ILLINOIS TECH

College of Computing

Introduction to Software Security

Yue Duan

CS 595: Topics in Software Security

- Instructor:
  - Yue Duan, Assistant Professor who just joined this fall
    - 🏠 https://yueduan.github.io/
    - ✉ yduan12@iit.edu
  - PhD in Computer Science from UC Riverside (2019)
  - Postdoctoral training at Cornell University and University of Utah
  - Specialized in Computer Security, software engineering, AI security and blockchain
  - Actively looking for motivated students to join my lab :)

- Office hour:
  - Office: SB 209C
  - Wed 3pm - 5pm

CS 595: Topics in Software Security

- Course overview
  - Somewhat research-oriented
  - Binary analysis: code search, malware analysis, vulnerability detection, etc
  - Mobile security: Android app analysis, Android framework analysis
  - Program testing: most effective way to find bugs
  - IoT security: firmware analysis
  - Blockchain security: smart contract analysis

- Textbook
  - No textbook needed
  - Focus on research papers from top venues in computer security

CS 595: Topics in Software Security

- Prerequisite
    - Basic knowledge about OS and compiler
    - Programming skills
    - No prior security knowledge required

- Goal
    - Learn basic concepts in software security
    - Obtain hands-on experience with state-of-the-art analysis techniques
    - Develop the ability for analyzing and solving real-world security problems
    - Gain interest to conduct further research in this exciting field
    - Course project may be eventually publishable

CS 595: Topics in Software Security

- Course format and gradings
  - Paper presentation: 20%
  - Paper review: 15%
  - Discussion participation: 15%
  - Project: 50%
    - Proposal: 5%
    - Mid-term presentation: 15%
    - Final presentation: 15%
    - Final report: 15%

CS 595: Topics in Software Security

- Paper presentation
  - Each student needs to present one paper in the class
    - 10-15 min presentation
      - Hint: google the slides of the paper. You may find it but don’t directly use it
    - Lead the discussion
      - 5 - 10 mins
      - What are the pros and cons?
      - Why the authors do research the way it is?
      - Any thought for improvement?

CS 595: Topics in Software Security

- Paper review
  - Each student needs to write one review for papers from the reading list
    - At least 300 words
    - Summarize the paper
      - Content: What’s this paper about?
      - Motivation: Why do the authors want to conduct this research?
      - Contribution: How is the paper different from its peers?
      - Technique: How do the authors achieve their goal?
      - Evaluation: How is the work evaluated?
    - Read critically:
      - You should not assume that the authors are always correct. Instead, be suspicious
      - Any limitations?

CS 595: Topics in Software Security

- Project
  - Students can form groups (no more than 2 students) to work together
  - Some potential project topics will be provided
  - Students are encouraged to explore their own interest
  - Requirement:
    - Proposal presentation: 5-10 min
    - Mid-term presentation: 10-15 min
    - Final presentation: 15 min
    - Final report: research paper format (ACM template, double-column, minimum 4 pages excluding reference)
  - Example: conduct research on upgradeable smart contracts in blockchain

CS 595: Topics in Software Security

- Tentative course schedule
    - **8.24 - 9.16** introductions to different topics
    - **8.24** start looking for collaborator if you decide to work as a group
    - **9.16** start working on project topics
    - **9.21 - 10.5** binary analysis
    - **9.28** proposal presentation
    - **10.7 - 10.12** mobile security
    - **10.14 - 10.19** mid-term presentation
    - **10.21 - 11.2** program testing
    - **11.4 - 11.9** Iot security
    - **11.11 - 11.16** blockchain security
    - **11.23 - 11.30** paper presentation
    - **12.7 - 12.9** final presentation

What is Software Security?

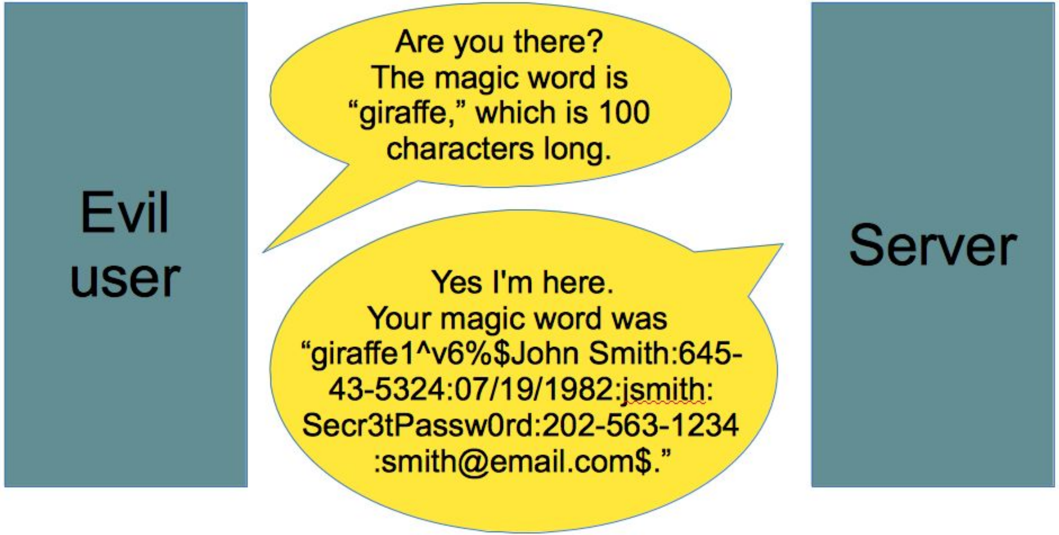
- From traditional PCs, mobile devices to IoT devices, software is literally ubiquitous in our everyday life.

What is Software Security?

- Protecting software is essential for us.
  - Huge impact
  - Malicious software is designed to cause damages
  - Normal software can and **will** contain vulnerabilities
    - Microsoft Applications: 10 - 20 defects per 1000 LOC during in-house testing
    - Industry Average: about 15 - 50 errors per 1000 LOC

What is Software Security?

- Heartbleed vulnerability
  - In popular OpenSSL library
  - Result in potential private keys leakage



Are you there? The magic word is "giraffe," which is 100 characters long.

Yes I'm here. Your magic word was "giraffe1^v6%$John Smith:645-43-5324:07/19/1982:jsmith:Secr3tPassw0rd:202-563-1234:smith@email.com$."

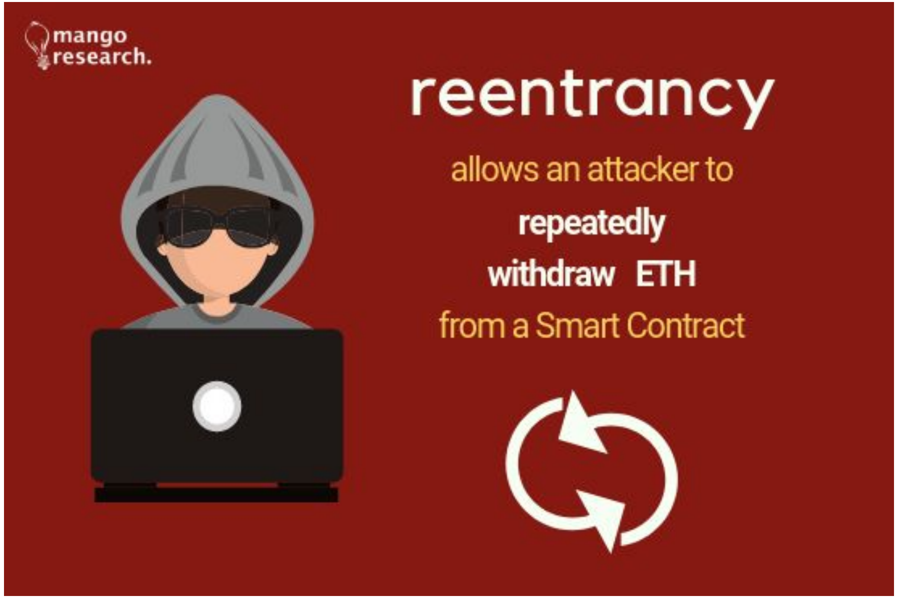
Reference: The Heartbleed Bug, explained
https://www.vox.com/2014/6/19/18076318/heartbleed

What is Software Security?

- Marriott Data Breach 2020
  - On March 31st, 2020, Marriott disclosed a security breach that impacted the data of more than 5.2 million hotel guests who used their company's loyalty application.

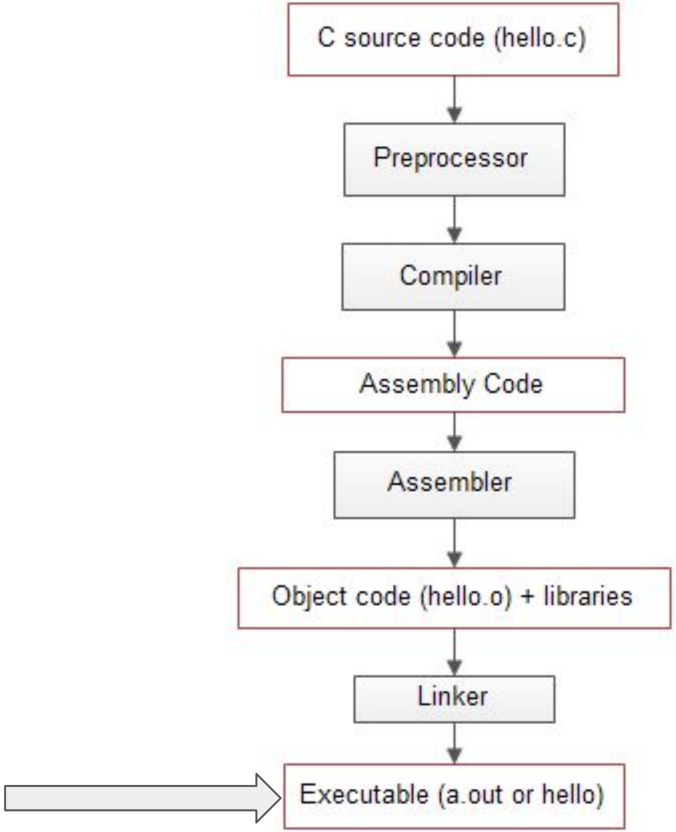
What is Software Security?

- The DAO attack
  - On 16 June 2016, the attacker managed to retrieve approximately 3.6 million Ether (1 Either = 410 USD) from the DAO fund abusing this loophole.



Topics covered

- Binary analysis



C source code (hello.c)

Preprocessor

Compiler

Assembly Code

Assembler

Object code (hello.o) + libraries

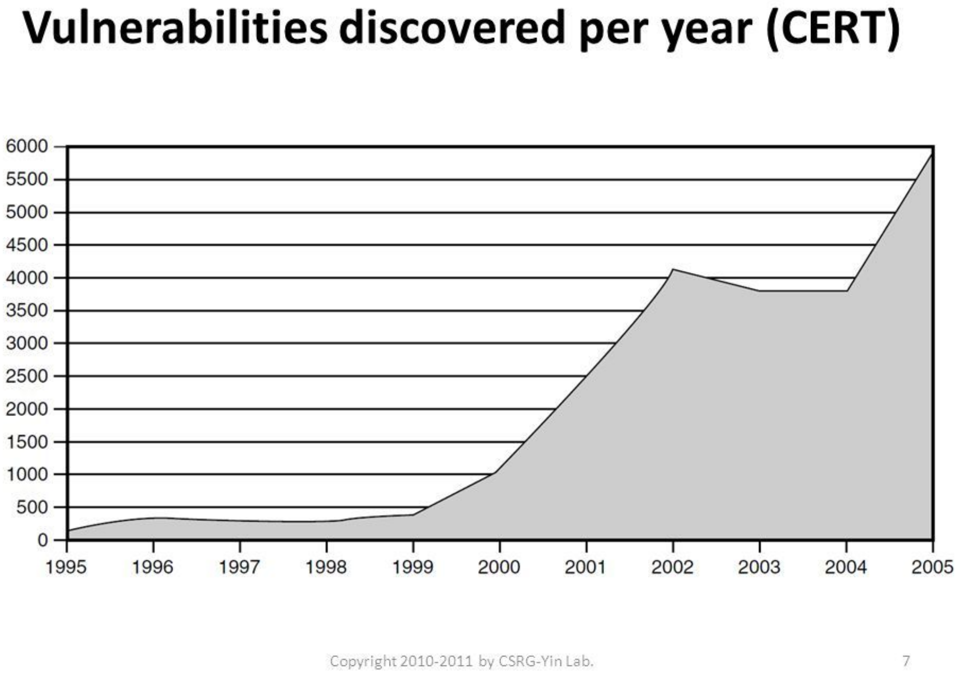
Linker

Executable (a.out or hello)

Binaries
No source code
Maybe no debug symbol

Topics covered

- Binary analysis
  - Common vulnerabilities
    - Buffer overflow
    - Format string
    - Integer overflow
    - Race condition
    - Dangling pointer
    - etc
  - Malware analysis
  - Defense mechanisms



Vulnerabilities discovered per year (CERT)

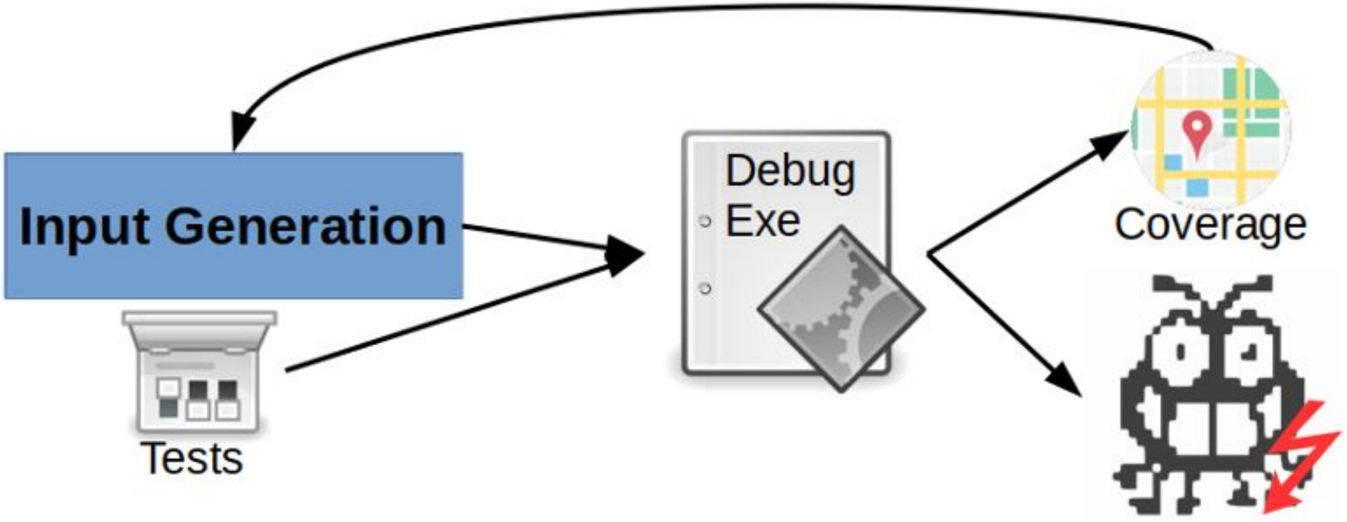
7

Topics covered

- Mobile Security
  - Is your phone secure?
    - Mobile system analysis
  - Are the apps on your phone secure?
    - Mobile app analysis
  - If no, how to fix?
    - System and app patching

Topics covered

- Program testing
  - Part of binary analysis
  - Dynamic approaches to detect vulnerabilities
  - Fuzzing, symbolic execution, hybrid approaches



Topics covered

- IoT Security
  - smart watch, smart TV, smart router, self-driving car, etc
  - Are they secure?
  - How are they different from traditional binary and mobile?

Topics covered

- Blockchain security
  - Smart contracts
    - piece of software running on blockchain
  - Attacks and vulnerabilities
  - Anonymity

Question?