UNIT 1: INTRODUCTION

LH-5

ROLISHA STHAPIT

CONTENTS

- Computer Security Concepts, Threats, Attacks and Assets, Security Functional Requirements, Security Design Principles, Attack Surfaces and Attack Trees, Computer Security Strategy, Access Control Principles, Subjects, Objects and Access Rights, Discretionary Access Control, Role Based Access Control, Attribute Based Access Control, Identity, Credential and Access Management, Trust Frameworks, Overview of the Bell-LaPadula Model and Biba integrity model.

Why do we need security?

- Increased reliance on Information technology with or with out the use of networks
- The use of IT has changed our lives drastically.
- We depend on E-mail, Internet banking, and several other governmental activities that use IT
- Increased use of E-Commerce and the World Wide Web on the Internet as a vast repository of various kinds of information (immigration databases, flight tickets, stock markets etc.)

Need of security

- To safeguard the confidentiality, integrity, authenticity and availability of data transmitted over insecure networks
- Internet is not the only insecure network in this world
- Many internal networks in organizations are prone to insider attacks
- In fact, insider attacks are greater both in terms of likelihood of happening and damage caused

- **Computer Security**
- It is a process and the collection of measures and controls that ensures the Confidentiality,
- Integrity and Availability (CIA) of the assets in computer systems. Computer Security protects you from both software and hardware part of a computer systems from getting compromised and be exploited.

- **Information Security:**
- Information security is primarily concerned with making sure that data in any form is kept secure in terms of preserving its confidentiality, integrity and availability.
- Information is a significant asset that can be stored in different ways such as digitally stored, printed, written on papers or in human memory. It can be communicated through different channels such as spoken languages, gestures or using digital channel such as email, SMS, social media, video, audio etc.
- Information security differs from cybersecurity such that information security aims to keep data in any form secure, whereas cybersecurity protects only digital data. Cybersecurity is the subset of information security.

- **Network Security:**
- It is any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies.
- An effective network security manages access to the network. It targets a variety of threats and stop them from entering or spreading on your network.
- Network security, a subset of cybersecurity, aims to protect any data that is being sent through devices in your network to ensure that the information is not changed or intercepted.

COMPUTER SECURITY CONCEPTS

- The NIST Computer Security Handbook [NIST95] defines the term computer security as

"The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/ data, and telecommunications)."

- This definition introduces three key objectives that are at the heart of computer security.
- **Confidentiality:** This term covers two related concepts:

- **Data confidentiality:** Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

- **Privacy:** Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

- **Integrity:** This term covers two related concepts:

- **Data integrity:** Assures that information and programs are changed only in a specified and authorized manner.

- **System integrity:** Assures that a system performs its intended function in an undamaged manner, free from deliberate or inadvertent unauthorized manipulation of the system.

- **Availability**: Assures that systems work promptly and service is not denied to authorized users.

CIA TRIAD

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

- **Integrity:** Guarding against improper information modification or destruction, including ensuring information, nonrepudiation and authenticity. A loss of integrity is the
unauthorized modification or destruction of information.
- **Availability**: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

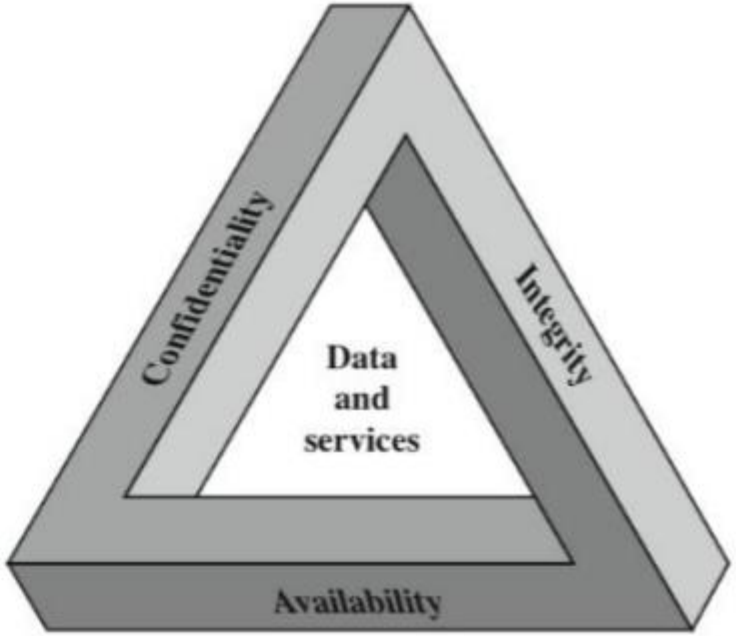


Figure: CIA Triad

Apart from the above three pillars of security, other important aspects of security include

- Authenticity and
- Accountability.
- **Authenticity :**The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.
- **Accountability :** Accountability relates to the capability of the information system to trace the activity of each entity to that particular entity. For example, if a person X does a certain change in a networked system, that system should have logs and audit trail facility to establish upon investigation that the change was actually done by X and not by other person.

- Because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party. Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.
- **Non-repudiation:**
- Non repudiation prevents either sender or receiver from denying transmitted message. When a message is sent, the receiver can prove that the alleged sender in fact sent the message. When a message is received, the sender can prove that the alleged receiver received the message.

- **Computer Security Challenges:**

1. Security is not simple it requires a lot of research and money

2. Potential attacks on the security features need to be considered.

3. Procedures used to provide particular services are often counter-intuitive (unexpected)

4. It is necessary to decide where to use the various security mechanisms.

5. Requires constant monitoring.

6. Security mechanisms typically involve more than a particular algorithm or protocol.

7. Security is essentially a battle of wits between a perpetrator and the designer.

8. Little benefit from security investment is perceived until a security failure occurs.

9. Strong security is often viewed as an impediment to efficient and user friendly operation.

THREATS, ATTACKS AND ASSETS

- **Assets:**
- An asset is any data, device or other component of an organization’s systems that is valuable often because it contains sensitive data or can be used to access such information.
- For example, an employee’s desktop computer, laptop or company phone would be considered an asset, as would applications on those devices. Likewise, critical infrastructure, such as servers and support systems, are assets.
- An organization’s most common assets are information assets. These are things such as databases and physical files i.e. the sensitive data that you store.
- A related concept is the “information asset container”, which is where that information is kept. In the case of databases, this would be the application that was used to create the database. For physical files, it would be the filing cabinet where the information resides.

- **Threats:**
- A threat to a computing system is a set of circumstances that has the potential to cause loss or harm. It is a potential violation of security, means that it is a possible danger that might exploit vulnerability.
- Threats can be categorized into four classes:
- **Disclosure-** Unauthorized access to information

Eg: Snooping

- **Deception-** Acceptance of false data

Eg: Modification, Spoofing, denial of receipt, Repudiation of origin

- **Disruption-** Interruption of correct operation

Eg: Modification

- **Usurpation-** Unauthorized control of some part of system

Eg: Modification, Spoofing, denial of service, delay

Interception: An Interception means that some unauthorized party has gained access to an asset. The outside party can be a person, a program or a computing system. Example: The illicit copying the data files or programs

Interruption: An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability. Example: the malicious destruction of a hardware device, malfunction of an operating system file manager, cutting of communication lines etc

Modification: If an authorized party not only gains access to but tampers with an asset, this threat is called modification. Example, changing the values in data files, altering a program so that it performs differently. This is an attack on integrity.

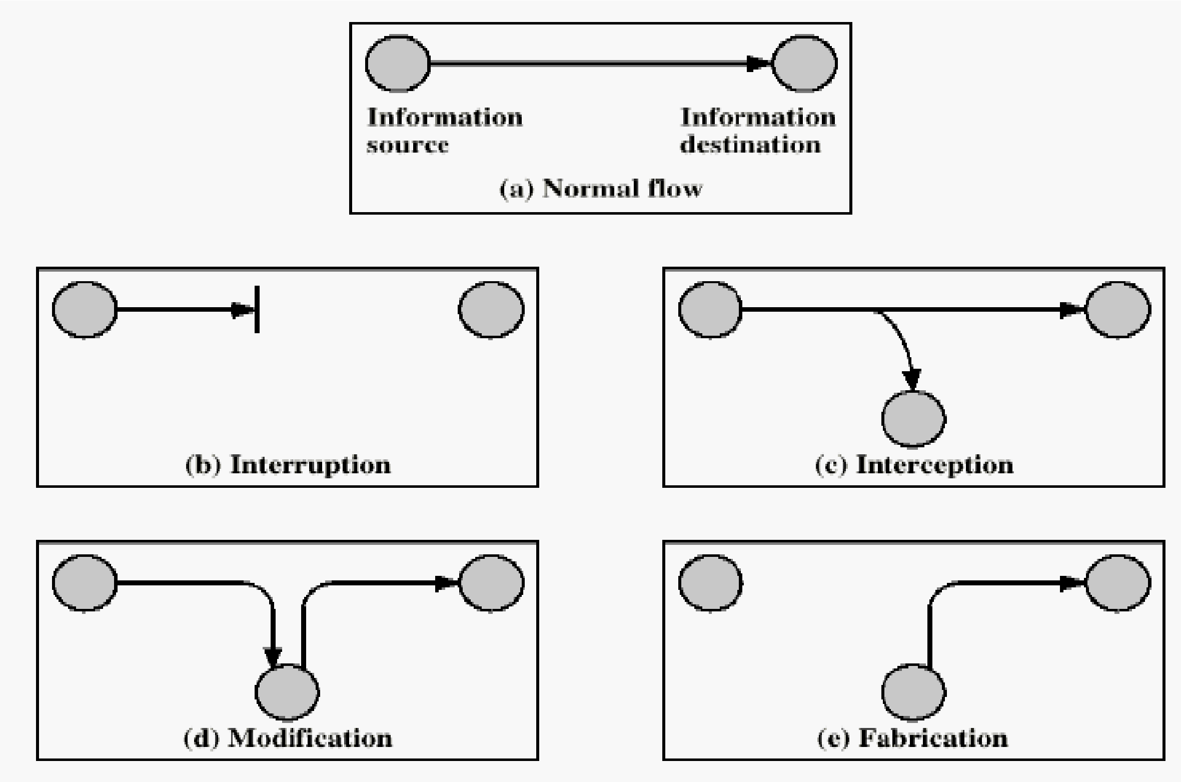


Figure 1.1 Security Threats

Fabrication: An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity. Example: include insertion of spurious message in network.

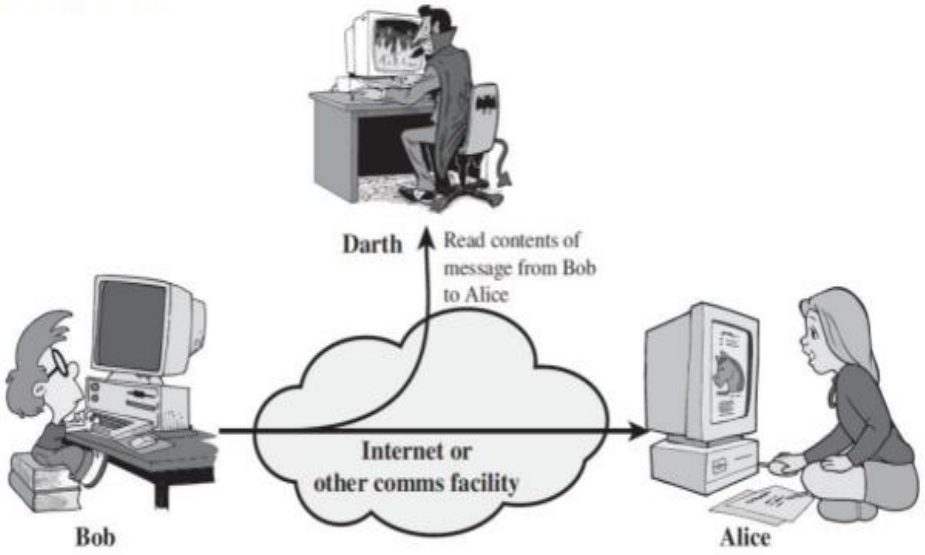
- **Attack:**
- An Attack is an intentional unauthorized action on a system. An attack always has a motivation to misuse system and generally wait for an opportunity to occur.
- Network security attacks can be classified as

- **Passive attacks:** It attempts to learn or make use of information from the system but does not affect system resources.
- **Active attacks:** It attempts to alter system resources or affect their operation.

- **Passive attacks:**
- Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions.
- The goal of the opponent is to obtain information that is being transmitted.
- No modification of content or fabrication
- Eavesdropping to learn contents or other information (transfer patterns, traffic flows etc.)
- Passive attacks are very difficult to detect, because they do not involve any alteration of the data.
- Typically, the message traffic is sent and received in an apparently normal fashion, and neither the sender nor the receiver is aware that a third party has read the messages or observed the traffic pattern.
- Two types of passive attacks are the release of message contents and traffic analysis.

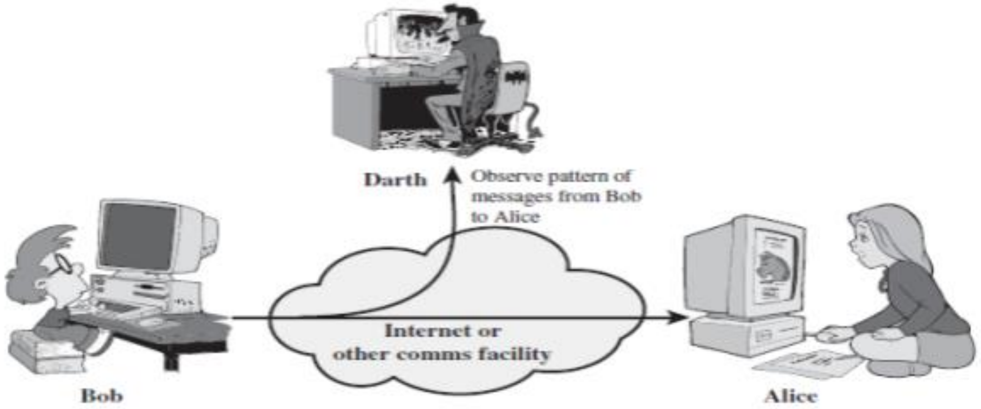
1.Release of message Contents

- A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information.


Darth
Read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

2.Traffic Analysis:

- Subtle form of attack
- Determine location/origin of hosts
- Observe frequency and length of messages being exchanged.


Darth
Observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

- **Active attacks:**
- Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories:

- Masquerade

- Replay

- Modification of messages, and

- Denial of service.

1. Masquerade:

- A masquerade takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack.

- For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

- An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account

2. Replay:

- Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

3. Modification of messages

- Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.

- For example, a message meaning “Allow John Smith to read confidential file accounts” is modified to mean “Allow Fred Brown to read confidential file accounts.”

4. DOS (Denial of Service)

- The denial of service prevents the normal use of facilities.

- This attack may have a specific target.

- It is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

- For example, an entity may suppress all messages directed to a particular destination

SECURITY REQUIREMENTS

- It is a specific prerequisite that a system needs to fulfill in order to achieve a specific security objective. It is a security feature required by system users or a quality the system must possess to increase the users trust in the system they use. In general, a security requirement is considered as a non-functional requirement. Following are the list of requirement needs to secure the system.

- **Access Control:**

- Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

- **Awareness and Training:**

- Ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, regulation, and policies related to the security of organizational information systems.
- Ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

- **Configuration Management:**

- Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
- Establish and enforce security configuration settings for information technology products employed in organizational information systems.

- **Contingency Planning:**

- Establish, maintain, and implement plans for emergency response, backup operations, and post disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

- **Identification and Authentication:**

- Identify information system users, processes acting on behalf of users, or devices, and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

- **Audit and Accountability:**

- Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.

- Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

- **Certification, Accreditation, and Security Assessments:**

- Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application;

- Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.

- Authorize the operation of organizational information systems and any associated information system connections.

- Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

- **Maintenance:**
- Perform periodic and timely maintenance on organizational information systems.
- Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.
- **Media Protection:**
- Protect information system media, both paper and digital.
- Limit access to information on information system media to authorized users.
- Sanitize or destroy information system media before disposal or release for reuse.

- **Physical and Environmental Protection:**

- Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals.

- Protect the physical plant and support infrastructure for information systems.

- Provide supporting utilities for information systems.

- Protect information systems against environmental hazards.

- Provide appropriate environmental controls in facilities containing information systems.

- **Planning:**

- Develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

- **Personnel Security:**

- Ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions.
- Ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers.
- Employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

- **Risk Assessment:**

- Periodically assess (evaluation) the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

- **Systems and Services Acquisition:**

- Allocate sufficient resources to adequately protect organizational information systems.
- Employ system development life cycle processes that incorporate information security considerations.
- Employ software usage and installation restrictions.
- Ensure that third party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

- **System and Communications Protection:**

- Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

- Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

- **System and Information Integrity:**

- Identify, report, and correct information and information system flaws in a timely manner.

- Provide protection from malicious code at appropriate locations within organizational information systems.

- Monitor information system security alerts and advisories and take appropriate actions in response.

SECURITY DESIGN PRINCIPLES

- Despite years of research and development, it has not been possible to develop security design and implementation techniques that systematically exclude security flaws and prevent all unauthorized actions. In the absence of such foolproof (reliable) techniques, it is useful to have a set of widely agreed design principles that can guide the development of protection mechanisms.
- The National Centers of Academic Excellence (NCAE) in Information Assurance/Cyber Defense, which is jointly sponsored by the U.S. National Security Agency and the U. S. Department of Homeland Security, list the following as fundamental security design principles [NCAE13]:
- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design

- Separation of privilege
- Least privilege
- Least common mechanism
- Psychological acceptability
- Isolation
- Encapsulation
- Modularity
- Layering
- Least astonishment

- **Economy of mechanism:**

- It means that the design of security measures embodied in both hardware and software should be as simple and small as possible. The motivation for this principle is that relatively simple, small design is easier to test and verify thoroughly.

- With a complex design, there are many more opportunities for an adversary to discover subtle weaknesses to exploit that may be difficult to spot ahead of time.

- **Fail-safe default:**

- It means that access decisions should be based on permission rather than exclusion (barring). That is, the default situation is lack of access, and the protection scheme identifies conditions under which access is permitted.

- **Complete mediation:**

- It means that every access must be checked against the access control mechanism. Systems should not rely on access decisions retrieved from a cache. In a system designed to operate continuously, this principle requires that, if access decisions are remembered for future use, careful consideration be given to how changes in authority are propagated into such local memories.

- To fully implement complete mediation, every time a user reads a field or record in a file, or a data item in a database, the system must exercise access control. This resource-intensive approach is rarely used.

- **Open design:**

- It means that the design of a security mechanism should be open rather than secret. For example, although encryption keys must be secret, encryption algorithms should be open to public scrutiny. The algorithms can then be reviewed by many experts, and users can therefore have high confidence in them.

- **Separation of privilege:**

- It is defined in [SALT75] as a practice in which multiple privilege attributes are required to achieve access to a restricted resource. A good example of this is multifactor user authentication, which requires the use of multiple techniques, such as a password and a smart card, to authorize a user.

- **Least Privilege:**

- It means that every process and every user of the system should operate using the least set of privileges necessary to perform the task.
- A good example of the use of this principle is role-based access control. The system security policy can identify and define the various roles of users or processes. Each role is assigned only those permissions needed to perform its functions. Each permissions specifies a permitted access to a particular resource such as read and write access to a specified file or directory, and connect access to a given host and port etc.

- **Least common mechanism:**

- It means that the design should minimize the functions shared by different users, providing mutual security. This principle helps reduce the number of unintended communication paths and reduces the amount of hardware and software on which all users depend, thus making it easier to verify if there are any undesirable security implications.

- **Psychological acceptability:**

- It implies that the security mechanisms should not interfere unduly (more than is necessary) with the work of users, while at the same time meeting the needs of those who authorize access. If security mechanisms hinder (hamper) the usability or accessibility of resources, users may opt (go for) to turn off those mechanisms. Where possible, security mechanisms should be transparent to the users of the system or at most introduce minimal obstruction.

- **Isolation:**

- It is a principle that applies in three contexts.
- First, public access systems should be isolated from critical resources (data, processes, etc.) to prevent disclosure or tampering (interfere).
- Second, the processes and files of individual users should be isolated from one another except where it is explicitly desired.
- Finally, security mechanisms should be isolated in the sense of preventing access to those mechanisms. For example, logical access control may provide a means of isolating cryptographic software from other parts of the host system and for protecting cryptographic software from tampering and the keys from replacement or disclosure.

- **Encapsulation:**

- It can be viewed as a specific form of isolation based on object oriented functionality. Protection is provided by encapsulating a collection of procedures and data objects in a domain of its own so that the internal structure of a data object is accessible only to the procedures of the protected subsystem and the procedures may be called only at designated domain entry points.

- **Modularity:**

- In the context of security refers to the development of security functions as separate, protected modules and to the use of a modular architecture for mechanism design and implementation. With respect to the use of separate security modules, the design goal here is to provide common security functions and services, such as cryptographic functions, as common modules.

- For example, numerous protocols and applications make use of cryptographic functions. Rather than implementing such functions in each protocol or application, a more secure design is provided by developing a common cryptographic module that can be invoked by numerous protocols and applications. The design and implementation effort can then focus on the secure design and implementation of a single cryptographic module, including mechanisms to protect the module from tampering.

- **Layering:**

- It refers to the use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems. By using multiple, overlapping protection approaches, the failure or circumvention of any individual protection approach will not leave the system unprotected. A layering approach is often used to provide multiple barriers between an adversary and protected information or services. This technique is often referred to as defense in depth.

- **Least astonishment (Surprising):**

- It means that a program or user interface should always respond in the way that is least likely to astonish the user. For example, the mechanism for authorization should be transparent enough to a user that the user has a good intuitive (feelings, vibes) understanding of how the security goals map to the provided security mechanism.

ATTACK SURFACES AND ATTACK TREES

Attack Surfaces

- An attack surface consists of the reachable and exploitable vulnerabilities in a system.
- Examples of attack surfaces are the following:
- Open ports on outward facing Web and other servers, and code listening on those ports
- Services available on the inside of a firewall
- Code that processes incoming data, email, XML, office documents, and industry specific custom data exchange formats
- Interfaces, SQL, and Web forms
- An employee with access to sensitive information vulnerable to a social engineering attack

(Social engineering is the term used for a broad range of malicious activities accomplished through human interactions.)

- Attack surfaces can be categorized in the following way:
- **Network attack surface**: This category refers to vulnerabilities over an enterprise network, wide-area network, or the Internet. Included in this category are network protocol vulnerabilities, such as those used for a denial-of-service attack, disruption of communications links, and various forms of intruder attacks.
- **Software attack surface**: This refers to vulnerabilities in application, utility, or operating system code. A particular focus in this category is Web server software.
- **Human attack surface:** This category refers to vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders.

- An attack surface analysis is a useful technique for assessing the scale and severity of threats to a system. A systematic analysis of points of vulnerability makes developers and security analysts aware of where security mechanisms are required. Once an attack surface is defined, designers may be able to find ways to make the surface smaller, thus making the task of the adversary more difficult. The attack surface also provides guidance on setting priorities for testing, strengthening security measures, or modifying the service or application.
- As illustrated in Figure the use of layering, or defense in depth, and attack surface reduction complement each other in mitigating security risk.

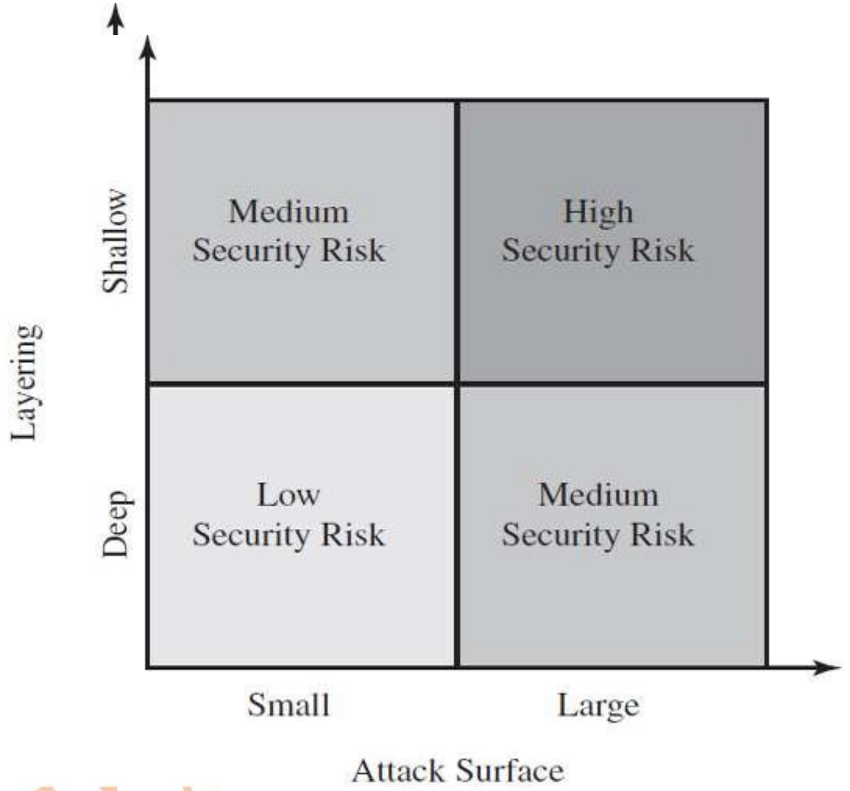


Fig: Defense in Depth and Attack Surface

- **Attack Trees**
- An attack tree is a branching, hierarchical data structure that represents a set of potential techniques for exploiting security vulnerabilities.
- The security incident that is the goal of the attack is represented as the root node of the tree, and the ways that an attacker could reach that goal are iteratively and incrementally represented as branches and subnodes of the tree. Each subnode defines a subgoal, and each subgoal may have its own set of further subgoals, etc. The final nodes on the paths outward from the root, i.e., the leaf nodes, represent different ways to initiate an attack.
- Each node other than a leaf is either an AND-node or an OR-node. To achieve the goal represented by an AND-node, the subgoals represented by all of that node’s subnodes must be achieved; and for an OR-node, at least one of the subgoals must be achieved. Branches can be labeled with values representing difficulty, cost, or other attack attributes, so that alternative attacks can be compared.

- Figure below is an example of an attack tree analysis for an Internet banking authentication application. The root of the tree is the objective of the attacker, which is to compromise a users account. The shaded boxes on the tree are the leaf nodes, which represent events that comprise the attacks. The white boxes are categories which consist of one or more specific attack events (leaf nodes). Note that in this tree, all the nodes other than leaf nodes are OR-nodes.
- The analysis used to generate this tree considered the three components involved in authentications:
- **User terminal and user (UT/U):** These attacks target the user equipment, including the tokens that may be involved, such as smartcards or other password generators, as well as the actions of the user.
- **Communications channel (CC):** This type of attack focuses on communication links.
- **Internet banking server (IBS):** These types of attacks are offline attack against the servers that host the Internet banking application.

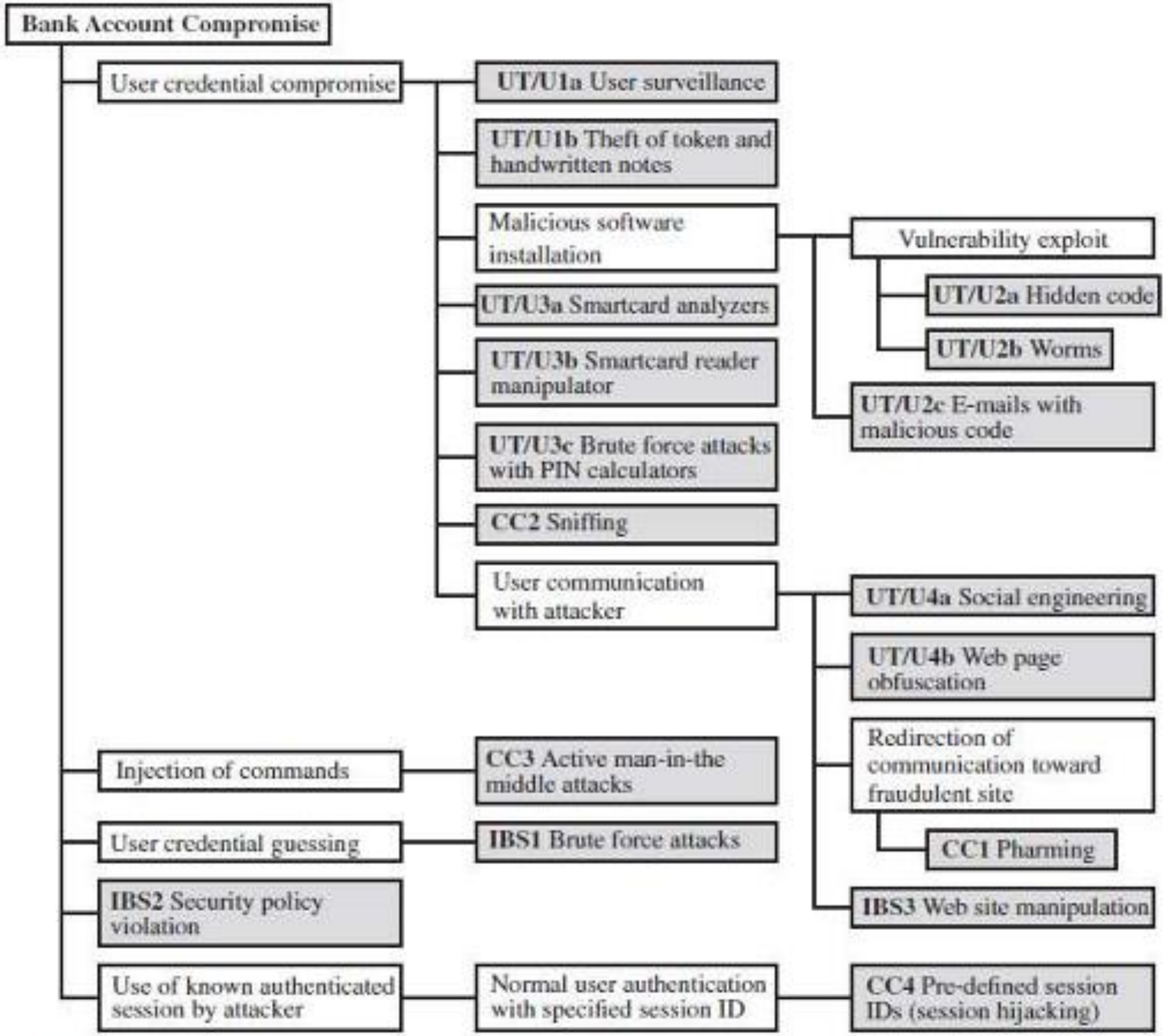

Bank Account Compromise
User credential compromise
UT/U1a User surveillance
UT/U1b Theft of token and handwritten notes
Malicious software installation
Vulnerability exploit
UT/U2a Hidden code
UT/U2b Worms
UT/U2c E-mails with malicious code
UT/U3a Smartcard analyzers
UT/U3b Smartcard reader manipulator
UT/U3c Brute force attacks with PIN calculators
CC2 Sniffing
User communication with attacker
UT/U4a Social engineering
UT/U4b Web page obfuscation
Redirection of communication toward fraudulent site
CC1 Pharming
IBS3 Web site manipulation
Injection of commands
CC3 Active man-in-the middle attacks
User credential guessing
IBS1 Brute force attacks
IBS2 Security policy violation
Use of known authenticated session by attacker
Normal user authentication with specified session ID
CC4 Pre-defined session IDs (session hijacking)

Fig: An Attack Tree for Internet Banking Authentication

- Five overall attack strategies can be identified, each of which exploits one or more of the three components. The five strategies are as follows:
- **User credential compromise:** This strategy can be used against many elements of the attack surface. There are procedural attacks, such as monitoring a user's action to observe a PIN or other credential, or theft of the user's token or handwritten notes. An adversary may also compromise token information using a variety of token attack tools, such as hacking the smartcard or using a brute force approach to guess the PIN. Another possible strategy is to embed malicious software to compromise the user's login and password. An adversary may also attempt to obtain credential information via the communication channel (sniffing). Finally, an adversary may use various means to engage in communication with the target user.
- **Injection of commands:**

- In this type of attack, the attacker is able to intercept communication between the UT and the IBS. Various schemes can be used to be able to impersonate the valid user and so gain access to the banking system.

- **User credential guessing:**

- The brute force attacks against some banking authentication schemes are feasible by sending random usernames and passwords. The attack mechanism is based on distributed zombie personal computers, hosting automated programs for username- or password-based calculation.

- **Security policy violation:**

- For example, violating the bank's security policy in combination with weak access control and logging mechanisms, an employee may cause an internal security incident and expose a customer's account.

- **Use of known authenticated session:**

- This type of attack persuades or forces the user to connect to the IBS with a preset session ID. Once the user authenticates to the server, the attacker may utilize the known session ID to send packets to the IBS, spoofing the user's identity.

- Above Figure provides a thorough view of the different types of attacks on an Internet banking authentication application. Using this tree as a starting point, security analysts can assess the risk of each attack and, using the design principles outlined in the preceding section, design a comprehensive security facility.

COMPUTER SECURITY STRATEGY

- A computer security strategy is a plan that involves selecting and implementing best practices to protect a computer system of a business organization from internal and external threats. This strategy also establishes a baseline for a company’s security program which allows it to continuously adapt to emerging threats and risks.
- A comprehensive security strategy involves three aspects:
- **Specification/policy:** What is the security scheme supposed to do?
- **Implementation/mechanisms:** How does it do?
- **Correctness/assurance:** Does it really work?

- **Security Policy:** The first step in devising security services and mechanisms is to develop a security policy. A security policy is an informal description of desired system behavior. Such informal policies may reference requirements for security, integrity, and availability. More usefully, a security policy is a formal statement of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.
- In developing a security policy, a security manager needs to consider the following factors:

- The value of the assets being protected
- The vulnerabilities of the system
- Potential threats and the likelihood of attacks.

- Further, the manager must consider the following trade-offs:
- **Ease of use versus security:**

- Virtually all security measures involve some penalty in the area of ease of use.
- The following are some examples
- Access control mechanisms require users to remember passwords and perhaps perform other access control actions.
- Firewalls and other network security measures may reduce available transmission capacity or slow response time.
- Virus-checking software reduces available processing power and introduces the possibility of system crashes or malfunctions due to improper interaction between the security software and the operating system.

- **Cost of security versus cost of failure and recovery:**
- In addition to ease of use and performance costs, there are direct monetary costs in implementing and maintaining security measures. All of these costs must be balanced against the cost of security failure and recovery if certain security measures are lacking. The cost of security failure and recovery must take into account not only the value of the assets being protected and the damages resulting from a security violation, but also the risk, which is the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
- Security policy is thus a business decision, possibly influenced by legal requirements.

- **Security Implementation:**
- Security implementation involves four complementary courses of action:
- **Prevention:** An ideal security scheme is one in which no attack is successful. Although this is not practical in all cases, there is a wide range of threats in which prevention is a reasonable goal. For example, consider the transmission of encrypted data. If a secure encryption algorithm is used, and if measures are in place to prevent unauthorized access to encryption keys, then attacks on confidentiality of the transmitted data will be prevented.
- **Detection:** In a number of cases, absolute protection is not feasible, but it is practical to detect security attacks. For example, there is intrusion detection systems designed to detect the presence of unauthorized individuals logged onto a system.

- **Response:** If security mechanisms detect an ongoing attack, such as a denial of service attack, the system may be able to respond in such a way as to halt the attack and prevent further damage.
- **Recovery:** An example of recovery is the use of backup systems, so that if data integrity is compromised, a prior, correct copy of the data can be reloaded.

- **Assurance and Evaluation**
- **Assurance** is the degree of confidence one has that the security measures, both technical and operational, work as intended to protect the system and the information it processes. This encompasses both system design and system implementation. Thus, assurance deals with the questions, “Does the security system design meet its requirements?” and “Does the security system implementation meet its specifications?”
- **Evaluation** is the process of examining a computer product or system with respect to certain criteria. Evaluation involves testing and may also involve formal analytic or mathematical techniques. The central thrust of work in this area is the development of evaluation criteria that can be applied to any security system (encompassing security services and mechanisms) and that are broadly supported for making product comparisons.

ACCESS CONTROL PRINCIPLES

- Access Control involves:

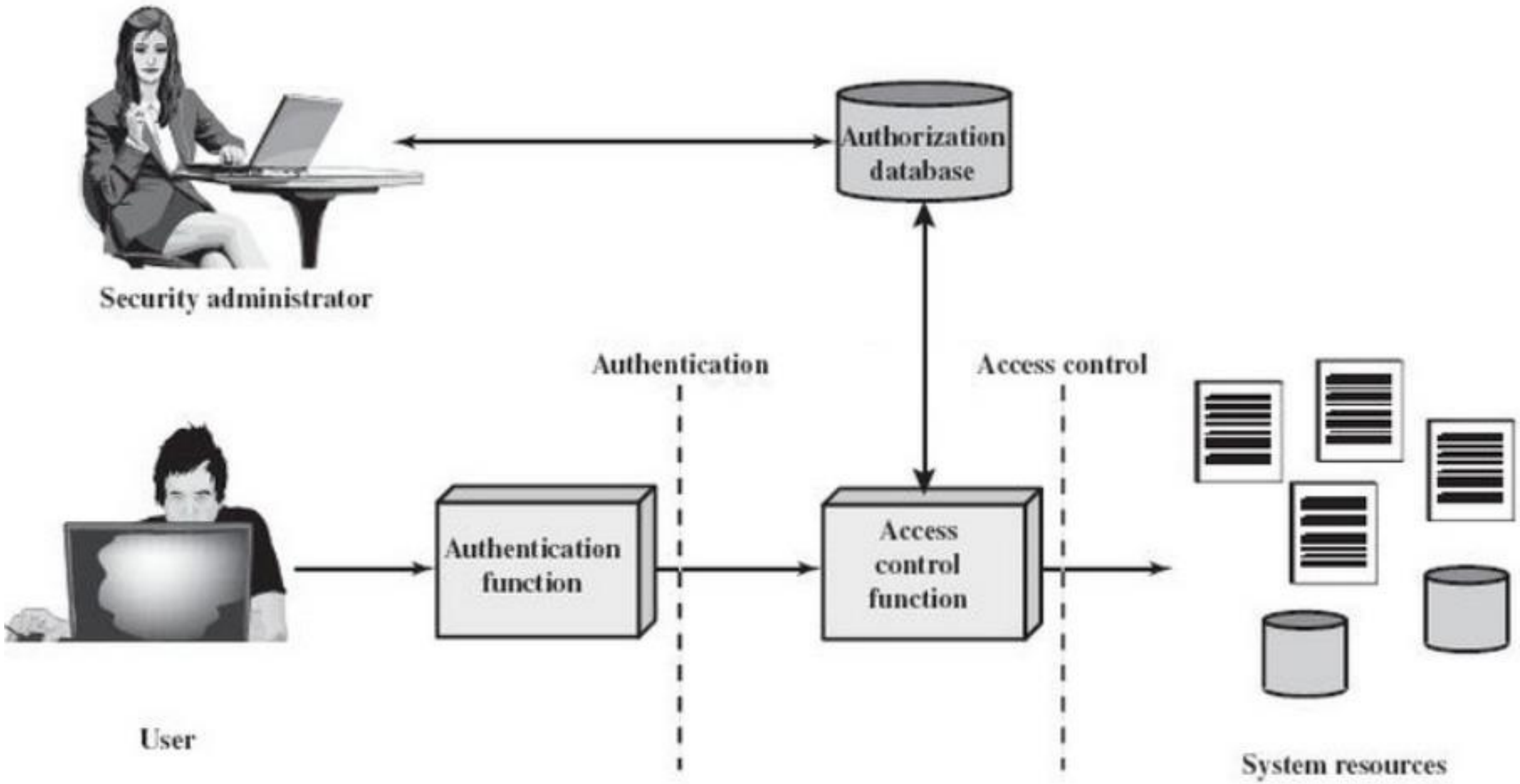
– Preventing unauthorized users from gaining access to resources (deals more with authentication)

– Preventing legitimate users from accessing resources in an unauthorized manner

– Enabling legitimate users to access resources in an authorized manner.

– Access control implements a security policy that specifies who or what (e.g. process may have access to each specific system resource and the type of access that is permitted in each instance.

- Access control deals with subjects, objects and access rights.


Security administrator
Authorization database
Authentication
Access control
User
Authentication function
Access control function
System resources

- **Basic Elements of Access Control**
- **Subject:** An entity capable of accessing objects.

– Subject typically represents a process (the process takes on the attributes, such as access rights, of the user or application)

• **Owner:** creator of a resource

• **Group:** group of users; membership in the group is sufficient for certain access rights

• **World:** Users who are not included in the categories of owner and group may be able to access the resources with limited permissions.

- **Object:** Resource to which access is controlled.

– An entity that contains and/or receives information.

– E.g.: Records, blocks, pages, segments, files, directories, messages, programs, etc.

- **Access right**: describes the way in which a subject may access an object:

– Read (incl. copy or print); Write (incl. read access; add, modify or delete); Execute; Delete; Create; Search (list the files in a directory or search the directory)

- **Access Control Principles**

- ***Principle of Least Privilege*****:** States that if nothing has been specifically configured for an individual or the groups, he/she belongs to, the user should not be able to access that resource i.e.Default no access

- ***Separation of Duties*****:** Separating any conflicting areas of responsibility so as to reduce opportunities for unauthorized or unintentional modification or misuse of organizational assets and/or information.

- ***Need to know*****:** It is based on the concept that individuals should be given access only to the information that they absolutely require in order to perform their job duties.

TYPES OF ACCESS CONTROL

- A security policy may use two types of access controls, alone or in combination.
- In one, access control is left to the discretion of the owner.
- In the other, the operating system controls access, and the owner cannot override the controls.

1. **Discretionary Access Control (DAC) or Identity Based Access Control (IBAC):**

- Individual user sets access control mechanism to allow or deny access to an object.
- Discretionary access controls base access rights on the identity of the subject and the identity of the object involved.
- Identity is the key; the owner of the object constrains who can access it by allowing only particular subjects to have access.
- The owner states the constraint in terms of the identity of the subject, or the owner of the subject

2. Mandatory Access Control (MAC) or Rule Based Access Control:

- System mechanism controls access to object, and individual cannot alter that access based on rule.
- The operating system enforces mandatory access controls.
- Neither the subject nor the owner of the object can determine whether access is granted.
- Typically, the system mechanism will check information associated with both the subject and the object to determine whether the subject should access the object.
- Rules describe the conditions under which access is allowed.

3. Originator Access Control (ORCON or ORGCON):

- Controlled by originator (creator) of information controls who can access information.
- The goal of this control is to allow the originator of the file (or of the information it contains) to control the dissemination of the information.
- The owner of the file has no control over who may access the file.

4. Role Based Access Control:

- The ability, or need, to access information may depend on one's job functions
- A role is a collection of job functions
- is an approach to restricting system access to authorized users

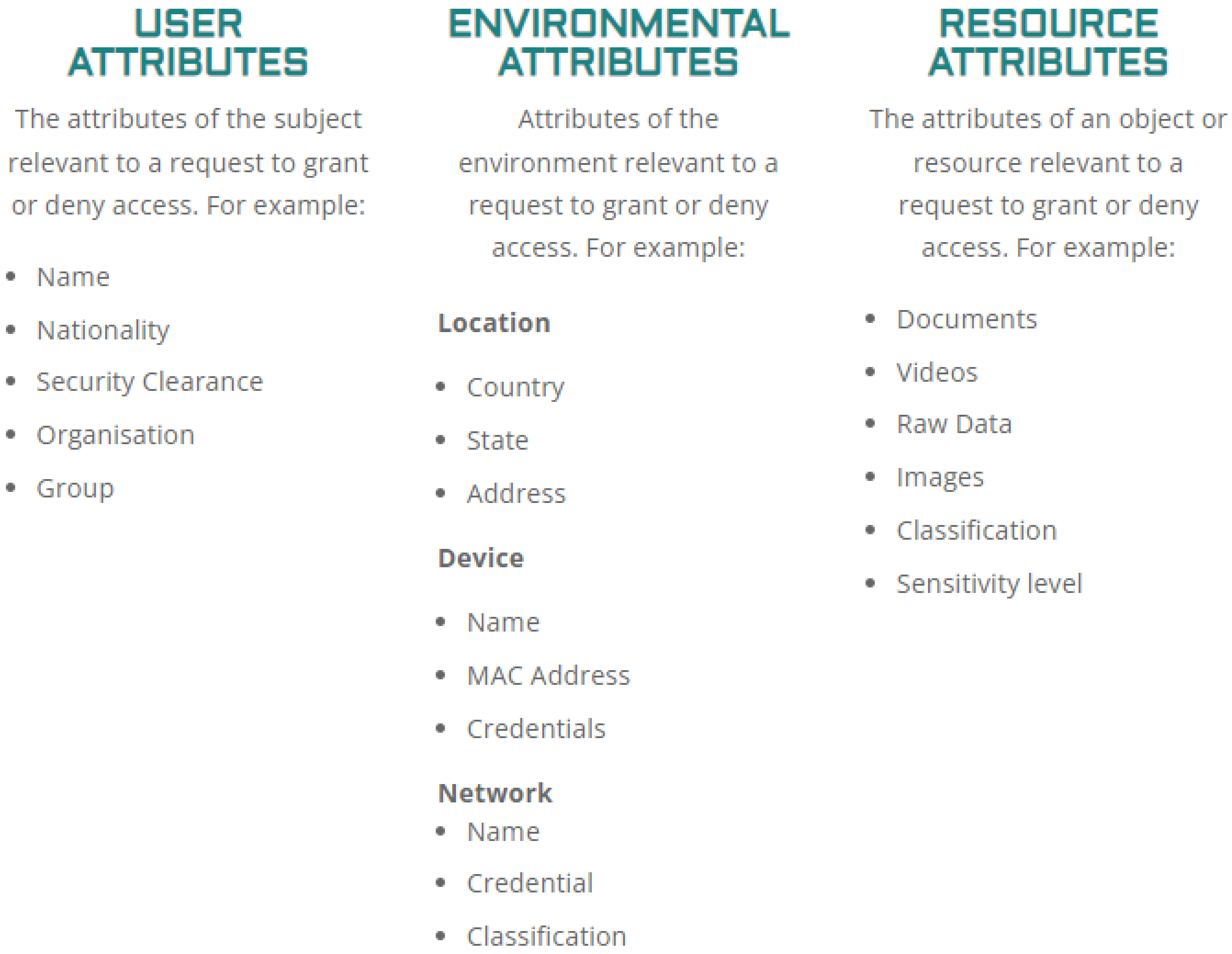
ATTRIBUTE-BASED ACCESS CONTROL (ABAC)

- Attribute-based access control (ABAC) is a security model that aims to control access to information by defining policies that dictate who can access information and under what circumstances.
- In ABAC, policies are created based on attributes such as user credentials, environment, and resource properties. By controlling access to information, the right people can access the right information at the right time.
- The ABAC methodology enables more flexible and precise control over user access than the traditional Role Based Access model. ABAC’s ability to determine a user’s access rights to infrastructure, data, or resources after initial authentication is called fine-grained access control.

- **How attribute-based access control works**
- ABAC grants permissions according to who a user is rather than what they do, which allows for granular controls. Attributes are analyzed to assess how they interact in an environment; then, rules are enforced based on relationships.
- Here is how the process typically works:

1. An access request is made.
2. The attribute-based access control tool scans attributes to determine if they match existing policies.
3. Based on the result of the ABAC tool’s analysis, permission is granted or denied.

- Attributes are the characteristics or values of a component involved in an access event. With ABAC, security is built around the combination of different attributes, including user attributes (subject), environmental attributes and resource attributes (object). ABAC enables more precise access control with flexible policies that can accommodate multiple attribute combinations that are only limited by the available attributes.



USER ATTRIBUTES

The attributes of the subject relevant to a request to grant or deny access. For example:

- Name
- Nationality
- Security Clearance
- Organisation
- Group

ENVIRONMENTAL ATTRIBUTES

Attributes of the environment relevant to a request to grant or deny access. For example:

Location

- Country
- State
- Address

Device

- Name
- MAC Address
- Credentials

Network

- Name
- Credential
- Classification

RESOURCE ATTRIBUTES

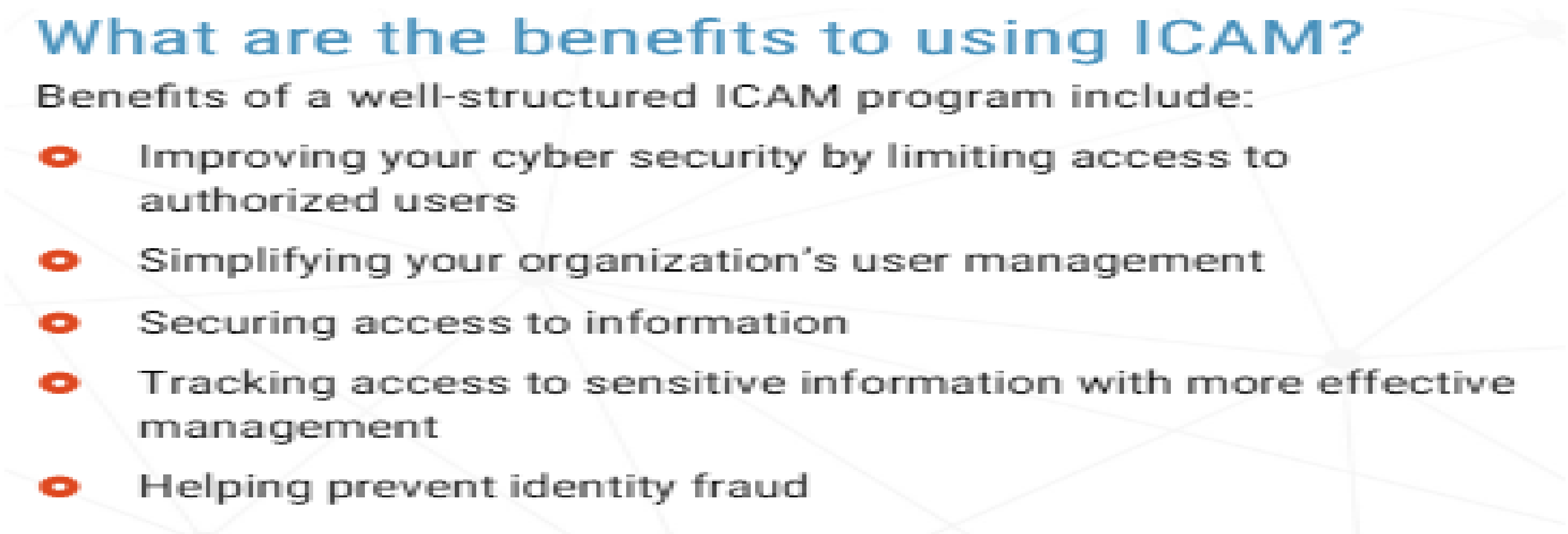
The attributes of an object or resource relevant to a request to grant or deny access. For example:

- Documents
- Videos
- Raw Data
- Images
- Classification
- Sensitivity level

IDENTITY, CREDENTIAL AND ACCESS MANAGEMENT

- Identity, Credential, and Access Management (ICAM) is a framework of policies, programs, and technologies used to create and manage digital identities, credentials and access controls to protect an organization’s digital assets and systems. This framework can help government agencies and private sector organizations reduce the risk of cyber attacks by ensuring that the right person is accessing the right information at the right time for the right reason.
- ICAM covers three fundamental aspects that protect sensitive information systems and ensure compliance with regulatory requirements. They include:

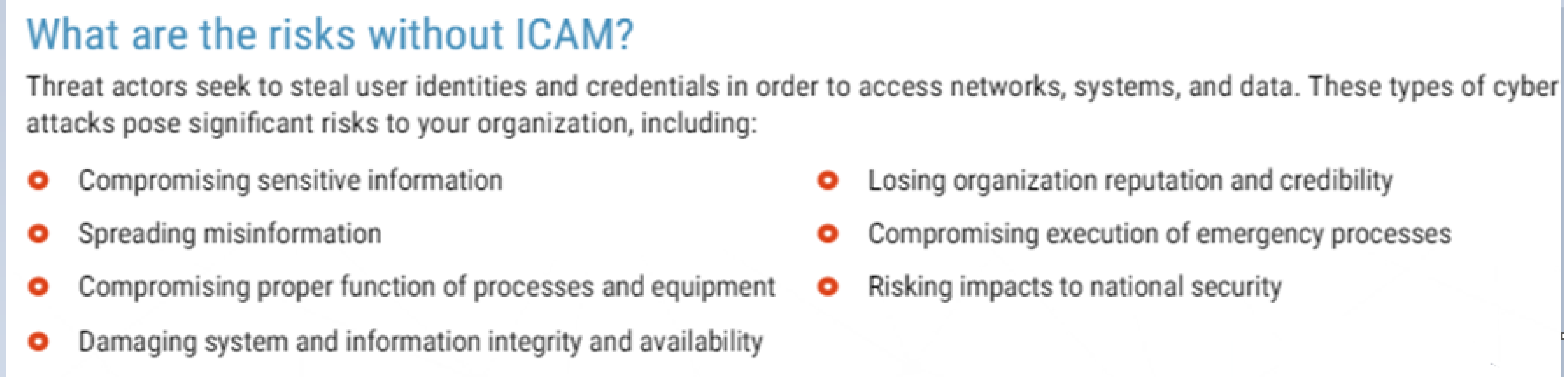
1. **Identity Management** – the processes and technologies used to identify, authenticate, and manage subjects in a system, including verifying users’ identities, devices, or procedures when connecting to a network.
2. **Credential Management** – the creation, distribution, and lifecycle management of credentials used for authentication. Credentials are proof of identity, often in the form of passwords, cryptographic keys, biometrics, or tokens.
3. **Access Management** – the control and management of access to networks, systems, applications, functions, and data. Access controls determine who or what is allowed to view or use resources based on their identity and authentication status.



What are the benefits to using ICAM?

Benefits of a well-structured ICAM program include:

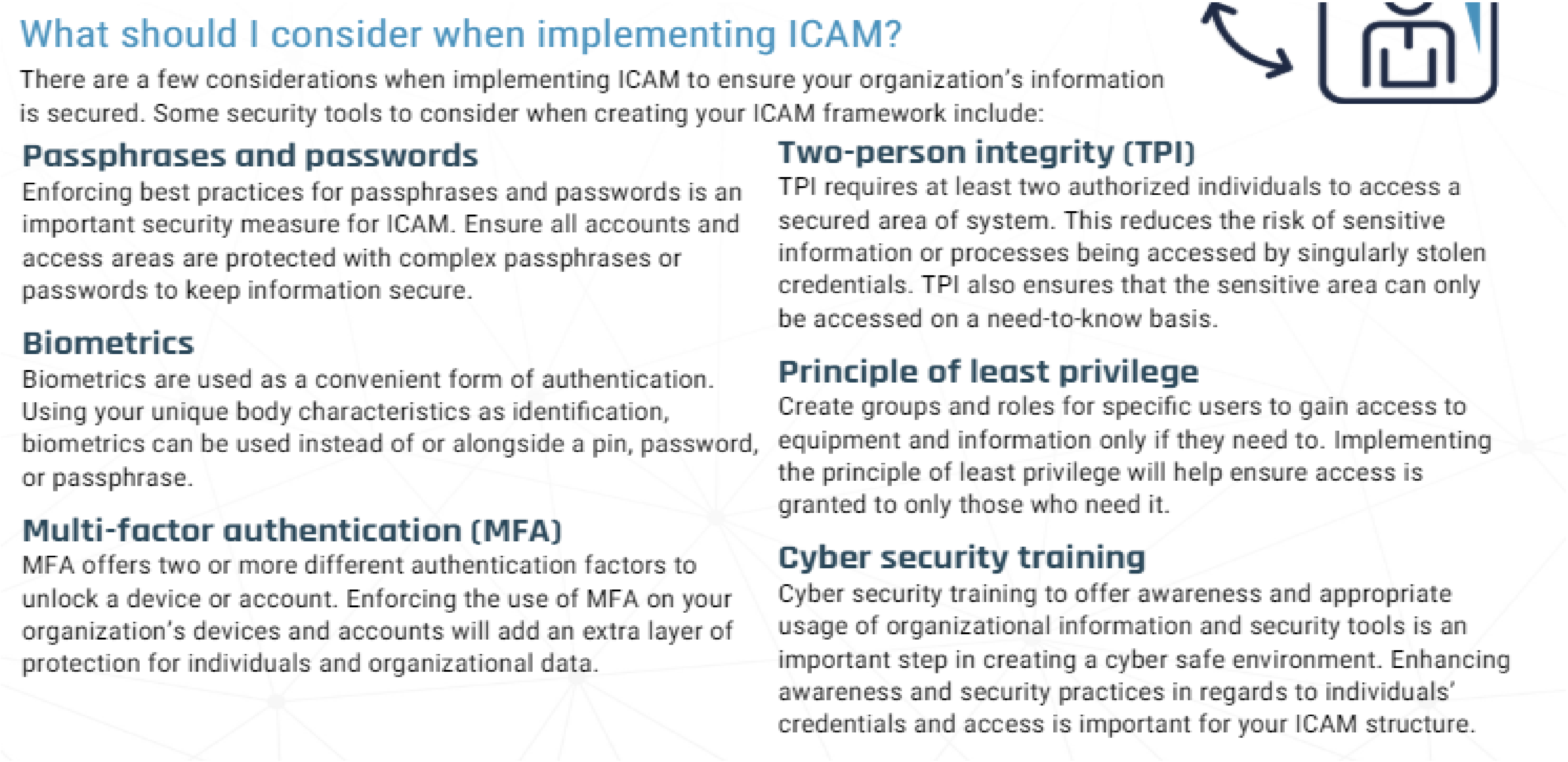
- Improving your cyber security by limiting access to authorized users
- Simplifying your organization's user management
- Securing access to information
- Tracking access to sensitive information with more effective management
- Helping prevent identity fraud



What are the risks without ICAM?

Threat actors seek to steal user identities and credentials in order to access networks, systems, and data. These types of cyber attacks pose significant risks to your organization, including:

- Compromising sensitive information
- Spreading misinformation
- Compromising proper function of processes and equipment
- Damaging system and information integrity and availability
- Losing organization reputation and credibility
- Compromising execution of emergency processes
- Risking impacts to national security



What should I consider when implementing ICAM?

There are a few considerations when implementing ICAM to ensure your organization’s information is secured. Some security tools to consider when creating your ICAM framework include:

Passphrases and passwords

Enforcing best practices for passphrases and passwords is an important security measure for ICAM. Ensure all accounts and access areas are protected with complex passphrases or passwords to keep information secure.

Biometrics

Biometrics are used as a convenient form of authentication. Using your unique body characteristics as identification, biometrics can be used instead of or alongside a pin, password, or passphrase.

Multi-factor authentication (MFA)

MFA offers two or more different authentication factors to unlock a device or account. Enforcing the use of MFA on your organization’s devices and accounts will add an extra layer of protection for individuals and organizational data.

Two-person integrity (TPI)

TPI requires at least two authorized individuals to access a secured area of system. This reduces the risk of sensitive information or processes being accessed by singularly stolen credentials. TPI also ensures that the sensitive area can only be accessed on a need-to-know basis.

Principle of least privilege

Create groups and roles for specific users to gain access to equipment and information only if they need to. Implementing the principle of least privilege will help ensure access is granted to only those who need it.

Cyber security training

Cyber security training to offer awareness and appropriate usage of organizational information and security tools is an important step in creating a cyber safe environment. Enhancing awareness and security practices in regards to individuals’ credentials and access is important for your ICAM structure.

TRUST FRAMEWORKS

- The interrelated concepts of trust, identity, and attributes have become core concerns of Internet businesses, network service providers, and large enterprises. These concerns can clearly be seen in the e-commerce setting. For efficiency, privacy, and legal simplicity, parties to transactions generally apply the need to know principle:
- What do you need to know about someone in order to deal with them? The answer varies from case to case, and includes such attributes as professional registration or license number, organization and department, staff ID, security clearance, customer reference number, credit card number, unique health identifier, allergies, blood type, social security number, address, citizenship status, social networking handle, pseudonym, and so on. The attributes of an individual that must be known and verified to permit a transaction depend on context.
- The same concern for attributes is increasingly important for all types of access control situations, not just the e-business context. For example, an enterprise may need to provide access to resources for customers, users, suppliers, and partners. Depending on context, access will be determined not just by identity but by the attributes of the requestor and the resource

- ***Traditional Identity Exchange Approach***
- Online or network transactions involving parties from different organizations, or between an organization and an individual user such as an online customer, generally require the sharing of identity information. This information may include a host of associated attributes in addition to a simple name or numerical identifier. Both the party disclosing the information and the party receiving the information need to have a level of trust about security and privacy issues related to that information.

- Following figure shows the traditional technique for the exchange of identity information. This involves users developing arrangements with an identity service provider to procure digital identity and credentials, and arrangements with parties that provide end-user services and applications and that are willing to rely on the identity and credential information generated by the identity service provider.

The arrangement of above figure must meet a number of requirements. The relying party requires that the user has been authenticated to some degree of assurance, that the attributes imputed to the user by the identity service provider are accurate, and that the identity service provider is authoritative for those attributes. The identity service provider requires assurance that it has accurate information about the user and that, if it shares information, the relying party will use it in accordance with contractual terms and conditions and the law.

The user requires assurance that the identity service provider and relying party can be entrusted with sensitive information and that they will abide by the user's preferences and respect the user's privacy. Most importantly, all the parties want to know if the practices described by the other parties are actually those implemented by the parties, and how reliable those parties are.

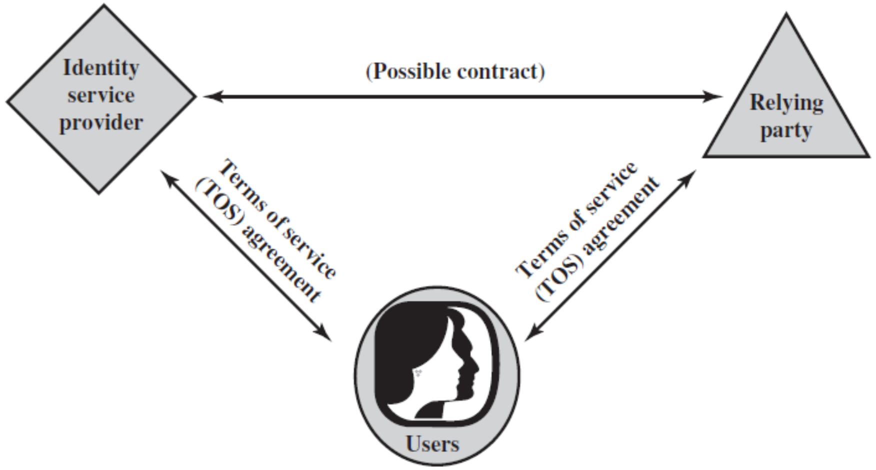
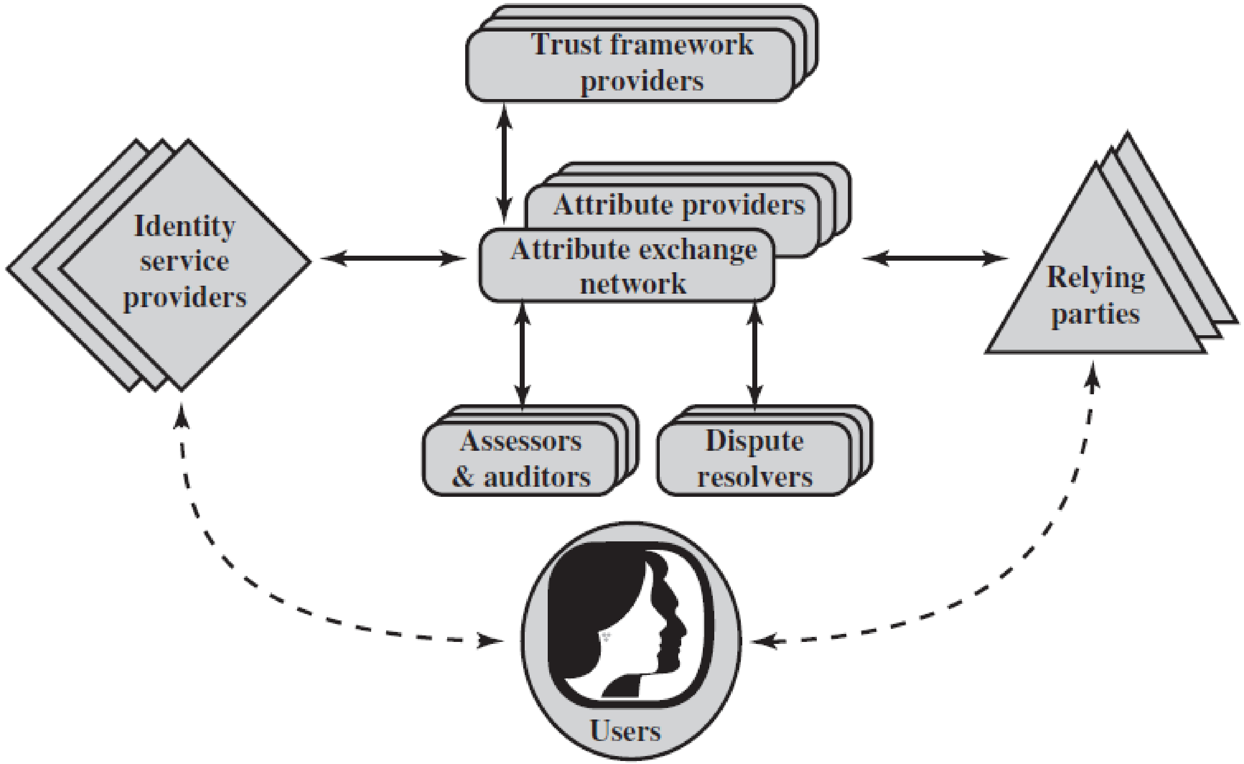

Identity service provider
(Possible contract)
Relying party
Terms of service (TOS) agreement
Terms of service (TOS) agreement
Users

Fig: Traditional triangle of parties involved in an exchange of identity information

- ***<u>Open Identity Trust Framework:</u>***
- Without some universal standard and framework, the arrangement of above figure must be replicated in multiple contexts. A far preferable approach is to develop an open, standardized approach to trustworthy identity and attribute exchange.


Trust framework providers
Identity service providers
Attribute providers
Attribute exchange network
Relying parties
Assessors & auditors
Dispute resolvers
Users

- Above figure shows the elements involved in the OITF. Within any given organization or agency, the following roles are part of the overall framework:
- **Relying parties (RPs):** Also called service providers, these are entities delivering services to specific users. RPs must have confidence in the identities and/or attributes of their intended users, and must rely upon the various credentials presented to evince those attributes and identities.
- **Subjects:** These are users of an RP’s services, including customers, employees, trading partners, and subscribers.
- **Attribute providers (APs):** APs are entities acknowledged by the community of interest as being able to verify given attributes as presented by subjects and which are equipped through the attribute exchange network to create conformant attribute credentials according to the rules and agreements of the attribute exchange network. Some APs will be sources of authority for certain information; more commonly APs will be brokers of derived attributes.

- **Identity providers (IDPs):** These are entities able to authenticate user credentials and to vouch for the names (or pseudonyms or handles) of subjects, and which are equipped through the attribute exchange network or some other compatible Identity and Access Management (IDAM) system to create digital identities that may be used to index user attributes.
- There are also the following important support elements as part on an attribute exchange network:
- **Assessors:** Assessors evaluate identity service providers and RPs and certify that they are capable of following the OITF provider's blueprint.
- **Auditors:** These entities may be called on to check that parties' practices have been in line with what was agreed for the OITF.
- **Dispute resolvers:** These entities provide arbitration and dispute (*controversy*) resolution under OIX guidelines.
- **Trust framework providers:** A trust framework provider is an organization that translates the requirements of policymakers into an own blueprint for a trust framework that it then proceeds to build, doing so in a way that is consistent with the minimum requirements set out in the OITF specification.

THE BELL-LAPADULA MODEL

- It is based on Confidentiality Policy
- The Bell-LaPadula model is one of the first models that was created to control access to data.
- The properties of the Bell-LaPadula model are:

  - The simple security property which is —no read up

  - The star property which is —no write down.
- A problem with this model is it does not deal with the integrity of data.
- The Bell-LaPadula Model corresponds to military-style classifications.

- A confidentiality policy, also called an *information flow policy*, prevents the unauthorized disclosure of information.
- Unauthorized alteration of information is secondary.
- The simplest type of confidentiality classification is a set of *security clearances* arranged in a linear (total) ordering.
- These clearances represent sensitivity levels.
- The higher the security clearance, the more sensitive the information (and the greater the need to keep it confidential).
- A subject has a *security clearance*.

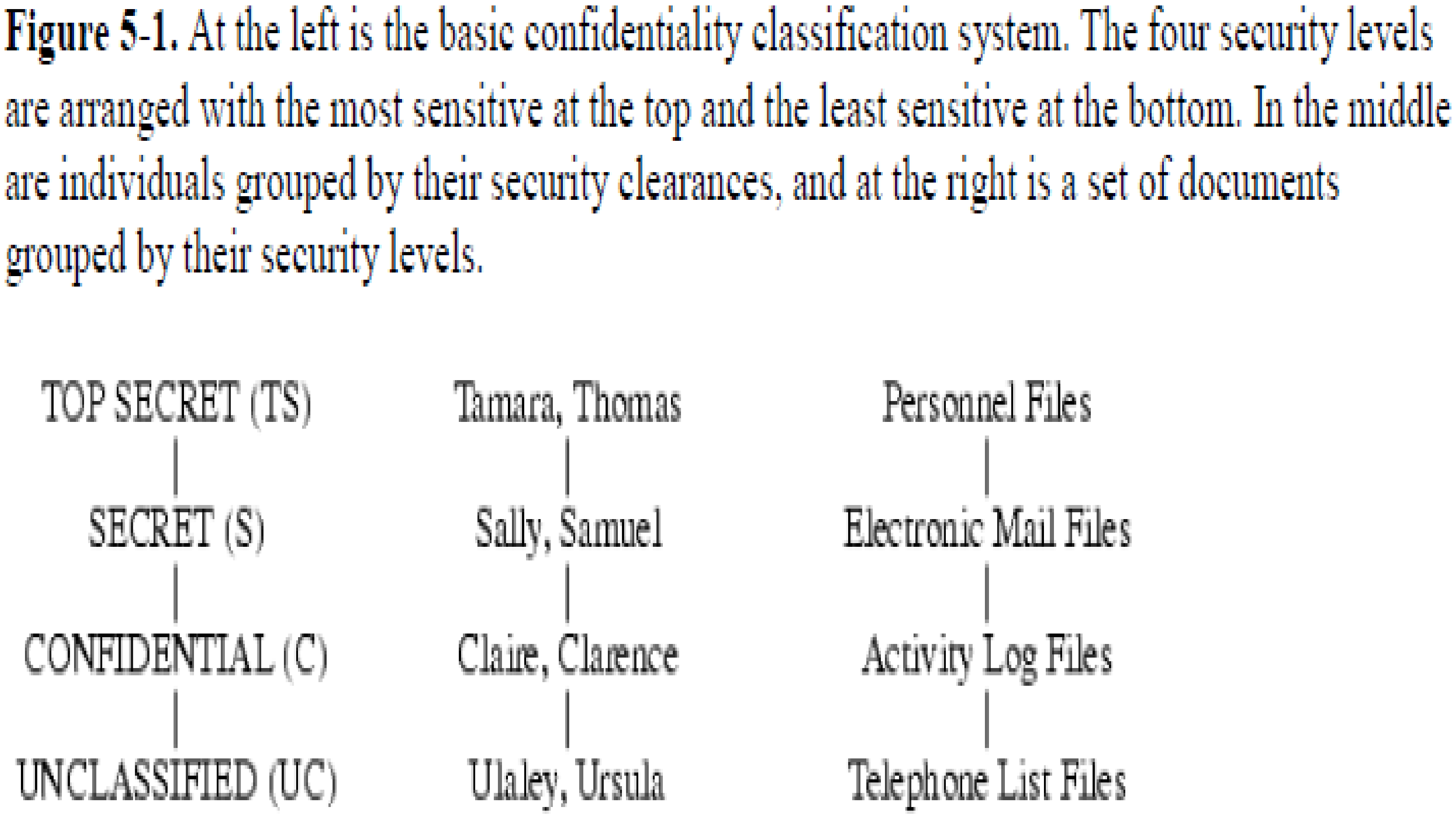


Figure 5-1. At the left is the basic confidentiality classification system. The four security levels are arranged with the most sensitive at the top and the least sensitive at the bottom. In the middle are individuals grouped by their security clearances, and at the right is a set of documents grouped by their security levels.

TOP SECRET (TS)	Tamara, Thomas	Personnel Files
SECRET (S)	Sally, Samuel	Electronic Mail Files
CONFIDENTIAL (C)	Claire, Clarence	Activity Log Files
UNCLASSIFIED (UC)	Ulaley, Ursula	Telephone List Files

- In the figure, Claire's security clearance is C (for CONFIDENTIAL), and Thomas' is TS (for TOP SECRET). An object has a security classification; the security classification of the electronic mail files is S (for SECRET), and that of the telephone list files is UC (for UNCLASSIFIED).
- The goal of the Bell-LaPadula security model is to prevent read access to objects at a security classification higher than the subject's clearance.

BIBA INTEGRITY MODEL

- In 1977, Biba studied the nature of the integrity of systems.
- The Biba security model was developed to address a weakness in the Bell-La Padula model.
- The Biba model addresses integrity which was missing in the confidentiality focused Bell-La Padula model.
- Much like the Bell-La Padula model, the Biba model uses objects and subjects.
- However, objects and subjects are grouped into integrity levels instead of given security labels.
- The Biba Model also carries a clever catch phrase: **—no read down, no write up.**

- In order to preserve integrity, subjects may create content at or below their own integrity level and view content at or above their own integrity level.
- This helps to prevent data corruption thus preserving integrity. In similar fashion to the Bell-La Padula model, the Biba model also has a couple of security rules:

- A subject at a given level of integrity must not read an object at a lower integrity level (no read down). This is known as the Simple Integrity Axiom.

- A subject at a given level of integrity must not write to any object at a higher level of integrity (no write up). This is known as the * (star) Integrity Axiom.