CSC309 *Programming on the Web*

week 10: security

Amir H. Chinaei, Spring 2017

Office Hours: M 3:45-5:45 BA4222

ahchinaei@cs.toronto.edu
http://www.cs.toronto.edu/~ahchinaei/

some contents are from:
- Security in Computing: Pfleeger et al.
- Computer Security: Principles and Practice, Stallings et al.

computer security

- triad architectural requirements

- **computer security definition:** *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).*
  NIST95

all main arch. req's

- **confidentiality**
  - data (& system services) is not accessible to unauthorized parties
- **integrity**
  - data (& system services) are the right ones
- **availability**
  - data (& system services) is accessible to authorized parties

- authenticity
  - the triad req's (above) should be verifiable
- accountability
  - all actions in the system should be traceable

preserving security is difficult (1)

- a battle of human vs human!
  - no one is smarter!
  - $-\infty$ to $+\infty$!

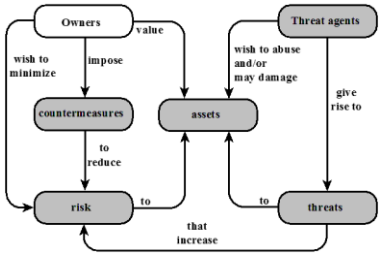
preserving security is difficult (2)

- defense vs offense
  - defender needs to close **all** holes
  - attacker needs only **one** open hole
    - One bad component in defense side is sufficient enough to fail

preserving security is difficult (3)

- complex mechanisms, although simple req's
- requires considering potential attacks
  - requires avoiding counterintuitive procedures
- developing error-free software is challenging
  - recursive nature (developing software to protect software)
- requires deciding where to deploy mechanisms
- requires possession of secret info
- requires constant teamwork and cooperation
  - hence, good training becomes even more critical
- battle of wits between attacker / admin
- not perceived on benefit until fails
- requires regular monitoring
- too often an afterthought
- regarded as impediment to using system

security terminology (1)



security terminology (2)

Adversary (threat agent)
An entity that attacks, or is a threat to, a system.

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.

Countermeasure
An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

Risk
An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Security Policy
A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

System Resource (Asset)
Data contained in an information system; or a service provided by a system; or a system capability, such as processing power or communication bandwidth; or an item of system equipment (i.e., a system component--hardware, firmware, software, or documentation); or a facility that houses system operations and equipment.

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.

Vulnerability
A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

attacks

- attacks are threats carried out and may be
  - passive: attempt to learn or make use of information from the system that does not affect system resources
    - Eavesdropping on, or monitoring of, transmissions
    - Goal of attacker is to obtain information that is being transmitted
    - Two types:
      - Release of message contents
      - Traffic analysis
    - are hard to detect, so aim to prevent them
  - active: attempt to alter system resources or affect their operation
    - Involve some modification of the data stream or the creation of a false stream
    - Four categories:
      - Replay
      - Masquerade
      - Modification of messages
      - Denial of service
    - are hard to prevent, so aim to detect them

defense methods (countermeasures)

- means used to deal with security attacks
  - prevent it
  - deter it (make attacks harder)
  - deflect it (make attacks look not worthy)
  - detect it
  - recover from it
- may result in new vulnerabilities
- will have residual vulnerability
- the goal is to minimize risk given constraints
- depth defense (layering)

some countermeasure mechanisms (1)

- for data
  - cryptography
- for systems
  - authentication
  - access control
  - os security measures
  - anti virus scanner
  - firewalls

some countermeasure mechanisms (2)

- physical countermeasures
  - physical protection of hardware
  - locks
  - guards
  - surveillance systems
  - off-site backup
- policies and procedures
  - covers data, systems, and physical controls