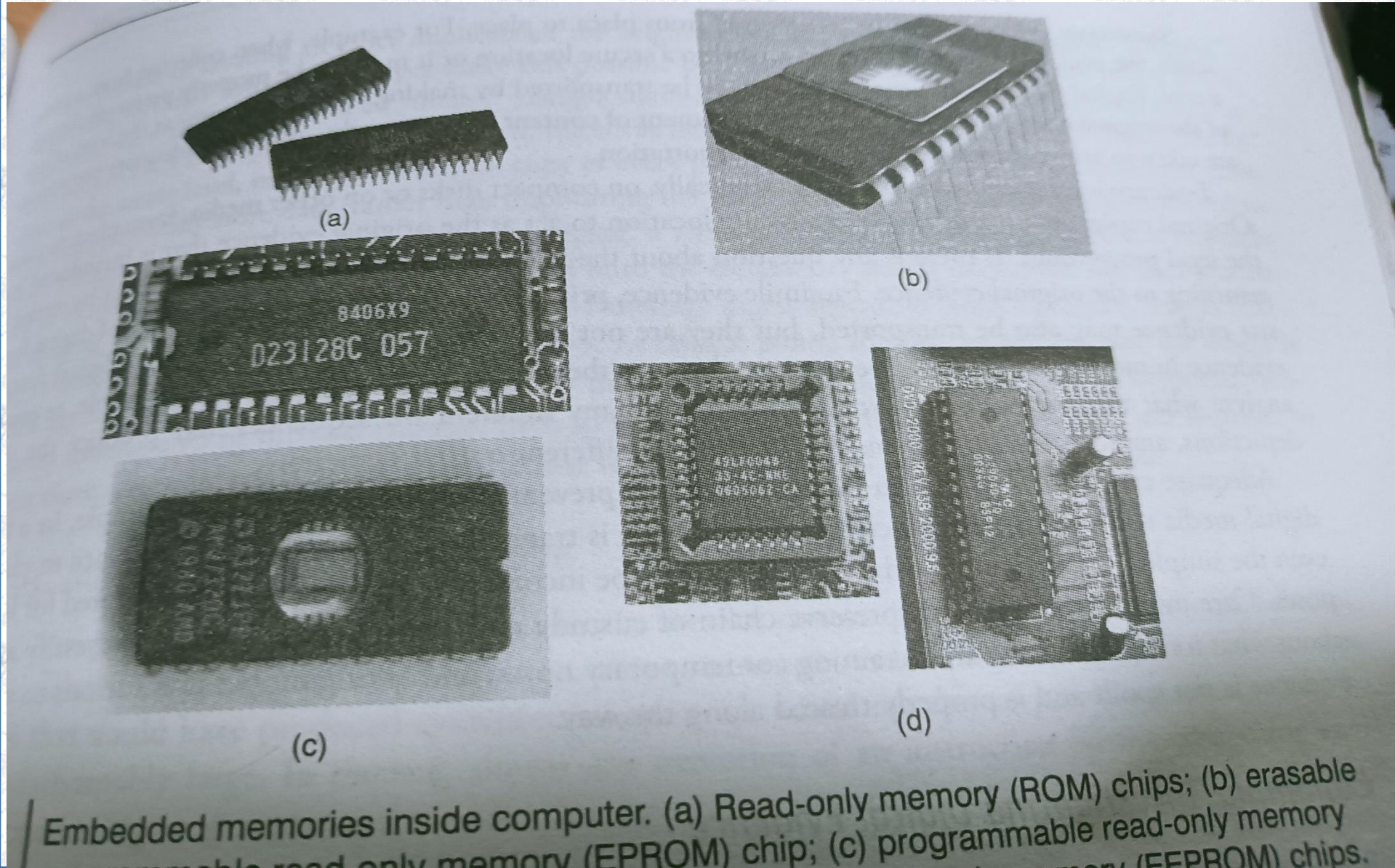
7.6 Media that can hold digital evidences.
Sources: http://www.homeofficebuddy.com; http://oldcomputers.net; http://www.homecomputertalk.com; http://www.cyberindian.net; http://www.srs-electronicmall.com; http://transcriptdivas.co.uk and http://images.google.co.in; http://www.mobileshop.com; http://images.google.co.in; http://www.slipperybrick.com; http://images.google.co.in; http://www.letsgodigital.org; http://www.computerrepairmaintenance.com; http://www.indigoshop.co.uk; http://www.adorama.com, http://sp.sony-europe.com/media/4/1914, http://www.video99.co.uk/dat.jpg

Some more media that can hold digital evidences.

Figure 7.7 | Some more media that can hold digital evidences.

Collecting volatile da...

Storing and Transporting Digital Evidence



Embedded memories inside computer. (a) Read-only memory (ROM) chips; (b) erasable

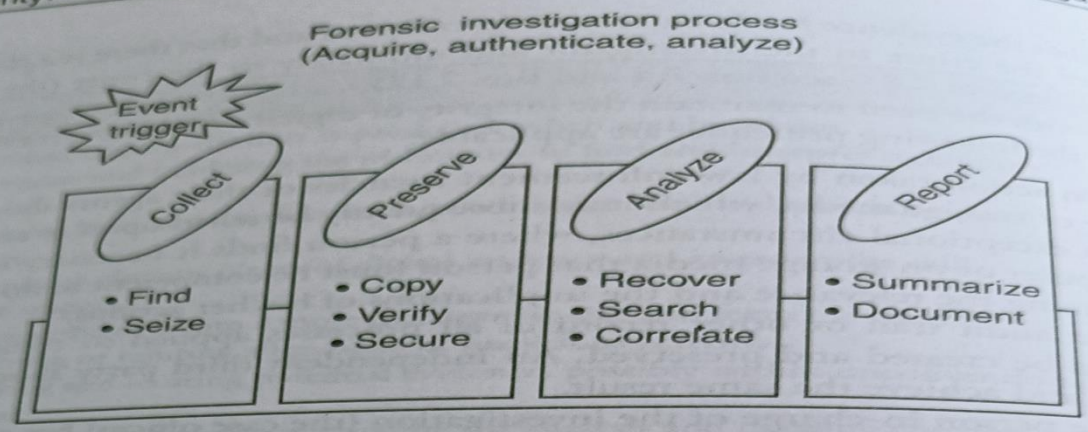


Figure 7.10 | Maintaining chain of custody – 1.

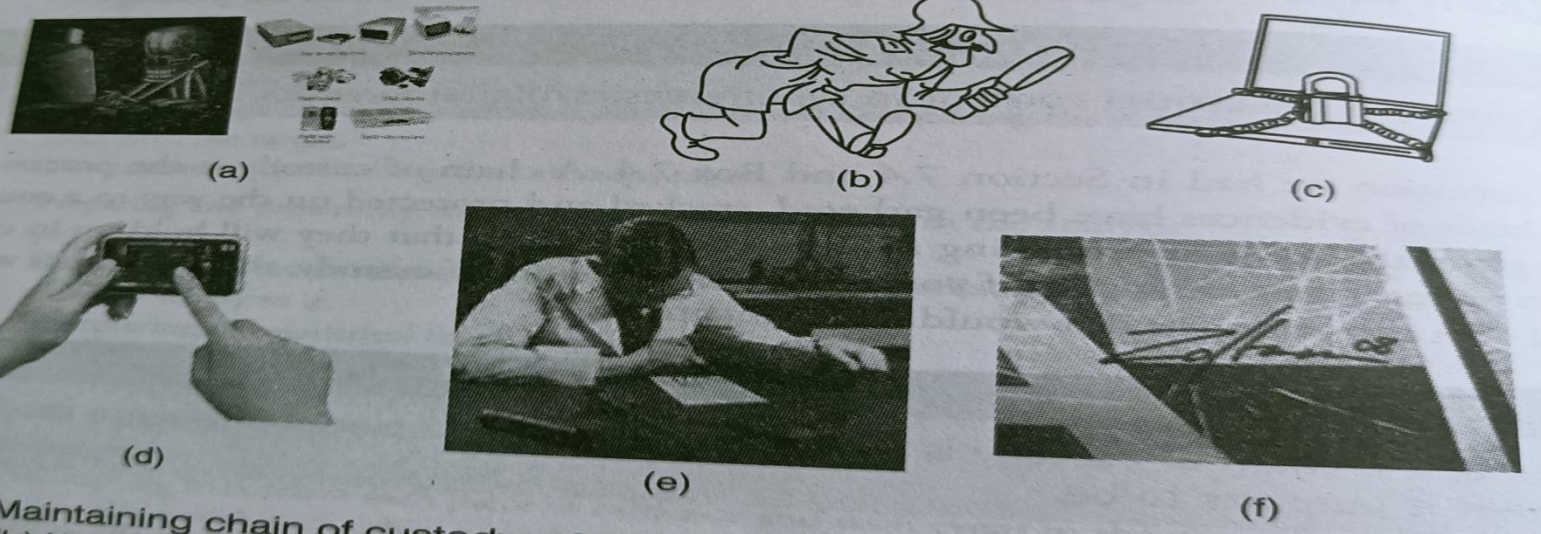


Figure 7.11 | Maintaining chain of custody – 2. (a) Source of evidence – where did it come from? (b) Who found it? (c) Where was it stored/locked up? (d) Who touched it/tampered with it? (e) What did they do to it? What did they do with it? (f) Human signature is always required.

Common Forms of Identity Theft

- Credit Card Fraud
- Communications services fraud
- Bank Fraud
- Fraudulent loans
- Internet fraud

How Identity Theft Occurs

Identify Thieves….

- Steal wallets and purses containing your ID
- Steal your mail
- Complete false “change of address” forms
- Rummage through trash (“dumpster diving”)
- Pose fraudulently as someone else to get your information

More ways Identity Theft Occurs

Identify Thieves….

- Steal business or personnel records at your workplace.
- Find personal information in your home
- Use info you put on the Internet
- Buy personal info from “inside sources.”
- “Shoulder surf” at ATMs and telephones

How Identity Thieves Use Your Information

- Change mailing addresses on credit card accounts
- Open new credit card accounts
- Establish phone or wireless service in your name
- Open new bank accounts and write bad checks
- File for bankruptcy under your name
- Counterfeit checks or debit cards
- Buy and take out car loans in your name.

Reducing the Risk of Identity Theft

- Destroy credit card applications, receipts, bank, and billing statements
- Avoid giving your SSN unless it's absolutely necessary – use other identifiers.
- Pay attention to billing cycles
- Guard your mail from theft
- Put passwords on credit card, bank, and phone accounts.
- Carry as little identification information as possible
- Limit the number of credit cards you carry.
- Don't give personal identification on the phone unless you initiate the call.
- Be cautious with personal info in your home.
- Check on who has access to your personal info at work.

More ways of reducing the Risk of Identity Theft

- Don’t carry your SS Card
- Save ATM and credit card receipts to check against statements
- Alert family members to dangers of pretexting.
- Be informed about your financial institutions’ policies of sharing information.
- Make sure your credit reports are accurate.

How to Get your Credit Reports

- 3 National Credit Reporting Agencies
- Equifax
- Experian
- Trans Union

U.S. residents can receive one free credit report per year from each credit reporting agency

www.annualcreditreport.com

999-999-9999

If you're a Victim….

- 1: Contact the fraud handling departments of the three major credit bureaus.
- Contact creditors or financial institutions for any accounts that have been tampered with.
- File a report with local police or police where the theft took place.

Techniques of ID Theft.

Methods of Identity Theft

Physical **Theft**: examples of this would be dumpster diving, mail **theft**, skimming, change of address, reshipping, government records, **identity** consolidation.

Technology-Based: examples of this are phishing, pharming, DNS Cache Poisoning, wardriving, spyware, malware and viruses.

The Indian IT ACT 2000 and amendments.

https://www.slideshare.net/YogendraWagh/it-act-ppt-1111

Information Technology Act 2000 (IT Act) and Cyber Crime

Birth of Cyber Laws

- The United Nations General Assembly have adopted the Model Law on Electronic Commerce on 30th January 1997.
- It is referred to as the "UNCITRAL Model Law on E-Commerce".
- Enacted on 17th May 2000- India is 12th nation in the world to adopt cyber laws.
- India passed the Information Technology Act, 2000 on 17th October, 2000.
- Amended on 27th October 2009. Amended Act is known as - The Information Technology (amendment) Act, 2008.

- Source: https://www.slideshare.net/YogendraWagh/it-act-ppt-1111

Information Technology Act 2000 (IT Act) and Cyber Crime

Birth of Cyber Laws

- The United Nations General Assembly have adopted the Model Law on Electronic Commerce on 30th January 1997.
- It is referred to as the "UNCITRAL Model Law on E-Commerce".
- Enacted on 17th May 2000- India is 12th nation in the world to adopt cyber laws.
- India passed the Information Technology Act, 2000 on 17th October, 2000.
- Amended on 27th October 2009. Amended Act is known as - The Information Technology (amendment) Act, 2008.

- Source: https://www.slideshare.net/YogendraWagh/it-act-ppt-1111

THE IT ACT, 2000 –OBJECTIVES

- To provide legal recognition for transactions:-
- Carried out by means of electronic data interchange, and
- Other means of electronic communication, commonly referred to as "electronic commerce", involving the use of alternatives to paper-based methods of communication and storage of information,
- To facilitate electronic filing of documents with the Government agencies
- To amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934

- Source: https://www.slideshare.net/YogendraWagh/it-act-ppt-1111

Act is not applicable to…

(a) a negotiable instrument (Other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881;
(b) a power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882;
(c) a trust as defined in section 3 of the Indian Trusts Act, 1882;
(d) a will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition
(e) any contract for the sale or conveyance of immovable property or any interest in such property;
(f) any such class of documents or transactions as may be notified by the Central Government

- Source: https://www.slideshare.net/YogendraWagh/it-act-ppt-1111

Terms under IT ACT 2000

- "Adjudicating officer“
- "Digital signature“
- "Affixing digital signature;
- "Appropriate Government“
- "Certifying Authority“
- "Cyber Appellate Tribunal“
- "Electronic form“
- "Secure system“
- "Electronic Gazette"

- Source: https://www.slideshare.net/YogendraWagh/it-act-ppt-1111

Impact on Banking Sector

- Pressure from competition and regulatory environment .
- Threat of Competition and Retaining Customer Base.
- IT used for Communication, Connectivity and Business Process Re- engineering.
- Improve efficiency of money, capital and foreign exchange markets.
- Lead to convergence of computer and communication technology to enable TBA.

- Source: https://www.slideshare.net/YogendraWagh/it-act-ppt-1111

Cyber Law: Indian Culture And Government's Role"

- Source: https://www.slideshare.net/YogendraWagh/it-act-ppt-1111

- Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime"

Need of Cyber Crime Law:

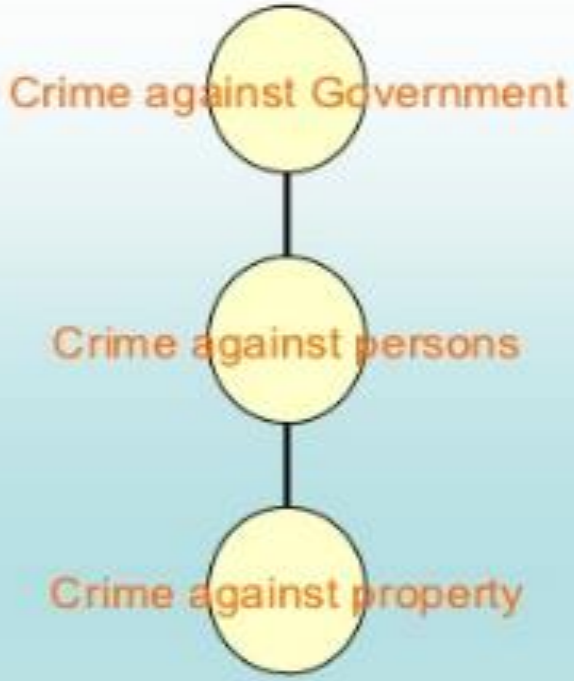
•Cyber space is an intangible and provides an extreme mobility events taking place on the internet are not happening in the locations where participants or servers are physically located, but "in cyberspace".

•Cyber space offers great economic efficiency. Billions of dollars worth of software can be traded over the Internet without the need for any government licenses, shipping and handling charges and without paying any customs duty.

•Cyber space has Complete disrespect for national boundaries. A person in India could break into a bank's electronic vault hosted on a computer in USA and transfer millions of Rupees to another bank in Switzerland, all within minutes. All he would need is a laptop computer and a cell phone.

TYPES OF CYBER CRIMES

- Cyber terrorism
- Cyber pornography
- Defamation
- Cyber stalking (section 509 IPC)
- Sale of illegal articles-narcotics, weapons, wildlife
- Online gambling
- Intellectual Property crimes- software piracy, copyright infringement, trademarks violations, theft of computer source code
- Email spoofing
- Forgery
- Phising
- Credit card frauds



- Source: https://www.slideshare.net/YogendraWagh/it-act-ppt-1111

CYBER CRIMES : CLASSIFICATION

Against Individuals: –
i. Harassment via e-mails.
ii. Cyber-stalking.
iii. Dissemination of obscene material.
iv. Defamation.
v. Unauthorized control/access over computer system.
vi. Indecent exposure
vii. Email spoofing†
viii. Cheating & Fraud

Against Organization (Government / Pvt Firm/ Company): -
i. Unauthorized control/access over computer system
ii. Possession of unauthorized information.
iii. Cyber terrorism against the government organization.
iv. Distribution of pirated software etc.

Against Individual Property: -†
i. Computer vandalism.
ii. Transmitting virus.
iii. Netrespass
iv. Unauthorized control/access over computer system.
v. Intellectual Property crimes
vi.†Internet time thefts

Against Society at large: -
i.†††† Pornography (basically child pornography).
ii.††† Polluting the youth through indecent exposure.
iii.†† Trafficking
iv. Financial crimes
v. Sale of illegal articles
vi. Online gambling
vii.† Forgery

- Source: https://www.slideshare.net/YogendraWagh/it-act-ppt-1111

CYBER CRIME CASES REGISTERED & PERSON ARRESTED UNDER IT ACT (2006-2009)

Cyber Crimes/Cases Registered and Persons Arrested under IT Act during 2006 - 2009

SL. NO.	Crime Heads	Cases Registered				% Variation in 2009 over 2008	Persons Arrested				% Variation in 2009 over 2008
		2006	2007	2008	2009		2006	2007	2008	2009	
1	Tampering computer source documents	10	11	26	21	-19.2	8	2	26	6	-76.9
2	Hacking with Computer System										
	i) Loss/damage to computer resource/utility	25	30	56	115	105.3	34	25	41	63	53.6
	ii)Hacking	34	46	82	118	43.9	29	23	15	44	193.3
3	Obscene publication/transmission in electronic form	69	99	105	139	32.4	81	86	90	141	56.7
4	Failure										
	i) Of compliance/orders of Certifying Authority	0	2	1	3	200.0	0	1	2	6	200.0
	ii) To assist in decrypting the information intercepted by Govt. Agency	0	2	0	0	@	0	0	0	0	@
5	Un-authorised access/attempt to access to protected computer system	0	4	3	7	133.3	0	0	1	16	1500.0
6	Obtaining licence or Digital Signature Certificate by misrepresentation/suppression of fact	0	11	0	1	@	0	11	0	1	@
7	Publishing false Digital Signature Certificate	0	0	0	1	@	0	0	0	0	@
8	Fraud Digital Signature Certificate	1	3	3	4	33.3	0	3	0	6	@
29	Breach of confidentiality/privacy	3	9	8	10	25.0	2	3	3	5	66.6
10	Other	0	0	4	1	-75.0	0	0	0	0	@
	Total	142	217	288	420	45.8	154	154	178	288	61.8

- Source: https://www.slideshare.net/YogendraWagh/it-act-ppt-1111

Cyber Crime Cases Registered & Person Arrested under IT ACT (2017 to 2019), Source:https://ncrb.gov.in/en/crime-in-india-table-addtional-table-and-chapter-contents?page=23

TABLE 9A.1

Cyber Crimes (State/UT-wise) – 2017-2019

S. No	State/UT	2017	2018	2019	Percentage Share of State/UT (2019)	Mid-Year Projected Population (in Lakhs) (2019)	Rate of Total Cyber Crimes (2019)+
1	2	3	4	5	6	7	8
STATES:							
1	Andhra Pradesh	931	1207	1886	4.2	523.2	3.6
2	Arunachal Pradesh	1	7	8	0.0	15.1	0.5
3	Assam	1120	2022	2231	5.0	344.2	6.5
4	Bihar	433	374	1050	2.4	1201.1	0.9
5	Chhattisgarh	171	139	175	0.4	288.5	0.6
6	Goa	13	29	15	0.0	15.4	1.0
7	Gujarat	458	702	784	1.8	682.5	1.1
8	Haryana	504	418	564	1.3	288.1	2.0
9	Himachal Pradesh	56	69	76	0.2	73.2	1.0
10	Jammu & Kashmir	63	73	73	0.2	135.3	0.5
11	Jharkhand	720	930	1095	2.5	375.8	2.9
12	Karnataka	3174	5839	12020	27.0	659.7	18.2
13	Kerala	320	340	307	0.7	351.9	0.9
14	Madhya Pradesh	490	740	602	1.4	826.1	0.7
15	Maharashtra	3604	3511	4967	11.2	1225.3	4.1
16	Manipur	74	29	4	0.0	31.1	0.1
17	Meghalaya	39	74	89	0.2	32.3	2.8
18	Mizoram	10	6	8	0.0	12.0	0.7
19	Nagaland	0	2	2	0.0	21.6	0.1
20	Odisha	824	843	1485	3.3	437.3	3.4

Cybercrime provisions under IT Act,2000

Tampering with Computer source documents	Sec.65
Hacking with Computer systems, Data alteration	Sec.66
Publishing obscene information	Sec.67
Un-authorized access to protected system	Sec.70
Breach of Confidentiality and Privacy	Sec.72
Publishing false digital signature certificates	Sec.73

- Source: https://www.slideshare.net/YogendraWagh/it-act-ppt-1111

Amendment of IT Act 2000

- **Criminal Provisions : Section 66**
- Provision has been significantly changed.
- Under IT Act, 2008 all the acts referred under section 43, are also covered u/Sec. 66 if they are done *"dishonestly"* or *"fraudulently"*.
- Many cybercrimes on which there were no express provisions made in the IT Act, 2000 are now included in the IT Act, 2008.

Section 66(A)

- **Sending of offensive or false messages** - new provision
- Also known as "**Cyber Stalking**"
- Covers sending of menacing, offensive or false messages via **SMS/EMAIL/MMS**
- Punishment – imprisonment up to 3 years and fine

- Source: https://www.slideshare.net/YogendraWagh/it-act-ppt-1111

Cont.....

- **Section 66(B)**
- **Dishonestly receiving stolen computer resource or communication device** - new provision
- Also covers **use of stolen Computers, mobile phones, SIM Cards, etc**
- Punishment – imprisonment upto 3 years or fine upto Rs. 1 lakh or both

- **Section 66(C)**
- **Identity theft** - new provision
- Fraudulently or dishonestly using someone else's electronic signature, password or any other unique identification feature
- Punishment - imprisonment upto 3 years and fine upto Rs. 1 lakh

- Source: https://www.slideshare.net/YogendraWagh/it-act-ppt-1111

Cont.....

- **Section 66(E)**
- **Violation of privacy** - new provision
- Popularly known as **Voyeurism**
- Pune spy cam incident where a 58-year old man was arrested for installing spy cameras in his house to 'snoop' on his young lady tenants
- Covers acts like hiding cameras in changing rooms, hotel rooms, etc
- Punishment –imprisonment upto 3 years or fine upto Rs. 2 lakh or both

- **Section 66(F)**
- **Cyber terrorism** - new provision
- Whoever uses cyberspace with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people
- Punishment - Imprisonment which may extent to life imprisonment

- Source: https://www.slideshare.net/YogendraWagh/it-act-ppt-1111

Cyber Pornography

- **Section 67**
- **Publishing or transmitting obscene material in electronic form**
- Punishment –

  First instance - imprisonment up to 3 years and fine up to Rs. 5 lakh.

  Subsequent - imprisonment up to 5 years and fine up to Rs. 10 lakh.
- **Section 67(A)** – new provision
- **Publishing or transmitting sexually explicit acts in the electronic form**
- Similarity with **Sec. 292 IPC**
- Punishment –

  First instance - imprisonment upto 5 years Subsequent - imprisonment up to 7 years Fine up to Rs. 10 lakh.

- Source: https://www.slideshare.net/YogendraWagh/it-act-ppt-1111

Cont.....

- **Section 67(B)** – new provision
- Creating, collecting, browsing, downloading, etc of **Child Pornography**
- Punishment –

  First instance - imprisonment up to 5 years.

  Subsequent – imprisonment up to 7 years

  Fine up to Rs. 10 lakh.

- **Preservation of information by intermediaries**

  Section 67(C) – new provision
- Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.

- Source: https://www.slideshare.net/YogendraWagh/it-act-ppt-1111

Famous BPO Cyber Crime Cases

- The recently reported case of a Bank Fraud in Pune in which some ex employees of BPO arm of MPhasis Ltd MsourcE, defrauded US Customers of Citi Bank to the tune of RS 1.5 crores has raised concerns of many kinds including the role of "Data Protection".

- The crime was obviously committed using "Unauthorized Access" to the "Electronic Account Space" of the customers. It is therefore firmly within the domain of "Cyber Crimes".

- Source: https://www.slideshare.net/YogendraWagh/it-act-ppt-1111

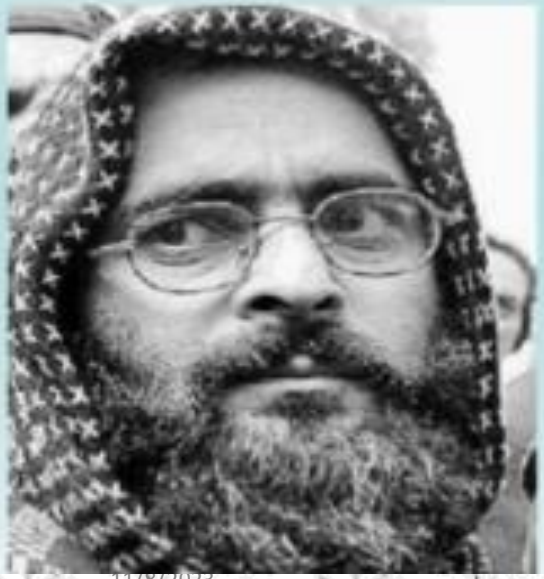
Ahmadabad Blast : *Haywood*

- Five minutes before the blast, an e-mails sent to national TV channels warning about blasts in Ahmedabad. The e-mail is traced to Kenneth Haywood's computer, who stayed at Gunina apartment in Navi Mumbai. Haywood claimed that his computer was hacked. A technician associated with VSNL had asked him not to change the password of his wireless Internet network. Haywood's laptop and computer was then sent to the forensic science laboratory at Kalina.
- Wi-Fi system used to hack Haywood's account to send the mail.

- Source: https://www.slideshare.net/YogendraWagh/it-act-ppt-1111

Parliament Attack Case

The Laptop seized from the gunned down terrorist contained several evidences of terrorist's motives. The sticker of the Ministry of home that they had made on the laptop and pasted on their ambassador car to gain entry into the parliament house and the fake ID card that one of the two terrorists was carrying with the Government of India emblem and seal.



- Source: https://www.slideshare.net/YogendraWagh/it-act-ppt-1111

- **References:**
  https://slideplayer.com/slide/4242962/
  https://www.vadesecure.com/en/blog/5-common-phishing-techniques

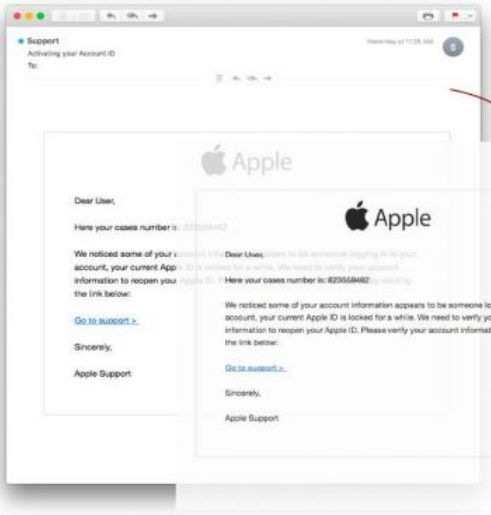
The below slides are additional material for quick reference.

Phishing

- **Phishing** is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

Techniques of Phishing

1. Using legitimate Links
2. Mixing legitimate and malicious code
3. Abusing redirections and URL shorteners
4. Obfuscating brand logos
5. Confusing the filter with little content or excess noise



Helpful Resources

Sign in to the service portal.

Have Questions? Visit the Community.

This is a mandatory service communication. To set your contact preferences for other communications, click here.

This message was sent from an unmonitored e-mail address. Please do not reply to this message.
Privacy | Legal

Microsoft Office
One Microsoft Way
Redmond, WA
98052-6399 USA

Microsoft

Wells Fargo Online.

WV

Wells Verification <wfbank.connect.auth@t-online.de>
no-reply.message@wellsfargo.com
Tuesday, April 9, 2019 at 9:52 AM
Show Details

To protect your privacy, some pictures in this message were not downloaded.

Wells Fargo wellsfargo.com

Verify Your Account

Dear Customer

During our safety inspection we noticed that your account has not been completely verified and protected, so we require you to verify some of your information in order to automatically secure and encrypt your account with the latest update.

Verify your account now by signing in to wellsfargo.com/update.

Failure to verify your account immediately might lead to the temporary suspension/restriction of your account.

Thank you. We appreciate Your Compliance.

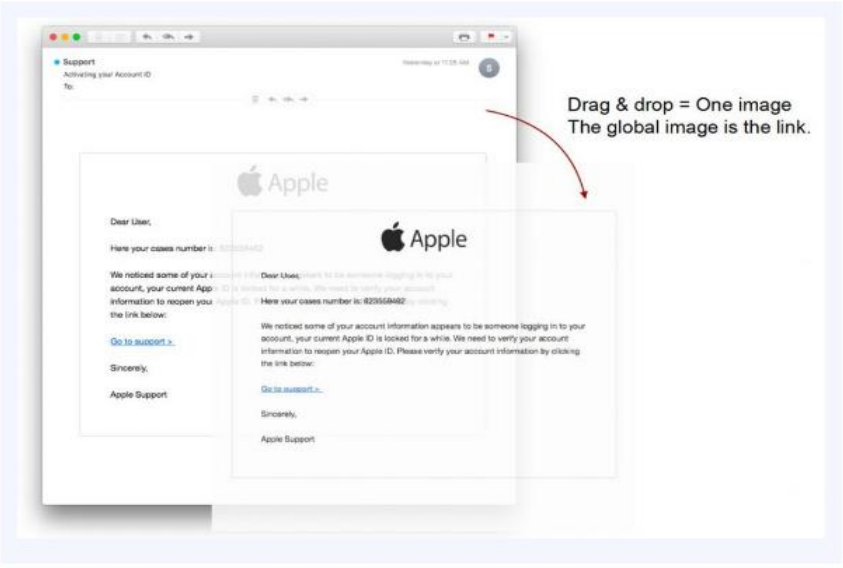
Wells Fargo Online Customer Service

wellsfargo.com | Fraud Information Center

ec3ac241-6f58-432f-a86c-83cb93bb0c60

Methods of Phishing

1. Email Phishing
2. Spear Phishing



Helpful Resources

Sign in to the service portal.

Have Questions? Visit the Community.

This is a mandatory service communication. To set your contact preferences for other communications, click here.

This message was sent from an unmonitored e-mail address. Please do not reply to this message.
Privacy | Legal

Microsoft Office
One Microsoft Way
Redmond, WA
98052-6399 USA

Microsoft

Wells Fargo Online.

WV

Wells Verification <wfbank.connect.auth@t-online.de>
no-reply.message@wellsfargo.com
Tuesday, April 9, 2019 at 9:52 AM
Show Details

To protect your privacy, some pictures in this message were not downloaded.

Wells Fargo wellsfargo.com

Verify Your Account

Dear Customer

During our safety inspection we noticed that your account has not been completely verified and protected, so we require you to verify some of your information in order to automatically secure and encrypt your account with the latest update.

Verify your account now by signing in to wellsfargo.com/update.

Failure to verify your account immediately might lead to the temporary suspension/restriction of your account.

Thank you. We appreciate Your Compliance.

Wells Fargo Online Customer Service

wellsfargo.com | Fraud Information Center

ec3ac241-6f58-432f-a86c-83cb93bb0c60

References

- https://slideplayer.com/slide/13426045/
- https://www.slideshare.net/YogendraWagh/it-act-ppt-1111
- https://www.strongdm.com/blog/types-of-access-control
- https://www.slideshare.net/primeteacher32/access-controls-65868136
- https://www.slideshare.net/pln9/security-audit-view
- https://www.slideshare.net/emolagi/the-information-security-audit
- https://www.slideshare.net/officialRishikant/cyber-threat-management
- https://www.cse.unr.edu/~bebis/CS790Q/Lect/Chapters_1_2.ppt
- https://www.slideshare.net/emolagi/security-policy-45924360