

IT Security

Lecture 02

LAW 614

English Language for Digital Law

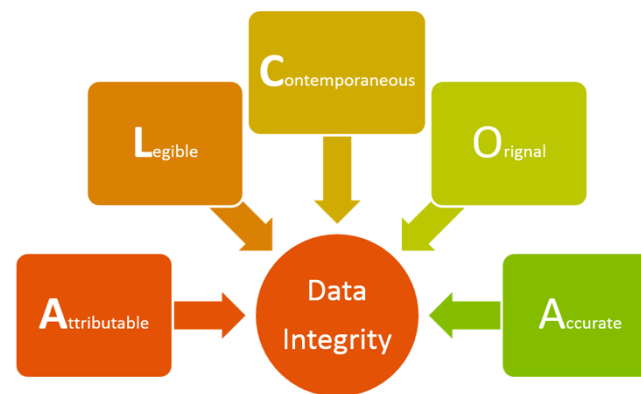
IT Security is the protection of computing systems and the data that they store or access.

IT Security rests on **confidentiality**, **integrity**, and **availability** (CIA).



1. **Confidentiality** is the concealment of information or resources. The need for keeping information secret arises from the use of computers in sensitive fields such as government and industry. For example, military and civilian institutions in the government often restrict access to information to those who need that information.

2. **Integrity** refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change. Integrity includes data integrity (the content of the information) and origin integrity (the source of the data, often called authentication).



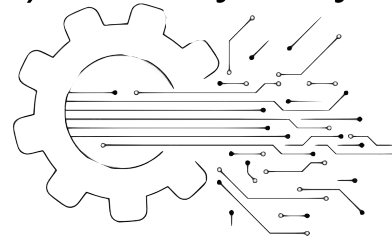
Integrity mechanisms fall into two classes: prevention mechanisms and detection mechanisms.

Prevention mechanisms seek to maintain the integrity of the data by blocking any unauthorized attempts to change the data or any attempts to change the data in unauthorized ways.

Detection mechanisms do not try to prevent violations of integrity; they simply report that the data's integrity is no longer trustworthy.



****** The mechanisms may report the actual cause of the integrity violation (a specific part of a file was altered), or they may simply report that the file is now corrupt.



Working with **integrity** is very different from working with **confidentiality**. With confidentiality, the data is either compromised or it is not, but integrity includes both the correctness and the trustworthiness of the data.

3. Availability refers to the ability to use the information or resource desired. It is an important aspect of reliability as well as of system design because an unavailable system is at least as bad as no system at all. The aspect of availability that is relevant to security is that someone may deliberately arrange to deny access to data or to a service by making it unavailable.



A threat is a potential violation of security. The violation need not actually occur for there to be a threat. The fact that the violation might occur means that those actions that could cause it to occur must be guarded against (or prepared for). Those actions are called attacks. Those who execute such actions, or cause them to be executed, are called attackers.



The three security services—confidentiality, integrity, and availability— counter threats to the security of a system.

Threats are four broad classes:

1. Disclosure, or unauthorized access to information;



2. Deception, or acceptance of false data;



3. Disruption, or interruption or prevention of correct operation; and



4. Usurpation, or unauthorized control of some part of a system.



1. Snooping, the unauthorized interception of information, is a form of disclosure. It is passive, suggesting simply that some entity is listening to (or reading) communications or browsing through files or system information.
2. Wiretapping, or passive wiretapping, is a form of snooping in which a network is monitored. Confidentiality services counter this threat.



3. Modification or alteration, an unauthorized change of information, covers three classes of threats. The goal may be deception, in which some entity relies on the modified data to determine which action to take, or in which incorrect information is accepted as correct and is released.

Unlike snooping, modification is active; it results from an entity changing information.



Active wiretapping is a form of *modification* in which data moving across a network is altered . An example is the man-in-the-middle attack, in which an intruder reads messages from the sender and sends (possibly modified) versions to the recipient, in hopes that the recipient and sender will not realize the presence of the intermediary. Integrity services counter this threat.



Examples of Threats

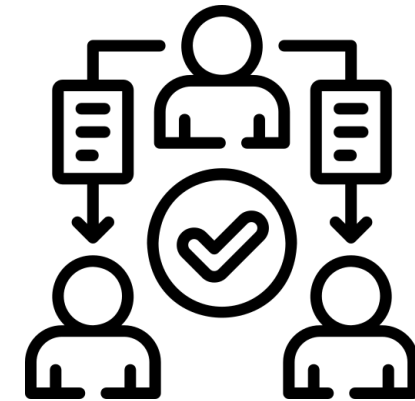
4. Masquerading or spoofing, an impersonation of one entity by another, is a form of both deception and usurpation. It lures a victim into believing that the entity with which it is communicating is a different entity.

For example, if a user tries to read a file, but an attacker has arranged for the user to be given a different file, another spoof has taken place. This may be a passive attack (in which the user does not attempt to authenticate the recipient, but merely accesses it), but

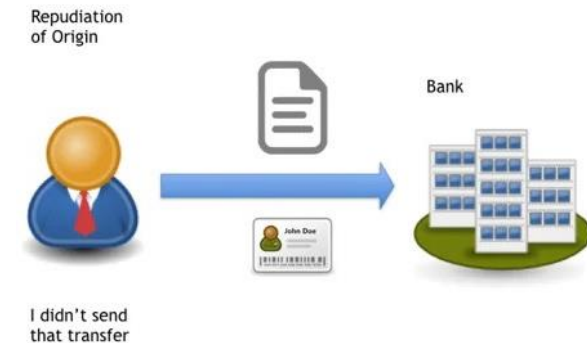


it is usually an active attack (in which the masquerader issues responses to mislead the user about its identity). Integrity services (called “authentication services” in this context) counter this threat.

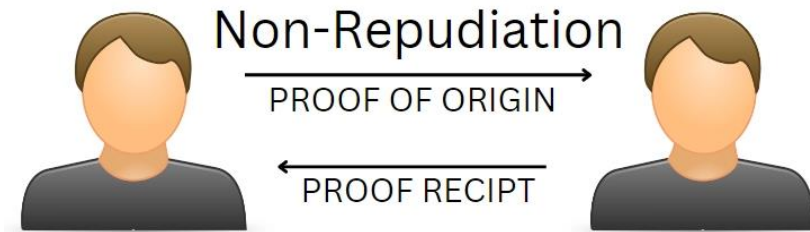
Some forms of masquerading may be allowed. Delegation occurs when one entity authorizes a second entity to perform functions on its behalf. *The distinctions between delegation and masquerading are important.*



5. *Repudiation of origin*, a false denial that an entity sent (or created) something, is a form of deception. For example, suppose a customer sends a letter to a vendor agreeing to pay a large amount of money for a product. The vendor ships the product and then demands payment. The customer denies having ordered the product and by law is therefore entitled to keep the unsolicited shipment without payment.



The customer has *repudiated the origin* of the letter. If the vendor cannot prove that the letter came from the customer, the attack succeeds. A variant of this is denial by a user that he created specific information or entities such as files. Integrity mechanisms cope with this threat.



6. *Denial of receipt*, a false denial that an entity received some information or message, is a form of deception. Suppose a customer orders an expensive product, but the vendor demands payment before shipment. The customer pays, and the vendor ships the product. The customer then asks the vendor when he will receive the product.



If the customer has already received the product, the question constitutes a denial of receipt attack. The vendor can defend against this attack only by proving that the customer did, despite his denials, receive the product. Integrity and availability mechanisms guard against these attacks.



Policy and Mechanism

A *security policy* is a statement of what is, and what is not, allowed. Policies may be presented mathematically, as a list of allowed (secure) and disallowed (nonsecure) states.



A *security mechanism* is a method, tool, or procedure for enforcing a security policy.



Mechanisms can be nontechnical, such as requiring proof of identity before changing a password; in fact, policies often require some procedural mechanisms that technology cannot enforce.



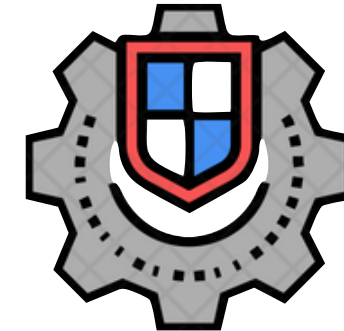
Policy and Mechanism

As an example, suppose a university's computer science laboratory has a policy that prohibits any student from copying another student's homework files. The computer system provides mechanisms for preventing others from reading a user's files. Anna fails to use these mechanisms to protect her homework files, and Bill copies them. A breach of security has occurred, because Bill has violated the security.



Goals and Security

Given a security policy's specification of “secure” and “nonsecure” actions, these security mechanisms can prevent the attack, detect the attack, or recover from the attack. The strategies may be used together or separately.



Prevention means that an attack will fail. For example, if one attempts to break into a host over the Internet and that host is not connected to the Internet, the attack has been prevented. preventative mechanisms, such as passwords (which aim to prevent unauthorized users from accessing the system)



Detection is most useful when an attack cannot be prevented, but it can also indicate the effectiveness of preventative measures. Detection mechanisms accept that an attack will occur; the goal is to determine that an attack is under way, or has occurred, and report it. The attack may be monitored, however, to provide data about its nature, severity, and results.



Recovery has two forms:

1. to stop an attack and to assess and repair any damage caused by that attack.

As an example, if the attacker deletes a file, one recovery mechanism would be to restore the file from backup tapes. In some cases, retaliation (by attacking the attacker's system or taking legal steps to hold the attacker accountable) is part of recovery.



Recovery has two forms:

2. the system continues to function correctly while an attack is under way. This type of recovery is quite difficult to implement because of the complexity of computer systems.

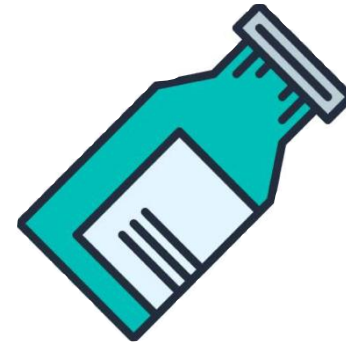
It differs from the first form of recovery, because at no point does the system function incorrectly. However, the system may disable nonessential functionality. Of course, this type of recovery is often implemented in a weaker form whereby the system detects incorrect functioning automatically and then corrects (or attempts to correct) the error.

Assurance:

Trust cannot be quantified precisely. System specification, design, and implementation can provide a basis for determining “how much” to trust a system. This aspect of trust is called assurance. It is an attempt to provide a basis for bolstering (or substantiating or specifying) how much one can trust a system.



EXAMPLE: In the United States, aspirin from a nationally known and reputable manufacturer, delivered to the drugstore in a safety-sealed container, and sold with the seal still in place, is considered trustworthy by most people. The bases for that trust are as follows:



- The testing and certification of the drug (aspirin) by the Food and Drug Administration. The FDA has jurisdiction over many types of medicines and allows medicines to be marketed only if they meet certain clinical standards of usefulness.
- The manufacturing standards of the company and the precautions it takes to ensure that the drug is not poisoned. National and state regulatory commissions and groups ensure that the manufacture of the drug meets specific acceptable standards.

Goals and Security

- The safety seal on the bottle. To insert dangerous chemicals into a safety-sealed bottle without damaging the seal is very difficult.

The three technologies (certification, manufacturing standards, and preventative sealing) provide some degree of assurance that the aspirin is not contaminated. The degree of trust the purchaser has in the purity of the aspirin is a result of these three processes.

Assurance in the computer world is similar. It requires specific steps to ensure that the computer will function properly. The sequence of steps includes (1) detailed specifications of the desired (or undesirable) behavior; (2) an analysis of the design of the hardware, software, and other components to show that the system will not violate the specifications; (3) and arguments or proofs that the implementation, operating procedures, and maintenance procedures will produce the desired behavior.

The legal frameworks that govern IT security practices vary across countries and jurisdictions. However, there are several key legal frameworks that have a global impact and influence IT security practices. These include:

1. **General Data Protection Regulation (GDPR):** The GDPR, enforced in the European Union (EU) and applicable to organizations handling EU citizens' personal data, sets stringent requirements for data protection and privacy. It outlines obligations for organizations to implement appropriate technical and organizational measures to ensure the security of personal data.

2. **California Consumer Privacy Act (CCPA):** The CCPA is a state-level regulation in California, United States, that grants consumers certain rights regarding their personal information and imposes obligations on businesses to implement reasonable security measures to protect personal data.



3. **Payment Card Industry Data Security Standard (PCI DSS)**: PCI DSS is a global standard developed by major credit card companies to secure payment card data. It mandates specific security measures for organizations that handle cardholder information, aiming to prevent fraud and protect sensitive payment card data.



4. National Institute of Standards and Technology (NIST)

Frameworks: NIST, a U.S. federal agency, provides guidelines, standards, and best practices for various aspects of IT security. The NIST Cybersecurity Framework and NIST Special Publication 800-series documents offer comprehensive guidance on risk management, security controls, incident response, and other critical areas.



In conclusion, the lecture on IT security in digital law has shed light on the critical importance of safeguarding our digital systems and data in the modern era. The digital age has brought about unparalleled connectivity and convenience, but it has also introduced significant risks and vulnerabilities that must be addressed.

Ultimately, the lecture emphasized that IT security is not merely a technical concern but a legal and societal imperative. By prioritizing IT security, we protect sensitive information, mitigate cyber threats, comply with legal requirements, ensure business continuity, and safeguard national security and critical infrastructure.

By equipping ourselves with knowledge, raising awareness, and working together, we can navigate the digital age with confidence, safeguarding our digital assets, and preserving the trust and integrity of the interconnected world we inhabit.



Thank You