Computer Security

Lecture 2: Key Concepts of Computer Security

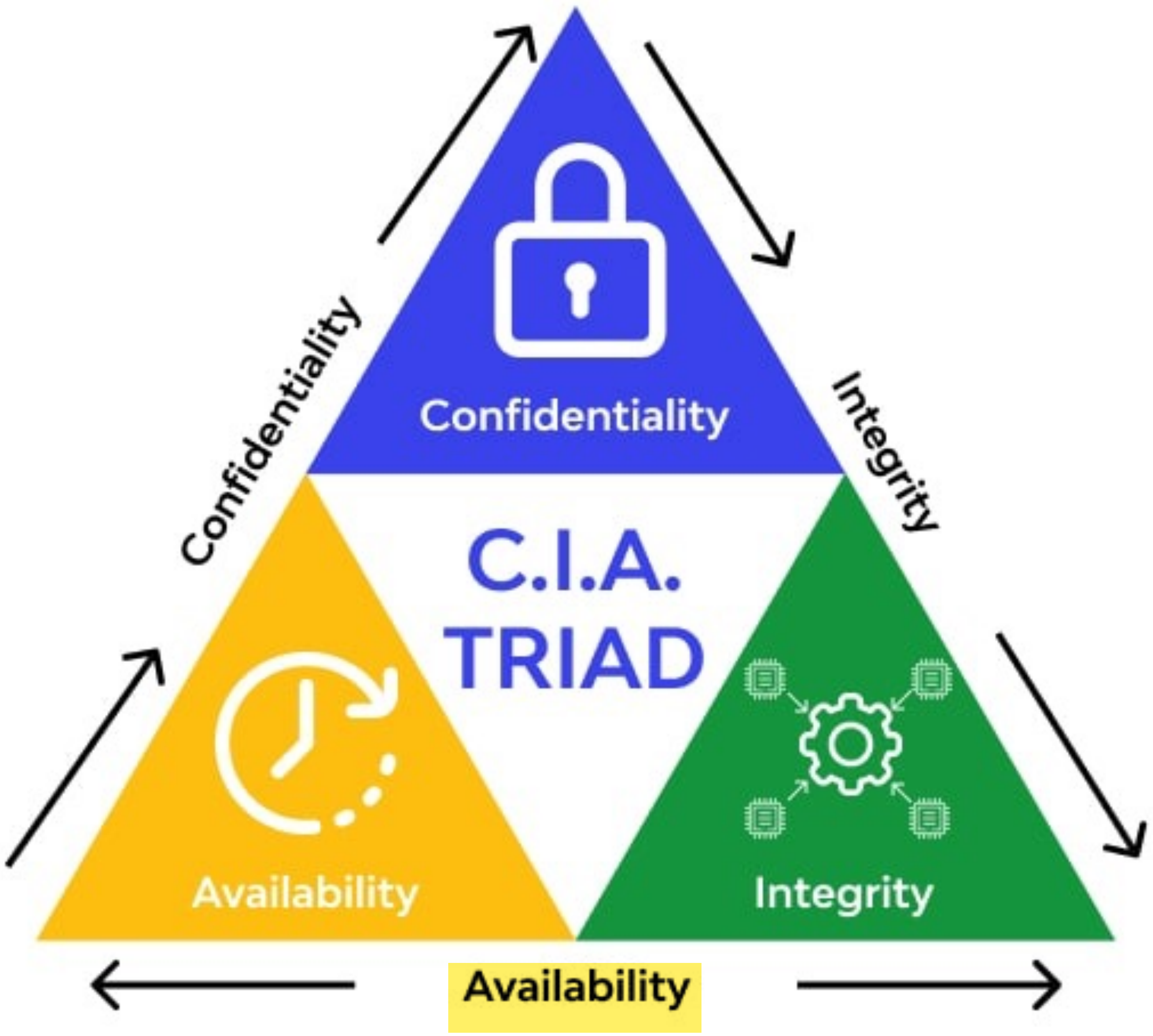
Prof. Dr. Sadeeq Jan

Department of Computer Systems Engineering
University of Engineering and Technology Peshawar

Lecture Outline

- Goals of Information Security
- Aspects of Security
- OSI Security Architecture
- Security Threats/Attacks (X.800)
- Classes of Threats
- Why Security is hard?
- Goal of Security
- Model for Network Security
- Policies and Mechanisms
- Trust and Assumptions
- Assurance
- Tying Together
- Top 10 Cyber Crime Prevention Tips
- Risk and Analysis
- Risk Management vs. Cost of Security
- The Security, Functionality, and Usability Triangle

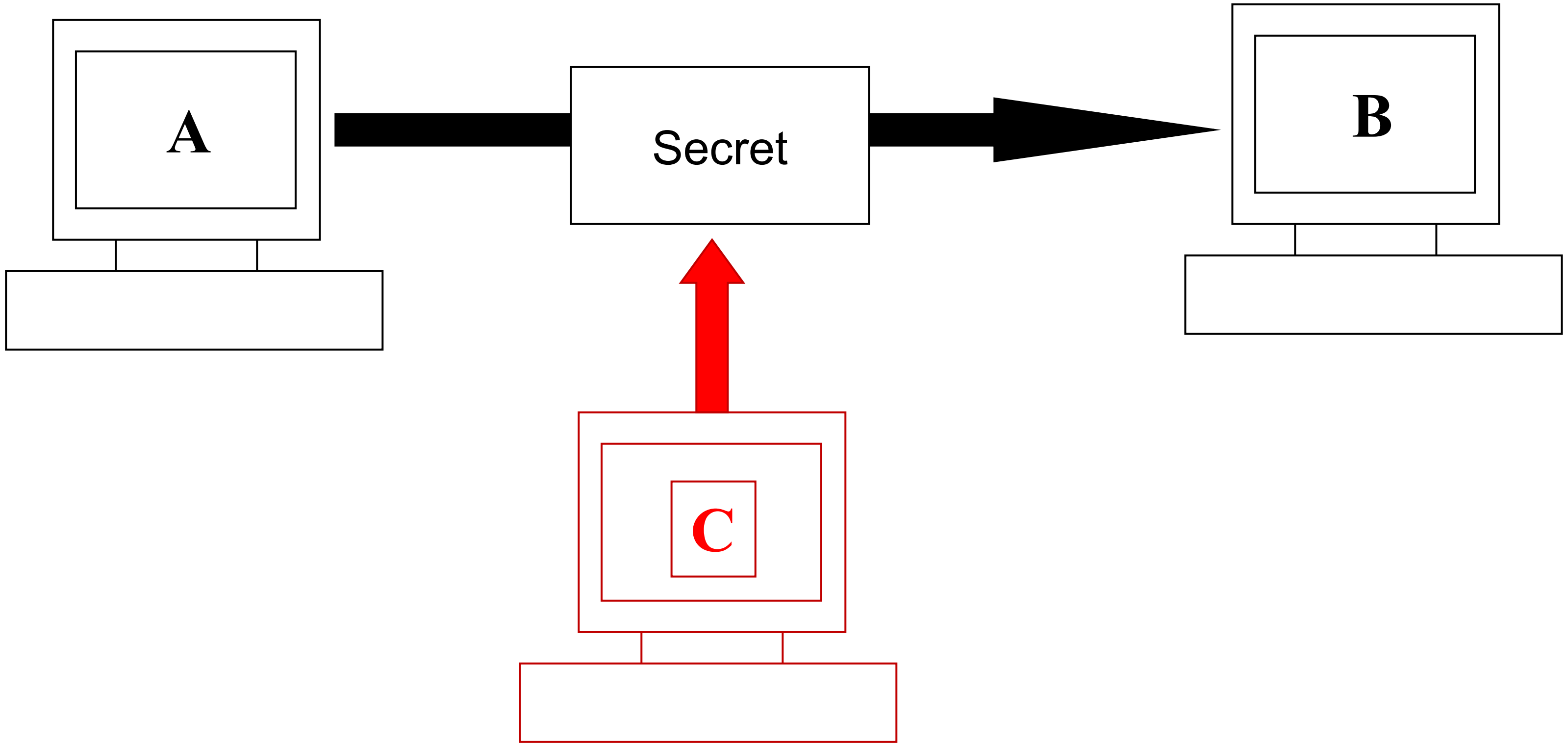
Goals of Information Security



Confidentiality

- Prevent unauthorized disclosure of information
- Requires that data only be accessible for reading by authorized parties
- Access control mechanism e.g., cryptography (encryption)
  - e.g., enciphering an income tax return

Loss of Confidentiality



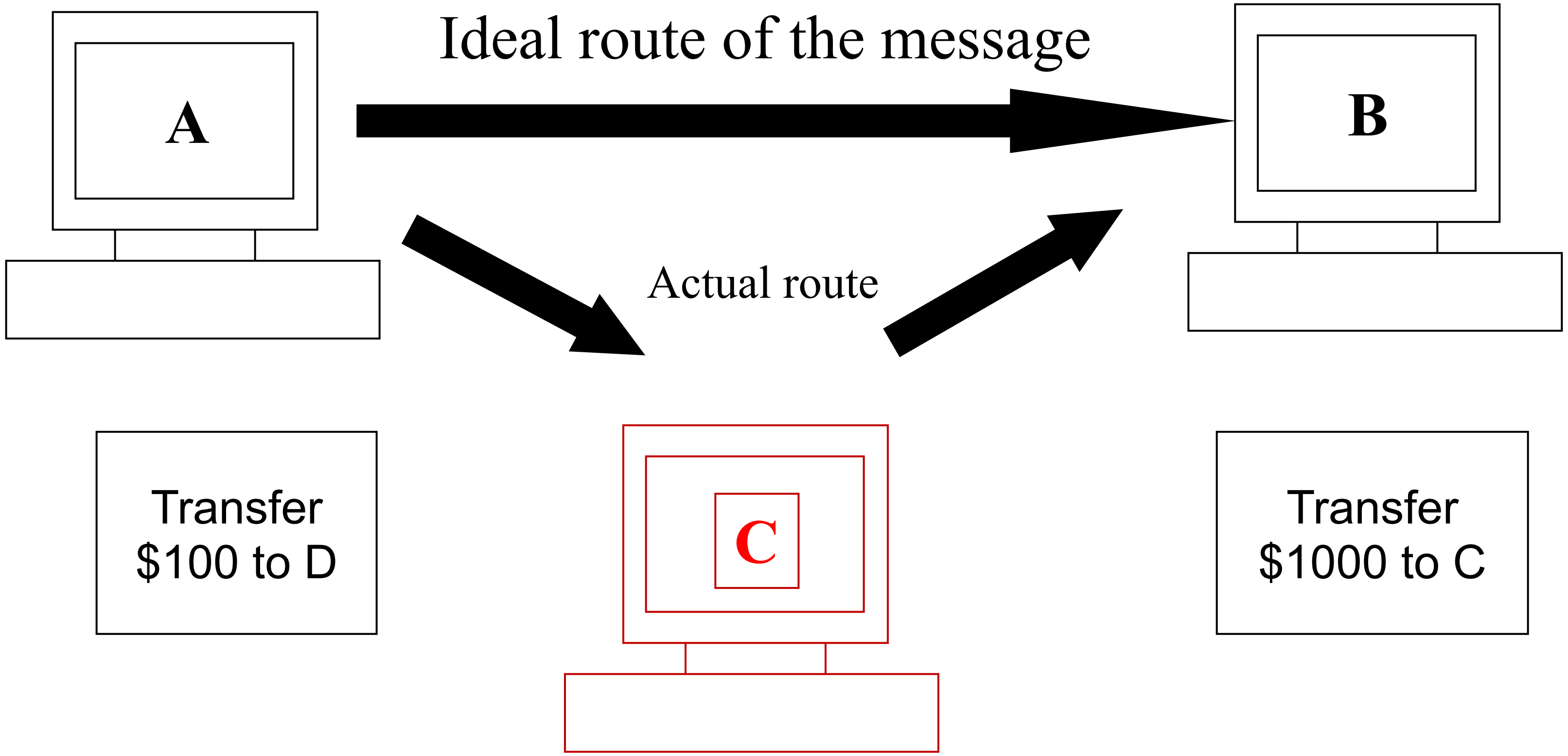
Interception causes loss of message confidentiality

Integrity

- Prevent unauthorized modification of information
- Data integrity (the content of information)
- Origin integrity (the source of information, often called authentication)

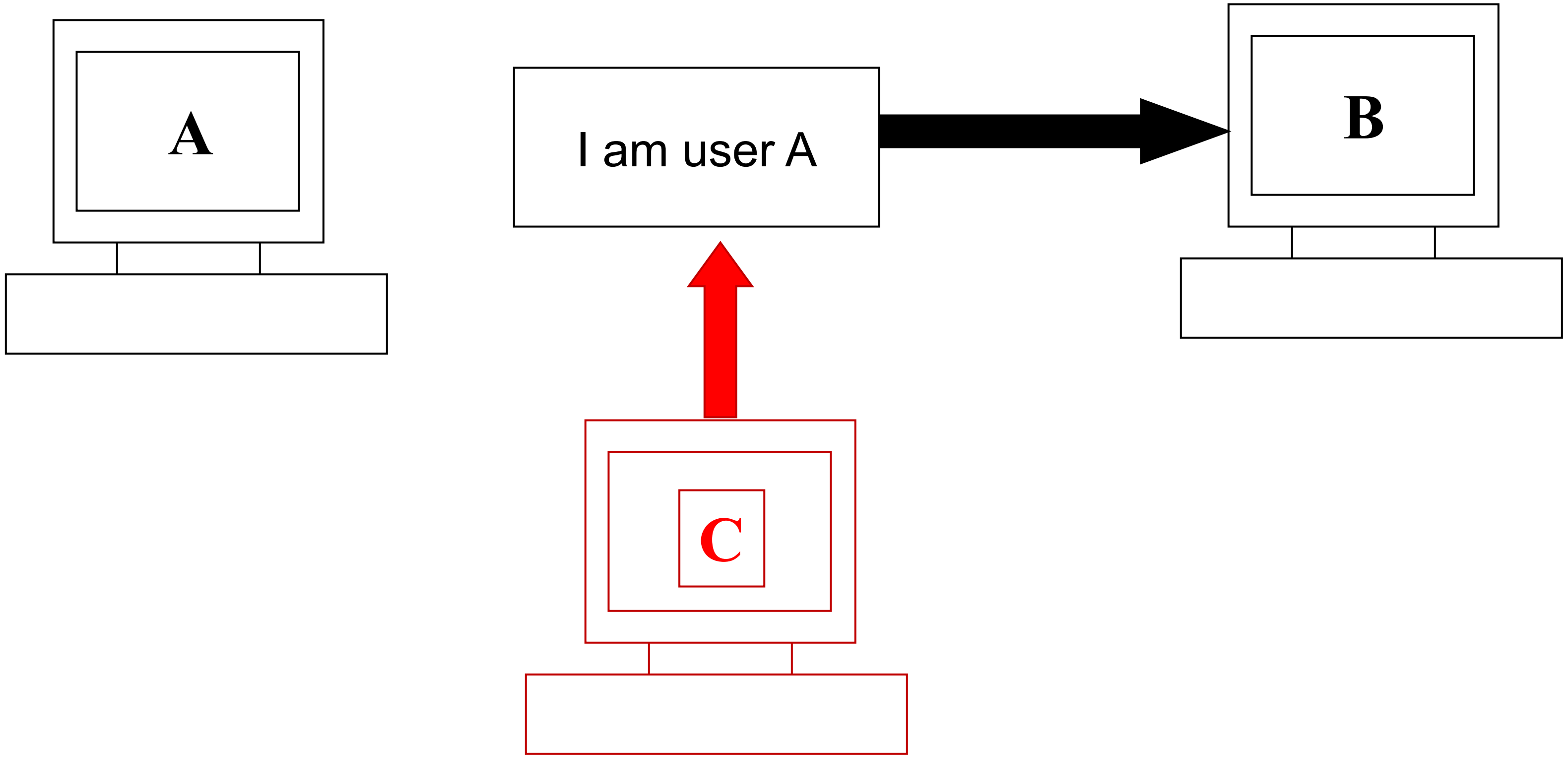
In summary, origin integrity verifies that data hasn't been tampered with in transit, while source integrity assures that the data comes from a trusted and verified source

Loss of Integrity



Modification causes loss of message integrity

Absence of Authentication



. to invent or produce something false in order to deceive someone:

Fabrication is possible in absence of proper authentication mechanism

Integrity

- Prevention and detection mechanism
  - **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.
    - e.g. a digital signature can be used to determine if data has changed.
- Maintaining integrity is very difficult than confidentiality
  - Confidentiality→ data is either compromised or it is not.
  - integrity → correctness and the trustworthiness of the data

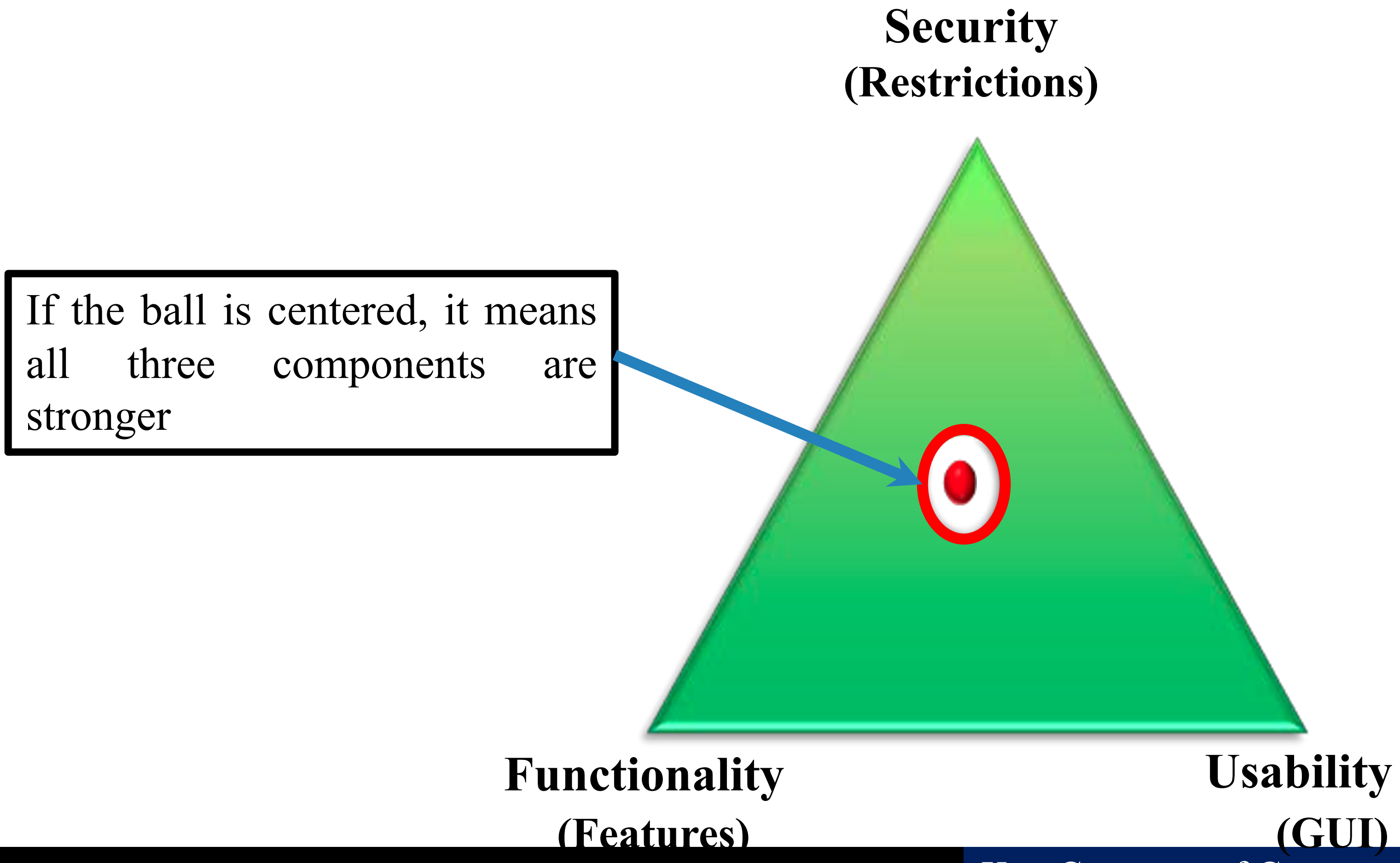
Availability

- Ability to use the information or resource desired.
- Usually defined in terms of "quality of service"
- Authorized users are expected to receive a specific level of service.
- Denial of service attacks are attempts to block availability
  - Most difficult to detect

CIA	RISK	CONTROL
Confidentiality	Loss of privacy. Unauthorized access to information. Identity theft.	Encryption. Authentication. Access Control
Integrity	Information is no longer reliable or accurate. Fraud.	Maker/Checker. Quality Assurance. Audit Logs
Availability	Business disruption. Loss of customer's confidence. Loss of revenue.	Plans and test. Backup storage. Sufficient capacity.

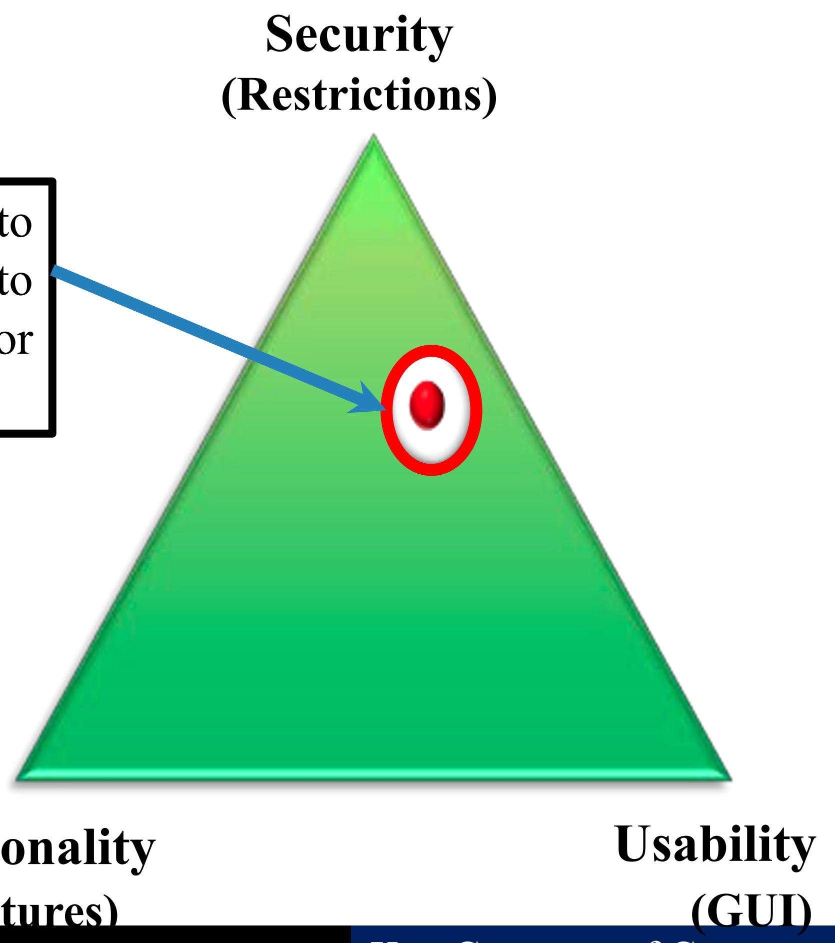
Risk and Its Protection by Implementing CIA

The Security, Functionality, and Usability Triangle



If the ball is centered, it means all three components are stronger

The Security, Functionality, and Usability Triangle



Moving the target closer to Security causes loss to "Ease of Use" and /or "Functionality"

Aspects of Security

- Need systematic way to define requirements
- Consider three aspects of information security:
  - **Security Attack**
  - **Security Mechanism**
  - **Security Service**
- Consider in reverse order

Security Service

- Is something that enhances the security of the data processing systems and the information transfers of an organization
- Intended to counter security attacks
- Make use of one or more security mechanisms to provide the service
- Replicate functions normally associated with physical documents
  - eg. Physical document have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

Security Mechanism

- A mechanism that is designed to detect, prevent, or recover from a security attack
- No single mechanism that will support all functions required
- However, one particular element underlies many of the security mechanisms in use: **cryptographic techniques**

Security Threats/Attacks

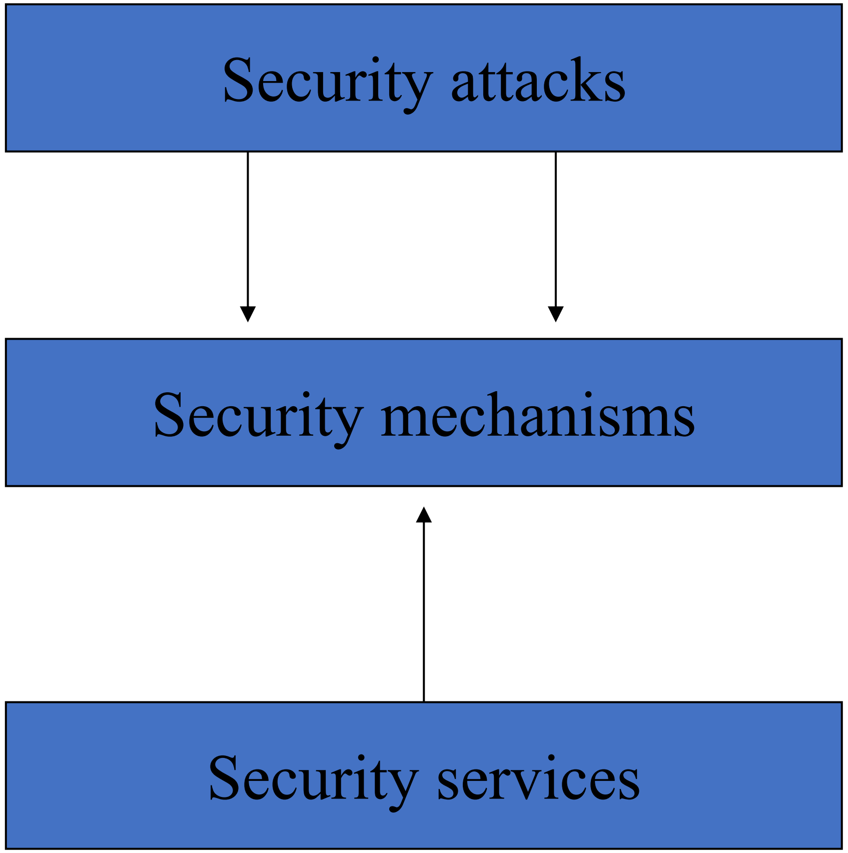
- A threat is a potential violation of security.
  - The violation need not actually occur for there to be a threat.
- The fact that the violation might occur means that those actions that could cause it to occur must be guarded against (or prepared for).
- Those actions are called attacks. Those who execute such actions, or cause them to be executed, are called attackers.
- An attack tends to be an act which is in process while a threat tends to be a promise of an attack to come
- have a wide range of attacks
- can focus of generic types of attacks: passive & active

A passive attack is like eavesdropping or spying. The attacker intercepts or listens to data without altering

An active attack involves manipulating or altering data or systems. The attacker actively makes changes to achieve a specific goal, such as stealing information,

OSI Security Architecture

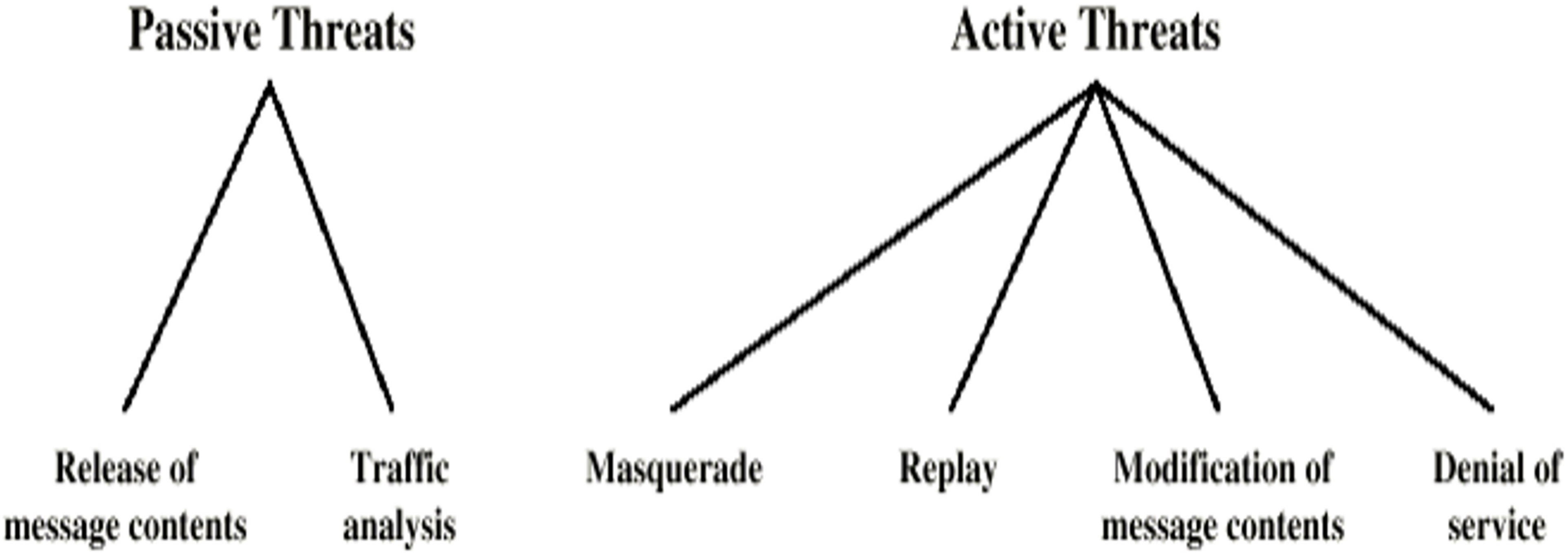
- ITU-T X.800 Security Architecture for OSI
  - defines a systematic way of defining and providing security requirements



Security Service (X.800)

- **Authentication** - assurance that the communicating entity is the one claimed
- **Access Control** - prevention of the unauthorized use of a resource
- **Data Confidentiality** –protection of data from unauthorized disclosure
- **Data Integrity** - assurance that data received is as sent by an authorized entity
- **Non-Repudiation** - protection against denial by one of the parties in a communication

Security Threats/Attacks (X.800)



Passive Threats

- Release of message contents
- Traffic analysis

Active Threats

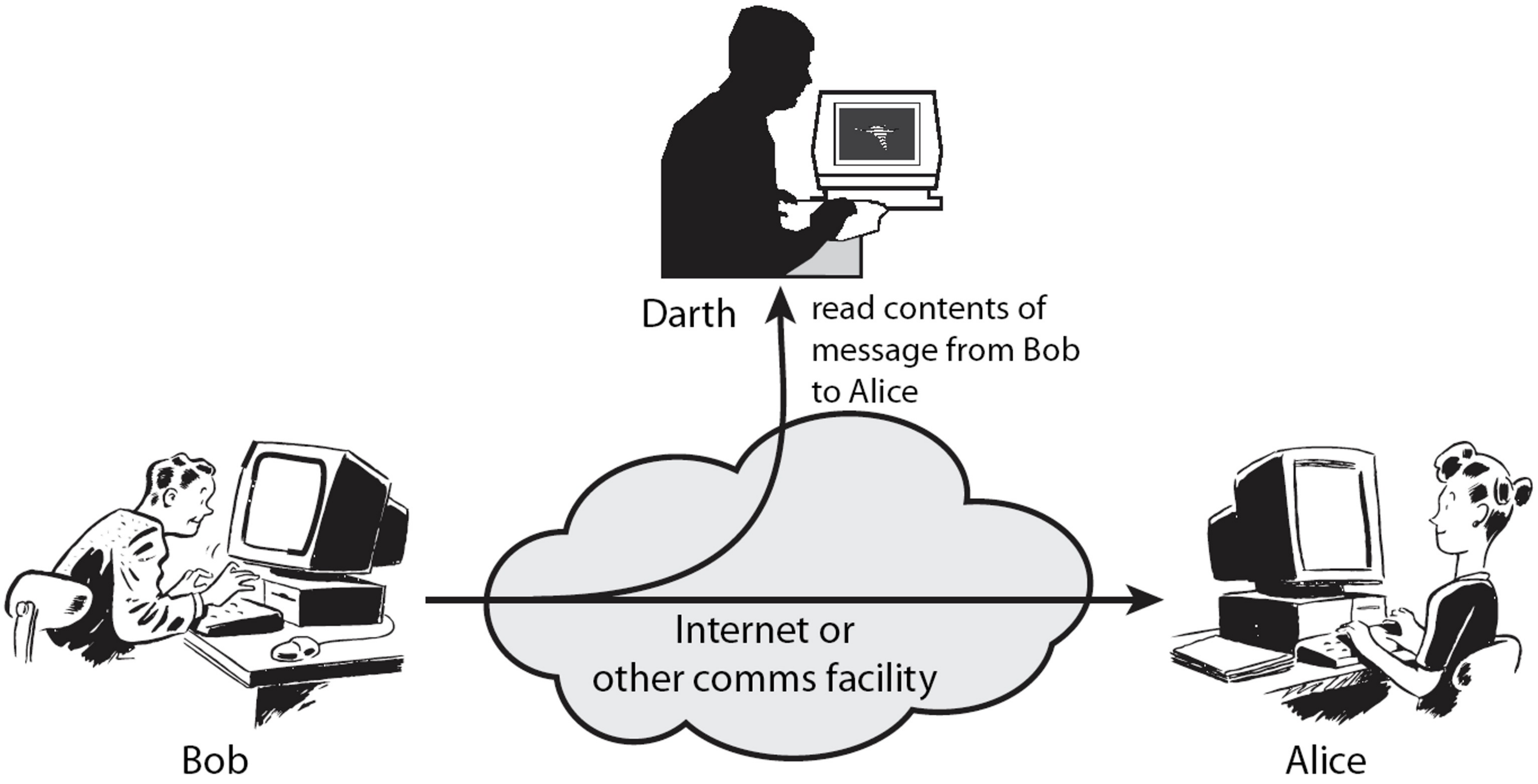
- Masquerade
- Replay
- Modification of message contents
- Denial of service

/snooping

Passive Attacks

- It doesn't involve any modification to the original message
- Eavesdropping on transmissions, to obtain information
- **Snooping/Release of message contents**
  - Outsider learns content of transmission
  - Unauthorized interception of information, disclosure
  - Passive wiretapping
- **Traffic analysis**
  - By monitoring frequency and length of messages, even encrypted, nature of communication may be guessed
- Difficult to detect but can be prevented

Passive Attacks


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

Active Attacks

- **Modification/alteration of original message/creation of a false message i.e. unauthorized change of information**
  - active wiretapping, where the attacker injects something into a communication or modifies parts of the communication.
  - Goal may be deception
  - e.g. man-in-the-middle attack
  - Integrity services counter this threat

Active Attacks

- **Masquerading or spoofing**
    - Pretending to be a different entity
    - For example, if a user tries to log into a computer across the Internet but instead reaches another computer that claims to be the desired one, the user has been spoofed.
    - Similarly, 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
    - Integrity services (called “authentication services”) counter this threat
- Some form of masquerading may be allowed. e.g. delegation

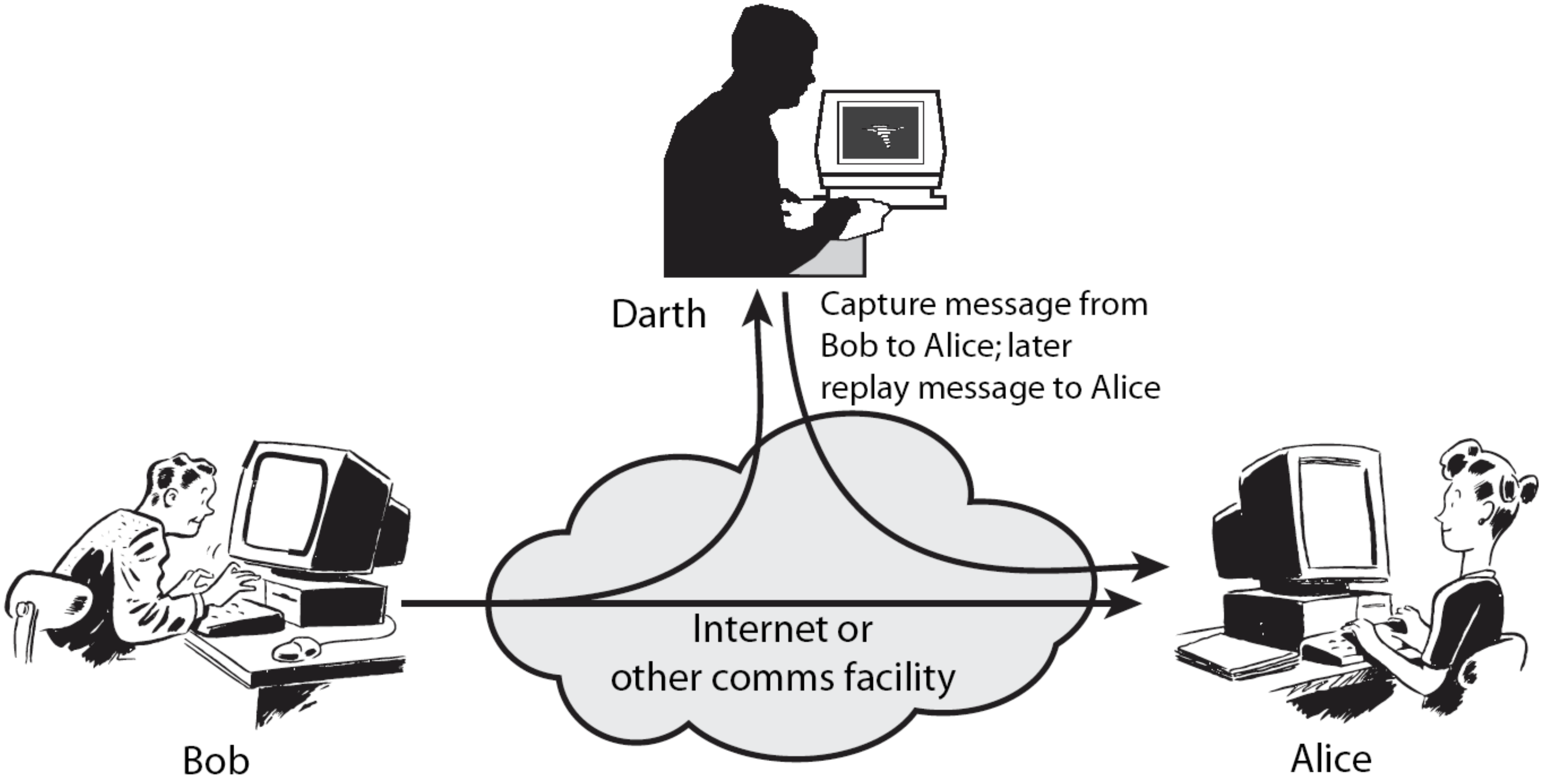
Active Attacks

- **Repudiation of origin-** a false denial that an entity sent (or created) something, is a form of deception.
  - For example, customer denial of ordering a product when the product is received (but in fact the customer has ordered this product)
  - Or denial by a user that he created specific information or entities such as files. Integrity mechanisms cope with this threat.
- **Denial of receipt-** a false denial that an entity received some information or message, is a form of deception.
  - For example customer denial that he has not received the product (but in fact he has already received it).
- **Replay-**involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

Active Attacks

- **Delay** (temporary inhibition of a service)
- **Denial of service** (long term inhibition of a service, infinite delay)
  - Denial may occur at the source, at the destination or along the intermediate path
  - This may not be due to security attack but limited resources
- Active attacks are easy to detect but Hard to prevent

Active Attacks


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

Classes of Threats

- **Disclosure**
  - Snooping
- **Deception**
  - Modification, spoofing, repudiation of origin, denial of receipt
- **Disruption**
  - Modification
- **Usurpation**
  - Taking someone's power or property by force.
  - Masquerading/spoofing, delay, DoS

Why Security is hard?

- **Identifying security requirements** of a system is non-trivial
  - – must take into account services, environment, etc.
- **Finding adequate (often complex) solutions** is not easier
  - – the decision must take into account known attacks and threats
  - – security mechanisms must be logically placed
- **Securing a system is not a one-time task**
  - – the system must be constantly monitored in face of changing threats
  - – security mechanisms need to be re-evaluated

Why Security is hard?

- **Managers** do not perceive value in security investment (until a security failure occurs)

  – system administrators might not influence decisions or not make good decisions

- **Users** view security measures as an obstacle on the way of getting their work done

  – we would like security mechanisms to be as intuitive and robust as possible

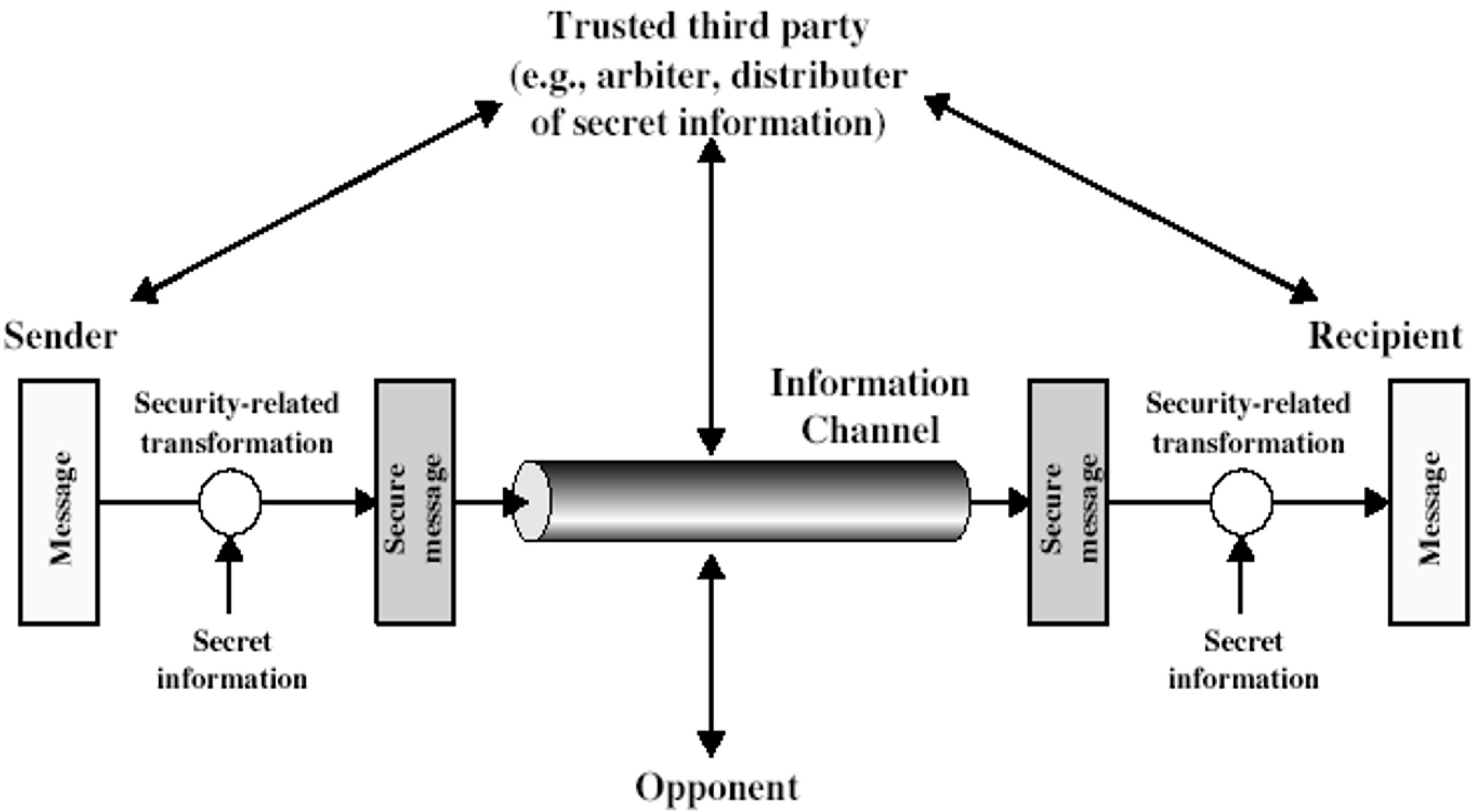
- **Adding security to an existing system** might not be pretty

  – ideally, security is an integral part of the design

Goal of Security

- **Prevention**
  - Prevent attackers from violating security policy
  - Prevention is ideal, because then there are no successful attacks.
- **Detection**
  - Detect attackers’ violation of security policy
  - Occurs after someone violates the policy.
- **Recovery**
  - Stop attack, assess and repair damage
  - Continue to function correctly even if attack succeeds

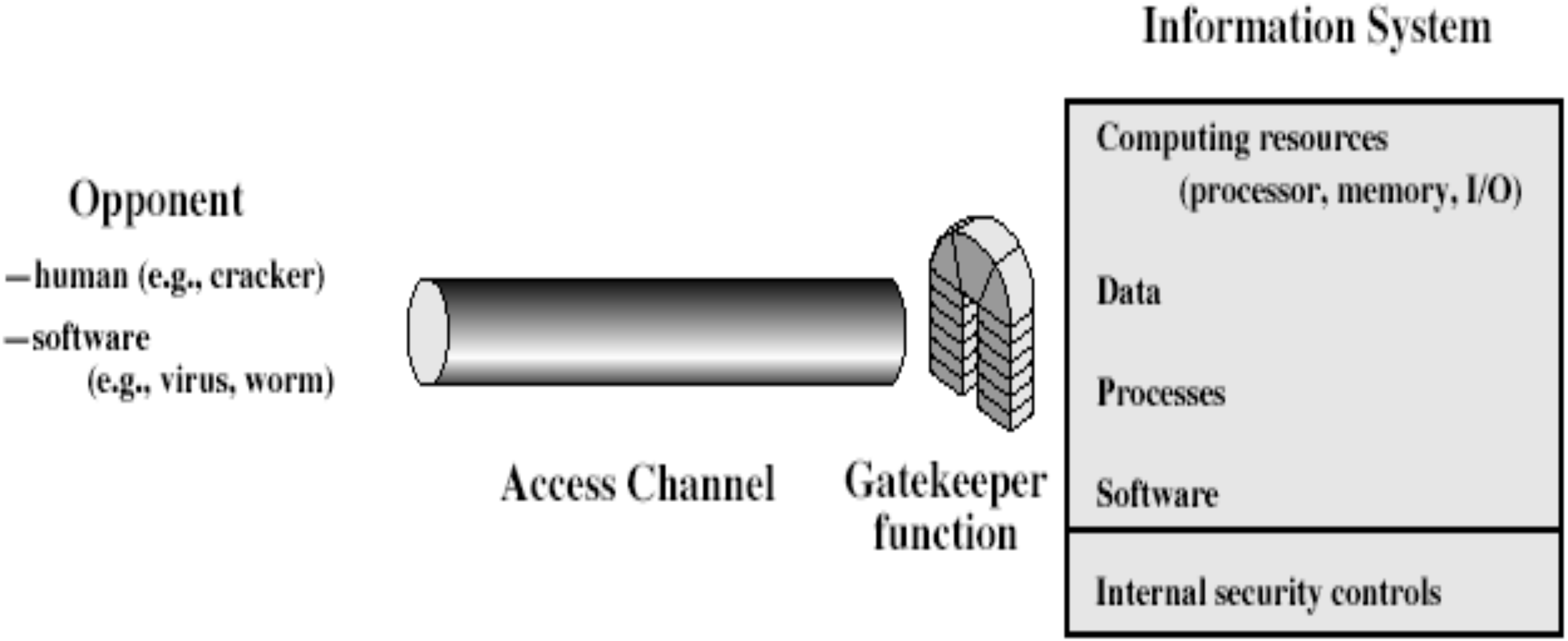
Model for Network Security



Model for Network Security

- using this model requires us to:
  - design a suitable algorithm for the security transformation
  - generate the secret information (keys) used by the algorithm
  - develop methods to distribute and share the secret information
  - specify a protocol enabling the principals to use the transformation and secret information for a security service

Model for Network Access Security



Model for Network Access Security

- using this model requires us to:
  - select appropriate gatekeeper functions to identify users
  - implement security controls to ensure only authorised users access designated information or resources

Top 10 Cyber Crime Prevention Tips

1. Use Strong Passwords

- ✓ Use different user ID / password combinations for different accounts
- ✓ avoid writing them down.
- ✓ Make the passwords more complicated by combining letters, numbers, special characters (minimum 10 characters in total)
- ✓ change them on a regular basis.

2. Secure your computer

- ✓ **Activate your firewall**
  Firewalls are the first line of cyber defence; they block connections to unknown or bogus sites and will keep out some types of viruses and hackers.
- ✓ **Use anti-virus/malware software**
  Prevent viruses from infecting your computer by installing and regularly updating anti-virus software.
- ✓ **Block spyware attacks**
  Prevent spyware from infiltrating your computer by installing and updating anti-spyware software.

Top 10 Cyber Crime Prevention Tips

3. Be Social-Media Savvy

Make sure your social networking profiles (e.g. Facebook, Twitter, Youtube, MSN, etc.) are set to private. Check your security settings. Be careful what information you post online. Once it is on the Internet, it is there forever!

4. Secure your Mobile Devices

Be aware that your mobile device is vulnerable to viruses and hackers. Download applications from trusted sources.

5. Install the latest operating system updates

Keep your applications and operating system (e.g. Windows, Mac, Linux) current with the latest system updates. Turn on automatic updates to prevent potential attacks on older software.

6. Protect your Data

Use encryption for your most sensitive files such as tax returns or financial records, make regular back-ups of all your important data, and store it in another location.

Top 10 Cyber Crime Prevention Tips

7. Secure your wireless network

Wi-Fi (wireless) networks at home are vulnerable to intrusion if they are not properly secured. Review and modify default settings. Public Wi-Fi, a.k.a. “Hot Spots”, are also vulnerable. Avoid conducting financial or corporate transactions on these networks.

8. Protect your E-identity

Be cautious when giving out personal information such as your name, address, phone number or financial information on the Internet. Make sure that websites are secure (e.g. when making online purchases) or that you’ve enabled privacy settings (e.g. when accessing/using social networking sites).

Top 10 Cyber Crime Prevention Tips

9. Avoid being scammed

Always think before you click on a link or file of unknown origin. Don’t feel pressured by any emails. Check the source of the message. When in doubt, verify the source. Never reply to emails that ask you to verify your information or confirm your user ID or password.

10. Call the right person for help

Don’t panic! If you are a victim, if you encounter illegal Internet content or if you suspect a computer crime, identity theft or a commercial scam, report this to your local police. If you need help with maintenance or software installation on your computer, consult with your service provider or a certified computer technician.

More Definitions

- **Asset (or resource)**
  - – software, hardware, data, communication lines and equipment that we want to protect
- **Security policy**
  - – a set of rules or practices that specify how a system or organization is prescribed to protect its assets
- **Attack**
  - – a deliberate and intelligent attempt to violate the security policy of a system or get around security services
- **Adversary (or attacker)**
  - – an entity that attacks a system or is a threat to it

More Definitions

- **Zero-Day Attack**
  – an attack that exploits computer application vulnerabilities before the software developer releases a patch for the vulnerability.
- **Exploit**
  – a breach of IT system security through vulnerabilities, zero-day attacks or any other hacking techniques.
- **Countermeasure**
  – an action, procedure, or technique that reduces a threat or vulnerability, prevents or mitigates an attack

END