UNIVERSITY OF TEXAS ARLINGTON

CSE 4380/5380:

Information Security I

Fall 2023

Faysal Hossain Shezan

Who am I?

Dr. Faysal Hossain Shezan

- Email: faysal.shezan@uta.edu
- Office hours: Wednesday. 2:30 PM – 3:30 PM
- Office location: ERB 345

Research Interests: Security and Privacy in Cyber Physical System, Medical Health Data and Software Security

[Optional] Contact me if you are interested in related research projects.

https://fhshezan.github.io/course/CSE-4380-5380-InfoSec-Syllabus-Fall2023.pdf

Who is the TA?

- Sankalp Sunil Kadam
- Email: ssk2320@mavs.uta.edu

- Office hours: Monday and Wednesday, 10:00 AM to 12:00 PM
- Where: ERB 501

Who are you?

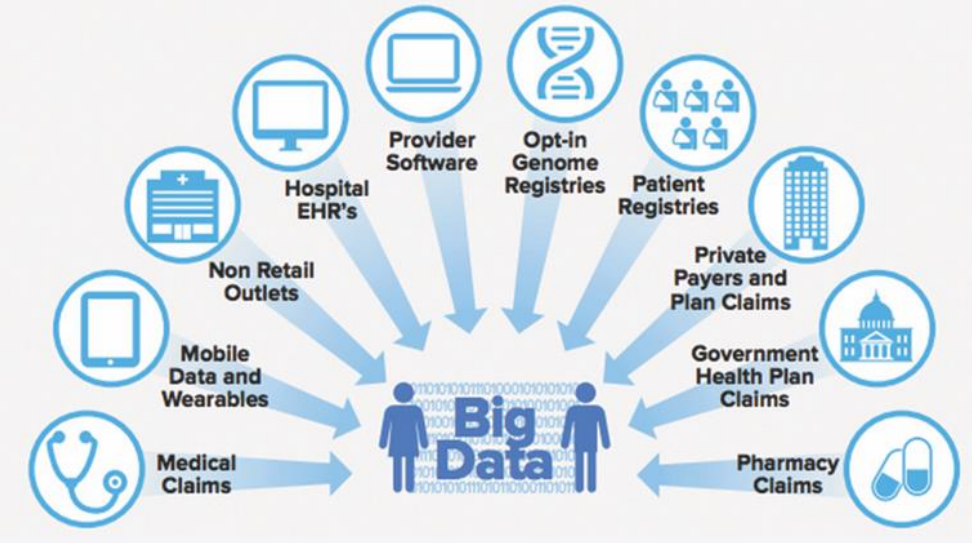
- Please briefly introduce yourself to the class: (1 minute)
  - What is your background and what are your interests?
  - Why this class? What do you expect?

Every minute a massive amount of data is generated

eCommerce is a daily part of our lives

https://www.x-cart.com/ecommerce-101.html

Health data and its many beneficial applications



- Personalize health services
- Adapt public health plans according to population symptoms and disease evolution
- Optimize hospital operations
- …

Big data and the Internet of Things (IoT) work in conjunction

The Duality of Big Data: The Angel and the Demon (in terms of Security and Privacy)

Privacy and Anonymity

Abusive Behavior (bots, compromised accounts, …)

Active and Passive Adversaries

Unauthorized access

Unauthorized use

Sharing/ Publishing Sensitive Data

Disruption, modification, or destruction of service and data

Information Security

The **protection** **of** information and information systems **from** **unauthorized** access, use, disclosure, disruption, modification, or destruction in order to provide **confidentiality**, **integrity**, **and** **availability**.

NIST Glossary of Key Information Security Terms

Three Key Security Concepts (CIA)

- **Confidentiality:** Assures that confidential information is not disclosed to unauthorized individuals.

- **Integrity:** Assures that information and programs are changed only in a specified and authorized manner. Integrity involves maintaining the consistency, accuracy, and trustworthiness of data.

- **Availability**: Assures that systems work promptly, and service is not denied to authorized users.

Examples

- Think about an example that illustrates the importance of **Confidentiality**. (2 minutes)
- Then, share them with the class.

- Think about an example that illustrates the importance of **Integrity**. (2 minutes)
- Then, share them with the class.

- Think about an example that illustrate the importance of **Availability**. (2 minutes)
- Then, share them with the class.

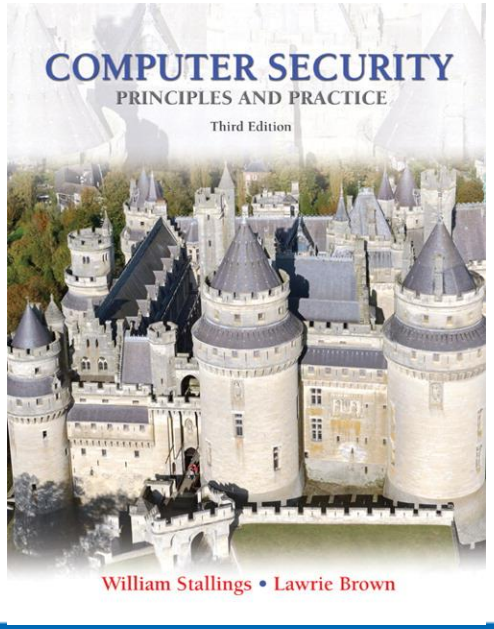
Course Description

- Hands-on introductory security course
- Basics of cryptography and methods for protecting systems from attack
- Malicious software and other attacks that occur over the network, and the defenses used to stop these attacks
- Program vulnerabilities that lead to most of the security problems
- Administrative issues that security professionals must consider in their jobs.

Prerequisites & Textbook

- Operating Systems (CSE 3320 or equivalent) is required.

- Computer Security: Principles and Practices, by William Stallings and Lawrie Brown (3rd edition)



Course Grades

- **Exams (in-class):** 40%
  - Exam 1 on Oct 18
  - Exam 2 on Nov 27
- **Lab Exercises (4 labs with 4 pre-lab exercises):** 36%
  - Labs 1 & 3 worth 7%, Labs 2 & 4 worth 11%
- **CTF Lab:** 11%
- **CTF Write-up:** 4%
- **Presentation:** 5%
- **Class Participation**: 4%

Class Presentation

- Students will give a 7-minute presentation in class to talk about a recent security/ privacy attack.
- It is nice, though not required, that your news topic be related to what is being covered in class that week.
- Students are required to upload their slides to the **Presentation assignment.**
- Some Resources:
  - Bruce Schneier's Security Blog,
  - Blackhat articles and presentations: https://www.blackhat.com/
  - RSA Conference: https://www.rsaconference.com/
  - The Risks Digest: http://catless.ncl.ac.uk/Risks/
  - Security Magazine: http://www.securitymagazine.com/
  - InfoSecurity News: http://www.alliedinfosecurity.com/newsletter.aspx

Class Presentation

Presentation Schedule: Schedule [each student needs to select 2 days]
Select the day that no other two students have chosen.[Due by 27 Aug]

- When preparing your presentations on a recent attack, collect and present the answers to the following questions:
  - When did the attack happen? (Pick a recent attack)
  - What was the actual technical vulnerability?
  - How could the attackers use the vulnerability?
  - What did the attackers gain, and what were their intentions? For example, what assets they got access to?
  - What were the consequences of the attack? How many people/ systems were affected, how much money was lost, etc.?
  - What reactions have professionals and society shown since these vulnerabilities were reported? Legal actions, reports, News, social media, etc.

Labs

- Meeting Times:
  - Tuesday 1:30- 3:20 pm
  - Thursday 1:30- 3:20 pm

Attendance is mandatory!

- Lab 1: Cryptography: Week 5
- Lab 2: User, system, network security: Weeks 7 and 8
- Lab 3: Buffer overflows: Week 11
- Lab 4: Security testing software: Weeks 12 and 13
- CTF: Lab 14

Pre-Labs

- Each lab exercise includes a pre-lab assignment due by Sunday midnight before the lab week.

- There will be 4 assignments through the semester.
  - Pre-Lab 1. Cryptography: due by Sept. 17
  - Pre-Lab 2. User, System, Network Security: due by Oct. 1
  - Pre-Lab 3: Malware: due by Oct. 29
  - Pre-Lab 4: Buffer Overflows: due by Nov. 5

Lab Preparation

- **Pre-Lab Assignments**
- **Linux basic knowledge**
  - file system
    - home directory(~) and disk root directory(/)
    - path display command: pwd
    - path format: absolute path and relative path
  - file operation commands: ls, cd, mv, cp, rm, mkdir, touch, cat
  - file editors: vim, nano, gedit
  - **file transfer command: scp**
  - local IP address: 127.168.0.1
- **C programming (Lab 3+4)**
  - basic syntax grammar: variable initialization and declaration
  - usage of pointer manipulation
  - commands of compile: gcc compiler
  - execution C program in Linux OS

CTF Lab

- **CTF Lab:** In this lab exercise, students will work in teams in a jeopardy-style capture-the-flag game to earn points awarded by performing security tasks and exercises that you have learned in class and even some new ones.
- Students will write a team report showing how they applied class knowledge to the game.

- Pre-CTF: due by Nov. 19
- CTF Lab will be during week 14

Exams

- Exam 1: in-class, Oct. 18
  - Covers everything discussed up to Week 8

- Exam 2: in-class, Tuesday, Nov. 27
  - Comprehensive; focus on Week 9-14

Assignment Late Policy

- Manage your time well and start early!
- **Grace periods:** To accommodate for unavoidable circumstances, you will be given **one** 3-day grace period for your assignments.
- Beyond the deadline (and grace period if applicable), you will be penalized 25% a day. For example, if you score 73% and are 5 minutes late, you will be penalized 25% for 1 day, resulting in a score of 73 – 25 = 48%). Use these freebies wisely — they are meant for circumstances such as falling ill or interviewing. I will not grant any additional extensions.
- Send an email to the GTA and cc me. You can only use this 3-day grace period **once** in the semester.
- When submitting your assignments specify that you have sent an email and want to use your grace period.

Attendance

- Attendance is graded based on your participation in each lecture.
- Let's concentrate in class!
- Take notes! (not all the details are on the slides)
- Do not use your cell phone
- In case of observed infractions, you will be treated as absent.

Academic Integrity: Students enrolled all UT Arlington courses are expected to adhere to the UT Arlington Honor Code:

- *I pledge, on my honor, to uphold UT Arlington's tradition of academic integrity, a tradition that values hard work and honest effort in the pursuit of academic excellence.*
  I promise that I will submit only work that I personally create or contribute to group collaborations, and I will appropriately reference any work from other sources. I will follow the highest standards of integrity and uphold the spirit of the Honor Code.

- Suspected violations of university's standards for academic integrity (including the Honor Code) will be referred to the Office of Student Conduct. Violators will be disciplined in accordance with University policy, which may result in the student's suspension or expulsion from the University. Additional information is available at https://www.uta.edu/conduct/.

- Additionally, there is a special ethics form for this course about malicious hacking that you must sign and uphold.

Academic Integrity

- Give credit where it's due and don't plagiarize. Don't copy or read others' solutions. Remember, when you cheat, you cheat yourself above all else.

- You may discuss readings with other students in the course or with me**. Each student must submit their own written answers to pre-lab and lab assignments. You may not read or copy anybody else's written answers** — all submitted work must be your own, based on your own understanding of the content after such discussions.

- **Credit your sources.** In your assignments, list all your collaborators (e.g., "I discussed this assignment with Alice, Bob, ...") and credit any sources (including software) used. You must also credit sources that are permitted by the instructor. For example, you must credit code that we give you if it helps you with your work (either by direct use of the code, or by simply enhancing your understanding by reading the code).

Information Assurance Education Certificate

- UT Arlington is authorized by DHS and NSA to offer certificates in Information Assurance Education. We offer certificates on the following basis
  - You get a 'B' or better in InfoSec 1
  - Your score 70% or better on this quiz
  - You pass undergraduate-level or higher courses (at UTA or elsewhere) on computer networks and operating systems

Quiz
(optional, if you want to get the certificate)

Reading materials:

- Part 3 of the book (Chapters 14-19), plus these short readings:

- http://en.wikipedia.org/wiki/Communications_security
  (stop before Related Terms)
- http://en.wikipedia.org/wiki/EMSEC
  (skip the "Measurement standards" and "Certification" sections)
- http://en.wikipedia.org/wiki/Opsec
- http://en.wikipedia.org/wiki/TRANSEC (very short)
- http://www.ni.com/white-paper/4450/en (just the short introduction)

Reading for next week

- Chapter 1 (focus on Sections 1.1, 1.4, and 1.6)
- Chapter 2 (Sections 2.1 to 2.6)