İTÜ

Computer Security

Introduction to Computer Security

Dr. Şerif Bahtiyar

bahtiyars@itu.edu.tr

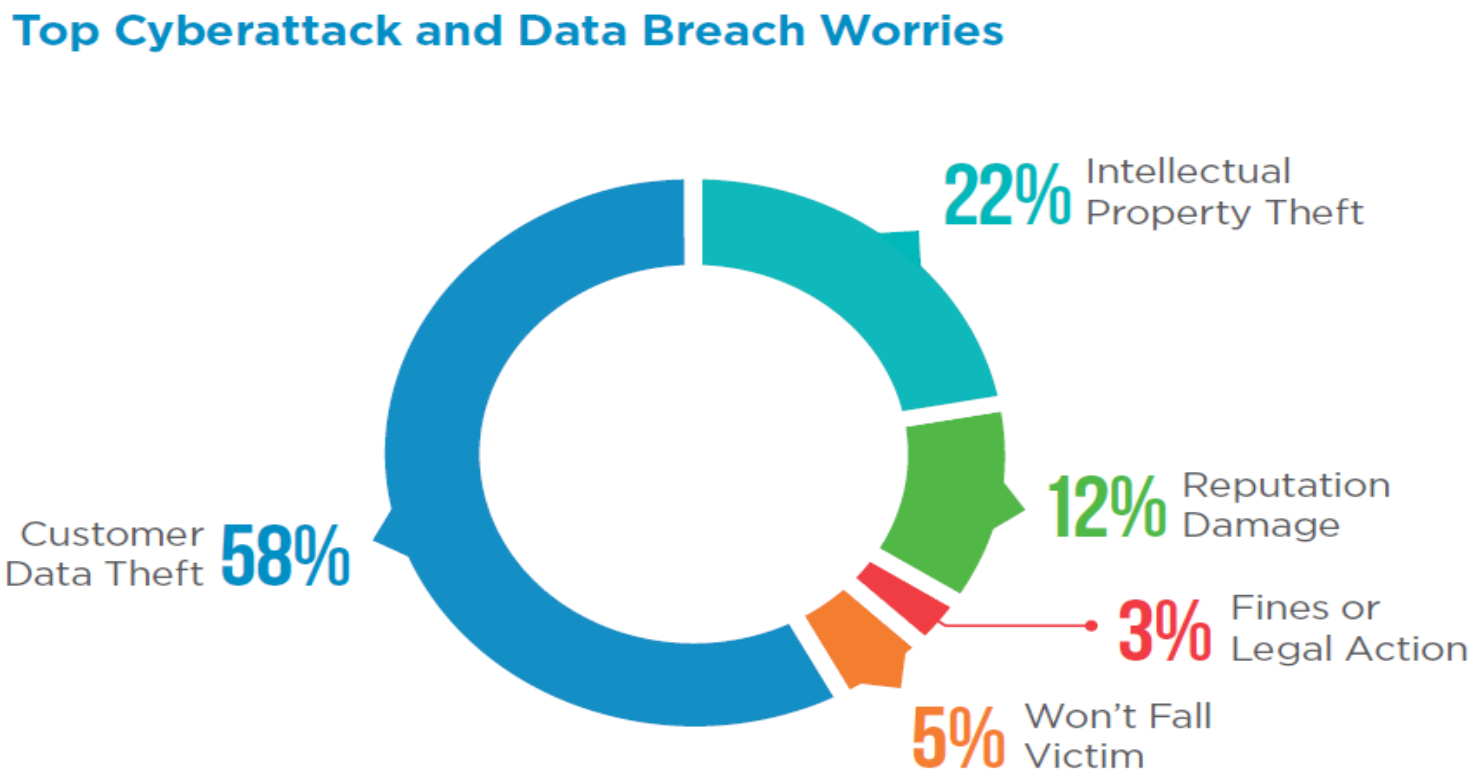
Fall 2015

What is this course about ?

This course is to

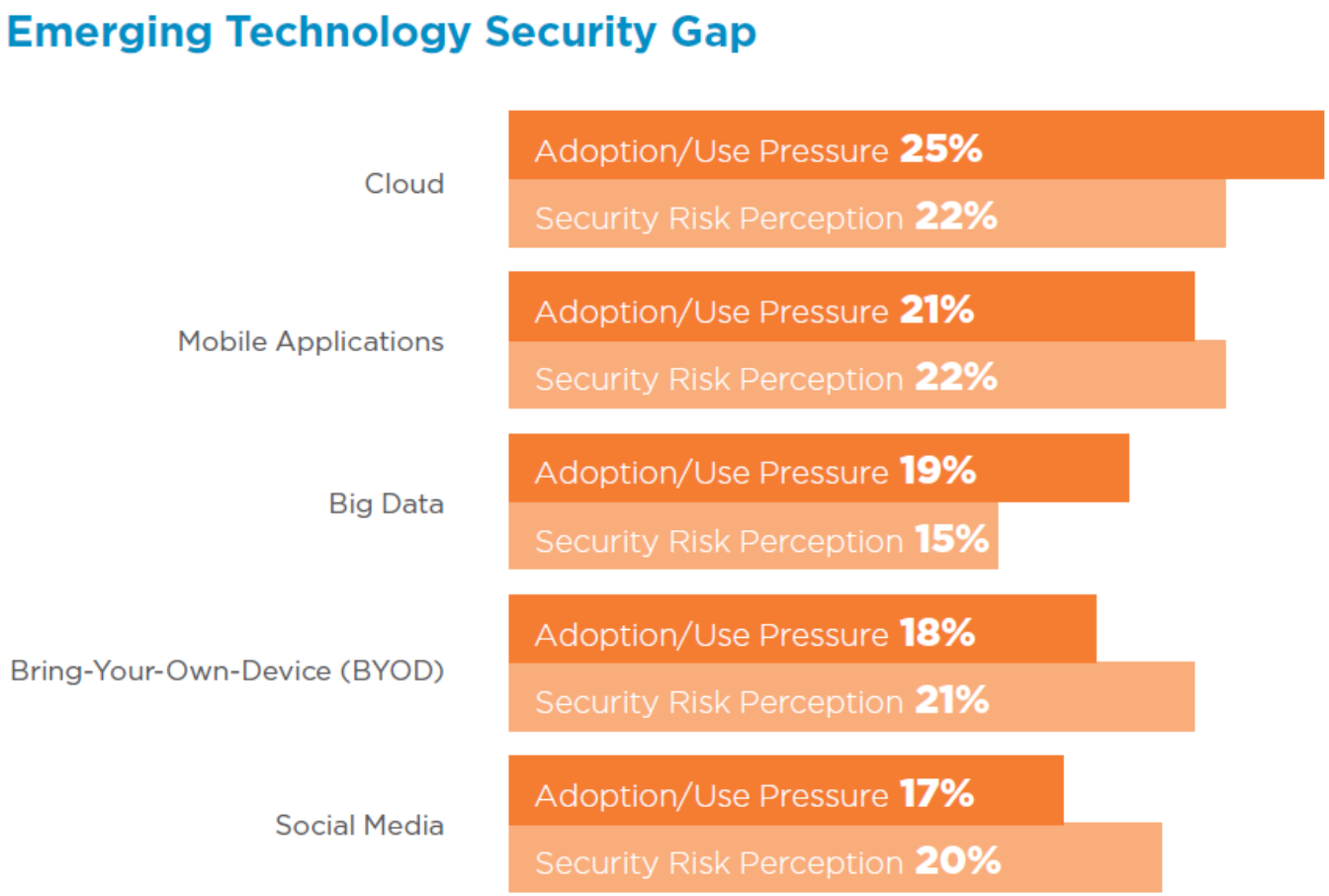
- provide general overview of computer security
  - requirements
  - services
  - mechanisms
- discuss basic principles of threats
- discuss methods of securing computer systems

Motivation - 1

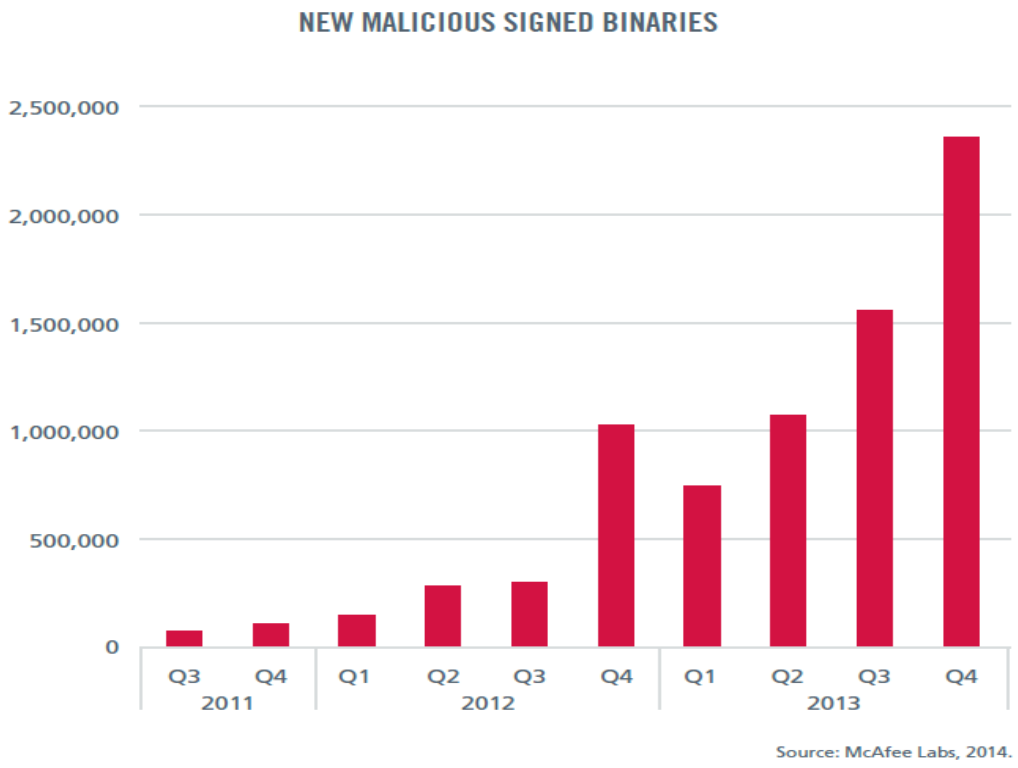


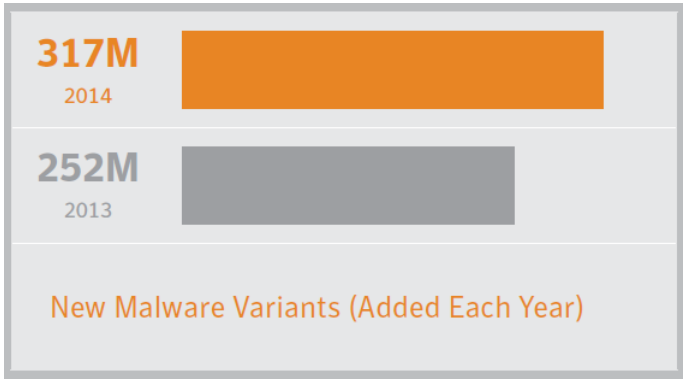
Motivation - 2

Source: Trustwave 2014 Security Pressure Report

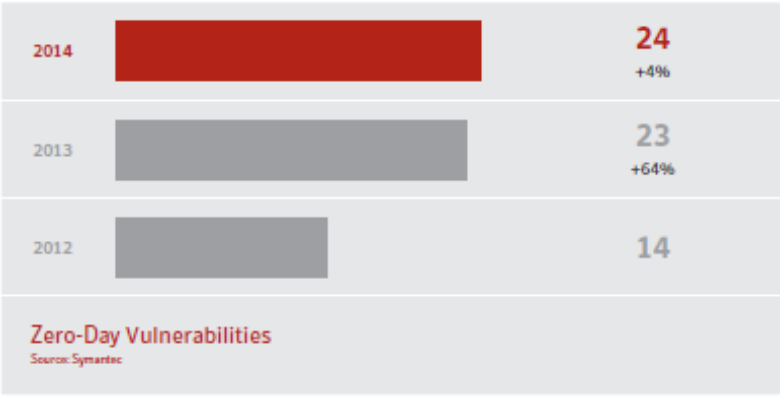


Motivation - 3





Source: Symantec 2015 Internet Security Threat Report



Motivation - 4

The gang behind Gozi made millions by stealing from online bank accounts

http://www.bbc.com/news/technology-34173422

Item	2014 Cost
1,000 Stolen Email Addresses	$0.50 to $10
Credit Card Details	$0.50 to $20
Scans of Real Passports	$1 to $2
Stolen Gaming Accounts	$10 to $15
Custom Malware	$12 to $3500
1,000 Social Network Followers	$2 to $12
Stolen Cloud Accounts	$7 to $8
1 Million Verified Email Spam Mail-outs	$70 to $150
Registered and Activated Russian Mobile Phone SIM Card	$100

Value of Information Sold on Black Market

Security vulnerabilities and attacks

Economic losses

We need secure systems!

This course is NOT!

- Project Course
- Cryptography
- Network Security
- Software Security
- Operating Systems
- Computers in general
- **Hacking**

Tentative Outline

- Basic concepts of computer security.
- Basic cryptography.
- Human factors.
- Malicious software.
- User authentication and access control.
- Software security and operating system security.
- Midterm
- Trusted computing.
- Network security.
- Firewalls and intrusion detection systems.
- Physical and infrastructure security.
- Project Presentations.

Grading (tentative)

- Midterm : 30%
- Pop up Quiz : 5%
- Term Project : 30% (will be a research project)
- Final : 35%
- Extra Points : ?

Make up policy: No make up!

(I do not recommend you mandotary make-ups that I have to make!)

Text Book: William Stallings, Lawrie Brown, Computer Security: Principles and Practice, 2nd edition, 2012

Other References: -Ross Anderson, Security Engineering, 2nd edition, 2008

- Matt Bishop, Introduction to Computer Security, 2004

-William Stallings, Lawrie Brown, Computer Security: Principles and Practice, 3nd edition, 2014

What security is about in real world?

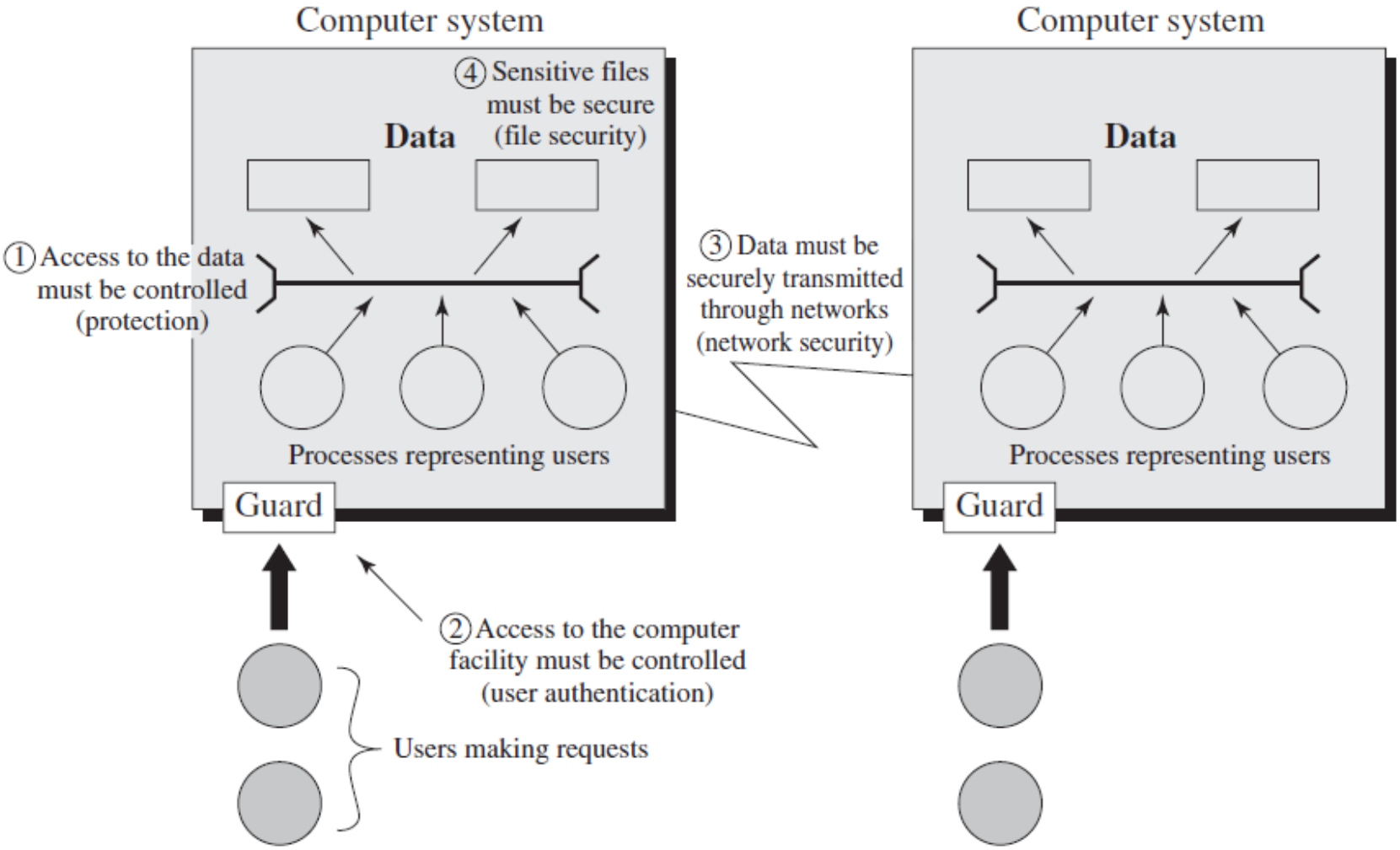
- Protection of assests
- How?
  - **Prevention:** prevent your assets from being damaged or stolen, such as hire a guard
  - **Detection:** detect when, how, and by whom an asset has been damaged, such as alarms
  - **Reaction:** recover your assets, such as call police or make an insurace claim.

What is computer security?

- It deals with computer related assets that are subject to a variety of threats and for which various measures are taken to protect those assets. (Stallings and Brown)

- The protection afforded to an automated information system in order to attain the applicable objectives of preventing the integrity, availability, and confidentiality of information system resources. (NIST Computer Security Handbook)

What is computer security?



Terminology

- No single and consistent terminology in the literature!
- Be careful not to confuse while reading papers and books

- Stallings and Brown, Computer Security: Principles and Practices, 2nd Edition (RFC2828, Internet Security Glossary)

Objectives of Computer Security

Confidentiality

-It is concealment of information or resources.

- Data confidentiality
- Privacy
- A loss of confidentiality is unauthorized disclosure of information.

Objectives of Computer Security

Integrity

- It prevents improper or unauthorized change of data or system resources.

- Data integrity
- System integrity
- A loss of integrity is the unauthorized modification or destruction of information.

Objectives of Computer Security

Availability

- It assures that systems work promptly and service is not denied to authorized users.

- A loss of availability is the disruption of access to or use of information or an information system.

Confidentiality, integrity, and availability are known as the security requirements triad (**CIA triad**).

Additional Goals

Authenticity

The property of being genuine and being able to be verified and trusted; confidence in the validity of transmission, a message, or a message originator.

Accountability

The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

Terminology (Concepts)

- Adversary (threat agent)
- Attack
- Countermeasure
- Risk
- Security Policy
- Security Resource (Asset)
  - Hardware, software, data, communication facilities and networks
- Vulnerability
- From RFC2828

Origin of attacks

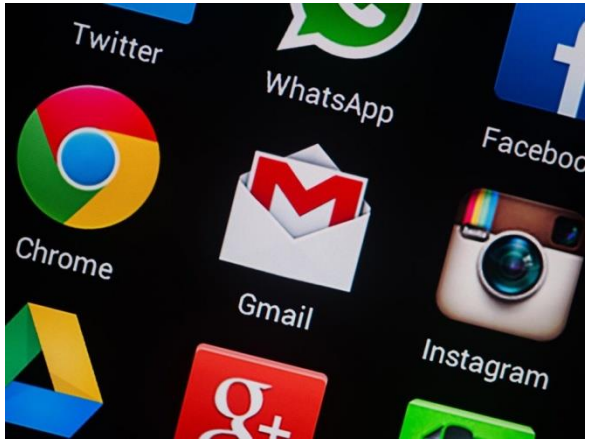
Inside attack

Initiated by an entity inside the security perimeter.

Outside attack

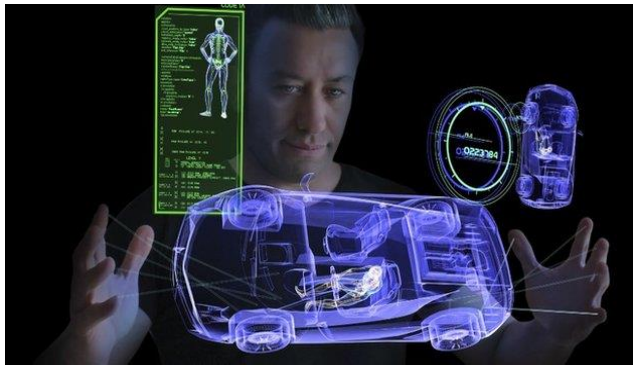
Initiated from the outside perimeter.

Goals of Attacks



- Destroy information
- Steal information

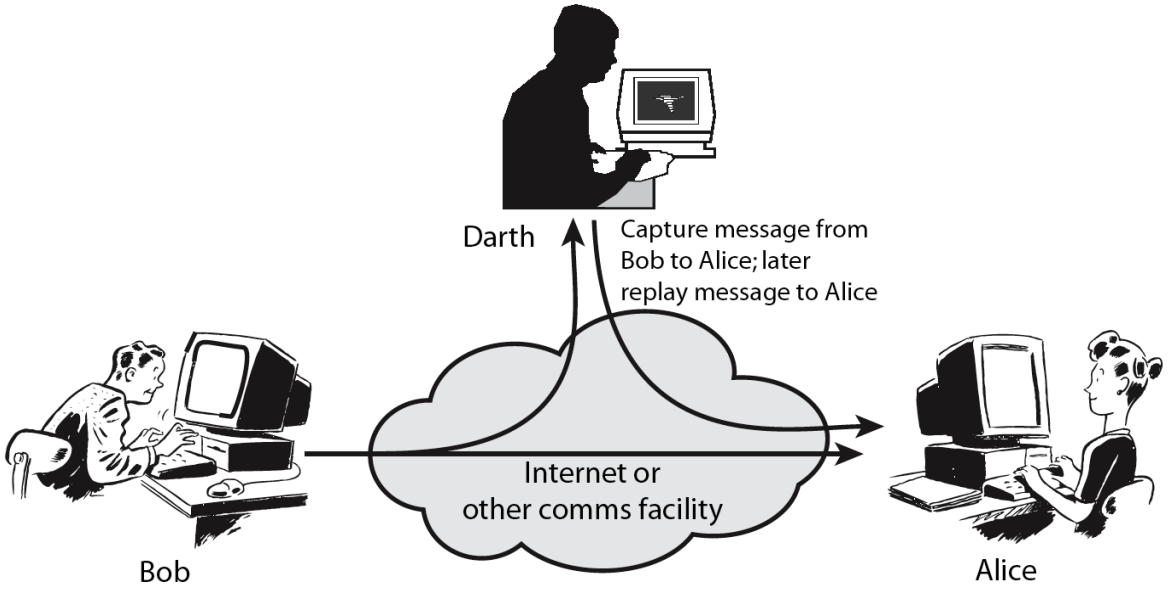
- Blocking to operate properly (denial of service)
- Physical damage
  - Hi-tech cars are security risk, warn researchers (http://www.bbc.com/news/technology-28886463)



Types of Attacks-1 (Networks)

Active attack

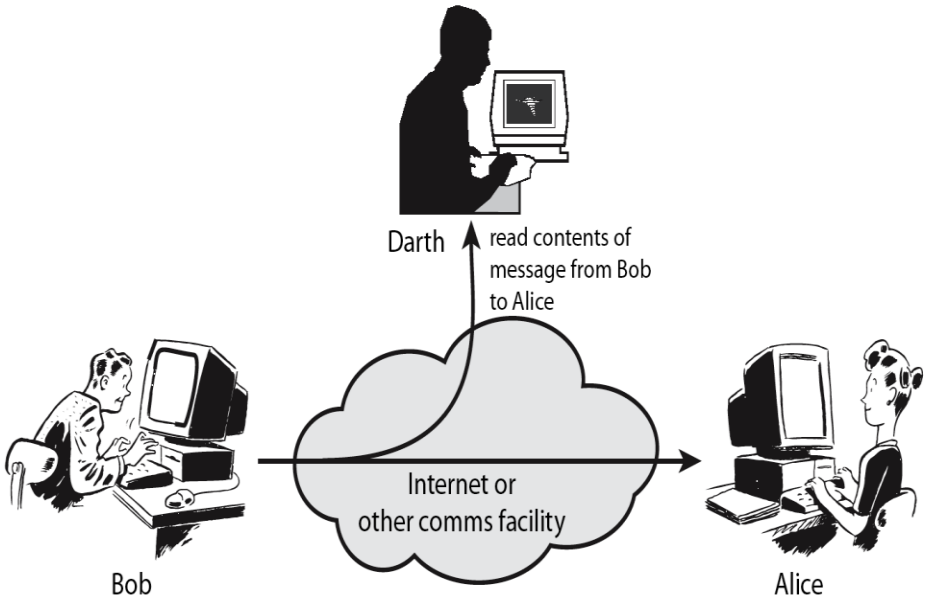
- Attacker actively manipulates the communication
- Masquerade
- Replay
- Denial-of-service



Types of Attacks-2 (Networks)

Passive attack

- Interception of the messages
- Release the content (can be understood)
- Traffic analysis (hard to avoid)
- Hard to detect, try to prevent



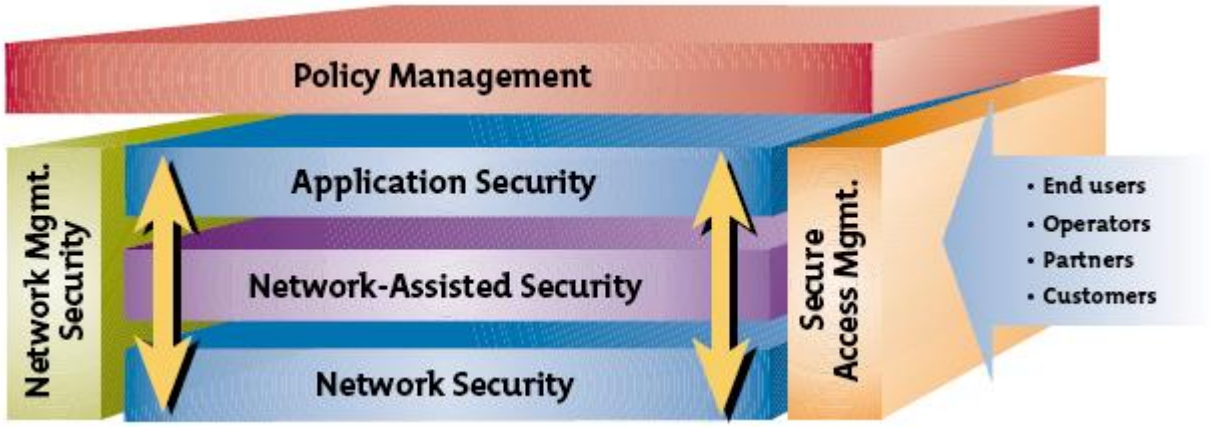
Some Security Requirements

- Access control
- Awareness and training
- Audit and accountability
- Certification, accreditation, and security assessments
- Configuration management
- Identification and authentication
- Incident response
- Maintenance
- Physical and environmental protection
- Planning
- Risk assessment

Security Architecture-1

The need for a security architecture

- To assess effectively the security needs of an organization
- To evaluate and choose various security products and policies
- Requirements should be defined in a systematic way.



Security Architecture-2

- ITU-T Recommendation X.800 (Security Architecture for OSI) defines a systematic approach in the context of networks and communications that is also applied to computer security.

- The OSI (*Open Systems Interconnections*) security architecture focuses on
  - security attacks,
  - mechanisms, and
  - services

Security Service

- A 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.
- Security services implement security policies and are implemented by security mechanisms.

Security Services-1

Authentication

- The assurance that the communicating entity is the one that it claims to be.
- Peer entity authentication
  - mutual confidence in the identities of the parties involved in a connection
- Data-origin authentication
  - assurance about the source of the received data is as claimed

Security Services-2

Access Control

- Prevention of the unauthorized use of a resource

Data Confidentiality

- Protection of data from unauthorized disclosure
  - Connection confidentiality
  - Connectionless confidentiality
  - Selective-field confidentiality
  - Traffic flow confidentiality

Security Services-3

Availability

- Ensures that there is no denial of authorized access to network elements, stored information, information flows, services and applications due to events impacting the network.

Data Integrity

- The assurance that the data received are exactly as sent by authorized entity, such as, no modification, insertion, deletion

Security Services(4)

Non-Repudiation

- Protection against denial by one of the parties in a communication
- Origin non-repudiation
  - Proof that the message was sent by the specified party
- Destination non-repudiation
  - Proof that the message was received by the specified party

Security Mechanism (X.800)(1)

- A mechanism that is designed to prevent, detect, or recover from a security attack.
- **Specific security mechanisms**
  - Encipherment
  - Digital signature
  - Access control
  - Data integrity
  - Authentication exchange
  - Traffic padding
  - Routing Control

Security Mechanism (X.800)(2)

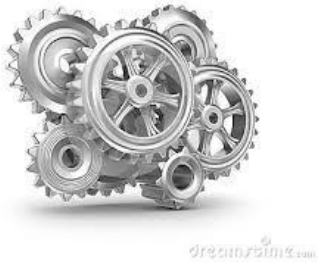
Pervasive security mechanisms

- Trusted functionality
- Security label
- Event detection
- Security audit trial
- Security recovery

Computer Security Strategy

- Specification/policy
  - What is the security scheme supposed to do?

- Implementation/mechanisms
  - How does it do it?



- Correctness/assurance
  - Does it really work?

Summary

- About this course
- What is computer security?
- Objective of computer security
- Terminology
- X.800 standard
  - Attacks, services, mechansisms
- Security strategy

Questions?