Introduction to Security

Dr. Talal Alkharobi

Why is security important?

- Computers and networks are the nerves of the basic services and critical infrastructures in our society
  - Financial services and commerce
  - Transportation
  - Power grids
  - Etc.
- Computers and networks are targets of attacks by adversaries

3

Why is security so hard?

- Computers and networks complexity
- The increase in Internet usage
- Lack of awareness of threats and risks
- Social engineering
- Defense is inherently more expensive
- Offense only needs the weakest link
- Ample cracking tools

Dr. Talal Alkharobi

4

Type of Attackers

- Amateurs
- Hacker/Cracker
- Career criminal

Dr. Talal Alkharobi

5

Type of Attackers
Amateurs

- Regular users, who exploit the vulnerabilities of the computer system
- Low experienced
- Motivation: easy access to vulnerable resources

Dr. Talal Alkharobi

6

Type of Attackers
Hackers/Crackers

- Attempt to access computing facilities for which they do not have the authorization
- Experts
- Motivation: Enjoy challenge, curiosity

Dr. Talal Alkharobi

7

Type of Attackers
Career criminals

- Professionals who understand the computer system and its vulnerabilities
- Motivation: personal gain (e.g., financial)

8

Methods of Defense

Prevent	block attack
Deter	make the attack harder
Deflect	make other targets more attractive, e.g. is honeypots
Detect	identify misuse
Tolerate	function under attack
Recover	restore to correct state

9

Computer Security Domains

- Physical security
- Operational/procedural security
- Personnel security
- System security
- Network security
- Information Security

10

Computer Security Domains
Physical security

- Controlling the comings and goings of people and materials
- Protection against the elements and natural disasters

Computer Security Domains
Operational/procedural security

11

- Covering everything from managerial policy decisions to reporting hierarchies

Dr. Talal Alkharobi

Computer Security Domains
Personnel security

12

- Hiring employees,
- background screening,
- training,
- security briefings,
- monitoring, and
- handling departures

Dr. Talal Alkharobi

13

Computer Security Domains
System security

- User access and authentication controls,
- assignment of privilege,
- maintaining file and filesystem integrity,
- backups,
- monitoring processes,
- log-keeping, and
- auditing.
- OS and database systems.

14

Computer Security Domains
Network security

- Protecting network and telecommunications equipment,
- protecting network servers and transmissions,
- combating eavesdropping,
- controlling access from untrusted networks,
- firewalls, and
- detecting intrusions

15

Computer Security Domains
Information Security

- Hiding of information (cryptography)
- Security of information in transit over a network.
  - e-commerce transactions,
  - online banking,
  - confidential e-mails,
  - file transfers,
  - record transfers,
  - authorization messages, etc.

Dr. Talal Alkharobi

16

What is Security?

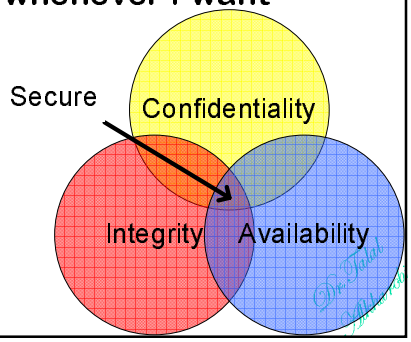
- Keeping something (e.g. information) secure against
  - Someone stealing it
  - Someone destroying it
  - Someone changing it
  - Someone preventing me from using it

Dr. Talal Alkharobi

17

What is Security?

- More Specifically
  - **Confidentiality**: nobody else can see it
  - **Integrity**: nobody else can change it
  - **Availability**: I can get at it whenever I want



18

Basic Components of Security

- **Confidentiality**: Keeping data and resources secret or hidden
- **Integrity**: Ensuring authorized modifications
- **Availability**: Ensuring authorized access to data and resources when desired
- **Accountability**: Ensuring that an entity's action is traceable uniquely to that entity
- **Security assurance**: Assurance that all four objectives are met

The need for Information security

19

- Emergence of the Internet and distributed systems
- Increasing system complexity
- Financial losses due to computer crimes
- Digital information needs to be kept secure
  - Competitive advantage
  - Protection of assets
  - Liability and responsibility

The need for Information security

20

- National defense:
  - Protection of critical infrastructures
  - Interlinked government agencies

21

Threat

- Any circumstance or event with the potential to adversely impact an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.
- A threat is a "potential" violation of security
- A violation *might* occur makes it a threat
- It is important to guard against threats and be prepared for the actual violation

22

Reasons for Threats

- The internet provides different sources of information on known security flaws in hardware and software: average internet users can quickly find information on how to break into various systems
- Attackers may use automated tools to probe network systems, then exploiting any identified security weaknesses to gain access
- Apart from attacks originated from external parties, many break-ins occur due to poor information security policies and procedures, or internal misuse of information systems.

23

Reasons for Threats

- New security risks could arise from evolving attack methods or newly detected holes and bugs in existing software and hardware.

24

Attack

- Attempt to gain unauthorized access to an IS's services, resources, or information, or the attempt to compromise an IS's integrity, availability, or confidentiality.
- The actual violation of security is called an attack

25

Types of security attacks

- **Interruption**, delay, denial of receipt or denial of service: System assets or information become unavailable or are rendered unavailable
- **Interception** or snooping: Unauthorized party gains access to information by browsing through files or reading communications
- **Modification** or alteration: Unauthorized party changes information in transit or information stored for subsequent access
- **Fabrication**, masquerade, or spoofing: Spurious information is inserted into the system or network by making it appear as if it is from a legitimate entity.

26

Goals of Security

- **Prevention**
- **Detection**
- **Recovery**

27

Goals of Security Prevention

- To prevent someone from violating a security policy
- Ideal, because then there are no successful attacks.

28

Goals of Security Detection

- To detect activities in violation of a security policy
- Verify the efficacy of the prevention mechanism
- occurs after someone violates the policy
- The mechanism determines that a violation of the policy has occurred (or is underway), and reports it.
- The system (or system security officer) must then respond appropriately.

29

Goals of Security Recovery

- Stop policy violations (attacks)
- Assess and repair damage
- Ensure availability in presence of an ongoing attack
- Fix vulnerabilities for preventing future attack
- Retaliation against the attacker

30

Goals of Security Recovery

- Usually, recovery means that the attack is stopped, the system fixed (which may involve shutting down the system for some time, or making it unavailable to all users except the system security officers), and then the system resumes correct operations.
- Recovery means that the system continues to function correctly, possibly after a period during which it fails to function correctly.
- If the system functions correctly always, but possibly with degraded services, it is said to be intrusion tolerant.

31

Operational Issues

- Security does not end when the system is completed. Its operation affects security.
- A “secure” system can be breached by improper operation (an account created with no password).
- The question is how to assess the effect of operational issues on security.

32

Operational Issues Cost-Benefit Analysis

- The cost of protecting data and resources vs. the costs associated with losing the data: Is it cheaper to prevent or recover?

Operational Issues
Cost-Benefit Analysis

33

- The following should be considered when analysing cost-Benefit
  - The overlap of mechanisms' effects (one mechanism may protect multiple services, so its cost is amortized)
  - The non-technical aspects of the mechanism (will it be impossible to enforce), and
  - Ease of use (if a mechanism is too cumbersome, it may cost more to retrofit a decent user interface than the benefits would warrant).

Operational Issues
Risk Analysis

34

- Should we protect something?
- How much should we protect this thing?
- Risk depends on environment and change with time
- what happens if the data and resources are compromised? This tells you what you need to protect and to what level.
- Cost-benefit analyses help determine the risk here, but there may be other metrics involved (such as customs).

35

Operational Issues
Laws

- Are desired security measures illegal?
- Will people do them?
- Will it affects the availability and/or the use of technology.

Dr. Talal Alkharobi

36

Human Issues
Organizational Problems

- Power and responsibility: those responsible for security should have have the power to enforce security.
- Problems arise when system administrators are responsible for security, but only security officers can make the rules.
- We need to preventing this problem: no power without responsibility, or vice versa

Dr. Talal Alkharobi

37

Human Issues
Financial benefits

- Security is not a direct financial incentive for most companies because it doesn't bring in revenue.
- It merely prevents the loss of revenue obtained from other sources.

38

Human Issues
People problems

- People problems are by far the main source of security problems.
- Outsiders and insiders: *Which do you think is the real threat?*
- Outsiders are attackers from out the organization;
- Insiders are people who have authorized access to the system and, possibly, are authorized to access data and resources, but use the data or resources in unauthorized ways.
- Attackers may be dishonest vendors, disgruntled current employees or former employees.

Human Issues
People problems

- Social engineering, or lying, is quite effective, especially if the people gulled are inexperienced in security (possibly because they are new, or because they are tired).