CSIS 641 – Advanced Cybersecurity
Research Project

Goals:

1. Students will apply the knowledge from the course, such as vulnerability analysis, pen testing, and software security testing.
2. Students will:
    a. develop a new tool, or
    b. discover a protocol or system vulnerability, or
    c. perform pen testing for a system or software suite.
3. Students will write a 10-page conference style publication and present their work in class during the exam week (instead of a final exam)

Teams:

The project will be completed in teams of two students. If you would like to work on an idea individually you will need to discuss this with me.

Milestones:

There will be several presentations in the form of lighting talks or short presentations. You will receive feedback from me on all presentations. I will grade the final project product, not the intermediate presentations. The presentations and dates are:

1. **Project proposal**: short presentation (up to 15 mins) will be performed on **Feb. 1**. Depending on my feedback, you may change the proposal. The presentation will include:
    a. Title, team members, team name (optional)
    b. Motivation: why is what you are doing important
    c. Related work: you need to search thoroughly and make sure that something similar or same method/tool has not been created by other researchers.
    d. What you are proposing: Description of the system or network protocol that you are planning to analyze or implement, or the tool that you intend to build or extend. Description of security properties you intend to investigate. Tools and/or analysis techniques you are planning to use. Clear description of project deliverables. Possible deliverables are a software prototype, a substantial case study, or, in the case of a purely theoretical study, proofs (manual or machine-assisted).
2. **Project progress report 1**: lighting talk on your progress on **March 22**. What has worked, what needs to be refined, and what did not work and why?
3. **Project progress report 2:** lighting talk on your progress on **April 12**. What has worked, what needs to be refined, and what did not work and why?
4. **Project final presentation:** conference style presentation with duration 25 mins on final exam date (TBA). A demo can be included in the presentation in the form of live demo or video.

Evaluation:

You will be evaluated on all the presentations and final products at the end of the semester. Parts of the evaluation include:

1. Your preparedness and timely delivery of the 3 presentations. *Project points: 10*
2. The degree of originality of your final products. If you have fulfilled at least one of the following: created a new security tool or a substantial extension of an already existing tool, discovered a new protocol vulnerability, found a new software weakness, proposed a new defense method for a system or software suite, developed a theoretical proof about the robustness or weakness of a system. The completeness of your deliverables, i.e., code, documentation of the hack, or proof, will be graded in this part. *Project points: 60*
3. Final presentation and paper: a professional presentation with a well written scientific paper that can be presented at a conference or workshop. *Project points: 30*

Project ideas

Some ideas are suggested below. You may propose your own topic.

Analyze a software system

Analyze a substantial program or suite of programs. Your objective is to verify the presence of known vulnerabilities, or try to find new ones. Look for both design and implementation vulnerabilities. I suggest choosing a popular open-source program from, for example, SourceForge or github. Pick a program that you find interesting and would like to learn more about.

I recommend using an **analysis tool to start**. One good source with several analysis tools is the OWASP Source Code Analysis Tools.

Implement a software protection method

Design and implement a prototype of a new tool for preventing or containing execution of malicious code. Evaluate its usefulness against various attacks.
Examples:

1. Implement a new tool that prevents shell code injection
2. Implement a novel mechanism or language/protocol that monitors untrusted software transactions.
3. Implement a mechanism that rejects untrusted applications such as privilege escalation, system transactions etc.
4. Create a tool that verifies if the behavior of a program or a network protocol complies with its specification

Design new evasion or attack techniques

Examples:

1. Design a tool or mechanism that evades firewalls or IDSs.

2. Automate the process of executing a well-known attack, such as MiTM, based on a system settings
3. Design/implement a worm/virus that evades IDS/IPS/Antivirus
4. Automate scanning for IoT devices with default passwords and other vulnerability (you can use shodan.io)
5. Design a pen testing framework for IoT
6. Perform security assessment of a specific set of IoT devices

Perform a Security assessment [1]

This project requires you to:

1. **Understand** a specific networking or communication protocol, software or hardware device (running software).
    1. You should feel free to limit your research to specific aspects of the target if it is very complicated.
    2. If a project requires the purchase of software or hardware, do not spend too much money! Throwing money at a problem should be a last resort, and it can reduce the value of the project.
2. **Analyze** the target for security vulnerabilities. You might want to limit yourself to a particular implementation (say, in a particular operating system). If possible, suggest methods of improving the security. The less you can change (and improve security), the better.
3. **Present**
    1. *Your own* understanding of the target's operation.
    2. A security analysis of the protocol's vulnerabilities and suggested security improvements.
    3. A live exercise for the class demonstrating an interesting (but legal and ethical!) misuse of the target.

Suggested targets:

1. Protocols:
    - Network Time Protocol
    - HTML 5
    - Tor
    - Simple Message Transfer Protocol
    - HyperText Transfer Protocol/1.1
    - Internet Message Access Protocol
    - Bonjour
    - Real Time Streaming Protocol
    - Network File System Protocol
    - Session Initation Protocol
    - Bitcoin
2. Software
    - Android contacts app (or e-mail or calendar)

[1] Inspired by: https://algorithmics.bu.edu/fw/EC521

    - Google maps
    - apache httpd
3. Hardware
    - Point Of Sale device
    - Parrot AR.Drone 2.0 quadracopter
    - WiFi-Enabled Programmable Thermostat (e.g. Nest)
    - Wireless security camera
    - Universal Serial Bus
    - Trusted Execution Environments such as ARM Trustzone
    - Electronic Locking System (e.g. from Onity)
    - Flash memory
    - Raspberry Pi
    - Pineapple
    - RAM
    - VGA port
    - Universal Integrated Circuit Code, SIM

Analyze a network protocol for the presence of security flaws.

You may create a proof of concept of a new weakness or use a well-known attack to show a novel weakness of a protocol.

Examples of protocols:

- Secure voice-over-IP protocols (for example, Skype)
- 802.11 wireless security
- Authentication in Bluetooth
- Secure location verification for mobile devices
- Secure routing in ad-hoc networks
- Software defined networking

Do a theoretical study

Examples:

- Develop a cryptographic proof of security for a network protocol such as TLS or Kerberos.
- Apply algorithmic techniques for efficient analysis of large data streams to the detection of distributed botnet activity.