Lecture 00
Course Description

Software Security Engineering

Winter 2023
Thompson Rivers University

Administrivia

Lecturer: Sina Keshvadi (skeshvadi@tru.ca)
Lectures:

Monday	17:30 - 18:20
Tuesday	14:30 - 16:20 (Lab)
Wednesday	17:00 - 17:50
Friday	12:30 - 13:20

- Website: All course materials will be posted on TRU Moodle

Recommended textbook

"Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin", Second Edition

by Paul C. van Oorschot. Springer, 2021.

Available online (free):

https://people.scs.carleton.ca/~paulv/toolsjewels.html

Course Materials

- Lectures will focus on big picture principles of security attacks and defenses.
- Lectures will cover some material that is **not** in the textbook **and you will be tested on it!**
- supplementary readings (i.e., academic papers) will also be made available

SENG 4220 at a glance

- Software Security Background
- Channel Security
- Cryptographic Building Blocks
- Authentication Protocols and Key Establishment - Kerberos
- Software Security - Exploits and Privilege Escalation
- Malicious Software
- Public-Key Certificate Management and Use Cases
- Web and Browser Security
- Code Injection and Clickjacking
- Intrusion Detection and Network-Based Attacks
- Detecting Attacks
- Bitcoin, Blockchains and Ethereum

Grading

Item	Weight	Due
Assignment 1	5 %	Jan 20, 2023 (11:59 pm)
Assignment 2	10 %	Feb 10, 2023 (11:59 pm)
Midterm	20 %	Mar 2, 2023 (in class)
Course Project	10 %	Mar 17, 2023 (11:59 pm)
Lab Activities	20 %	Each lab 2%
Final Exam	35 %	TBA

* Course project can be done in a group of two

Late Assignments and Lab activities

- You will have 3 days late date submission
  - 3 on one lab/assignment and 0 on others
  - 1 on three different ones
  - a ‘day’ is used for one minute past deadline until 24 hours past. You are required to manage this yourself
  - you do not need to inform me that you use a late day
  - you cannot use days past last day of class

Lab Sessions

- Lab sessions cover four topics
  - Software Security
  - Cryptography
  - Network Security
  - Web Security
- You will be given a lab activity instruction, and you will submit a lab report for each lab session
- Each Lab has 2% of your final grades (20% in total)
- You can submit your report until 23:59 in each lab day

Ethics and Law

- We will discuss **attacks** on computer security

NONE OF THIS IS IN **ANY WAY** AN INVITATION TO USE WHAT YOU LEARN OTHER THAN WITH INFORMED CONSENT OF ALL INVOLVED PARTIES

- The existence of a vulnerability is not an excuse to exploit it
- This isn't just ethics but the **law**

  some attacks are easy to do …

  ... and people are in jail for doing them

- If you're ever unsure if you should be doing this then talk to me first.

Some of the tools you'll learn about **cannot be used in practice** as in, they work, but then you'll get letters from your ISP.

Office Hours

Mondays 10:00–12:00 in OM 2736

Academic Misconduct

Academic Misconduct

I take academic misconduct extremely seriously.

Common Offenses

- sharing solutions, code, etc.
- posting your code publicly (e.g., github)
- using other people's code, solutions searching directly for solutions
- buying solutions or having someone else do the work

Misconduct

Misconduct

- Whenever you copy/paste text you didn't write yourself you need to cite it
- Putting cites at end of submission isn't enough: you need to point out where you use them
- If you have any text you did not write the text itself needs an indicator that this is not your own original work.
- Copying someone else's text and replacing words with synonyms ("tortured phrases") is misconduct

using citations

- whenever you are copying/pasting text or copying/pasting code to answer a question, you should think:
  - is this a reasonable answer to the question?
- even if you cite it properly, copying someone else's answer to the question is almost certainly not what I have in mind when giving an assignment/lab

working with others

- working with other people on the ideas is okay as long as it doesn't feel like cheating
- e.g., discuss question and solutions but don't take notes then do something else for 30 minutes
- whatever's still in your mind is yours to keep

use of third party code

- using other people's code is generally fine as long as it is not a direct solution
- ask yourself: does this make this question trivial / pointless / devoid of any learning?
- ask yourself: does this code make me not have to do any work myself relevant to course?
- assignments are not about how good you can search for an answer

searching for answer

- do not search directly for the question
- do not solicit answers to the question
- if you accidentally see a specific answer to a specific question your thinking is polluted even if you try not to use it your answer may converge to other people's answers that are also polluted

Question: Suppose You Knew Ahead Of Time How Much Randomness You Needed, Like One Megabyte. Describe Two Approaches That Use...

Suppose you knew ahead of time how much randomness you needed, like one megabyte. Describe two approaches that use a small (e.g., 256-bit) seed to generate a one-megabyte stream of randomness that:

1. achieves rollback resistance *but not* prediction resistance
2. achieves prediction resistance *but not* rollback resistance

That is, two different approaches that each achieve exactly one of the two desired properties. You may assume standard cryptographic assumptions hold.

Be sure to express your design clearly (i.e., use pseudocode if necessary). You may use basic cryptographic functions but just define what they mean. You can use the previous question's pseudocode as a good idea as to expectations.

Hint: think about the one-way property of hash functions!