Computer Security Topics

COMP 435
Fall 2017
Prof. Cynthia Sturton

TA Introductions

- Connor Hamlet
- Ahmed King
- Aaron Zhang

Course Goals

1. Security Literacy
2. Security Mindset
3. Independence

Target Audience: Every CS Major*

*Who has taken COMP 410 and 411 and hasn't taken 535.

Administrative

Contact Information

Class site:
https://cs.unc.edu/~csturton/courses/securityconcepts/

Piazza site:
https://piazza.com/unc/fall2017/comp435/home/

Email:
instr-435-cs@cs.unc.edu

Piazza

- Sign up!
- Help each other
- Be polite
- Never post code
- Never ask others to post code

Office Hours

- Day
- Time
- Location

} TBD

- Required:
  - Attend 1 time
  - Within first 3 weeks

Grades

In-class exercises: 10%

Assignments: 40%

Exams: 30%

Final: 20%

Textbook

Computer Security: Principles and Practice, 3rd Ed., by Stallings and Brown

Assigned reading is fair game for in-class exercises and exams

Policies

- No laptops in class
- Late assignments
  - Lose ⅓ grade every 24 hours
  - Receive a 0 after assignments are returned
- Never share code

Act Ethically

You will learn about known vulnerabilities and attacks on computer systems. This is not an invitation to exploit these vulnerabilities in real systems.

You may not attempt to break into any system that is not your own; you may not attempt to thwart or circumvent the security of any system that is not your own. Doing so is, at a minimum, a violation of the honor code and likely a violation of the law.

Use caution; even accidental exploits may be subject to prosecution.

Let's Begin

Def'n: Computer Security

A secure system is one that protects its resources even in the presence of an adversary

Def'n: Computer Security

A secure system is one that protects its **resources** even in the presence of an adversary

Def'n: Computer Security

A secure system is one that protects its resources even in the presence of an **adversary**

Def'n: Computer Security

A secure system is one that **protects** its resources even in the presence of an adversary

Security Policies

- Confidentiality
- Integrity
- Availability

C-I-A Triad

Security Policies

- Authentication
- Non-repudiation

Attack Surfaces

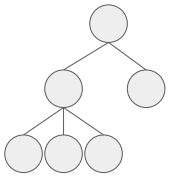
The reachable and exploitable vulnerabilities in a system

Attack Surfaces

The reachable and exploitable vulnerabilities in a system

- Network
- Software
- Hardware
- Human

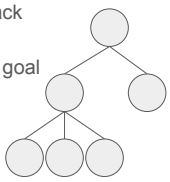
Attack Tree



Reference: Bruce Schneier, “Attack Trees”
https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Attack Tree

- A tree structure to represent one attack
- The tree’s root represents the attack goal



Reference: Bruce Schneier, “Attack Trees”
https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Threat Assessment

- Attacker’s resources
- Attacker’s method
- Attacker’s motivation
- Value of protected asset

Challenges in Security

- Attacker only needs to find one opening
- Security measures in conflict with usability
- Security policies are hard to get right
  - to close vulnerabilities
  - to maintain availability

Security Principles

- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privilege
- Least privilege
- Least common mechanism
- Psychological acceptability
- Defense in depth

Find the Flaw

```
int status = IsAccessAllowed(...);
if (status == ERROR_ACCESS_DENIED) {
   // security check failed, deny access.
} else {
   // security check ok, allow access.
}
```

Adapted from Computer Security: Principles and Practice, 3rd ed. Stallings and Brown.

"A security mindset means looking both ways before crossing a one-way street"

-- Unknown, Doug Linder, Laurence J. Peter (an apparent chain of misquotes).