CS 4173/5173
COMPUTER SECURITY

Course Overview

INSTRUCTOR

- Dr. Shangqing Zhao
  - Assistant Professor in School of Computer Science
  - Office: DEH 210D
  - Email: shangqing@ou.edu
- Hours
  - Class Meeting: T&R 3:00 PM to 4:15 PM in Dale Hall 0103
  - Office Hour:
    - T&R 4:15 PM to 5:15 PM in DEH 210D
    - Or appointment by email
- Discord server
  - https://discord.gg/TdYXDFcHUF
  - Feel free to send me chat messages any time in discord and expect response in a reasonable time frame.

ABOUT ME

- Research Areas: cyber security, network security, wireless/mobile computing and security, and adversary machine learning

- Security related projects
  - Data analytics based security
  - Wireless and network security
  - Internet and software security
  - Modeling and security analysis of infrastructures

ABOUT TA

- Mr. Guanchong Huang (guanchong.huang@ou.edu)
  Office hour: 2:00 PM - 4:00 PM Friday in DEH 115
- Mr. Ferial Najiantabriz (ferial@ou.edu)
  Office hour: 4:30 PM - 5:30 PM Tuesday & 12:00 PM to 1:00 PM Thursday in DEH 115
- Ms. Yu Cai (Yu.Cai-1@ou.edu)
  Office hour: 12:00 PM - 1:00 PM Tuesday & 12:00 PM to 1:00 PM Thursday in DEH 115
- Mr. Yan He (heyan@ou.edu)
  Office hour: 3:00 PM - 4:00 PM Friday on Discord
- Email TA regarding the following
  - Basic questions about the educational content in the class
  - Appointment to discuss in person
  - Grading/feedbacks in homework

WHY THIS COURSE?

- If you want to do the following
  - Know the big picture of computer security and crypto
  - Understand how to store data secretly
  - Make sure the person you talk to in a network is really the person you want to talk to?
  - Improve your own practices about computer security
  - Work towards a security-related professional
  - …

CONTENT OF THE CLASS

- Application-oriented with appropriate mathematical content.

- It helps you
  - Understand fundamentals and solve real-life security problems
  - Improve your own practices when handling personal information or data in computer and network systems

EXAMPLE I

- How to encrypt the message

Hello! Welcome to the class!

- to

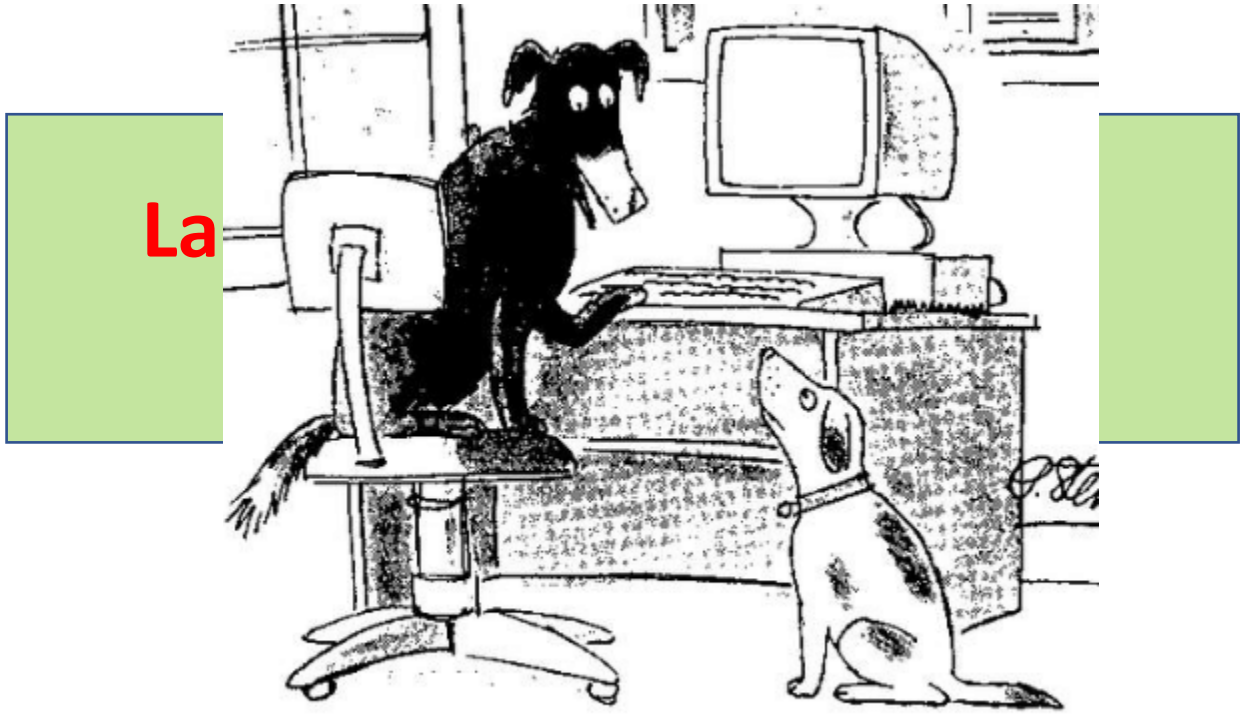
1010000101010100111100010110111011111000011010001001010101011110101001010100001101

EXAMPLE II

- How to define security?
  - A -> B, B -> C, C -> D, …
  - Good morning ? Hppe npsojoh
    - Is this secure?

EXAMPLE III

- Can you be sure of the authenticity of this message?



"On the Internet, nobody knows you're a dog."

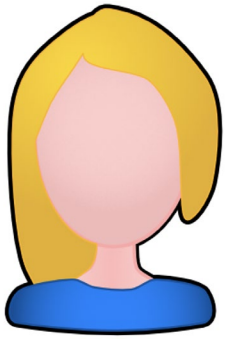
EXAMPLE IV

- How to save the password in a file system?

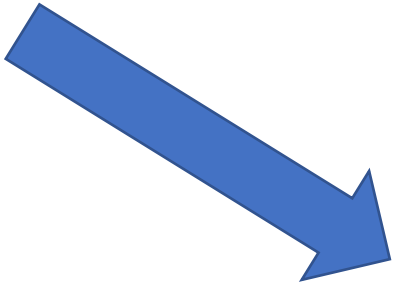
MyPass123

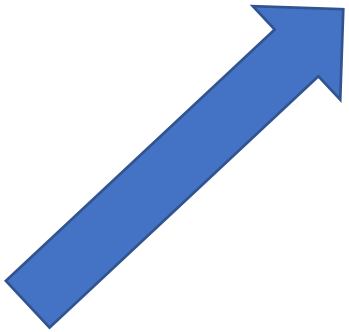
EXAMPLE V

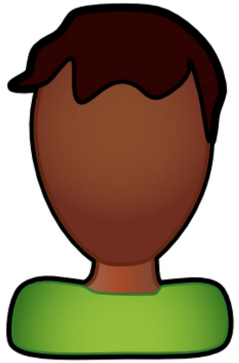
- Alice sends a file to Bob via Eve, can Bob be sure the file is NOT changed by Eve?



Alice





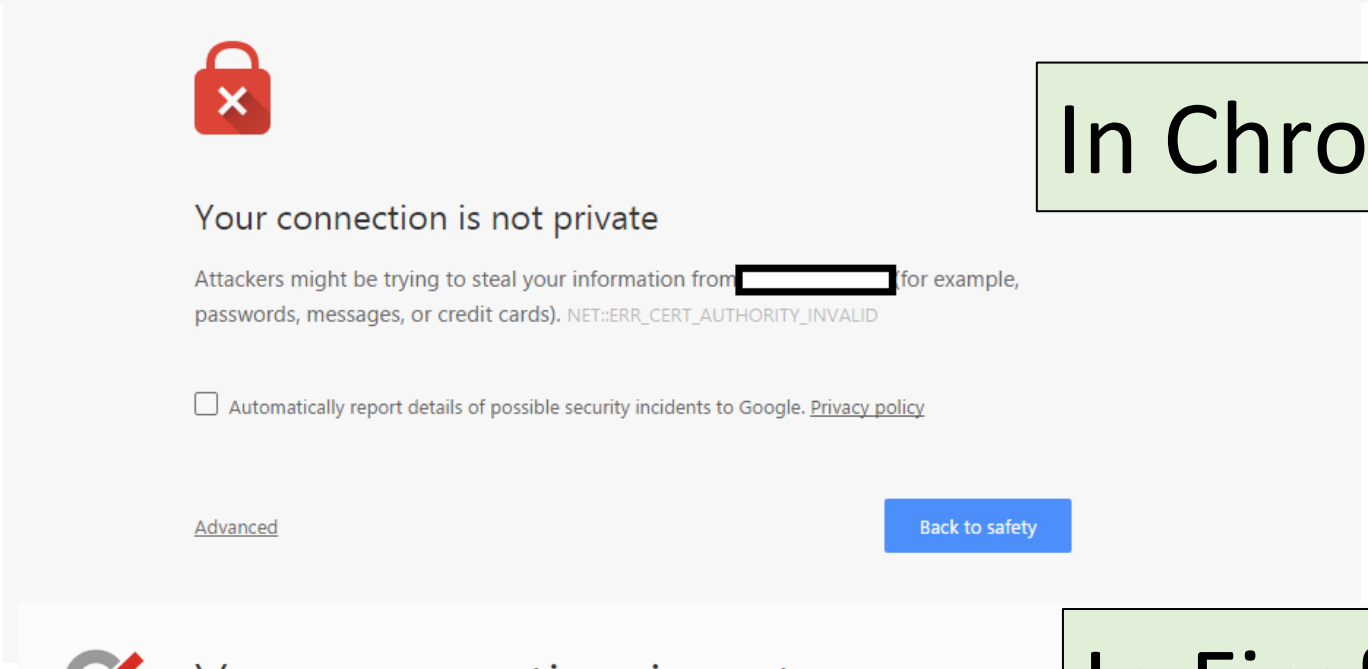


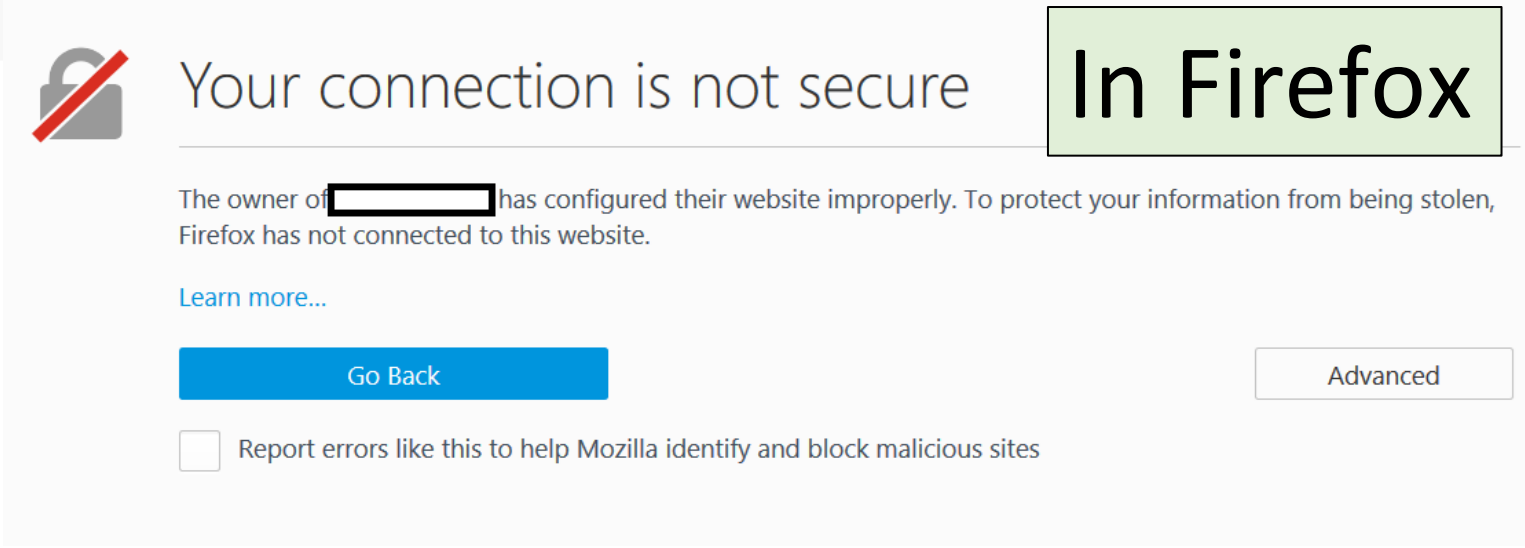
Bob

Q: Will OU IT spy on me when I visit my bank account on campus?

Eve

EXAMPLE VI


In Chrome
Your connection is not private
Attackers might be trying to steal your information from [redacted] (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID
Automatically report details of possible security incidents to Google. Privacy policy
Advanced
Back to safety


In Firefox
Your connection is not secure
The owner of [redacted] has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.
Learn more...
Go Back
Advanced
Report errors like this to help Mozilla identify and block malicious sites

EXAMPLE VII

In 2010, Florida
BitcoinTalk user
to pay **10,000** B

Known as “the first r
used with Bitcoin” (f

Screen shot fr
Finance on Ja

USD)
ency in USD
Add to watchlist
0 +336.74 (+0.79%)
t open.
Conversations Historical Data Profile

Food	Size	
	Pizzas Original and	
Cheese (Original)	Medium	$13.00
Cheese (Original)	Large	$15.00
Cheese (Original)	Extra Large	$17.00

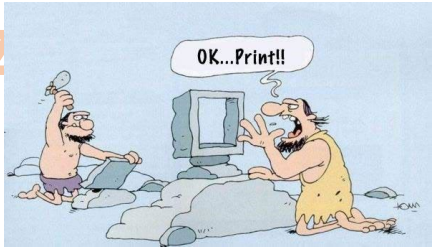
154 more rows

https://www.fastfoodmenuprices.com › papa-johns-prices

Papa John's Menu & Prices (Updated: January 2022)

25,000,000 Piz

22,000 Years



PREREQUISITES

- Basic understanding on how to use computers and basic programming skills.
  - How to program
  - Some algorithm knowledge.

- Basic math skills:
  - Basic probability
  - Basic discrete math
  - Modulo operation
  - Prime numbers

TEXTBOOK

- Recommended but NOT mandatory:
  - Charlie Kaufman, Radia Perlman, and Mike Speciner, *Network Security: Private Communication in a Public World, 2nd Edition*, Prentice Hall, ISBN: 0-13-046019-2.
  - Wenliang Du. Computer Security: A Hands-on Approach. 1st Edition, 2017.

GRADING

- Total: 100%
  - A: 90 – 100
  - B: 80 – 89
  - C: 70 – 79
  - D: 60 – 69
  - F: 0 – 59
  - Final average scores will not be curved!

GRADING

- Attendance: 5%
- Homework: 30%
- Midterm: 25% (20% for 5173)
- Final Exam: 30% (25% for 5173)
- Final Project: 10%
- In-class presentation 10% (5173 only)

ATTENDANCE POLICY

- Students should regularly attend the class
  - Up to 5 random sign-ups during the semester. The actual number could vary from 0 to any number up to 5.
  - One absence is allowed
  - Absence with reasonable email justification is excused.

- Total grading: 5%
  - No or one absence: 5%
  - Two absences: 4%
  - Three absences: 3%
  - Four or more: 0%

HOMEWORK ASSIGNMENTS

- Around 4 - 5 assignments in total
  - All works are done individually unless otherwise specified
  - Late homework: 15% penalty each day. Not accepted after THREE days unless there is documented emergency. There will be extra accommodation if you have been impacted by COVID-19, please let the instructor know.

- Homeworks are **VERY IMPORTANT!**

HOMEWORK ASSIGNMENTS

- Homework solutions are strongly encouraged written using word processing software
  - E.g., MS Word, Open Office, WPS, Google Doc, LaTex, …

- Submit in PDF file.

Q: why do we use PDF file?

How do you know if your instructor is malicious?

MIDTERM & FINAL EXAM

- They are both in-class exams
  - Work on your own, closed everything (neighbor, laptop, phone, book, …)
  - You are allowed to bring a one-page letter-sized (8.5 * 11 inches) cheat sheet.

- Make-up exams will not be normally allowed
  - Exceptions will be made if a student presents a police report or a doctor's note that show some emergency situations.
  - e.g., attending my friend's wedding is NOT an acceptable excuse

FINAL PROJECT

- All students should form a team of **1-5** to complete a final project.
  - There will be no extra credit for a student working individually on the final project.
  - Get familiar with your classmates to form teams

- The project details will be announced around the midterm.

FINAL PROJECT

- Assigned project
  - I will list a potential project for you to do.
  - Most students chose this one in the past.
- You own proposal
  - You can also propose your own idea to improve the security of a system.
- A survey on existing studies
  - You can write a comprehensive survey on a security topic.

PROJECT DELIVERABLES

- Assigned project and your proposal
  - Project report (at least 5 pages)
  - Source code

- Survey:
  - A survey paper (at least 15 pages)
    - Write using your own words
    - IEEE conference format (double column)
      - Link: https://www.ieee.org/conferences/publishing/templates.html
    - DON'T copy sentences from papers
    - Anti-plagiarism tool will scan your survey

- If we have time:
  - System demo and survey presentation in class

IN-CLASS PRESENTATION

- Up to **5** students form a team (5174 only)
- Each team will in turn present research papers after the midterm
- List of research papers will be uploaded on Canvas
- 20 minutes presentation + 5 minutes QA

ACADEMIC INTEGRITY

- A student must complete his/her tests and assignments on his/her own. Example cheating behaviors include but not limited to: direct and indirect plagiarizing another student's work.

- For student's guide to Academic Integrity, please visit

  http://integrity.ou.edu/students.html

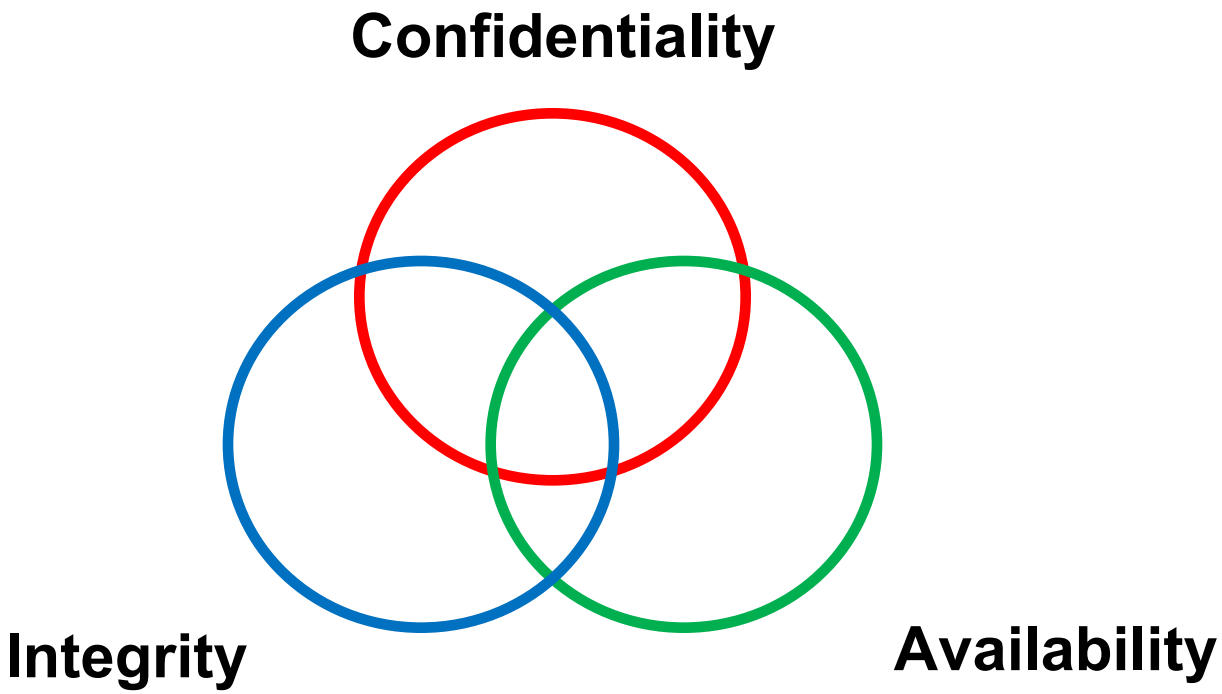
CS 4173/5173
COMPUTER SECURITY

Introduction

OUTLINE

- High-level Concepts:
  - security objectives, security services, threat, vulnerability, …
- Introduction to Denial-of-Service (DoS) attacks
- Introduction to cryptography
- Some earlier cryptographic methods.
- Some “key” issues

SECURITY OBJECTIVES



SECURITY OBJECTIVES (CIA)

- Confidentiality — Prevent/detect improper disclosure of information
- Integrity — Prevent/detect improper modification of information
- Availability — Prevent/detect improper denial of access to services provided by the system

COMMERCIAL EXAMPLES

- Confidentiality — An employee should not know the salary of his manager in a private company.

- Integrity — An employee should not be able to modify the employee's own salary.

- Availability — Paychecks should be printed on time, as stipulated by law

MILITARY EXAMPLES

- Confidentiality — The target coordinates of a missile should not be improperly disclosed

- Integrity — The target coordinates of a missile should not be improperly modified

- Availability — When the proper command is issued the missile should fire

QUESTION

- C, I, A
  - Which one is important than the other?

QUESTION

- _____ Which of the following design is to achieve availability

- [A] encrypt all data in a system
- [B] add redundant servers to process user requests
- [C] verify a user's password
- [D] use alias to hide a user's name

QUESTION

- _____ Which of the following design is to achieve integrity

- [A] require users change passwords each month
- [B] hide a server's location
- [C] a control system verifies a command is indeed sent from the control center without any change during transmission
- [D] post private information on the Internet

QUESTION

- _____ Which of the following design is to achieve confidentiality

- [A] a CRC check to verify whether a file downloaded from the Internet is corrupted.
- [B] use error-correction code to correct errors in computer communication
- [C] compress a file with a secure password
- [D] permute patients' records when release data

SECURITY SERVICES

- Security functions are typically made available to users as a set of security services through application program interfaces (APIs):

- Confidentiality: protection of any information from being exposed to unintended entities.

- Authentication: assurance that an entity of concern or the origin of a communication is authentic - it's what it claims to be or from

- Integrity: assurance that the information has not been tampered with

SECURITY SERVICES (CONT'D)

- Non-repudiation: offer of evidence that a party is indeed the sender or a receiver of certain information
- Access control: facilities to determine and enforce who is allowed access to what resources, hosts, software, network connections
- Monitor & response: facilities for monitoring security attacks, generating indications, surviving (tolerating) and recovering from attacks

SECURITY ASSURANCE

- How well your security mechanisms guarantee your security policy
  - Metrics to measure the level of security.

- Everyone wants high assurance
- High assurance implies high cost
  - May not be possible
- Trade-off is needed

SECURITY BY CRYPTOGRAPHY

- Essential way to ensure the goals of integrity and confidentiality.

- Question: Can cryptography achieve the goal of availability?
  - WannaCry ransomware attack on the Internet 2017.
  - https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

SECURITY BY OBSCURITY

- Security by obscurity
  - If we hide the inner workings of a system, it will be secure
- More and more applications open their standards (e.g., TCP/IP, 802.11)
- Widespread knowledge and expertise

SECURITY BY LEGISLATION

- Security by legislation says that if we instruct our users on how to behave we can secure our systems

- For example
  - Users should not share passwords
  - Users should not write down passwords
  - Users should not type in their password when someone is looking over their shoulder

- User awareness and cooperation is important!!

THREAT-VULNERABILITY

- Threats — *Possible* attacks on the system
  - The attacks targeting C, I, or A.

- Vulnerabilities — Weaknesses that may be exploited to cause loss or harm

THREAT MODEL AND ATTACK MODEL

- Threat model and attack model need to be clarified before any security mechanism is developed

- Threat model
  - Assumptions about potential attackers
  - Describes the attacker's capabilities

- Attack model
  - Assumptions about the attacks
  - Describe how attacks are launched

SUMMARY

- Security objectives
  - Confidentiality
  - Integrity
  - Availability
- Security services
- Security assurance
- Security by
  - Cryptography
  - Obscurity
  - Legislation
- Threat and vulnerability