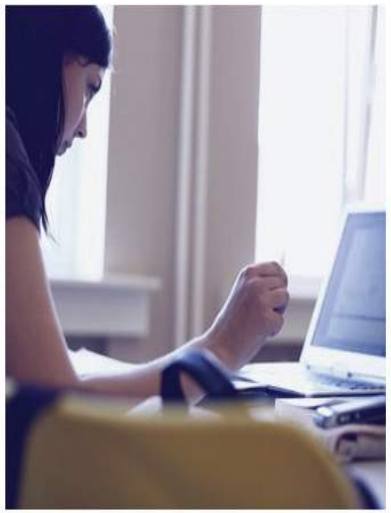
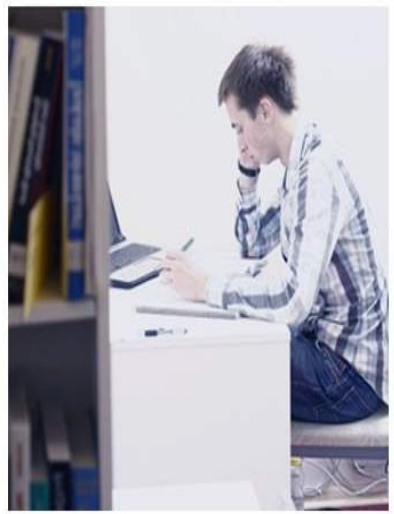





INF501 – IT for Business and Management

IntMA-1; IntMAk-1

Estonian Business School

http://andrewsai.com/

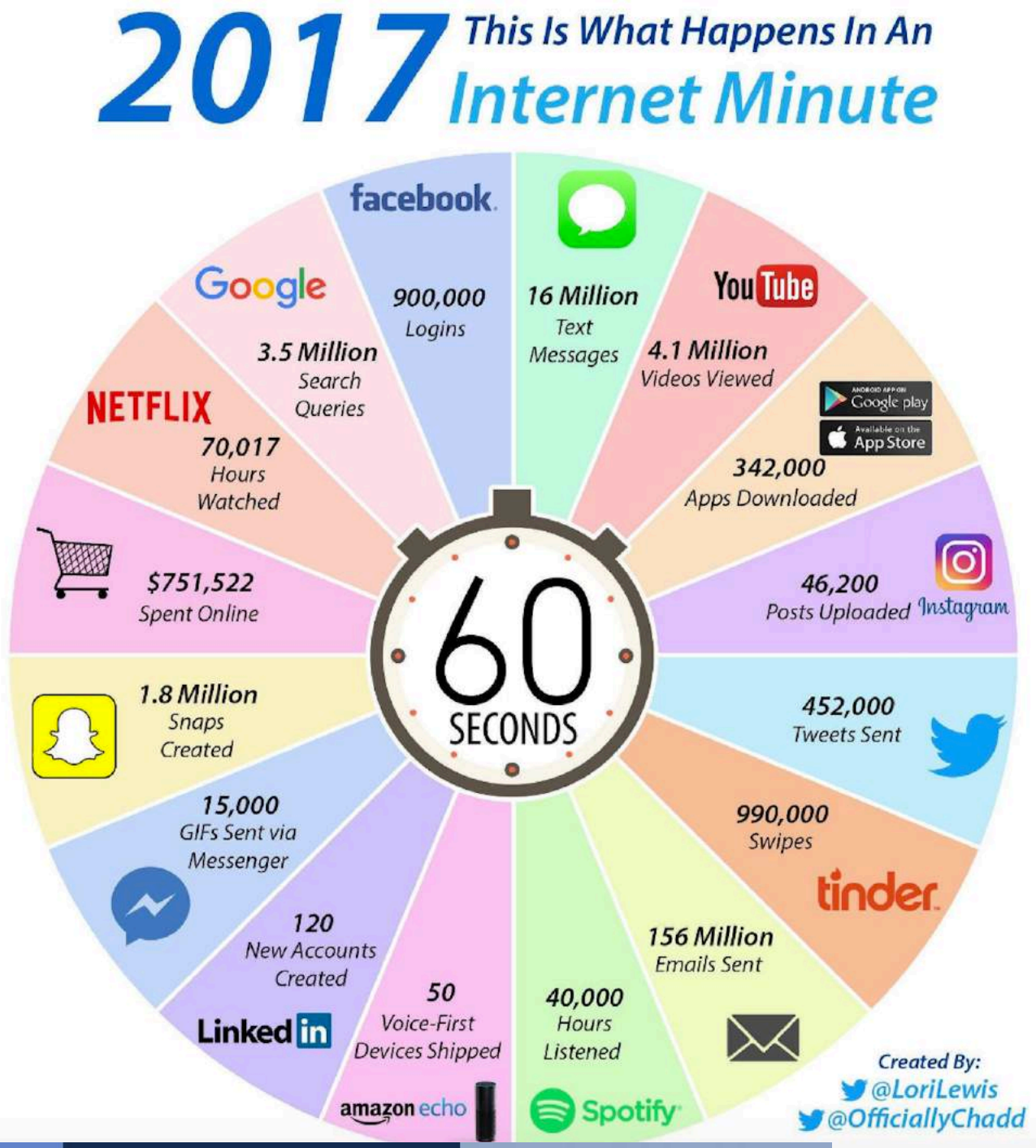
Information Systems Security

Estonian Business School

We have reached a point where all aspects of our lives have some internet component

Almost all records in recent times are stored on computers, making them available to compromise:

- How is the information **stored** safeguarded?
- What are the **vulnerabilities** to these systems that store them? and
- What **steps** can be taken to ensure some level of safety?



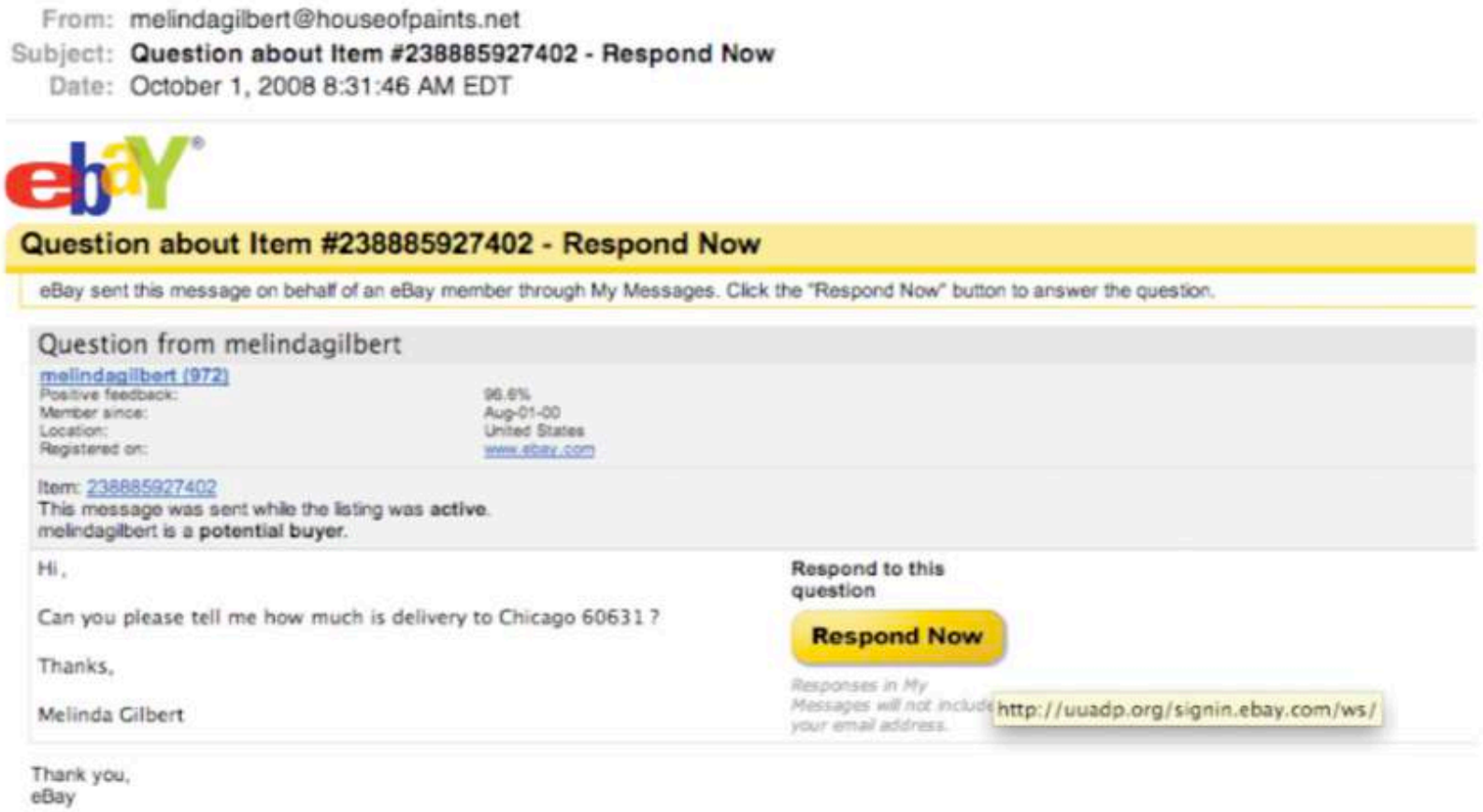
Potential Threats

- Account theft and illegal funds transfer
- Stealing personal or financial data
- Compromising computing assets for use in other crimes
- Extortion
- Espionage
- Cyberwarfare
- Terrorism
- Pranksters
- Protest hacking (hacktivism)
- Revenge (disgruntled employees)

Cyber Fraud Schemes

- **Investment Offers/scams**
  (CIA of US refers to it as ’Nigerian Letters’)
- **Auction Fraud**
- **Identity Theft**
- **Phishing**
- **Cyber Stalking**

Identifying Types of Threats



From: melindagilbert@houseofpaints.net
Subject: **Question about Item #238885927402 - Respond Now**
Date: October 1, 2008 8:31:46 AM EDT

Question about Item #238885927402 - Respond Now

eBay sent this message on behalf of an eBay member through My Messages. Click the "Respond Now" button to answer the question.

Question from melindagilbert

melindagilbert (972)
Positive feedback: 96.6%
Member since: Aug-01-00
Location: United States
Registered on: www.ebay.com

Item: 238885927402
This message was sent while the listing was **active**.
melindagilbert is a **potential buyer**.

Hi,

Can you please tell me how much is delivery to Chicago 60631 ?

Thanks,

Melinda Gilbert

Respond to this question

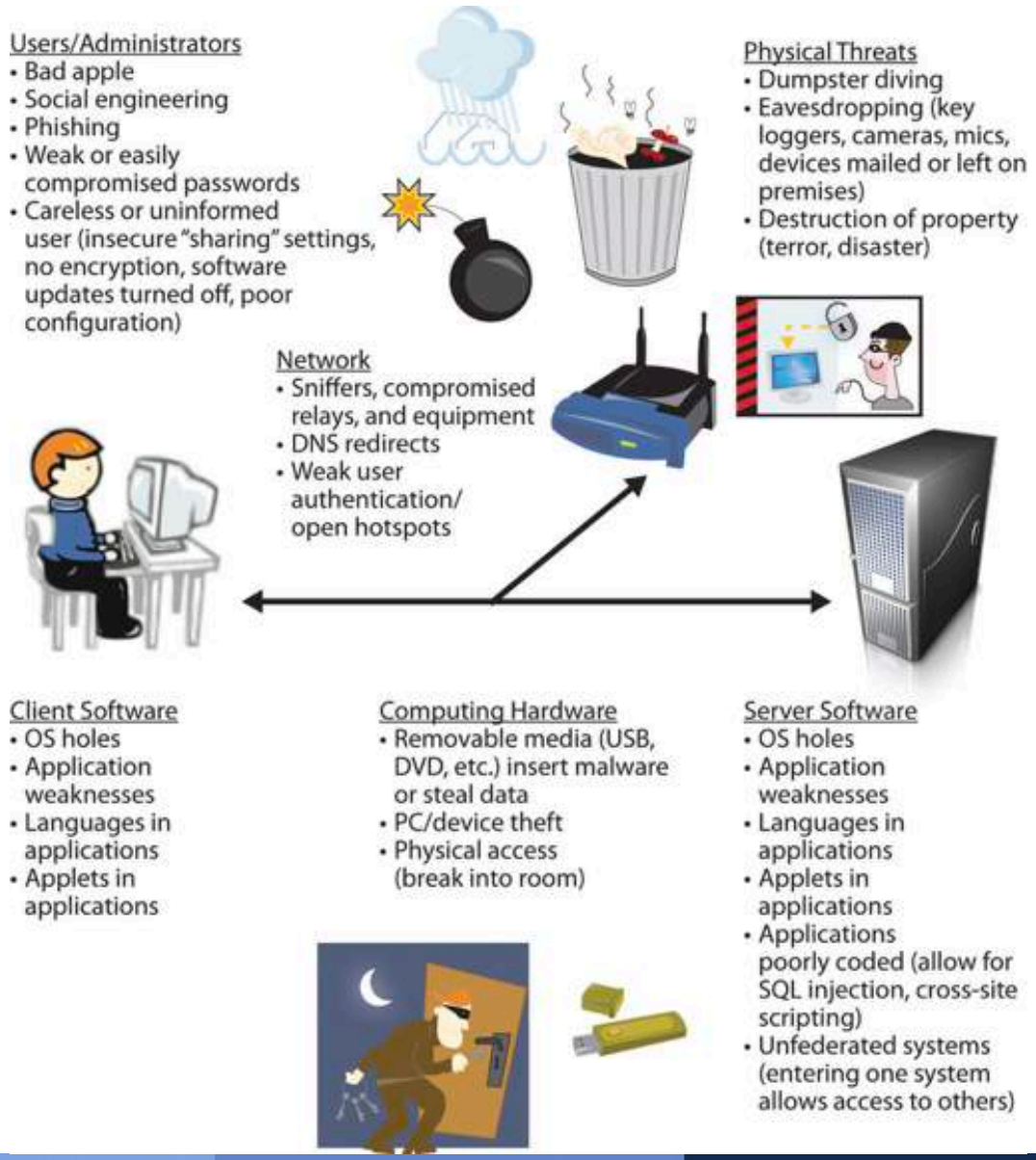
Respond Now

Responses in My Messages will not include your email address.

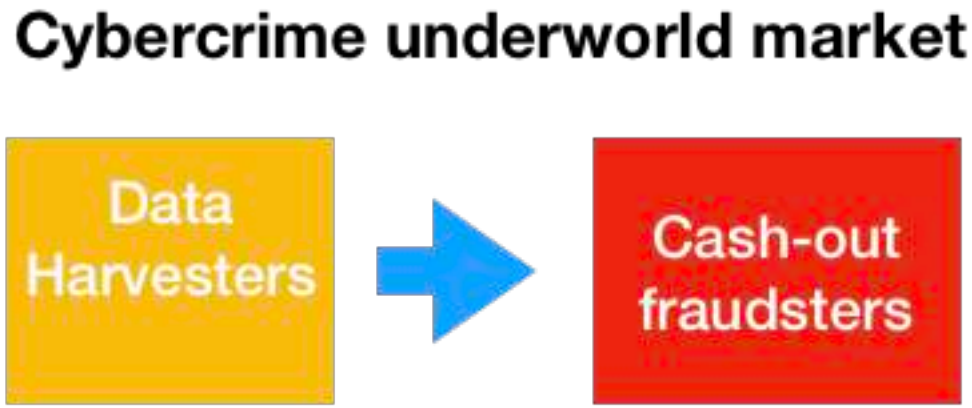
http://uuadp.org/signin.ebay.com/ws/

Thank you,
eBay

Identifying Types of Threats



Potential Threats



Cybercriminals who infiltrate systems and collect data for illegal resale.

Firms that purchase assets from data harvesters. Actions may include using stolen credit card numbers to purchase goods, creating fake accounts via identity fraud, and more.

Most attacks can be categorized as one of these broad classes:

A. MALWARE

B. SECURITY BREACHES

Cyber Hygiene Group Task

20 mins

Your task is to read/watch quickly the videos in ***Canvas***, as a precursor and answer, in about 5-10 points the following question(s):

What are the biggest behavior/hygiene problems facing:

- the single and collective citizen(s) - **Team 1**
- companies by way of cyber-threats - **Team 2**
- Regulations and national-level frameworks on cyber-security -**Team 3**

Cyber Hygiene Discussion Summary

Estonian Business School

Identifying Types of Threats

A. MALWARE: This is a generic term for software that has a malicious purpose. It includes *virus attacks, worms, adware, Trojan horses, and spyware*.

Trojan horses and **viruses** are the most widely encountered.

Viruses

- A virus is "a small program that replicates and hides itself inside other programs, usually without your knowledge" (Symantec, 2003). similar to a biological virus, designed to **replicate** and **spread.**

- Some viruses don't actually harm the system itself, but all cause network slowdowns (heavy network traffic from virus replication)

Identifying Types of Threats

Trojan Horses

Name from story of city of Troy, which was besieged.

Identifying Types of Threats

Spyware: A spyware can be as simple as a ***cookie*** – *a text file that your browser creates and stores on your hard drive – that a website you have visited downloads to your machine and uses to recognise you when you return to the site*. The means other sites can access your browsing history.

Identifying Types of Threats

- **Logic bomb**: is a software that lays dormant until some specific condition is met (such as date and time). Software then deletes files, alters system configuration or releases a virus.

- **Key logger**: records all your keystrokes. Some take periodic screenshots of your PC, which can be sent back to you as email for fraud.

Compromising System Security

B. SECURITY BREACHES

- Cracking Passwords,
- elevating privileges,
- unauthorised access

Compromising System Security

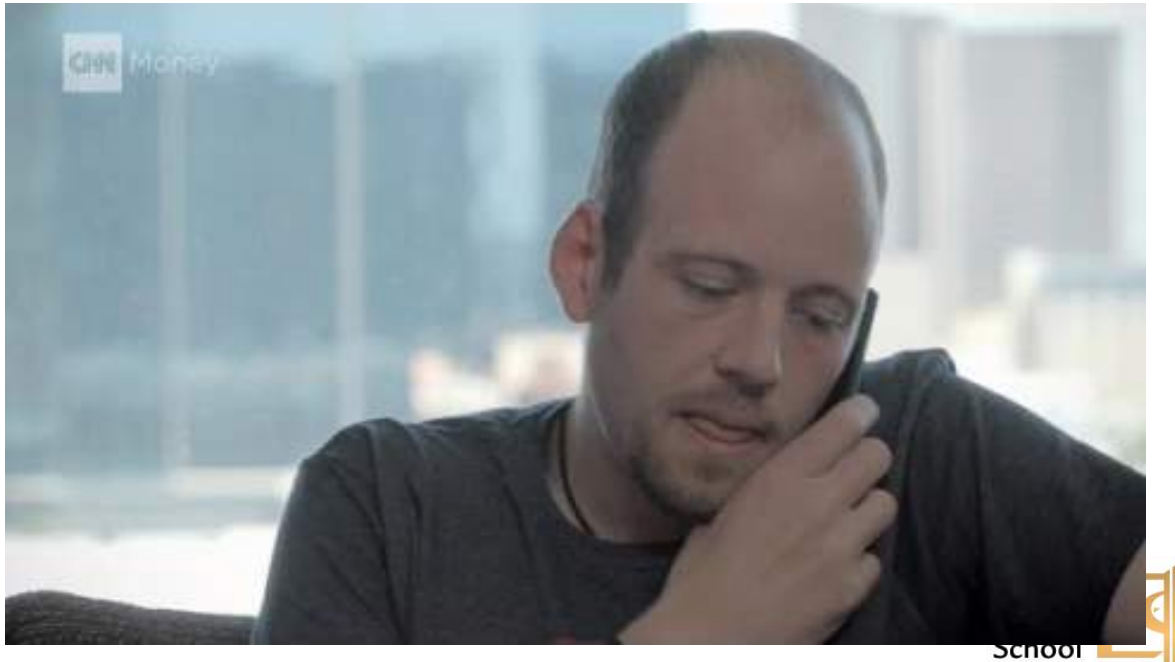
B. SECURITY BREACHES

main types:

1. **Hacking**: breaching a system's security

   White hacker, Black hacker and *Gray Hacker) ;*

2. **Phreaking**: breaking into telephone systems *Phone hacking video*



Identifying Types of Threats Hacking

Estonian Business School

Compromising System Security

B. SECURITY BREACHES

3. Cracking: is intruding into a system without permission, usually with malevolent intent. Any attack designed to breach security via some OS flaw or others means.

(e.g.OphCrack; https://cracksoftwarex.com/;crackfind.com, etc)

2. SOCIAL ENGINEERING

Compromising System Security

B. SECURITY BREACHES

- **Social Engineering**: is a technique for breaching a system's security by exploiting human nature rather than technology.

- Uses standard con techniques to get users to give up info needed to gain access to a target system.

Estonian Business School

Compromising System Security

B. SECURITY BREACHES

War-dialing: attack where a hacker sets up a computer to call phone numbers in sequence until another computer answers, to try to gain entry to its system.

War-driving: hacker simply drives around trying to locate vulnerable wireless networks to breach. (Wireless networks extend at least 100 feet)

C. DENIAL OF SERVICE (DoS)

Compromising System Security

[Distributed] Denial of Service (DDoS) Attacks: attacker does not actually access the system, **simply blocks owner's access**.

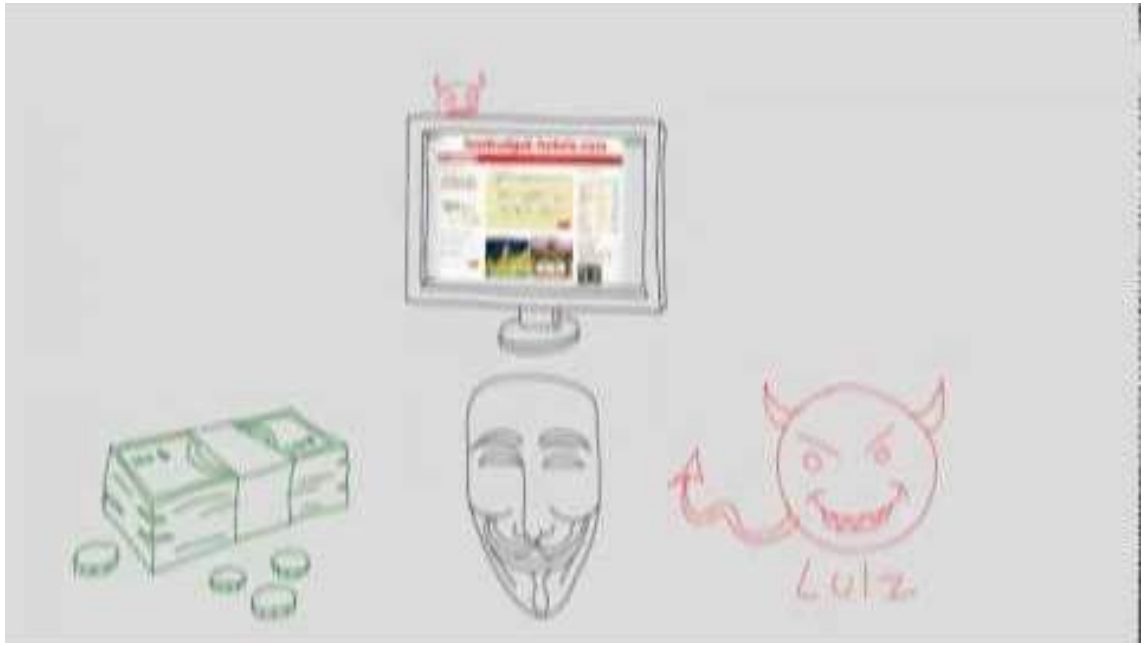
Flooding: flood targeted system with so many false connection requests so that the system cannot respond to legitimate requests. This is the most common attack on the web.

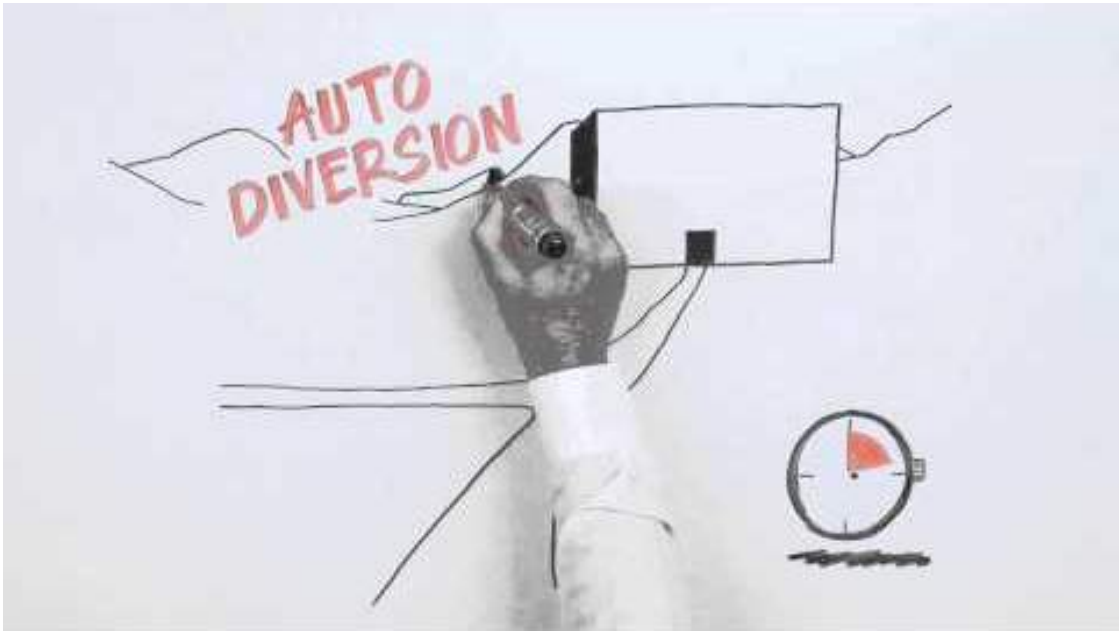
Compromising System Security

[Distributed] Denial of Service (DDoS) Attacks:

DDoS video; Mitigate DDos Attacks

-ipconfig; ping





Estonian Business School

D. WEB ATTACKS

Compromising System Security

Web Attacks: web servers have to allow communications, which is a potential point for web-based attacks.

- **SQL injection**: Passing SQL query language commands to a web application and getting the website to execute the statement.(username, PW in SQL)

E. SESSION HIJACKING

Compromising System Security

E. SESSION HIJACKING

- Not a common form of attack because, **it is very complex**.
- Attacker monitors an authenticated session between client machine and the server and takes over the session.

Estonian Business School

F. DNS POISONING

Compromising System Security

F. DNS POISONING:

- Most of the communication on the Internet involves *Domain Name Service* (DNS).
- DNS translates the domain names (e.g. www.yahoo.com) into IP addresses that computers and routers understand.
- DNS poisoning uses one of several techniques to compromise that process and redirect traffic to an illicit site for stealing information.

The Security Requirements Triad

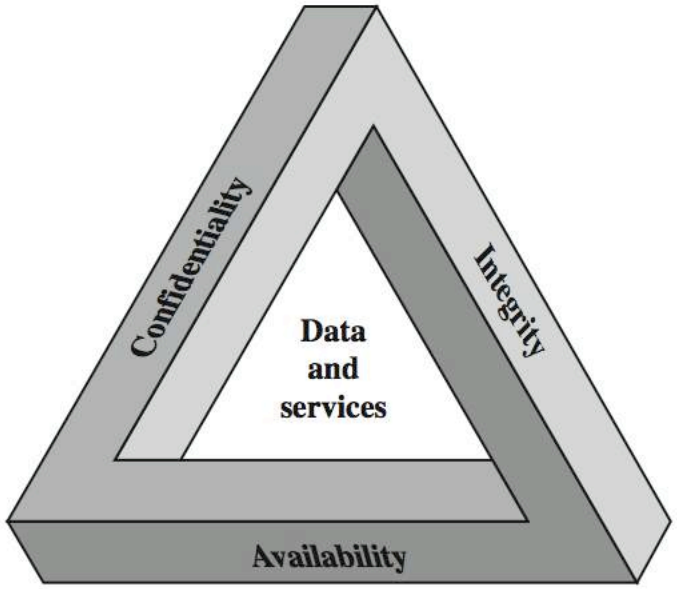


Figure 1.1 The Security Requirements Triad

NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

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)

http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

Estonian Business School

Concepts and Approaches

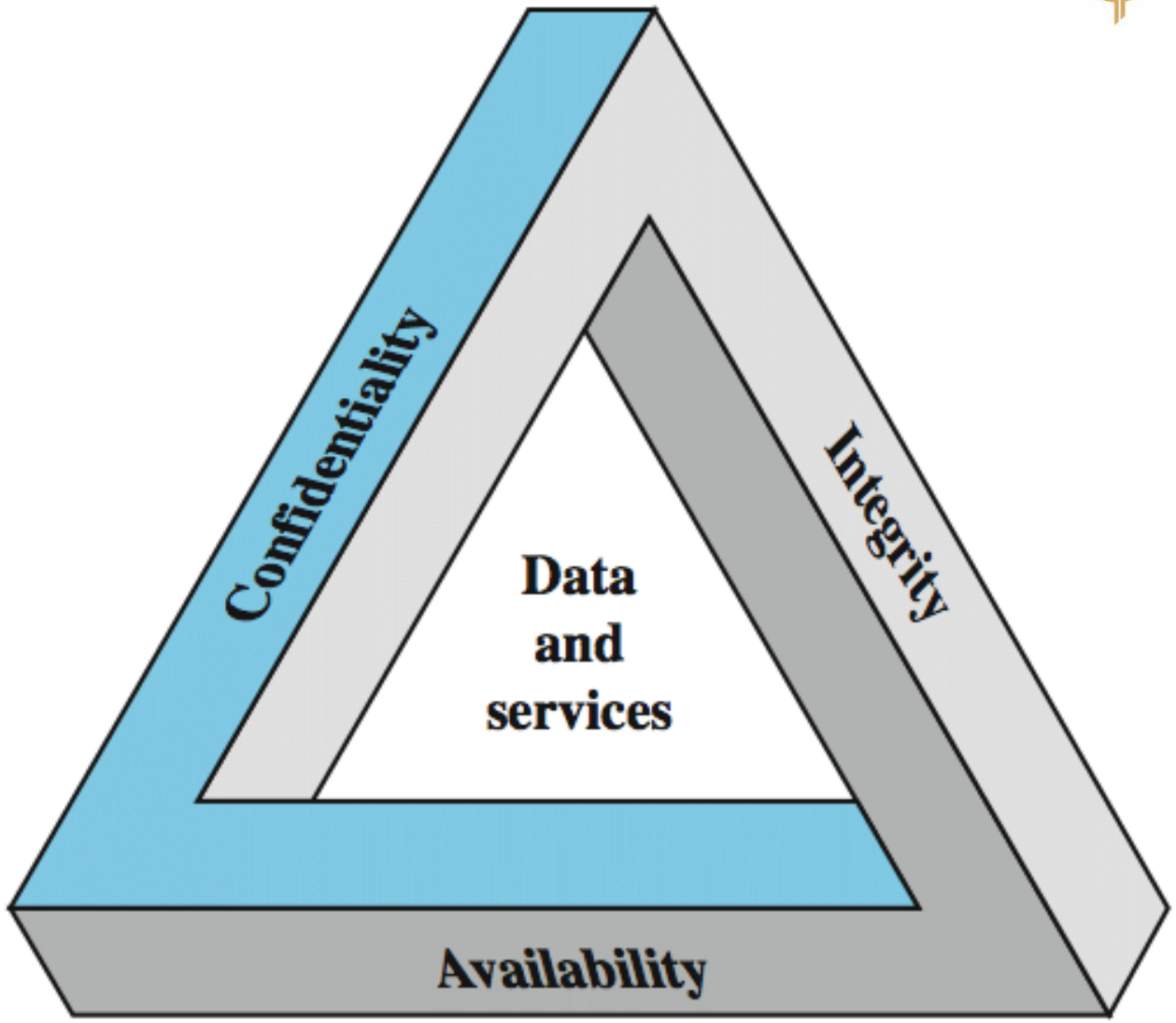
CIA Triangle

three pillars of security:

1. **Confidentiality-** are you keeping the data confidential?

2. **Integrity** - Does your approach help guarantee the integrity of data? **and**

3. **Availability** - does your approach still make the data readily available to authorized users?



Security Requirements

- **Confidentiality**
  - Preserving authorized restrictions on information ***access*** and ***disclosure***, including means for protecting personal privacy and proprietary information.
- **Integrity**
  - Guarding against information ***modifications*** or ***destruction***, including ensuring information non-repudiation and authenticity.
- **Availability**
  - Ensuring timely and reliable access to and ***use*** of information

Estonian Business School

Security Attacks, Mechanisms & Services

Security *Attack*	Security *Mechanism*	Security *Service*
• Any action that compromises the security of information	• A process / device that is designed to detect, prevent or recover from a security attack.	• A service intended to counter security attacks, typically by implementing one or more mechanisms.

Estonian Business School

Threats & Attacks

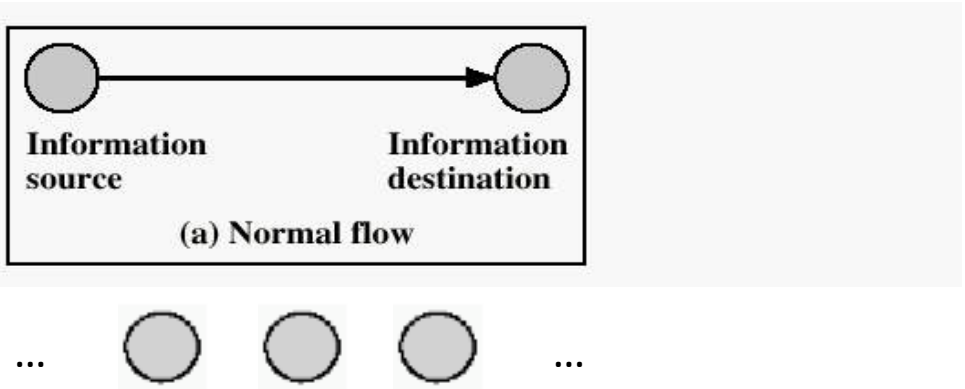
Table 1.1 Threats and Attacks (RFC 2828)

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.

… but *threat* and *attack* used nearly interchangeably

Estonian Business School

Security Threats / Attacks



Security Threats / Attacks

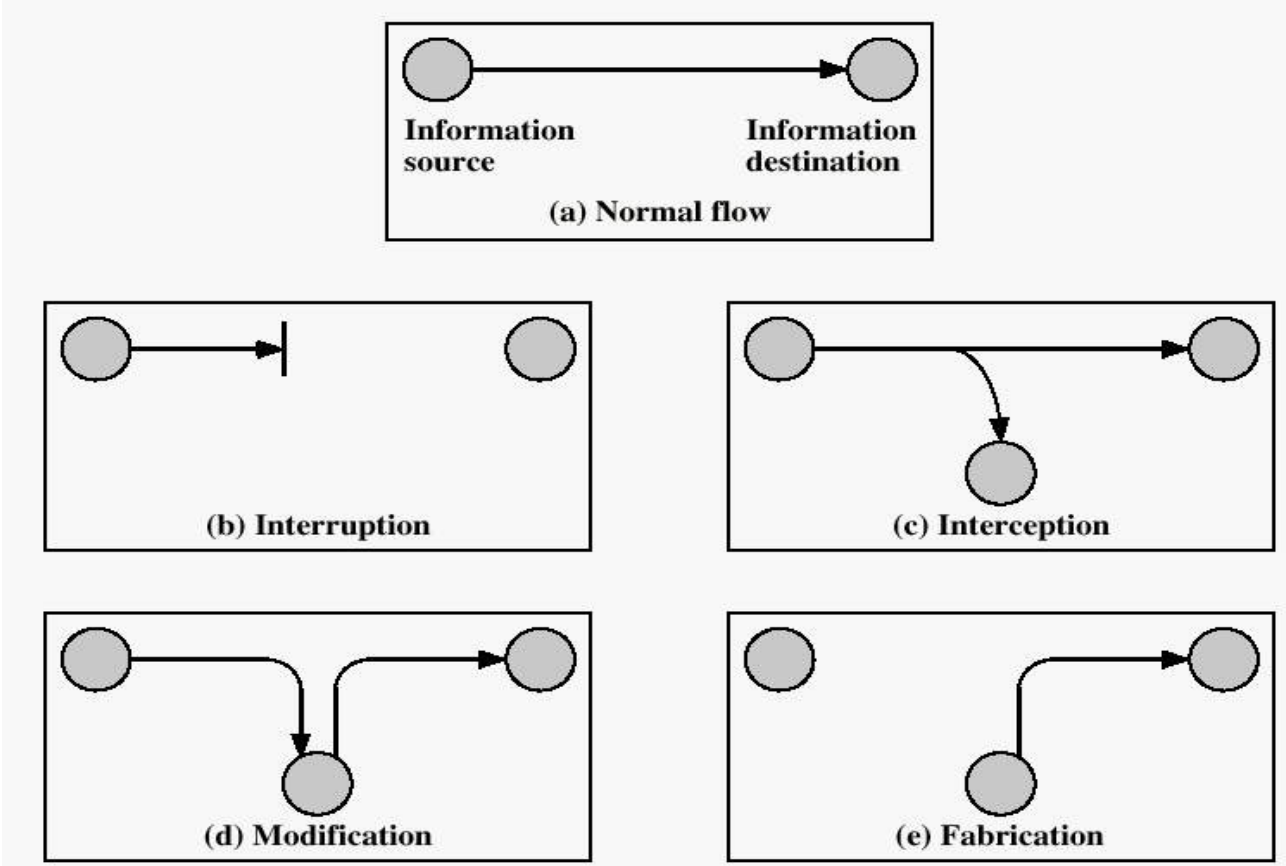
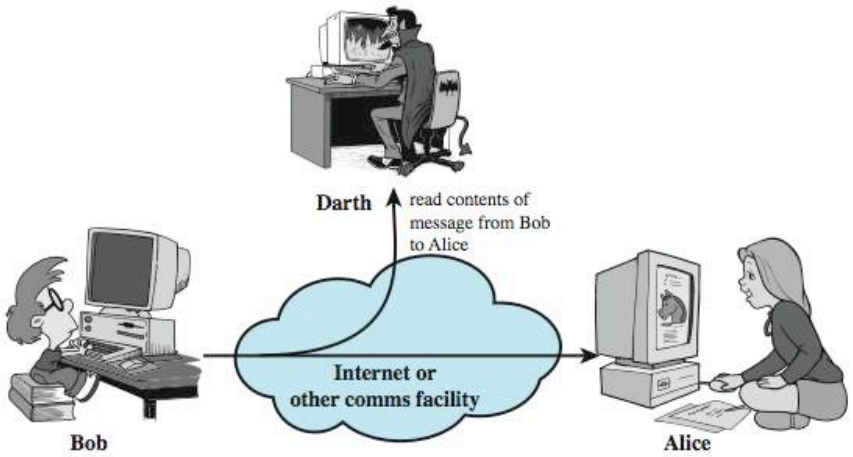


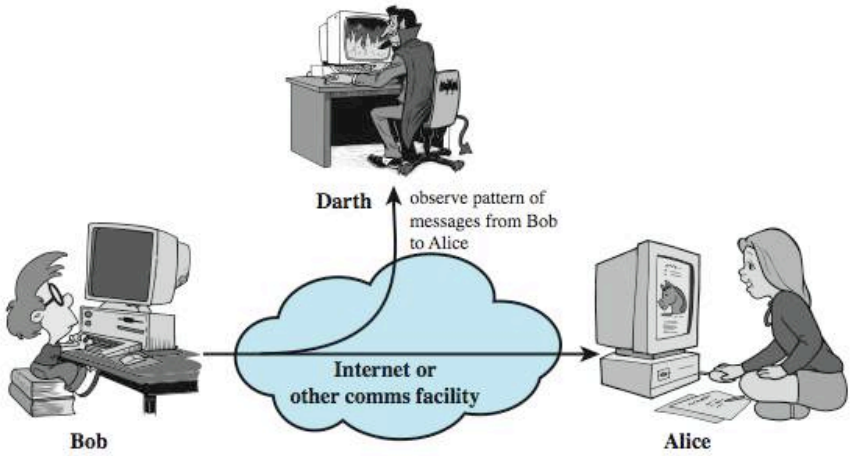
Figure 1.1 Security Threats

Estonian Business School

Passive Attacks



(a) Release of message contents

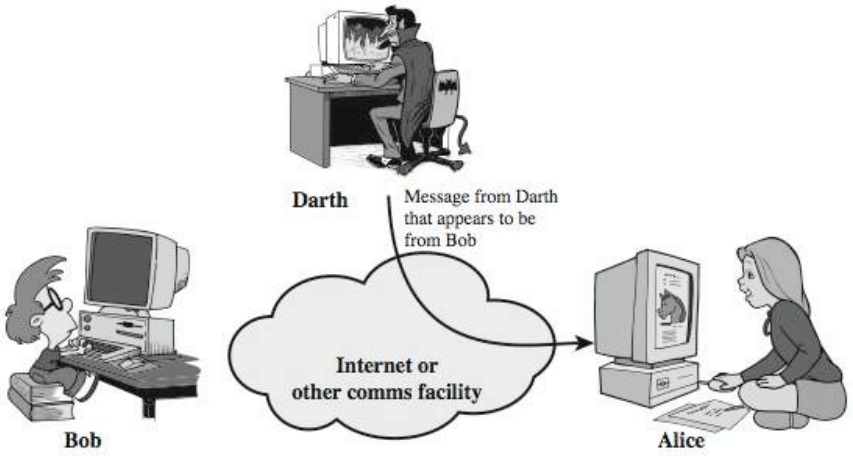


(b) Traffic analysis

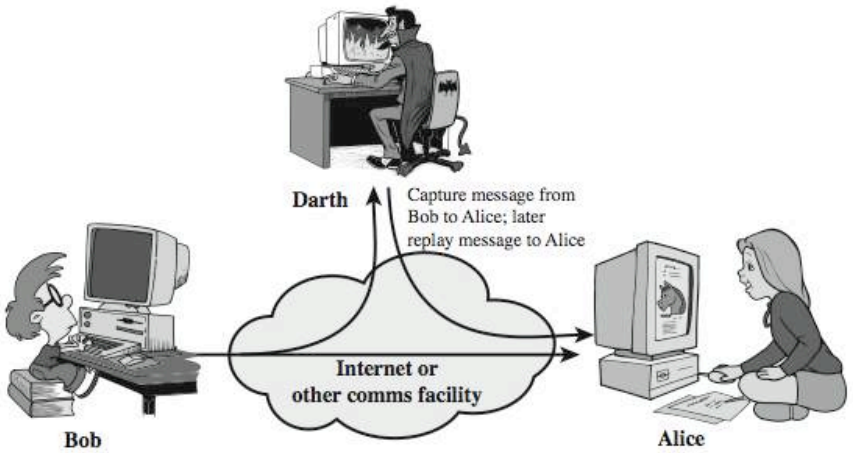
Figure 1.2 Passive attacks.

Estonian Business School

Active Attacks (1)



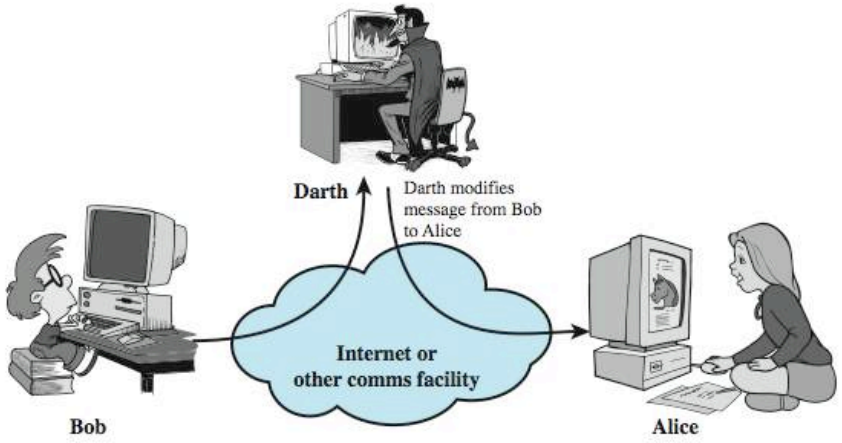
(a) Masquerade



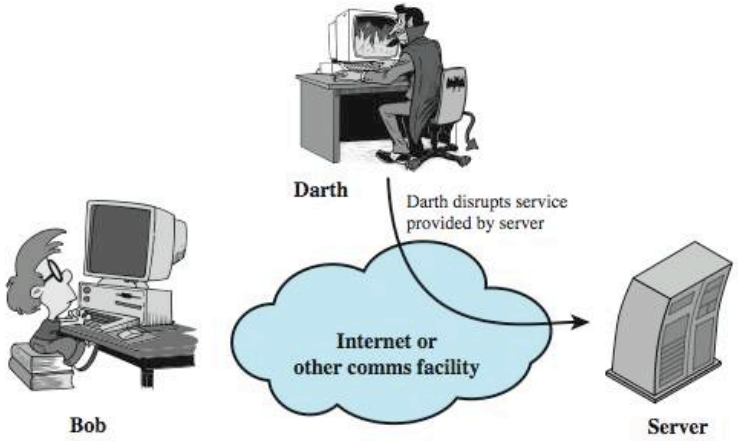
(b) Replay

Figure 1.3 Active attacks (page 1 of 2)

Active Attacks (2)



(c) Modification of messages



(d) Denial of service

Figure 1.3 Active Attacks (page 2 of 2)

Estonian Business School

Security Services (X.800)

- **Authentication**
  - The assurance that the communicating entity is the one it claims to be
- **Access Control**
  - The prevention of unauthorized use of a resource
    - who can have access to a resource,
    - under what conditions access can occur,
    - what those accessing the resource are allowed to do
- **Data Confidentiality**
  - The protection of data from unauthorized disclosure
- **Data Integrity**
  - The assurance that data received are exactly as sent by an authorized entity (i.e., contains no modification, insertion, deletion or replay).
- **Non-Repudiation**
  - Provides protection against denial by one of the entities involved in a communication of having participated in all/part of the communication.

[Source Document]

Security Mechanisms (X.800)

Table 1.4 Relationship Between Security Services and Mechanisms

	Mechanism							
Service	**Enciph-erment**	**Digital signature**	**Access control**	**Data integrity**	**Authenti-cation exchange**	**Traffic padding**	**Routing control**	**Notari-zation**
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

http://www.itu.int/rec/T-REC-X.800-199103-I/e

Model for Network Security

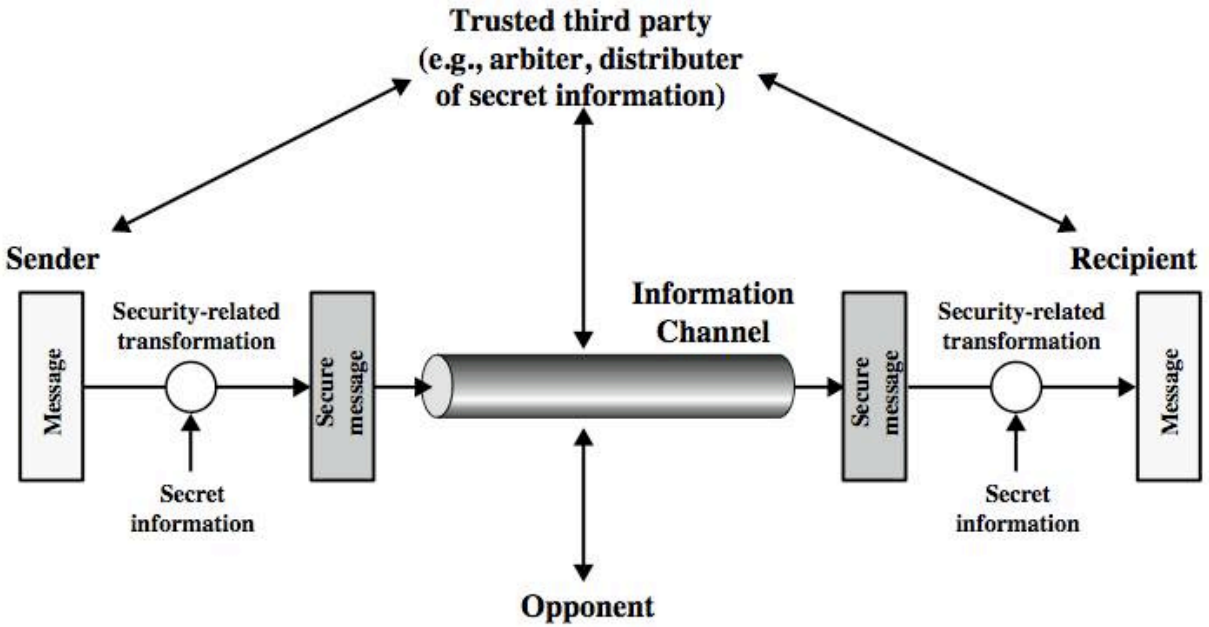


Figure 1.4 Model for Network Security

Estonian Business School

Access Control

- Access Control Overview
- Identification, Authentication, Authorization, Accountability
- Single Sign-on and Kerberos
- Access Control Models
- Access Control Techniques and Technologies
- Access Control Administration
- Access Control Monitoring: Intrusion Detection
- Threats to Access Control

Estonian Business School

Access Control Overview

Access control is a system which **enables an authority to control access to areas and resources** in a given physical facility or computer-based information system.

In computer security, access control includes **authentication**, **authorization** and **audit**.

It also includes measures such as **physical devices**, including biometric scans and metal locks, hidden paths, digital signatures, encryption, social barriers, and **monitoring** by humans and automated systems.

In any access control model, the **entities that can perform actions** in the system are called **subjects**, and the **entities representing resources to which access may need to be controlled** are called **objects** (see also Access Control Matrix). Subjects and objects should both be considered as software entities and as human users

Estonian Business School

Access Control

Access control **models** used by current systems tend to fall into one of two classes: **those based on capabilities** and those based on **access control lists (ACLs).**

In a **capability-based model**, **holding an unforgeable reference or *capability* to an object provides access to the object**

Access is conveyed to another party by **transmitting such a capability** over a **secure channel**.

In an ACL-based model, **a subject's access to an object** depends on whether **its identity is on a list associated with the object**

Business School

Identification, Authentication, Authorization

Access control systems provide the essential services of ***identification*** *and* ***authentication*** (*I&A*), ***authorization***, and ***accountability*** where:

identification and authentication determine who can log on to a system, and the association of users with the software subjects that they are able to control as a result of logging in;

authorization determines **what a subject can do**;

accountability identifies **what a subject** (or all subjects associated with a user) **did**.

Identification, Authentication, Authorization

Authenticators are commonly based on at least one of the following **four factors**:

- ***Something you know***, such as a **password** or a personal identification number (**PIN**). This assumes that only the owner of the account knows the password or PIN needed to access the account.
- ***Something you have***, such as a **smart card** or **security token**. This assumes that only the owner of the account has the necessary smart card or token needed to unlock the account.
- ***Something you are***, such as **fingerprint**, **voice**, **retina**, or **iris** characteristics.
- ***Where you are***, for example **inside** or **outside** a company **firewall**, or proximity of login location to a personal GPS device.

Estonian Business School

Identification, Authentication, Authorization

Authorization: Authorization applies to subjects. Authorization determines what a subject can do on the system.

Most modern operating systems define sets of permissions that are variations or extensions of three basic types of access:

- **Read (R)**: The subject can
  - Read file contents, List directory contents
- **Write (W):** The subject can change the contents of a file or directory with the following tasks:
  - Add, Create, Delete, Rename
- **Execute (X):** If the file is a program, the subject can cause the program to be run. (In Unix systems, the 'execute' permission doubles as a **'traverse directory**' permission when granted for a directory.)

Estonian Business School

Intrusion Detection System

For the purpose of dealing with IT, there are **two main types of IDS's**: **network-based** and **host-based IDS.**

- In a **network-based intrusion-detection system (NIDS),** the **sensors are located at choke points in the network to be monitored**, often in the demilitarized zone (DMZ) or at network borders. The sensor captures all network traffic and analyzes the content of individual packets for malicious traffic.
- In a **host-based system**, the **sensor usually consists of a software agent, which monitors all activity** of the host on which it is installed, including file system, logs and the kernel. Some application-based IDS are also part of this category.

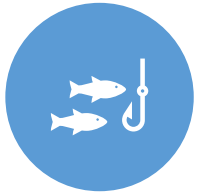
Estonian Business School

Threats to Access Control

Dictionary Attack

Brute Force Attack

Spoofing at Logon



Phishing

Identity Theft

Estonian Business School

Cryptography

Definition of Cryptography

Important concepts

Symmetric and Asymmetric, Hash, Digital Signature etc.

Steganography and Digital watermarking

Algorithms

Attacks

Definitions

Cryptography

Mathematical manipulation of information that prevents the information being disclosed or altered

Cryptanalysis

Defeating the protected mechanisms of cryptography

Cryptology

Study of Cryptography and Cryptanalysis

Estonian Business School

Goals of Cryptography

Confidentiality

Integrity

Authenticity

Non-repudiation

Access Control

Make compromise difficult

Estonian Business School

Process

Input (also called Plaintext or Clear Text)

Cryptosystem (device that performs encryption/decryption)

Cryptographic Algorithms (Mathematical functions)

Output (Cipher text or Cryptogram)

Key (Crypto variable)

What is Network Security

- Network security consists of the (1) **provisions made in an underlying computer network infrastructure**, (2) **policies adopted by the network administrator to protect the network** and t**he network-accessible resources from unauthorized access**, and (3) **consistent and continuous monitoring and measurement of its effectiveness**
- Network security **starts from authenticating the user**, commonly with a username and a password.
- Once authenticated, a **firewall enforces access policies** such as what services are allowed to be accessed by the network users.
- Though effective to prevent unauthorized access, this component **may fail to check potentially harmful content** such as computer worms or Trojans being transmitted over the network.

Estonian Business School

What is Network Security

Communication between two hosts using a network could be **encrypted** to maintain privacy.

- ***Honeypots*** essentially **decoy network-accessible resources**, could be deployed in a network as surveillance and early-warning tools. **Techniques used by the attackers** that attempt to compromise these decoy resources **are studied during and after an attack** to keep an eye on new exploitation techniques. Such analysis could be **used to further tighten security** of the actual network being protected by the honeypot.
- A **Botnet** is a **collection of software agents, or robots**, that run autonomously and automatically. The term is most commonly associated with malicious software, but it can also refer to a network of computers using distributed computing software.

Estonian Business School

Network Forensic

Network forensics is essentially **about monitoring network traffic** and determining if there is an attack and if so, determine the nature of the attack

- Key tasks include **traffic capture**, **analysis** and **visualization**
- Many tools are now available
- Works together with **IDs**, **Firewalls** and **Honeynets**
- Expert systems solutions show promise

Estonian Business School

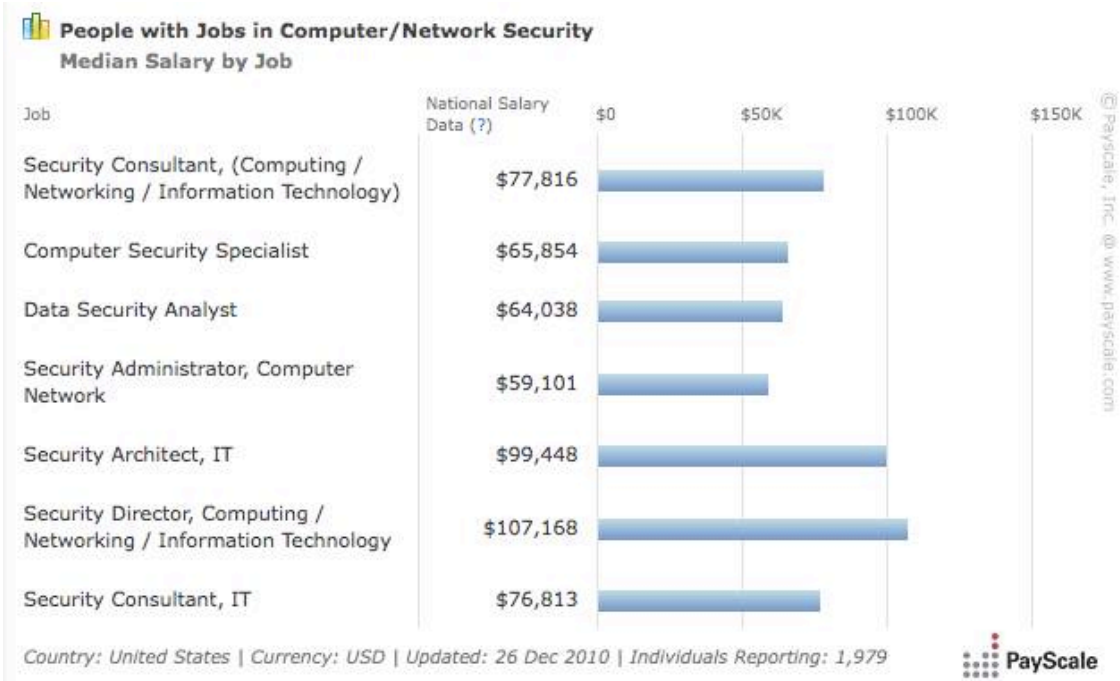
Network Security Jobs

CNNMoney.com
A Service of CNN, Fortune & Money

Job growth

Rank	Job title	Best Jobs rank	10-year growth	Total jobs
1	Telecommunications Network Engineer	30	53%	21,000
2	Systems Engineer	1	45%	88,000
3	Personal Financial Advisor	N.A.	41%	20,000
4	Veterinarian	25	35%	68,000
5	Senior Financial Analyst	21	34%	127,000
6	Business Analyst, IT	17	29%	125,000
7	Software Development Director	N.A.	28%	12,000
8	Physical Therapist	7	27%	181,000
9	Physician Assistant	2	27%	82,000
10	Computer/Network Security Consultant	8	27%	13,000

PayScale



SANS SECURITY ESSENTIALS CERTIFICATION
GSEC

Estonian Business School

Questions?

Estonian Business School