CSC 435 – Computer Security

Introduction

Course Topics

- Introduction to Computer Security
- Malicious Software (Attacks and Threats)
- Software Security / Vulnerabilities
- Identification and Authentication
- Access Control
- Cryptography

What is Information Security?

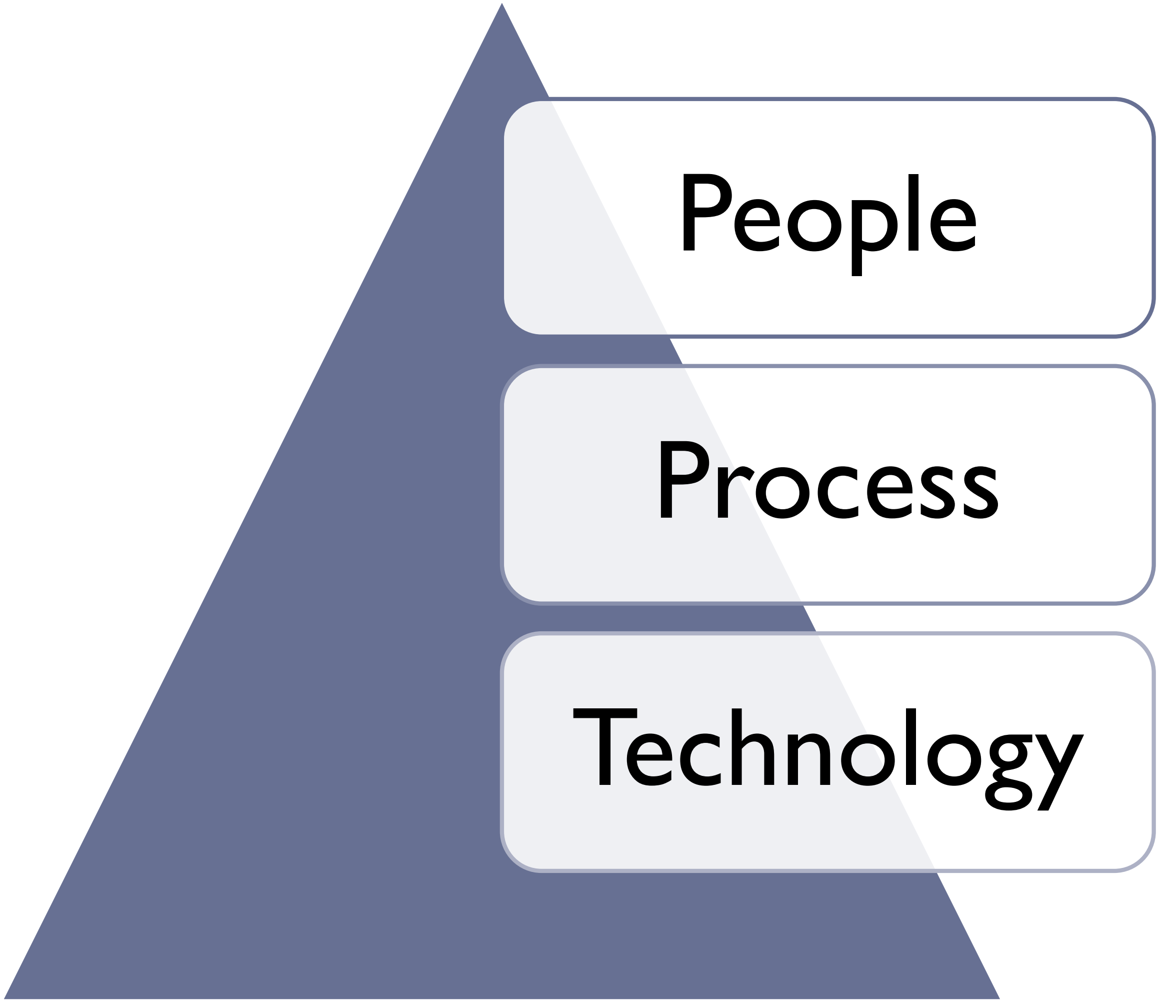
Introduction: Roadmap

- Security terminology
- Computer security: challenges and possible attacks
- Cybercrimes and Security Strategies

Security Terminology: Information Asset

- "**Information** is an **asset** which, like other **important business assets**, has **value** to an organization and consequently needs to be suitably **protected**" ISO/IEC 27002:2005
- "Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected" ISO/IEC 27002:2005
- Valued resources that can be misused:
  - Data (loss or integrity)
  - Time
  - Trust
  - Monetary

Information Security Elements



People

Process

Technology

Information Security Elements: People

- The biggest threat arise from people
  - Social engineers
  - Unethical competitors
  - Hackers
  - Fraudsters
  - Careless workers
- Yet the biggest asset is the people (ex. security-aware employees)

Information Security Elements: Processes

- Processes are work practices or workflows, the steps or activities needed to accomplish business objectives
  - Processes are described in procedures
  - Virtually all business processes involve and/or depend on information making information a critical business asset.
- Information security policies and procedures define how we secure information appropriately and repeatedly.

Information Security Elements: Technology

- Information technologies:
  - Cabling, data/voice networks and equipment
  - Telecommunications services (PABX, VoIP, ISDN, videoconferencing)
  - Phones, cellphones, PDAs
  - Computer servers, desktops and associated data storage devices (disks, tapes)
  - Operating system and application software
  - Paperwork, files
  - Pens, ink
- Security technologies
  - Locks, barriers, card-access systems, CCTV

Key Terms

- Information security is what keeps valuable information ‘free of danger’ (protected, safe from harm)
- It is not something you **BUY**; it is something you **DO**
  - It is a process not a product
- It is achieved using a combination of suitable strategies and approaches:
  - Determining the **RISKS** to information and **TREATING** them accordingly (proactive risk management)
  - Protecting CIA
  - Avoiding, preventing, detecting and recovering from Incidents
  - Securing people, processes and technology

Principles of Information Security - CIA

- Confidentiality (communication): Making information accessible only to those authorized to use it
- Integrity (personal or communication): safeguarding the accuracy and completeness of information and processing methods
- Availability: Ensuring that information is available when required

Security Terminology: Threats

- A threat is a specific means by which an attacker can put a system at risk
  - An ability/goal of an attacker (e.g., eavesdrop, fraud, access denial)

- A threat model is a collection of threats that deemed important for a particular environment
  - A collection of attackers abilities
  - E.g., a powerful attacker can read and modify all communications and generate messages on a communication channel

Security Terminology: Vulnerabilities

- A vulnerability is a systematic artifact that exposes the user, data, or system to a threat
  - E.g., buffer overflow, key leakage
- What is the source of a vulnerability?
  - Bad software (or hardware)
  - Bad design, requirements
  - Bad policy/configuration
  - System misuse

Security Terminology: Adversary

- An adversary is any entity trying to circumvent the security infrastructure
  - The curious and otherwise generally clueless (e.g., script-kiddies)
  - Casual attackers seeking to understand systems
  - Malicious groups of largely sophisticated users (e.g., chaos clubs)
  - Competitors (industrial espionage)
  - Governments/agencies (monitor activities)

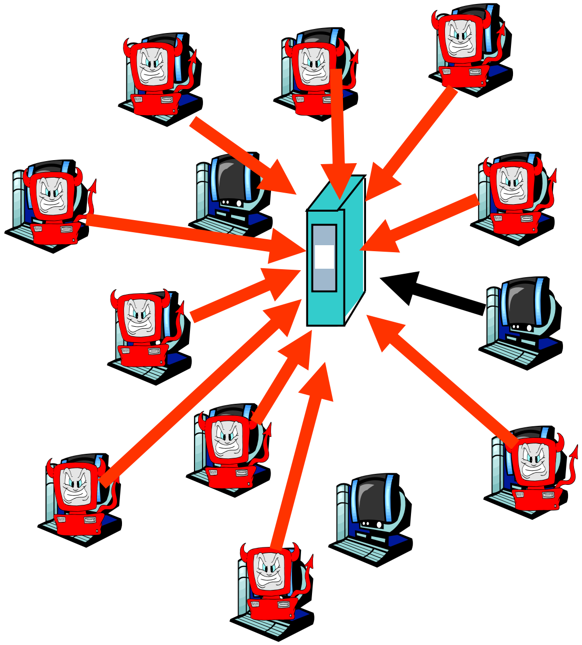
Are Users Adversaries?

- Have you ever tried to circumvent the security of a system you were authorized to access?
- Have you ever violated a security policy (knowingly or through carelessness)?

- This is known as the insider adversary (versus outsider adversary)

Security Terminology: Attacks

- An attack occurs when someone attempts to exploit a vulnerability
- Kinds of attacks:
  - Passive (e.g., eavesdropping)
  - Active (e.g., password guessing)
  - Denial of Service (DOS)
  - Distributed DOS (DDOS)



- Example attacks (network attacks):
  - IP spoofing, port scanning, "ping of death", ARP poisoning, routing manipulation, DNS spoofing, etc.
  - Spyware, adware, worms, viruses, spam, etc.

Security Terminology: Trust

- Trust refers to the degree to which an entity is expected to behave
- What the entity not expected to do?
  - E.g., not expose password
- What the entity is expected to do (obligations)?
  - E.g., obtain permission, refresh
- A trust model describes, for a particular environment, who is trusted to do what?
- Note: you make trust decisions every day
  - Q: What are they?
  - Q: Whom do you trust?

Security Terminology: Security Model

- A security model is the combination of trust and threat models that address the set of perceived risks:
  - The "security requirements" used to develop some comprehensive design
  - Every design must have a security model
    - LAN network or global information system
    - Java applet or operating system
- Security models:
  - What are the security concerns (risks)?
  - What are the threats?
  - Who are our adversaries?
  - How to deal with the threats?

More Definitions

- A computing system is a collection of hardware, software, storage media, data, and people that an organization uses to perform computing tasks.
- Computing Security: "Measures and controls that ensure **confidentiality**, **integrity**, and **availability** of information system assets including hardware, software, firmware, and information being processed, stored, and communicated."*
  - It is the protection of any computing system from threats.

***The NIST Internal/Interagency Report NISTIR 7298 (*Glossary of Key Information Security Terms* , May 2013)**

Computer Security Terminology, from RFC 2828, *Internet Security Glossary*, May 2000

Error: A human mistake in performing some software activity

Adversary (threat agent)

Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. Also called the attacker/hacker/cracker

Attack

Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

Countermeasure

A device or techniques that has as its objective the impairment of the operational effectiveness of undesirable or adversarial activity, or the prevention of espionage, sabotage, theft, or unauthorized access to or use of sensitive information or information systems.

Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence.

Security Policy

A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data.

System Resource (Asset)

A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.

Threat

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Exploit

A piece of software or technique that takes advantage of a security vulnerability to violate an explicit or implicit security policy. (Virus, worms)

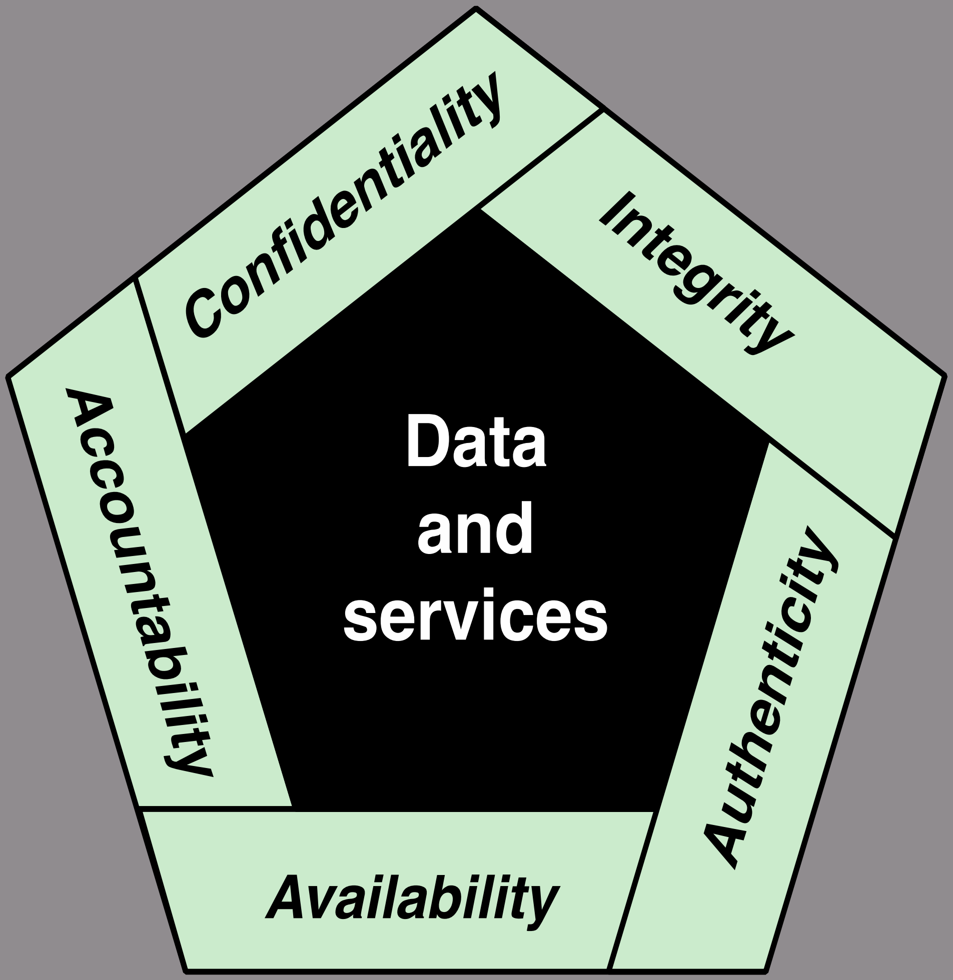


Figure 1.1 Essential Network and Computer Security Requirements

Key Security Concepts
The CIA Triad

- Confidentiality:
  Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
- Message Integrity:
  Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity
- Availability:
  Ensuring timely and reliable access to and use of information

Key Security Concepts
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.
  - Taken now more seriously by companies that want to be ‘trusted’ by their customers.
  - Also: the right to be left alone, e.g. not to be bothered by spam.

Key Security Concepts
Integrity

This term covers two related concepts:

- Data Integrity: Assures that information and programs are changed only in a specified and authorized manner. So data is the same as that in the source document and has not been exposed to accidental or malicious alteration or destruction.
- System Integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Key Security Concepts
Availability

- The property of being accessible and usable upon demand by an authorised entity.
- Denial of Service (DoS): The prevention of authorized access of resources or the delaying of time-critical operations.
- Maybe the most important aspect of computer security.
- Distributed denial of service (DDoS) receives a lot of attention; systems are now designed to be more resilient against these attacks.

Additional Security Concepts
Authenticity

- “know to whom you are talking”
- 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.

Additional Security Concepts
Accountability

- The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
- Truly secure systems aren't yet achievable, thus we must be able to trace a security breach to a responsible party.

Additional Security Concepts
Accountability

- At the operating system level, audit logs record security relevant events and the user identities associated with these events.
- If an actual link between a user and a "user identity" can be established, the user can be held accountable.
- In distributed systems, cryptographic non-repudiation mechanisms can be used to achieve the same goal.

Additional Security Concepts
Non-repudiation

- Non-repudiation services provide unforgeable evidence that a specific action occurred.
- Non-repudiation of origin: protects against a sender of data denying that data was sent.
- Non-repudiation of delivery: protects against a receiver of data denying that data was received.
- Typical application: signing emails; signatures in secure e-mail system.

Introduction: Roadmap

- Security terminology
- Computer Security: challenges and possible attacks
- Cybercrimes and Security Strategies

Computer Security Challenges

1. Computer security is not as simple as it might first appear to the novice

2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features

3. Procedures used to provide particular services are often counterintuitive

4. Physical and logical placement needs to be determined

5. Security mechanisms typically involve more than a particular algorithm or protocol and also require that participants be in possession of some secret information which raises questions about the creation, distribution, and protection of that secret information

Computer Security Challenges

6. Attackers only need to find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security

7. Security is still too often an afterthought to be incorporated into a system after the design is complete, rather than being an integral part of the design process

8. Security requires regular and constant monitoring

9. There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs

10. Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information

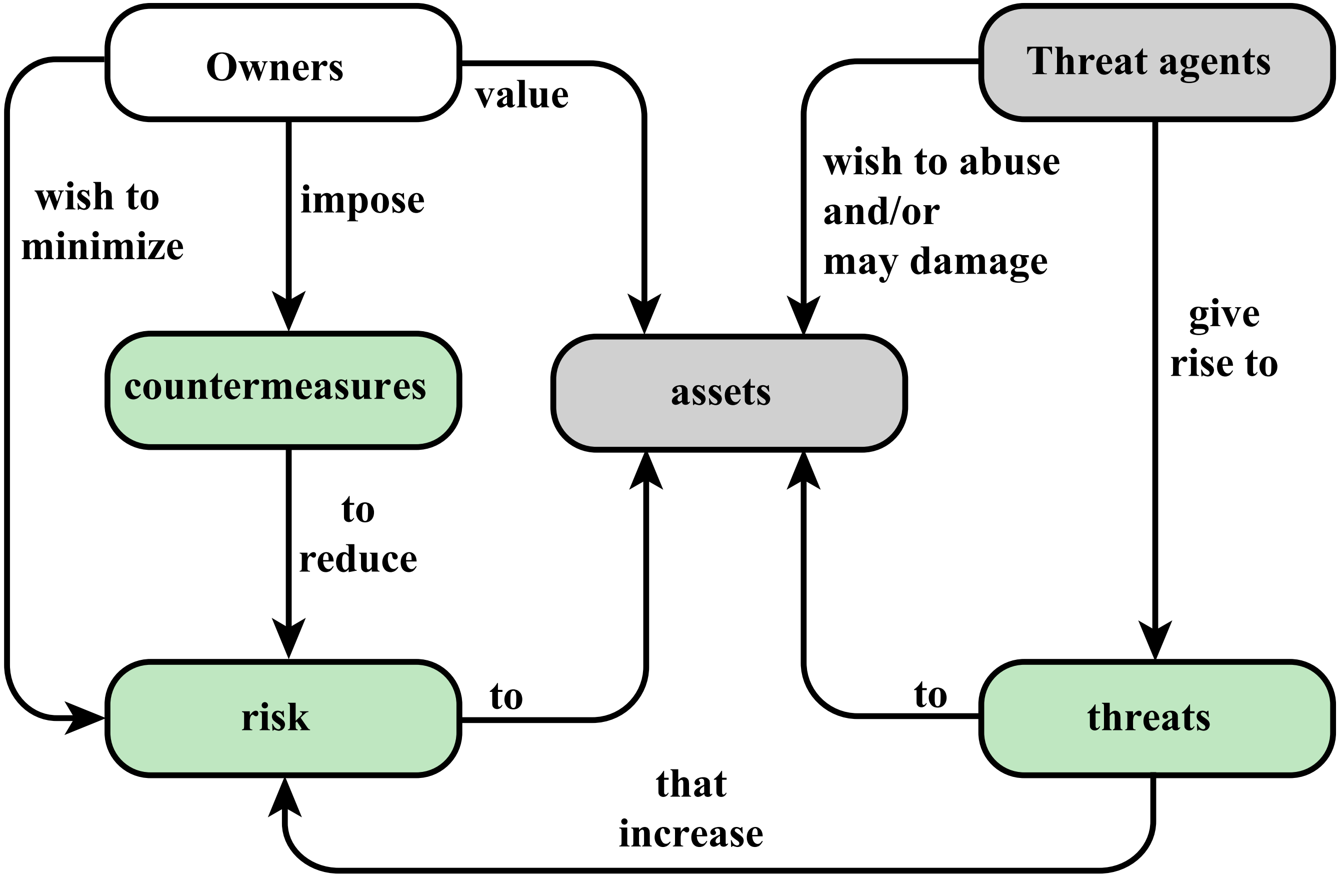


Figure 1.2 Security Concepts and Relationships

Table 1.3

Computer and Network Assets, with Examples of Threats

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Vulnerabilities, Threats, and Attacks

- Categories of vulnerabilities
  - Corrupted (loss of integrity)
  - Leaky (loss of confidentiality)
  - Unavailable or very slow (loss of availability)
- Threats
  - Capable of exploiting vulnerabilities
  - Represent potential security harm to an asset
- Attacks (threats carried out)
  - Passive – attempt to learn or make use of information from the system that does not affect system resources
  - Active – attempt to alter system resources or affect their operation
  - Insider – initiated by an entity inside the security parameter
  - Outsider – initiated from outside the perimeter

Passive and Active Attacks

Passive Attacks

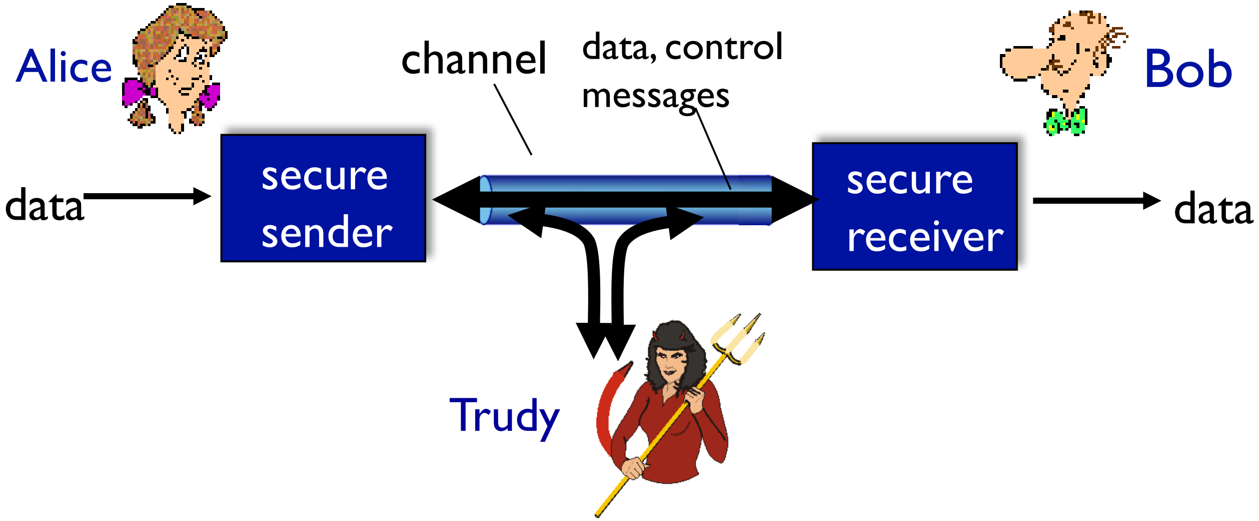
- Attempts to learn or make use of information from the system but does not affect system resources
- Eavesdropping or monitoring of transmissions
- Goal of attacker is to obtain information that is being transmitted
- Two types:
  - Release of message contents
  - Traffic analysis

Active Attacks

- Attempts to alter system resources or affect their operation
- Involve some modification of the data stream or the creation of a false stream
- Four categories:
  - Replay
  - Masquerade
  - Modification of messages
  - Denial of service

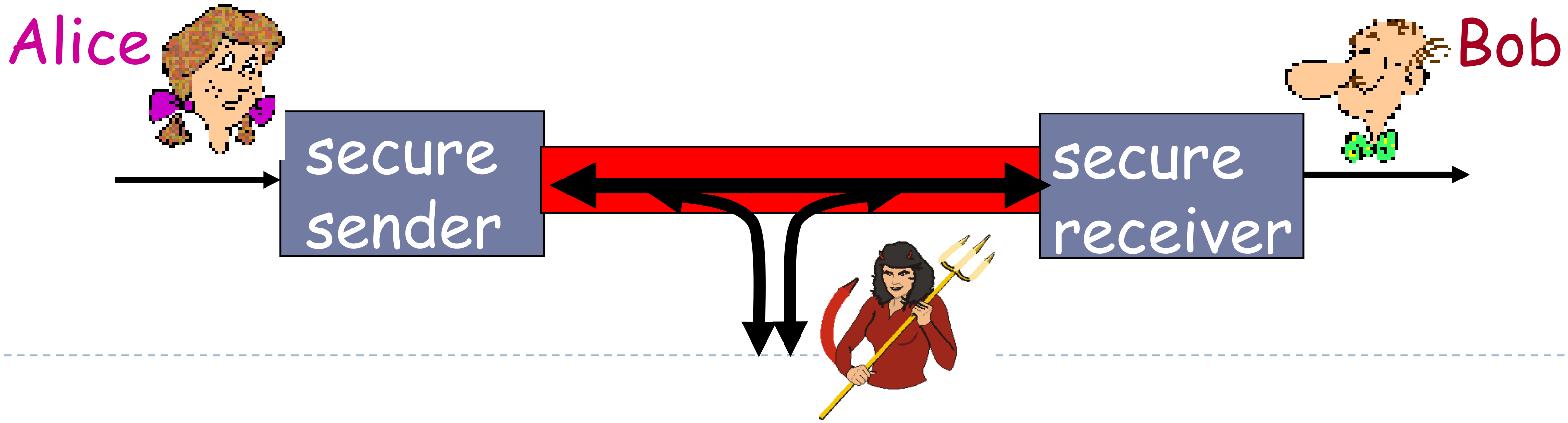
Friends and enemies: Alice, Bob, Trudy

- well-known in network security world
- Bob, Alice (lovers!) want to communicate "securely"
- Trudy (intruder) may intercept, delete, add messages



Possible Attacks

- Alice wants to communicate with Bob over a network:
  - No one should be able to disable her machine (denial of service) or misuse her machine
  - Or sniff information she exchanges
  - Or spoof her address and act in her name
  - Or plant malicious code on her machine
  - Or attack anything on route to Bob



Who Might Bob, Alice be?

- … Well, *real-life* Bobs and Alices!
- Web browser/server for electronic transactions (e.g., on-line purchases)
- On-line banking client/server
- DNS servers
- Routers exchanging routing table updates
- Other examples?

There are Bad Guys (and Girls) out there!

Q: What can a "bad guy" do?

A: a lot!

- *eavesdrop:* intercept messages
- actively *insert* messages into connection
- *impersonation:* can fake (spoof) source address in packet (or any field in packet)
- *hijacking:* "take over" ongoing connection by removing sender or receiver, inserting himself in place
- *denial of service*: prevent service from being used by others (e.g., by overloading resources)
- more…

Security Challenges

- Your security depends on others (unknowns)
  - Fighting a living enemy
  - New advances lead to improved attacks
- Good security solution must:
  - Handle the problem to a great extent (no perfect/complete solution)
  - Handle future variations of the problem, too
  - Be inexpensive
  - Require few deployment points
- Security professionals: play double game

What They Violate?

- Eavesdropping
- Alteration
- Denial of service
- Masquerading

What They Violate?

- Eavesdropping: Confidentiality
- Alteration: Data integrity
- Denial of service: Availability
- Masquerading: Origin integrity

Introduction: Roadmap

- Security terminology
- Computer security: challenges and possible attacks
- Cybercrimes and Security Strategies

What is cybercrime?

- Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device.
- Most, but not all, cybercrime is committed by cybercriminals or hackers who want to make money. Cybercrime is carried out by individuals or organizations.
- Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers.
- Rarely, cybercrime aims to damage computers for reasons other than profit. These could be political or personal.

© Kaspersky.com

Types of cybercrime

- Email and internet fraud.
- Identity fraud (where personal information is stolen and used).
- Theft of financial or card payment data.
- Theft and sale of corporate data.
- Cyberextortion (demanding money to prevent a threatened attack).
- Ransomware attacks (a type of cyberextortion).
- Cryptojacking (where hackers mine cryptocurrency using resources they do not own).
- Cyberespionage (where hackers access government or company data).

© Kaspersky.com

Types of Cybercrime

- Illegally intercepting or stealing data.
- Interfering with systems in a way that compromises a network.
- Infringing copyright.
- Illegal gambling.
- Selling illegal items online.
- Soliciting, producing or possessing child pornography.

© Kaspersky.com

Malware Attacks

- a computer system or network infected with a computer virus or other type of malware.
- Purposes include:
  - stealing confidential data
  - using the computer to carry out other criminal acts
  - or causing damage to data
- WannaCry ransomware attack, a global cybercrime committed in May 2017.
  - 230,000 computers in 150 countries.
  - Users were locked out of their files and sent a message demanding that they pay a BitCoin ransom to regain access.
  - Financial Losses: $4 billion Worldwid.

© Kaspersky.com

Phishing

- spam emails, or other forms of communication, sent en masse, with intention of tricking recipients into doing something that undermines their security or their organization's security.
- In 2018, the World Cup Phishing Scam.
  - phishing scam emails [containing links] sent to football fans
  - tried to entice fans with fake free trips to Moscow [World Cup host]
  - Opening and clicking the links cause personal data to be stolen
- Spear-phishing
  - targeted phishing campaigns [specific individuals]
  - jeopardizes the security of the organization

© Kaspersky.com

DDoS

- **Distributed DoS attacks (DDoS) brings down a system or network.**
- **Sometimes connected IoT (internet of things) devices are used to launch DDoS attacks.**
- UK National Lottery website DDoS Attack in 2017
  - brought the lottery's website and mobile app offline
  - preventing UK citizens from playing

© Kaspersky.com

Potection against cybercrime

- **Keep software and operating system updated**
- **Use anti-virus software and keep it updated**
- **Use strong passwords**
- **Never open attachments in spam emails**
- **Do not click on links in spam emails or untrusted websites**
- **Do not give out personal information unless secure**
- **Contact companies directly about suspicious requests**
- **Be mindful of which website URLs you visit**
- **Keep an eye on your bank statements**

© Kaspersky.com

Attack Steps (1)

Very often individual attacks will follow the same seven step pattern:

1. **Reconnaissance (Surveying, examination):** The is the preparation phase where the attacker seeks to learn all they can about the target organization.
2. **Scanning:**
   a) Scanning describes the pre-attack phase where the attacker scans the target network for specific information, typically vulnerabilities based on the results of the reconnaissance.

   b) Tools at an attacker's disposal include port scanners, network mapping tools, vulnerability scanners.

Attack Steps (2)

3. **Gain access and escalation:**

   a. This step is the actual penetration of the target system. The attacker exploits a vulnerability to gain access.

   b. escalate privilege and move undetected through the network

4. **Exfiltration:** extract any information that is needed (not taken in every cyber attack)

5. **Maintain access (Sustainment):**

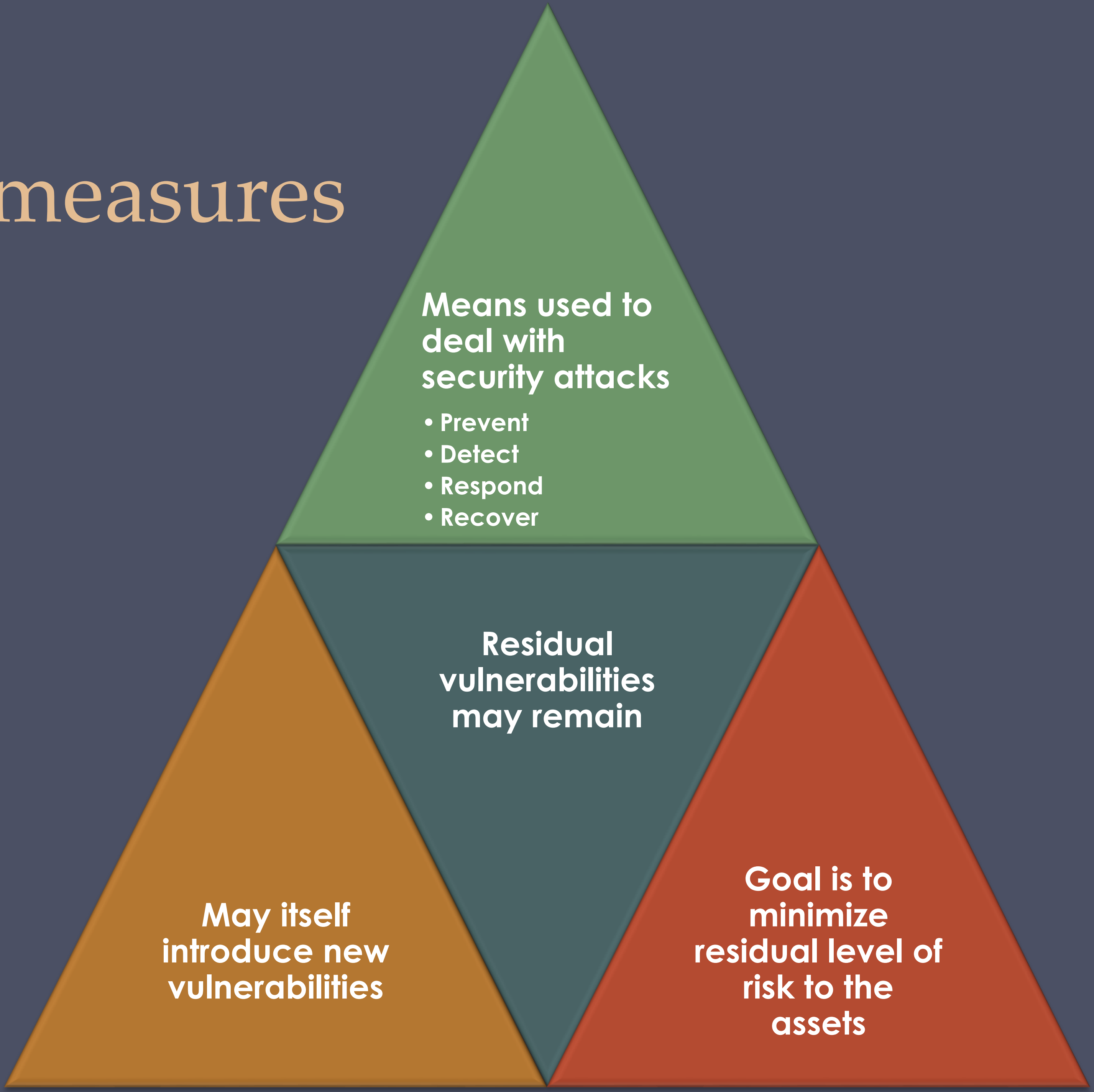
   a) This is the phase where the attacker delivers the desired payload. They have gained unauthorized access and now wish to exploit it. This can mean anything from obtaining files/data, planting spyware, cause damage directly, setup zombie machines, install backdoor, etc.

   b) attackers can come and go as they please

Attack Steps (3)

6. **Assault or Attack:** not taken in every cyber attack
7. **Obfuscation (Cover tracks):** This is how an attacker hides the evidence of his/her actions. Log files need to be modified.

Countermeasures



Means used to deal with security attacks

- Prevent
- Detect
- Respond
- Recover

Residual vulnerabilities may remain

May itself introduce new vulnerabilities

Goal is to minimize residual level of risk to the assets

Security Strategy

A security Strategy usually involves four steps:

1. **Security policy**
2. **Security Implementation**
3. **Assurance**
4. **Evaluation**

Security Policy (1)

- A **security policy** is
  - an informal description of desired system behavior
  - 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. **“RFC 4949”**
- 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

Security Policy (2)

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. Ex: Access control mechanisms, Firewalls, Antiviruses…
- 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. The cost of security failure and recovery must take into account:
  - the value of the assets being protected
  - the damages resulting from a security violation
  - the risk or the probability that a particular threat will exploit some vulnerability with a particular harmful result

Security Implementation (1)

Security implementation involves four complementary courses of action:

1. Prevention: An ideal security scheme where no attack is successful. Although not practical in all cases, there is a wide range of threats in which prevention is a reasonable goal. Ex. transmission of encrypted data.
2. Detection: In a number of cases, absolute protection is not feasible, but it is practical to detect security attacks. Ex. intrusion detection systems designed to detect unauthorized individuals logged onto a system, detection of a denial of service attack.

Security Implementation (2)

3. 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.
4. Recovery: An example of recovery is the use of backup systems, so that if data integrity is compromised, a previously saved correct copy of the data can be reloaded.

The more you invest into prevention, the more you have to invest into detection to make sure prevention is working.

Assurance

- Encompassing both system design and system implementation, assurance is an attribute of an information system that provides grounds for having confidence that the system operates such that the system's security policy is enforced.
  - "Does the security system design meet its requirements?"
  - "Does the security system implementation meet its specifications?"
- Assurance is expressed as a degree of confidence, not in terms of a formal proof that a design or implementation is correct.

Evaluation

- Process of examining a computer product or system with respect to certain criteria
- Involves testing and may also involve formal analytic or mathematical techniques

Thank You