Fundamentals of Computer Security

Lecture 1

Introduction Part 1

Lecture Outline

- Introduction to computer security
- Fundamental security objectives
  - Their organizational impact levels
- Challenges of computer security
- Computer Security Architecture

Introduction

The why for security

1. Introduction of the computer, the need for automated tools for protecting files and other information stored on the computer is evident.

- This is especially the case for a shared system, such as a time-sharing system
- The need is even more acute for systems that can be accessed over a public data network.

Definition 1(Computer security): The generic name for the collection of tools designed to protect data and to thwart hackers

2. Introduction of distributed systems and the use of networks and communications facilities for carrying data between terminal user and computer and between computers.

Introduction

Definition 2(Network security):

Measures needed to protect data during their transmission and to guarantee that data transmissions are authentic.

- The essential technology underlying virtually all automated network and computer security applications is encryption.
- Two fundamental approaches are in use:

1. Symmetric encryption/Classical encryption
2. Asymmetric encryption/ Public-keyencryption

Introduction

Definition 3(Computer Security)

- 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) [NIST Computer Security Handbook [NIST95]]

National Institute of Standards and Technology: NIST is a U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government use and to the promotion of U.S. private-sector innovation. Despite its national scope, NIST Federal Information Processing Standards (FIPS) and Special Publications (SP) have a worldwide impact.

Introduction

- The security of a cryptographic system can rely either on the

1. Computational security: The computational infeasibility of breaking it.
2. Information-theoretic/Unconditional security: The theoretical impossibility of breaking it, even using infinite computing power.

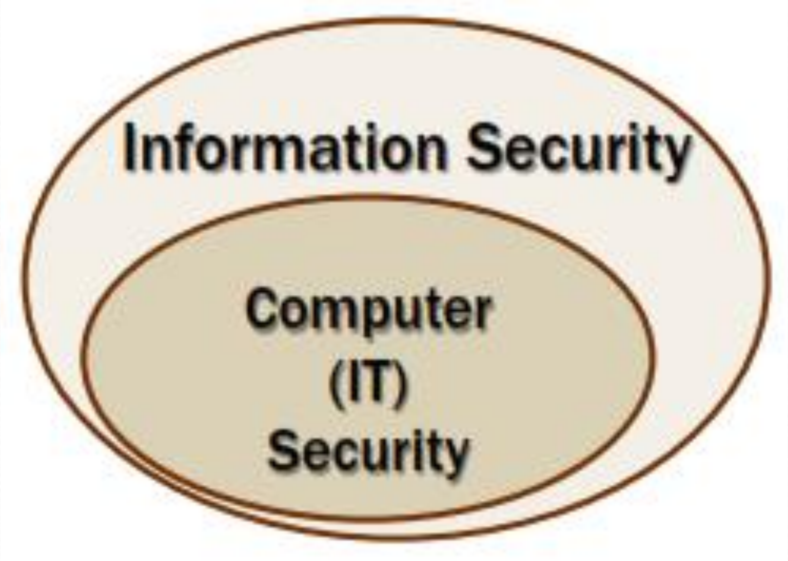
- Because no computational problem has been proved to be computationally difficult for a reasonable model of computation, the computational security of almost all cryptographic system used today relies on an unproven intractability assumption.
- In contrast, information-theoretically secure systems rely on no such assumptions but they rely on an assumption about the probabilistic behavior of the universe, for instance of a noisy channel or a quantum measurement.
- Note: Computationally-secure systems also rely on such assumptions, at least the tacitly made assumption that random keys can be generated and that they are independent of an adversary's entire a priori knowledge.

Introduction

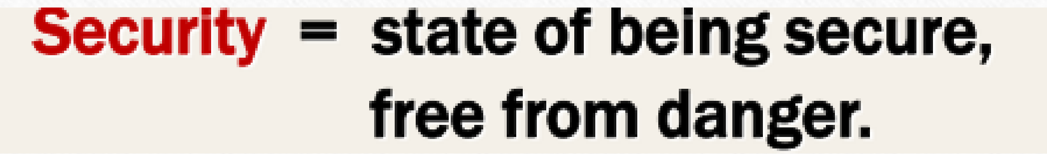
Computer Security vs. Information Security

Terms are often used interchangeably, but

- **Computer security** (aka IT security) is mostly concerned with information in ‘digital form’
- **Information security** is concerned with information in any form it may take: electronic, print, etc.

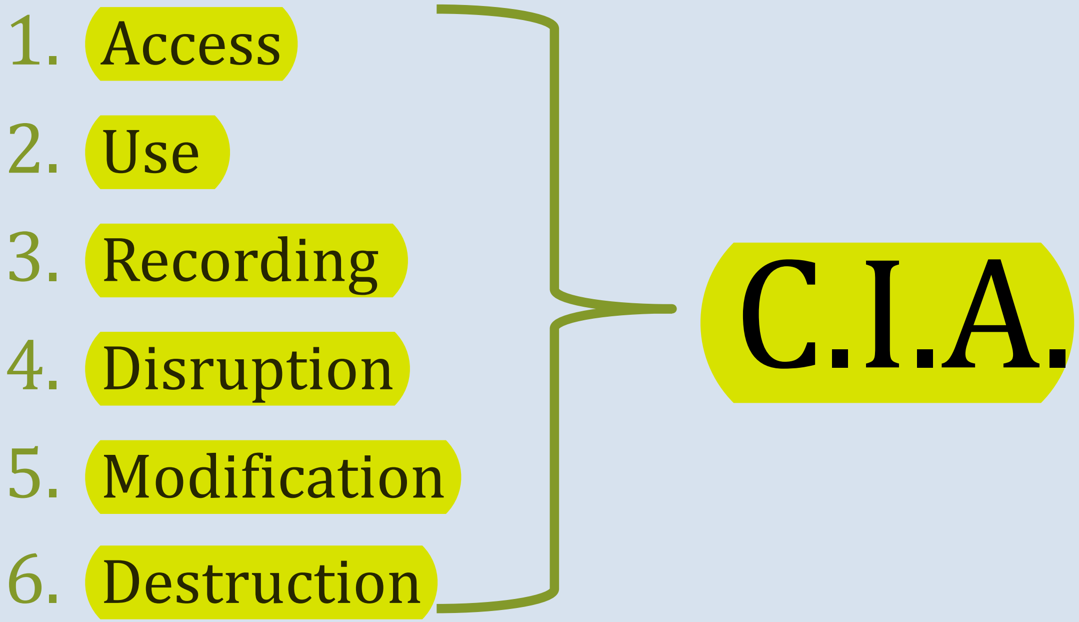


Introduction



Security = state of being secure, free from danger.

- Information Security – practice of defending digital information from unauthorized

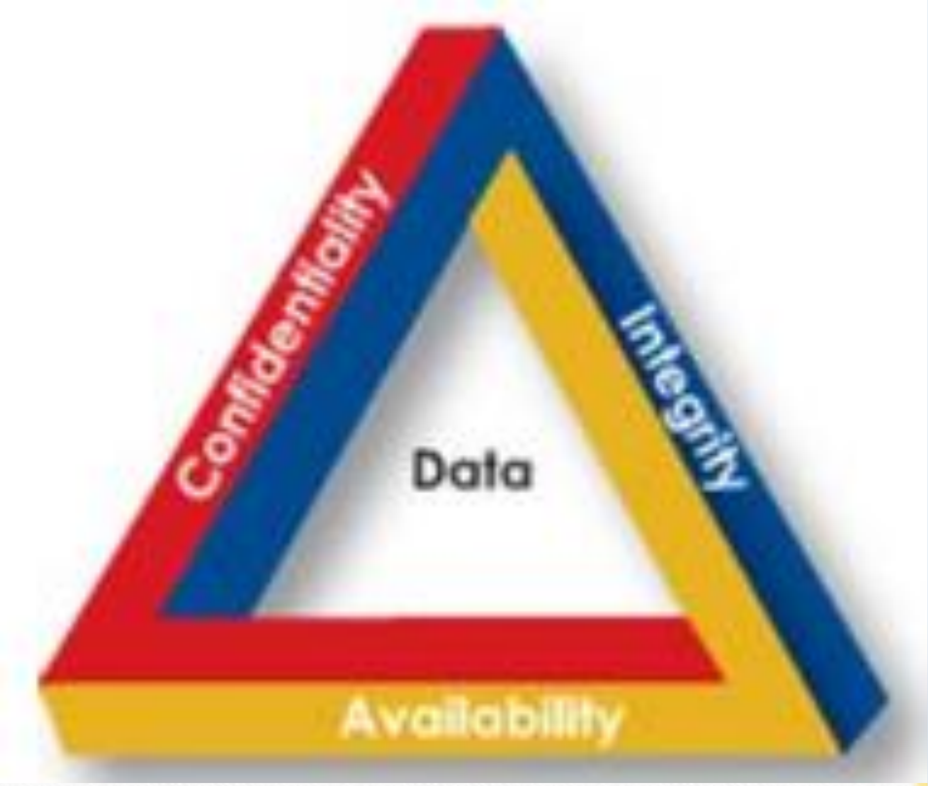


1. Access
2. Use
3. Recording
4. Disruption
5. Modification
6. Destruction

C.I.A.

Information C.I.A

Three key concepts are at the heart of computer security:



Security Requirements Triad

- The three concepts embody the fundamental security objectives for data and for information and computing services.
- For example, the NIST standard FIPS 199 *lists confidentiality, integrity, and availability as the three* security objectives for information and for information systems.
- FIPS 199 provides a useful characterization of these three objectives in terms of requirements and the definition of a loss of security in each category:

1. Confidentiality

- Preserving authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information.

A loss of confidentiality: The unauthorized disclosure of information.

This term covers two related concepts:

1. **Data confidentiality:** Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
2. **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.

2. Integrity

- Information is changed only in an a specified and authorized manner
- Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.

A loss of integrity: The unauthorized modification or destruction of information.

This term covers two related concepts:

1. **Data integrity:** Assures that information and programs are changed only in a specified and authorized manner.
2. **System integrity:** Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

3. **Availability**

- Ensuring timely and reliable access to and use of information.

A loss of availability: The disruption of access to or use of information or an information system.

Assures that systems work promptly and service is not denied to authorized users.

- These three concepts form what is often referred to as the **CIA triad** (before).
- They embody the fundamental security objectives for data, information and computing services.

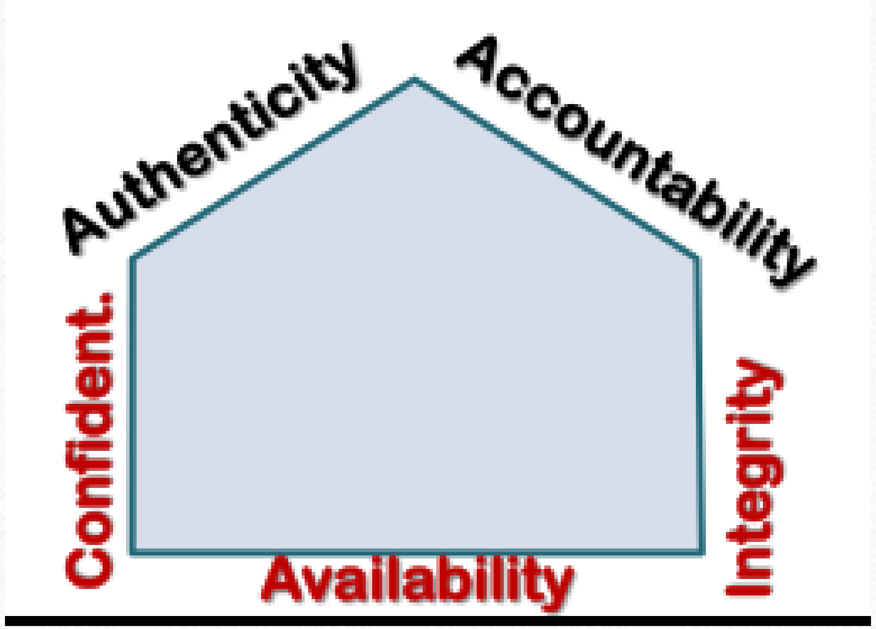
Extended C.I.A

- Although the use of the CIA triad to define security objectives is well established, others in the security field feel that additional concepts are needed to present a complete picture. Two of the most commonly mentioned are as follows:

1. **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.

2. **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. 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.

Extended C.I.A



Organizational Security impact levels

Organizational impact levels

- Levels of impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability).
- These levels are defined in FIPS PUB 199.
- **Low level:** The loss could be expected to have a limited adverse effect on

1. Organizational operations
2. Organizational assets
3. Individuals

- A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might,

1. Cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
2. Result in minor damage to organizational assets
3. Result in minor financial loss
4. Result in minor harm to individuals

Organizational impact levels

- **Moderate:** The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss might

(i) Cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;

(ii) Result in significant damage to organizational assets

(iii) Result in significant financial loss

(iv) Result in significant harm to individuals that does not involve loss of life or serious, life-threatening injuries

Organizational impact levels

- **High:** The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss might

(i) Cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;

(ii) Result in major damage to organizational assets

(iii) Result in major financial loss

(iv) Result in severe or catastrophic harm to individuals involving loss of life or serious, life-threatening injuries

Examples

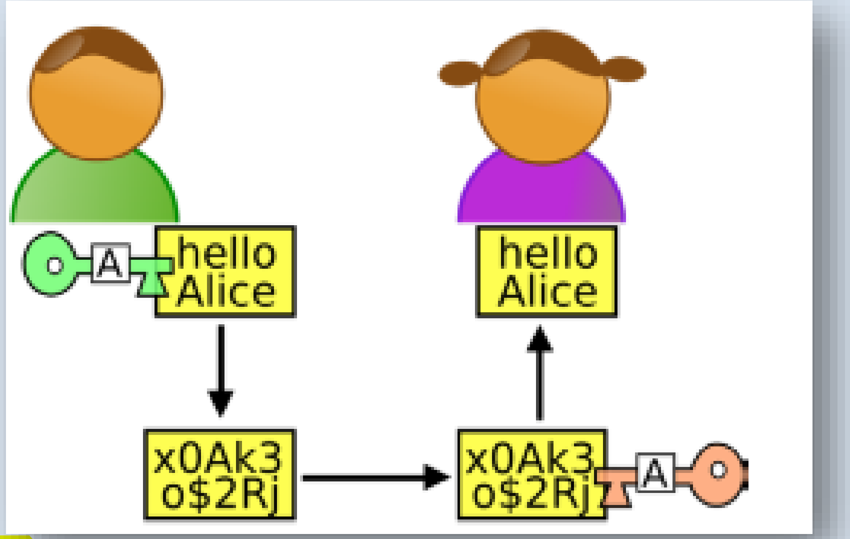
- *CONFIDENTIALITY*

1. **High:** Student grade information is an asset whose confidentiality is considered to be highly important by students. Grade information should only be available to students, their parents, and employees that require the information to do their job.
2. **Medium:** Student enrollment information may have a moderate confidentiality rating. This information is seen by more people on a daily basis and therefore less likely to be targeted than grade information, and results in less damage if disclosed.
3. **Low:** Directory information, such as lists of students or faculty or departmental lists, may be assigned a low confidentiality rating or indeed no rating. This information is typically freely available to the public and published on a school’s Web site.

Examples

HOW TO ENSURE CONFIDENTIALITY

- Example: How do you ensure data confidentiality?
- Cryptography



- Strong access control
- Limiting number of places where data can appear (e.g., read only, cannot be stored on an USB)

INTEGRITY

1. **High:** Several aspects of integrity are illustrated by the example of a hospital patient's allergy information stored in a database. The doctor should be able to trust that the information is correct and current. Now suppose that an employee (e.g., a nurse) who is authorized to view and update this information deliberately falsifies the data to cause harm to the hospital.
   - The database needs to be restored to a trusted basis quickly, and it should be possible to trace the error back to the person responsible.

- Patient allergy information is an example of an asset with a high requirement for integrity.
  - Inaccurate information could result in serious harm or death to a patient and expose the hospital to massive liability.

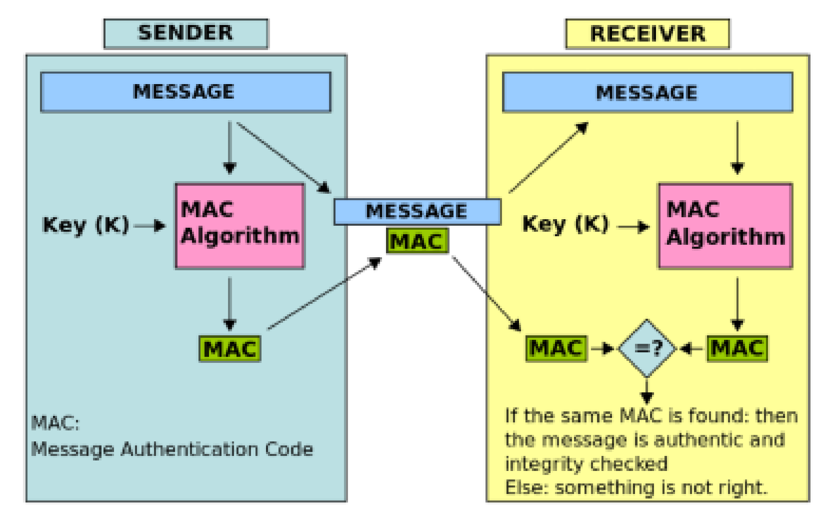
INTEGRITY

2. **Medium:** Web site that offers a forum to registered users to discuss some specific topic. Either a registered user or a hacker could falsify some entries or deface the Web site. If the forum exists only for the enjoyment of the users, brings in little or no advertising revenue, and is not used for something important such as research, then potential damage is not severe. The Web master may experience some data, financial, and time loss.
3. **Low:** An anonymous online poll. Many web sites, such as news organizations, offer these polls to their users with very few safeguards. However, the inaccuracy and unscientific nature of such polls is well understood.

Examples

HOW TO ENSURE INTEGRITY?

- Example: How do you ensure data integrity?
- Cryptography


SENDER
MESSAGE
Key (K)
MAC Algorithm
MAC
MAC:
Message Authentication Code
MESSAGE
MAC
RECEIVER
MESSAGE
Key (K)
MAC Algorithm
MAC
=?
MAC
If the same MAC is found: then the message is authentic and integrity checked
Else: something is not right.

- Strong access control
- Documenting system activity

AVAILABILITY

The more critical a component or service, the higher is the level of availability required.

1. **High:** Consider a system that provides authentication services for critical systems, applications, and devices. An interruption of service results in the inability for customers to access computing resources and staff to access the resources they need to perform critical tasks.

The loss of the service translates into a large financial loss in lost employee productivity and potential customer loss.

AVAILABILITY

The more critical a component or service, the higher is the level of availability required.

2. **Medium:** An example of an asset that would typically be rated as having a moderate availability requirement is a public Web site for a university; the Web site provides information for current and prospective students and donors. Such a site is not a "critical" component of the university's information system, but its unavailability will cause some embarrassment.

AVAILABILITY

The more critical a component or service, the higher is the level of availability required.

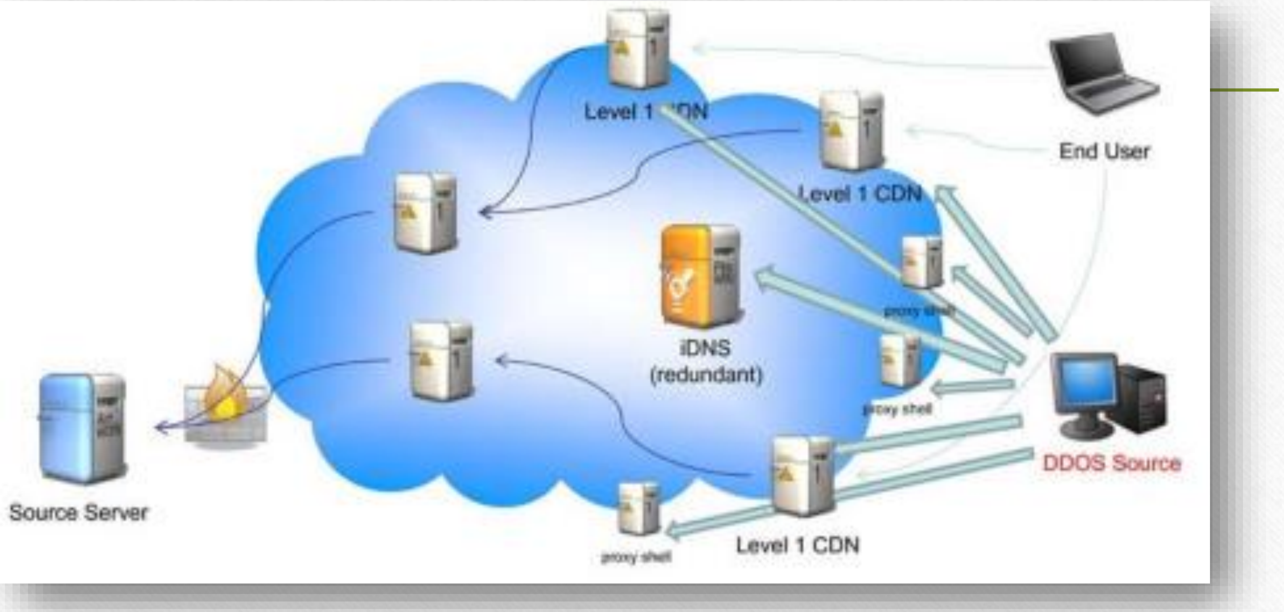
3. **Low:** An online telephone directory lookup application would be classified as a low availability requirement. Although the temporary loss of the application may be an annoyance, there are other ways to access the information, such as a hardcopy directory or the operator.

Examples

HOW TO ENSURE AVAILABILITY?

Example: How do you ensure data availability?

- Anti-DDoS system



- Well established backup procedure
- Effective data-recovery procedure

Challenges of Computer Security

Challenges of Computer Security

Computer and network security is both fascinating and complex. Reasons being:

1. Security is not as simple as it might first appear to the novice. The requirements seem to be straightforward; indeed, most of the major requirements for security services can be given self-explanatory, one-word labels: confidentiality, authentication, nonrepudiation, or integrity.
   - But the mechanisms used to meet those requirements can be quite complex, and understanding them may involve rather subtle reasoning.

Challenges of Computer Security

Computer and network security is both fascinating and complex. Reasons being:

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

In many cases, successful attacks are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism.

Challenges of Computer Security

3. Because of point 2, the procedures used to provide particular services are often counterintuitive. Typically, a security mechanism is complex, and it is not obvious from the statement of a particular requirement that such elaborate measures are needed. It is only when the various aspects of the threat are considered that elaborate security mechanisms make sense.

4. Having designed various security mechanisms, it is necessary to decide where to use them. This is true both in terms of physical placement (e.g., at what points in a network are certain security mechanisms needed) and in a logical sense [e.g., at what layer or layers of an architecture such as TCP/IP should mechanisms be placed].

Challenges of Computer Security

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

- There also may be a reliance on communications protocols whose behavior may complicate the task of developing the security mechanism.
- For example, if the proper functioning of the security mechanism requires setting time limits on the transit time of a message from sender to receiver, then any protocol or network that introduces this variable, unpredictable delays may render such time limits meaningless.

Challenges of Computer Security

6. Computer and network security is essentially a battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them.

   - The great advantage that the attacker has is that he or she need only find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security.

Challenges of Computer Security

7. 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.

8. Security requires regular, even constant, monitoring, and this is difficult in today’s short-term, overloaded environment.

9. 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.

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.

IT Security Challenges in 2015

IT Security Challenges in 2015

With big data and advanced-analytics management revolution in full swing, 2015 was a whole different ballgame for IT security.

According to surveys, Chief Information Officers (CIO) agreed that in case of budget cuts, security planning should be last on the list to receive it and stricter security policies must be enforced to stay one step ahead in the security arena.

Main challenges include;

1. Data Security: Increasingly more and more sensitive data is stored and handled by public clouds such as Amazon Web Services. This presented a paradigm shift in security management for IT teams managing this data. CIOs must have clear answers to questions such as how specifically data breach would affect the business, how zealously it must be guarded and what to do in case of a data breach.

IT Security Challenges in 2015

2. Visibility: Data is everywhere and this makes overall data visibility a challenge. Lack of visibility makes controlling data difficult leaving it vulnerable to breach.

- Usually CIOs are the last to know when a breach occurs due to lack of full visibility into the location of critical data. It is therefore critical that CIOs spend time and money in the security measures that will really protect the organization from an attack.

IT Security Challenges in 2015

3. Third Party Vendors: With increasing third party providers, organizations need to seriously think of processes to put in place to avoid situations where a vendor accidentally provides access to an organization's data, intellectual property, plans or negotiations that can lead to an unintended security breach.

- Cybercriminals generally take the path of least resistance, and they've learned that contractors and other third-party providers can provide an opening into otherwise-secured corporate networks.
- Major data breaches at retailers like Target and Home Depot occurred because attackers were able to obtain valid network credentials from trusted, third-party providers, and just walk right in.

IT Security Challenges in 2015

3. Third Party Vendors:

Third-Party Vendors a Weak Link in Security Chain

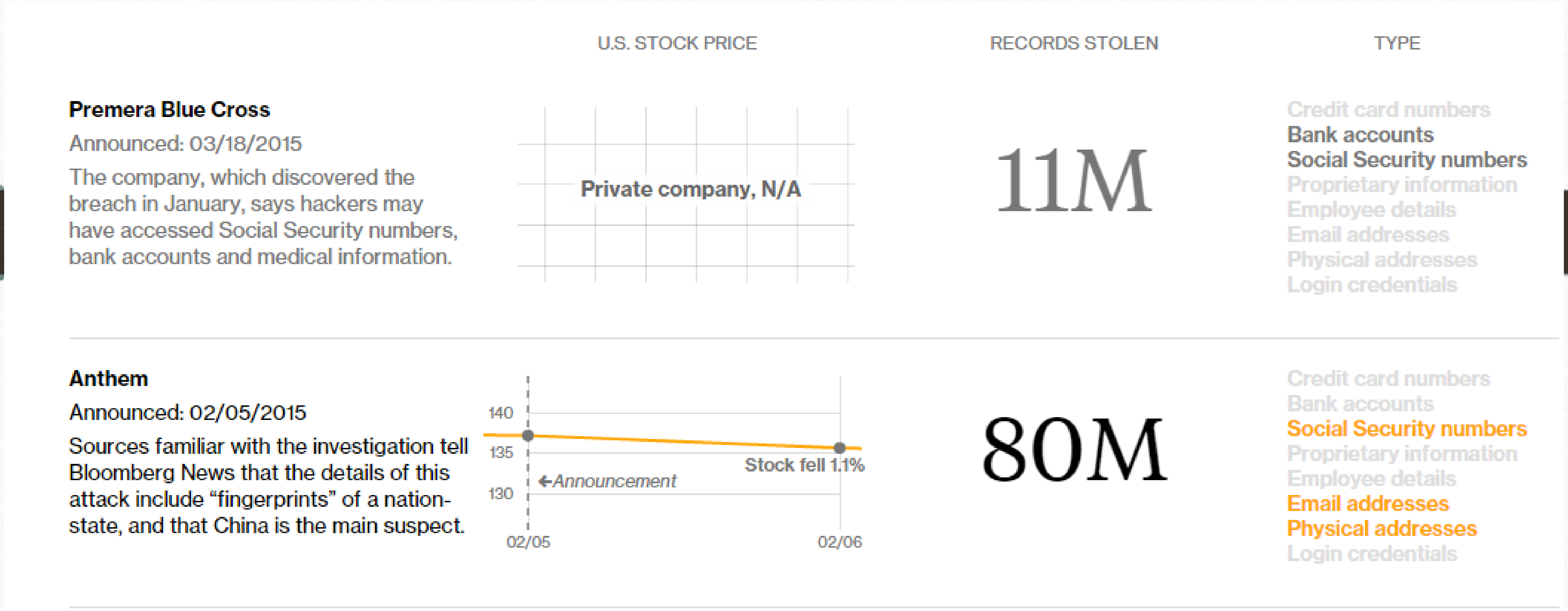
“Security shortcomings of third-party vendors are a cybercriminal's dream. So security pros should revisit how they manage vendor relationships.”

http://www.esecurityplanet.com/network-security/third-party-vendors-a-weak-link-in-security-chain.html March 6, 2015

- Credit card data of 40 million Target customers, 15,000 Boston Medical Center patients’ personal information, and payment card information of 868,000 Goodwill customers – all of this information was exposed as a result of data breaches not at the companies themselves, but at vendors with access to the companies’ systems.
- A recent BitSight Technologies study found that one third of U.S. retailers that experienced a data breach within the past year were compromised via third-party vendors.

IT Security Challenges in 2015

Data breaches in 2015



	U.S. STOCK PRICE	RECORDS STOLEN	TYPE
Premera Blue Cross Announced: 03/18/2015 The company, which discovered the breach in January, says hackers may have accessed Social Security numbers, bank accounts and medical information.	Private company, N/A	11M	Credit card numbers Bank accounts Social Security numbers Proprietary information Employee details Email addresses Physical addresses Login credentials
Anthem Announced: 02/05/2015 Sources familiar with the investigation tell Bloomberg News that the details of this attack include "fingerprints" of a nation-state, and that China is the main suspect.	140 135 130 ←Announcement Stock fell 1.1% 02/05 02/06	80M	Credit card numbers Bank accounts Social Security numbers Proprietary information Employee details Email addresses Physical addresses Login credentials

IT Security Challenges in 2015

4 Compartmentalization (separation of privileges): Traditional approach for data security of serving data on a ‘need to know’, ’least privilege’ and ‘breach containment’ basis ensured that if something went wrong, the breach was contained.

- In today’s era of ubiquitous data, CIOs need to protect data from multiple attack vectors and explore new techniques of compartmentalization to provide defensible security and privacy.

IT Security Challenges in 2015

5 Bring Your Own Device (BYOD): The BYOD trend is here to stay and very few organizations have good policy guidelines for these devices.

- The challenge is to manage risks stemming from device mismanagement, external manipulation of vulnerabilities in the device and deployment of unreliable business applications.

IT Security Challenges in 2015

6. Cloud migration: 2013 was the year companies moved critical systems into the cloud.

- This migration into virtual shared infrastructures changes how information security and risk management is addressed.
- Challenge: Cloud security processes and solutions are still being developed.
- Hope: Ultimately, with innovation and planning, cloud services could reduce business risks by providing greater flexibility, resiliency and security.

IT Security Challenges in 2015

6. Insider threat: A dissatisfied employee base provides a vector for insider security events, while the inadvertent injection of malware through removable media or web interconnections can make any employee the origination point for a network security violation.

IT Security Challenges in 2015

7. **Mobility:** Management and security of mobile networks and smart mobile devices becomes even more challenging when employees want to use their own devices for business purposes.

- The bring-your-own-device trend exasperates this challenge when we look at protecting the critical information needed to manage the organization and the network without sacrificing the privacy of employee's personal information and activities.

Major Data Breaches projected in 2016

Data Breaches - 2016

1. Evolving malware

- More sophisticated malware continue to defeat detection by hiding in common services and using non-traditional forms of communication such as TOR or peer to peer.
- Highly effective social engineering ploys, such as those utilized in ransomware, will continue to terrorize businesses.

  For all malware infections, prevention is definitely better than cure
- However, one cannot stop infections 100 percent of the time.
- So?

1. Keep operating systems and software updated
2. Install robust security defenses such as firewalls, IDS, spam and virus filtering and web filtering
3. Perform regular security awareness training to identify attacks
4. Always back up your data so if you do fall victim, you can simply restore your files

Data Breaches - 2016

2. Breach tsunami

- The many breaches that occurred in 2015, and the abundance of credit card and other personal information obtained from them, will lead to an increase in spear-phishing and other more targeted attacks.
- The amount of private personal information that exists on the cyber underground, coupled with further information gleaned from social media, means criminals can generate highly targeted attacks or used as convincers in fraudulent transactions.

Data Breaches - 2016

3. Cyber warfare

- Acts of cyber aggression will continue amongst many nation states including the US and China, as well as remain a tool of warring nations.
- While we may not be privy to the majority of these attacks against infrastructure or corporate espionage between our collective countries, evidence suggests that the Internet has become an important tool in every aspect of our lives including war and politics.

Data Breaches - 2016

4. Internet of Things

- Practically every business and even some individuals will have Wi-Fi enabled fixed devices that are controlled remotely: from switching on lights at home to cooling nuclear reactors in power plants.
- When vulnerabilities exist in any popular OS, and hackers know about them, it is only a matter of time before they are exploited.
  - Challenge: People are not installing security patches in a timely manner, and inadvertently leaving their devices vulnerable.

Data Breaches - 2016

5. Bring your own device (BYOD)

- No threat list would be complete without referencing this threat. BYOD often provides the business with cost savings and increased productivity/effectiveness from their workforce.
- Security challenge: This movement has created has also left IT departments in a bit of a quandary/confusion.
- Requirement: Organizations need to have a BYOD strategy and policy that is appropriate to their situation.
  - Points to address with the policy include: password enforcement; encryption; device management; access control, etc. should all be kept in mind while still maintaining enough freedom to keep the employee happy.

Data Breaches - 2016

6. TOR (The Onion Ring)

- Often referred to as the ‘Dark’ or ‘Deep’ Web, TOR continues to attract both the good and bad of society, lured by its promise of anonymity.
- Facebook’s move into the TOR network may inspire other reputable services to want to provide anonymous access thereby enticing new users who may have been unwilling to try them beforehand.

Data Breaches - 2016

7. Mobile payment systems

- Vendors have been trying hard to change the way we make transactions with features such as Near Field Communication and virtual wallets in mobile devices

8. Individual cloud storage

- The use of Dropbox, OneDrive, Box, Google Drive as well as all of the other cloud storage services by individuals as a means to more easily access documents in multiple locations will pose a greater risk to personal as well as professional targets as company documents and data co-mingle with personal files in the cloud.

Data Breaches – 2016 Kenya

Hackers Leak 1TB Data from Kenya's Ministry of Foreign Affairs (April 29, 2016)

- 1TB of files contains PDF files, DOCX files, other "non sensitive" information around 1 TB of total information
- Kenyan government confirmed data breach and said none of the stolen documents were labeled as "secret".

Data Breaches – 2016 Japan

Fraudsters stole ¥1.4 Billion from around 1,400 Japanese ATMs in just 3 hours (May 15, 2016)

- “In just three hours, over 100 criminals managed to steal ¥1.4 Billion (*approx. US$12.7 Million*) from around 1,400 ATMs placed in small convenience stores across Japan.
- The heist took place on May 15, between 5:00 am and 8:00 am, and looked like a coordinated attack by an international crime network.
    - The crooks operated around 1,400 convenience store ATMs from where the cash was withdrawn simultaneously in 16 prefectures around Japan, including Tokyo, Osaka, Fukuoka, Kanagawa, Aichi, Nagasaki, Hyogo, Chiba and Niigata, The Mainichi reports”.

BREAK

Computer Security Architecture

Computer Security Architecture

Provides a systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements.

Computer Security Architecture

Important Definitions: Threat vs. Attack

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

That is, a threat is a possible danger that might exploit a vulnerability.

Attack

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Computer Security Architecture

The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as

- ❑ **Security attack:** Any action that compromises the security of information owned by an organization.
- ❑ **Security mechanism:** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
- ❑ **Security service:** A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

Computer Security Architecture: **Security attack**

A useful means of classifying security attacks, used both in X.800 and RFC 2828, is in terms of *passive attacks and active attacks.*

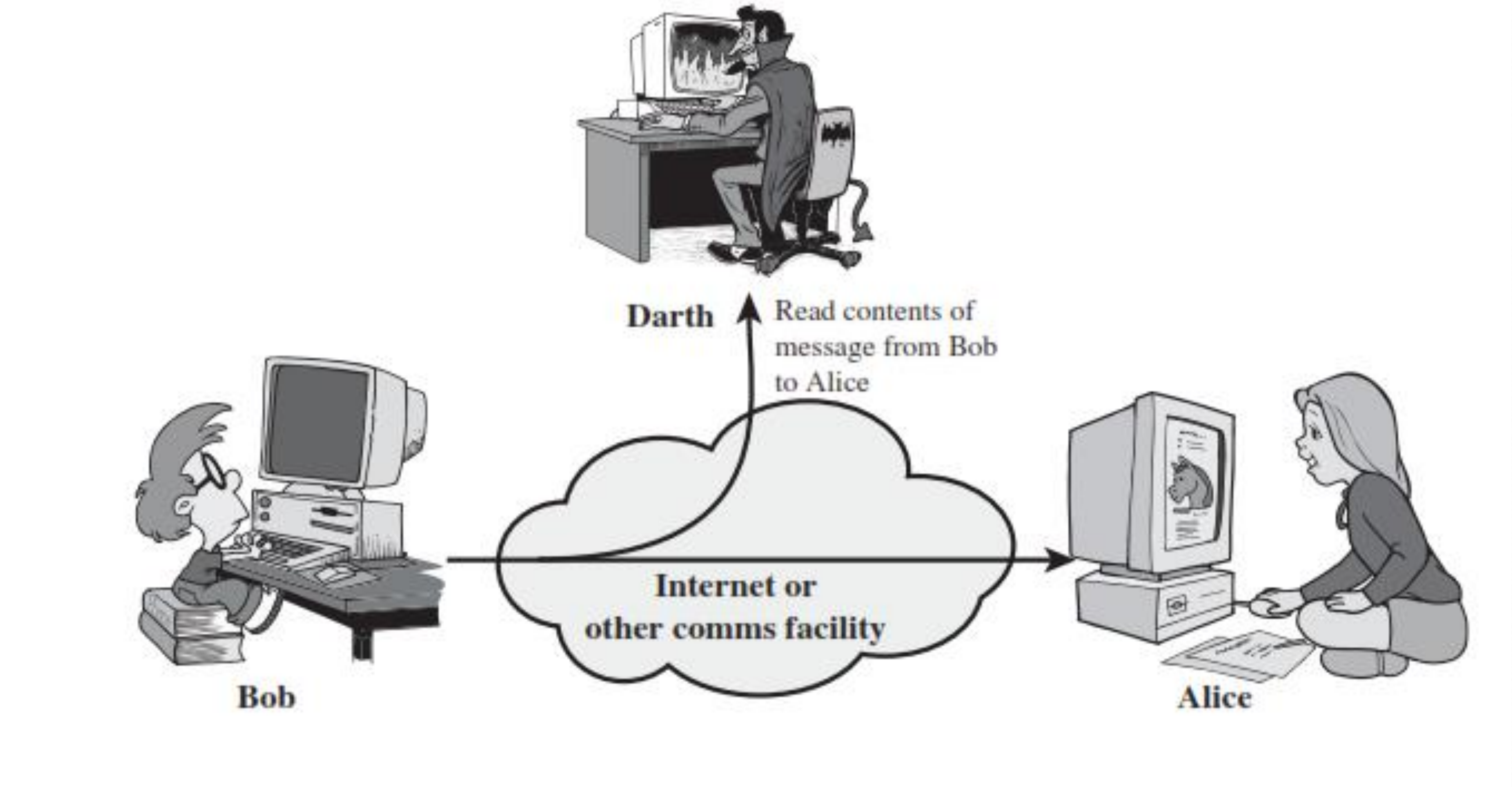
Passive Attacks

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. Two types of passive attacks are the release of message contents and traffic analysis.

1. **Release of message contents** is easily understood. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

Computer Security Architecture: **Security attack**

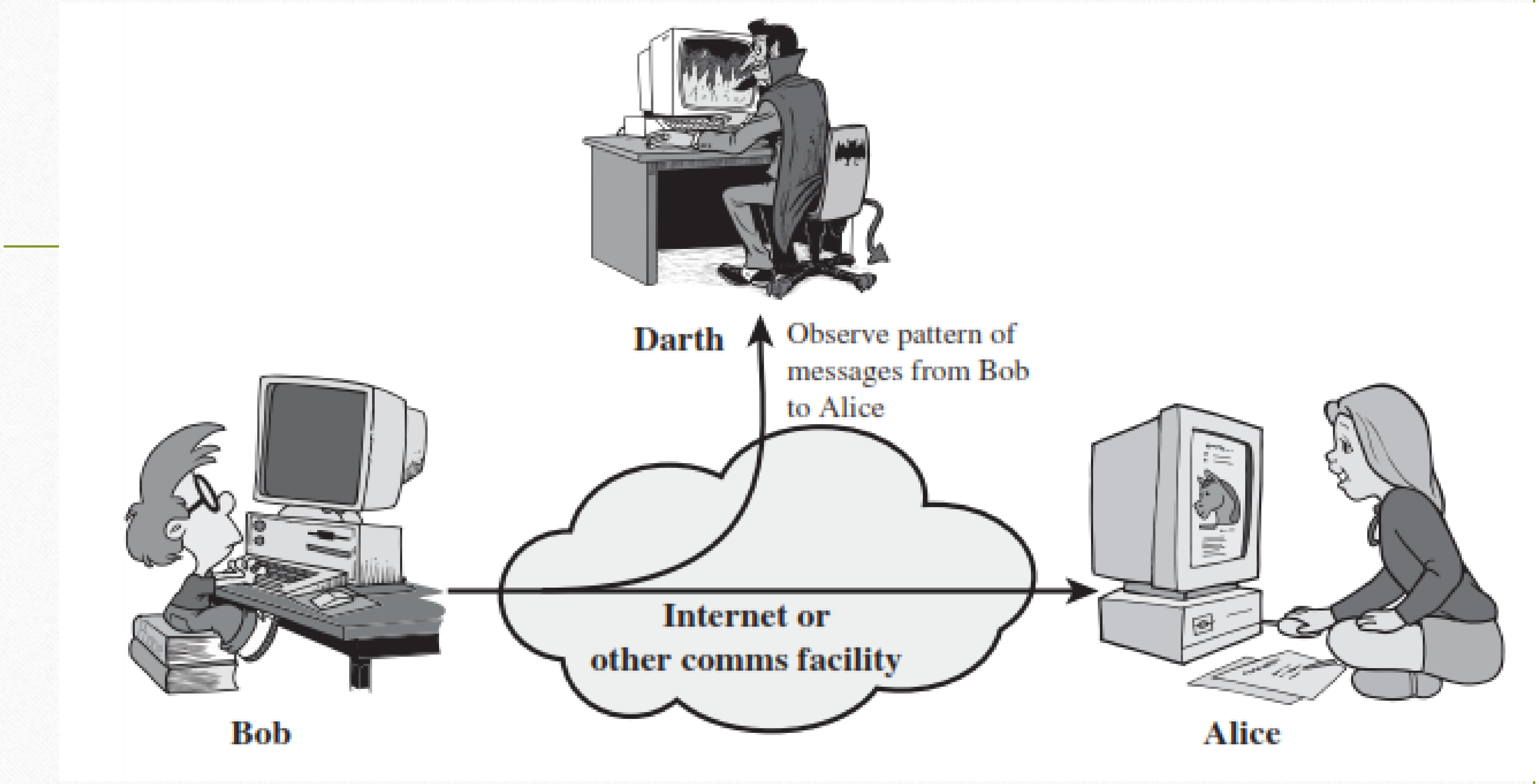

Darth
Read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

Computer Security Architecture: **Security attack**

2. **Traffic analysis:** Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption.

With encryption protection in place, an opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

Computer Security Architecture: **Security attack**


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

Computer Security Architecture: **Security attack**

Note:

- 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 receiver is aware that a third party has read the messages or observed the traffic pattern.
- However, it is feasible to prevent the success of these attacks, usually by means of encryption.
- Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.

Computer Security Architecture: **Security attack**

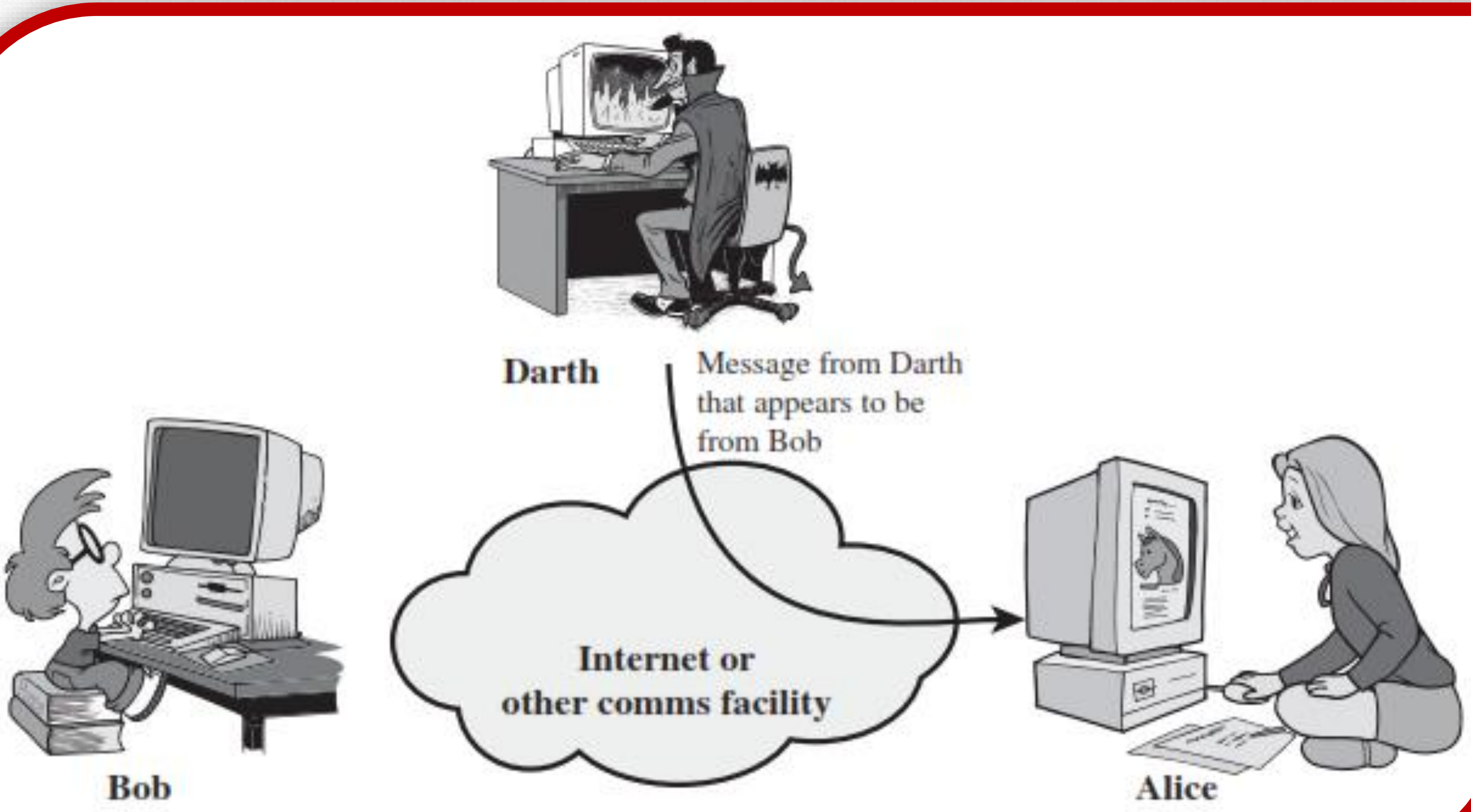
Active Attacks

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

1. Masquerade
2. Replay
3. Modification of messages
4. Denial of service

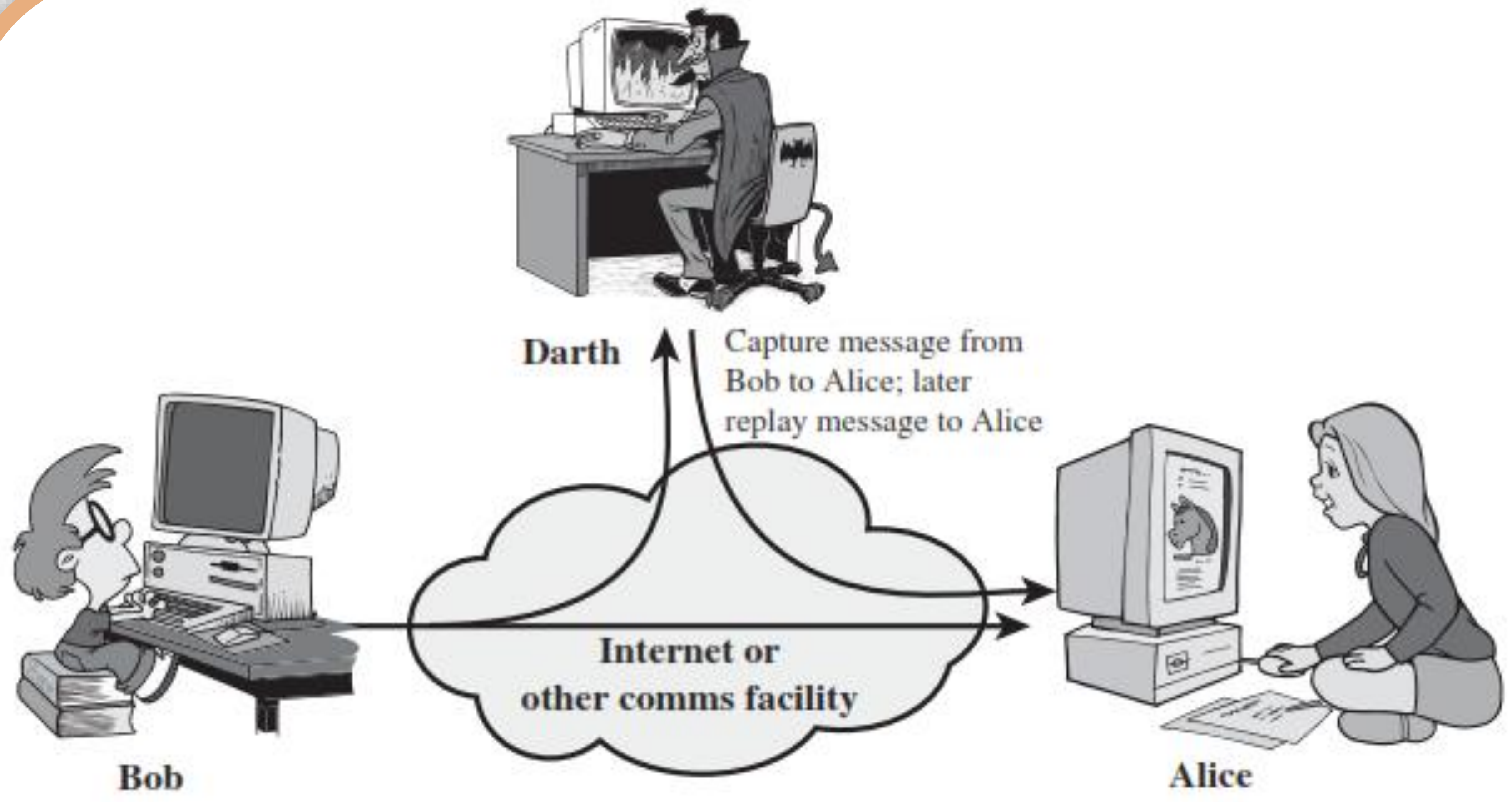
Masquerade

- 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.


Darth
Message from Darth that appears to be from Bob
Bob
Internet or other comms facility
Alice

Replay

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



Modification

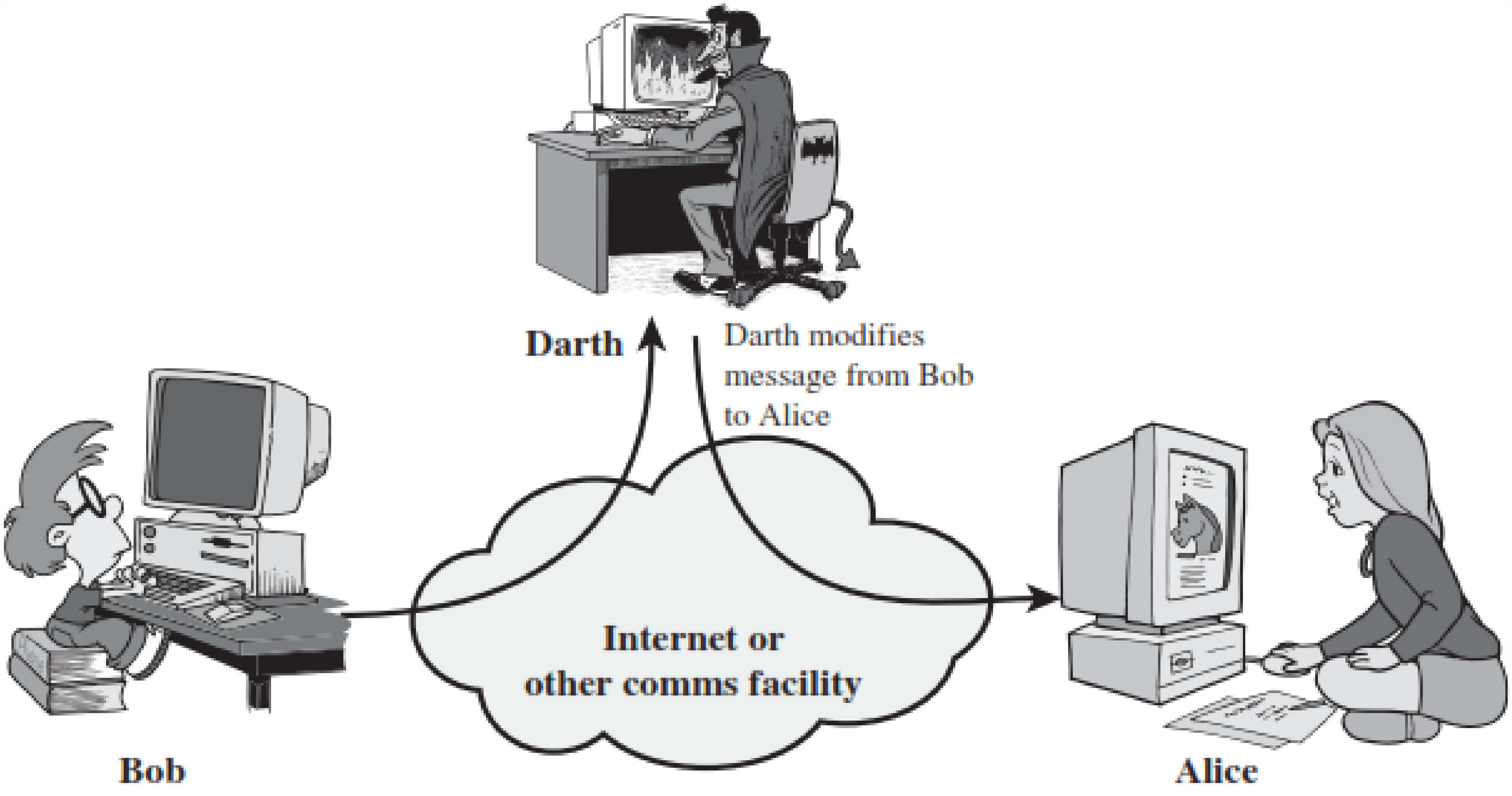
Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.

Example, a message meaning

"Allow John Odhiambo to read confidential file *accounts*"

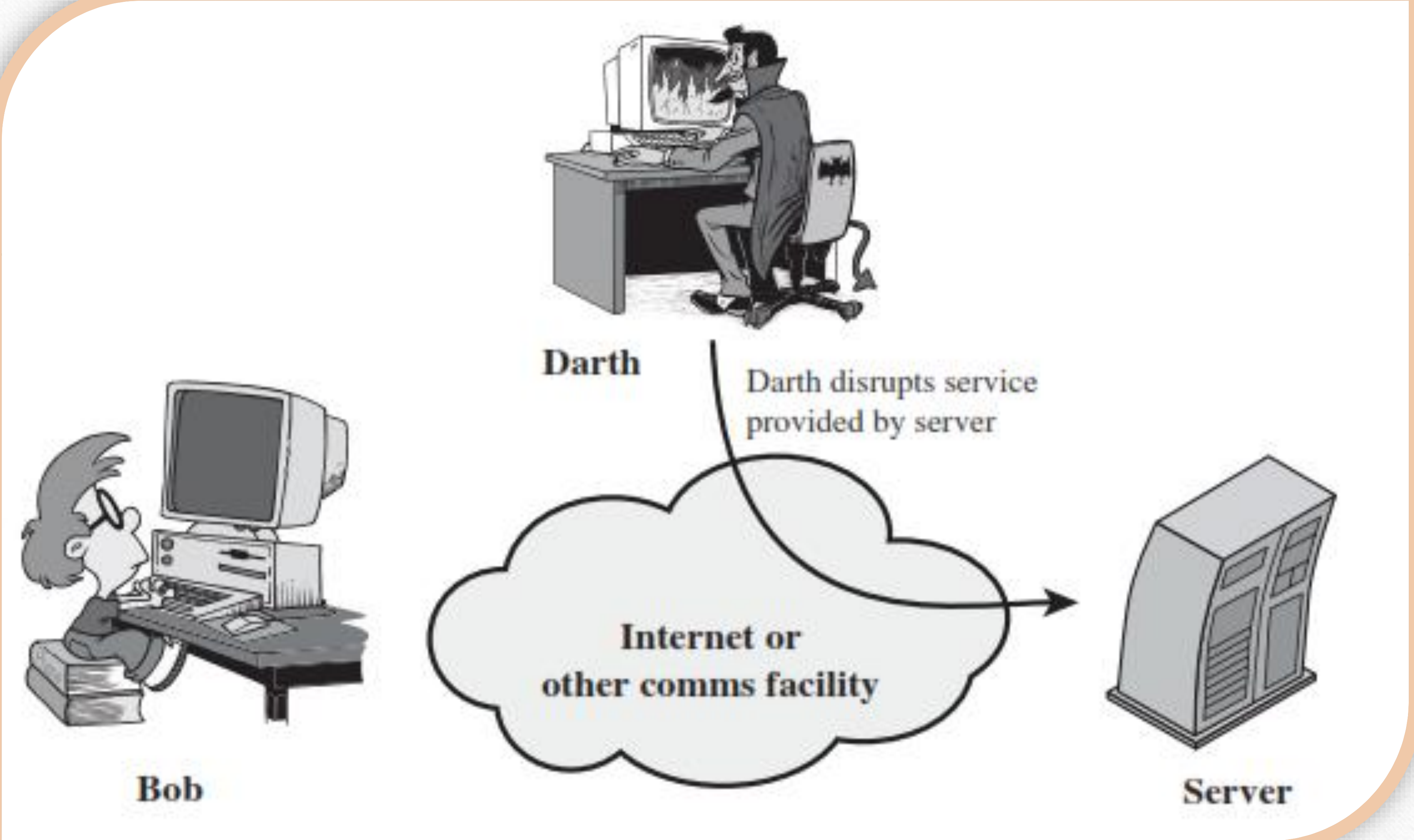
is modified to mean

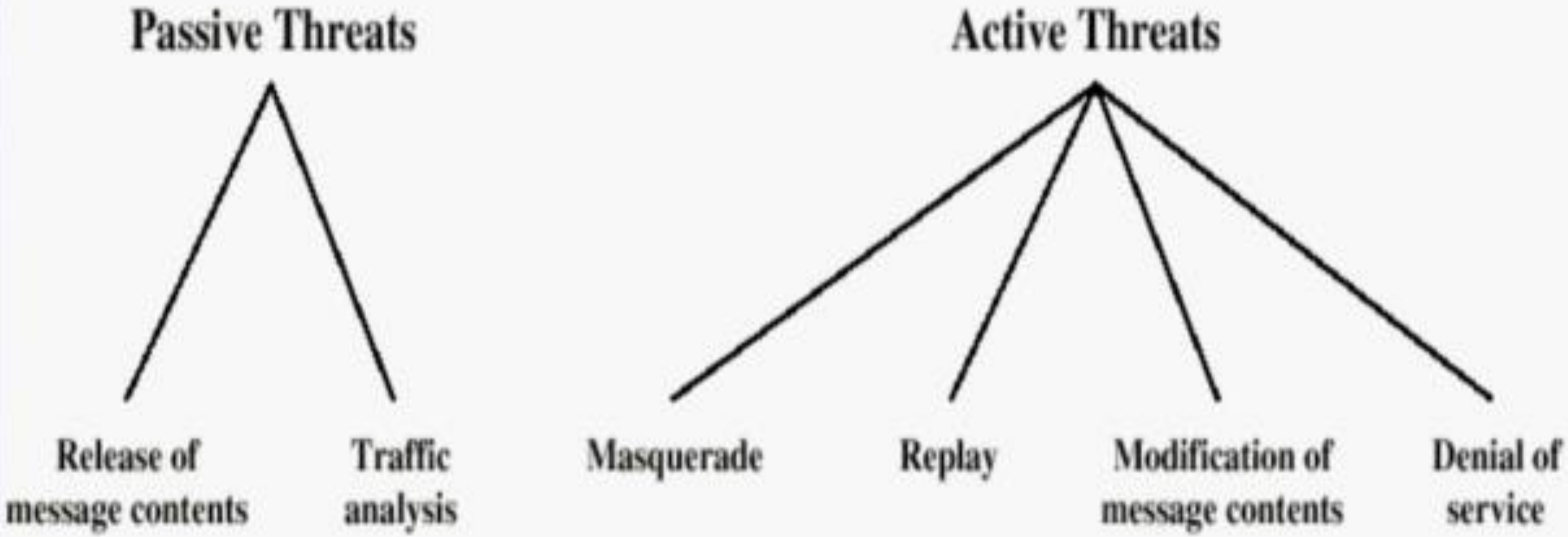
"Allow Fred Brown to read confidential file *accounts"*


Darth
Darth modifies message from Bob to Alice
Bob
Internet or other comms facility
Alice

Denial of service (DoS)

- **Denial of service** prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target.
- Example, an entity may suppress all messages directed to a particular destination (e.g. the security audit service).
- Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.


Darth
Darth disrupts service provided by server
Bob
Internet or other comms facility
Server


Passive Threats
Release of message contents
Traffic analysis
Active Threats
Masquerade
Replay
Modification of message contents
Denial of service

Handling Attacks:

Active attacks present the opposite characteristics of passive attacks

- Passive attacks – focus on Prevention

  Easy to stop

  Hard to detect
- Active attacks – focus on Detection and Recovery

  Hard to stop: because of the wide variety of potential physical, software, and network vulnerabilities.

  Easy to detect

BREAK