CEN-5079
Secure Application Programming

Class 1

Bogdan Carbunar
Outline

- Administrative Issues
- Textbooks
- Security Overview
Administrative Issues

- **Staff**
  - Bogdan Carbunar, assistant professor

- **Communications**
  - Class web page:
    - E-mail: carbunar@gmail.com

- **Office Hours**
  - Monday after class, ECS 383 (upon appointment)

- **What about you?**
Class Grading (subject to changes)

- 1 final worth: 35%
  - Date of exam: December 4, 2017
- Paper presentation: 35%
- Homeworks: 20%
- Class participation: 10%
Class participation: 10%
- Class presence does not mean participation
- But it is encouraged
- Participation means *asking* and *answering* questions

Student paper presentations: 35%
- Papers will be posted on class web page
- Let me know in time (FIFO assignment rule)
- Presence compulsory – part of grade
Outline

- Administrative Issues
- Textbooks
- Security Overview
Textbooks

- No textbook!

- Class presence and Slides

- Papers assigned for reading
  - See class webpage
Outline

- Administrative Issues
- Textbooks
- Security Overview
Information & Computer Security

- Protect **information** and information systems from **unauthorized** access

- Computer Security: security applied to **computers**
  - Objective: protect information and property
  - Against theft, corruption, or natural disaster
  - Information and property remain accessible to intended users

[Source: wikipedia]
Network Security

- Provisions and policies adopted by a network administrator to prevent and monitor
  - Unauthorized access
  - Misuse
  - Modification
  - Denial of access of network and resources

[Source: wikipedia]
System Security

- Goals: Protect
  - Confidentiality
  - Integrity
  - Availability
Confidentiality

- Information about system or its users cannot be learned by an attacker

- Data Confidentiality:
  - Private or confidential information is not revealed to unauthorized individuals

- Privacy:
  - Users control what information about them can be
    - Collected
    - Stored
    - By whom
Integrity

- The system continues to operate properly, only reaching states that would occur if there were no attacker

- Data Integrity
  - Information and programs are changed only in specified and authorized manner

- System Integrity
  - System performs intended function free from unauthorized system manipulation
Availability

- Actions by an attacker do not prevent users from having access to use of the system
  - Enable access to data and resources
  - Timely response
  - *Fair* resource allocation
Examples

- **Confidentiality**
  - Student grades
  - Available only to student, parents, employer

- **Integrity**
  - Patient information e.g., allergies
  - Can lead to loss of human life

- **Availability**
  - Authentication service
  - Unavailability can lead to financial loss
More Required Concepts

- **Authenticity**
  - Being able to be verified and trusted
  - Confidence in the validity of a message (originator)

- **Accountability**
  - Actions of an entity can be traced to it
  - Tracing a security breach to a responsible party
Security is about

- Honest user (e.g., Alice, Bob, ...)
- Attacker
- How the Attacker
  - Disrupts honest user’s use of the system (Integrity, Availability)
  - Learns information intended for Alice only (Confidentiality)
Aspects of Security

- **Threat**
  - Potential for violation of security
  - Possible danger exploiting a vulnerability

- **Security attack**
  - Action that compromises the security of a system
  - Confidentiality, integrity, availability
  - Deliberate attempt to evade security mechanisms
Aspects of Security (cont’d)

- **Security mechanism**
  - Process designed to detect, prevent or recover from attack

- **Security service**
  - Enhances security of data and its transfer
  - Counter security attack
Vulnerabilities

- Hardware: physical attack
  - Accidental
  - Voluntary machine slaughter / theft

- Software
  - Buffer overflows, incomplete mediation, time of check to time of use (TOCTOU)

- Data
  - Confidentiality, Integrity, Availability

- Networks
  - Hardware + software + data +
  - Communication media
What is Security?

- **System correctness**
  - If user supplies expected input, system generates desired output
  - Good input $\Rightarrow$ Good output
  - More features: better

- **Security**
  - If attacker supplies unexpected input, system does not fail in certain ways
  - Bad input $\Rightarrow$ Bad output
  - More features: can be worse
Security Attacks

- **Passive Attacks**
  - Learn and use information from a system without affecting system resources

- **Active Attacks**
  - *Attempt to affect and alter system resources*
Passive Attacks

1. Perform traffic analysis on encrypted messages

2. Eavesdrop

Alice

Eve

Bob
Active Attacks

- Impersonation
- Replay
- Modify messages
- Denial of Service (DoS)
Impersonation

1. Hi, A, unique id

2. Eavesdrop

3. Hi, “I’m A”, unique id

May enable M to obtain A’s privileges
Replay

1. "You owe me $10"

2. Eavesdrop

3. You owe me $10

Bob owes Alice $20 or Bob owes Malory $10
Message Modification

1. Give Carol access
2. Eavesdrop
3. Give Malory access

Note that A’s message is delayed or removed
Why Security Vulnerabilities?

- Some contributing factors
  - Few courses in computer security 😊
  - Programming text books do not emphasize security
  - Few security audits
  - *C is an unsafe language*
  - Programmers have many other things to worry about
  - Consumers do not care about security
  - Security is expensive and takes time