FYE – Cybersecurity
Project

Goals:
1. Students will apply the knowledge from the course, such as vulnerability analysis, security principles, hacking and society.
2. Students will:
   a. Perform research on a specific topic
   b. Prepare an activity or technical demonstration for the class
3. Students will write a 6-page workshop style publication and present their work in class during exam week (instead of a final exam)

Teams:
The project will be completed in teams of two to three students.

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. 16. 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. What you are proposing: Description of the topic and how it relates to the course. 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 an activity or game that proves the concept of the project, a qualitative or quantitative survey, or a technical artifact such as scripting or command line demonstration.

2. **Project progress report 1**: lighting talk on your progress on March 23. 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 13. 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 demo.

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: 15
2. The completeness and originality of your final products. If you have fulfilled at least one of the following: created a new security lab, or replicated a conference paper completely
with coding and testing, or performed security assessment thoroughly on a system or product you may receive full points on originality. The completeness of your deliverables, i.e., code, documentation of the hack and testing, as well as suggestions for resolution, will be evaluated. *Project points: 50*

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: 35*

**Project ideas**

You will perform research and security assessment on a suggested target. The phases of your research:

1. **Understand** a specific technology or hardware. Find sources such as blogs, white papers, academic publications from google scholar, and other articles.
2. **Analyze** the target for security vulnerabilities. Again research thoroughly and even try to think yourself something that could go wrong with the target from a technical perspective. Your analysis may also include:
   1. Historical view: older devices, how issues with this type of technology start
   2. Legal issues: are there regulations, laws, policies related to the technology that may make the technology vulnerable?
3. **Propose solutions** after research and thinking you may propose your own solutions to make the target more secure.
4. **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** *(you may choose the technology and not the exact product):*

- Bitcoin
- Android contacts app (or e-mail or calendar)
- Google maps
- Point Of Sale device – ex. Square card reader
- Parrot AR.Drone 2.0 quadacopter
- WiFi-Enabled Programmable Thermostat (e.g. Nest)
- Wireless security camera
- Amazon Echo
- Google Home
- Electronic Locking System (e.g. from Onity)
- Fitbit
- Vulnerable PC applications:
  1. Apple QuickTime
  2. Apple iTunes

---

1 Inspired by: https://algorithmics.bu.edu/fw/EC521
3. Adobe Reader
4. VLC Media Player
5. Adobe Shockwave Player
6. Mozilla Firefox
   - Ring video doorbell
   - Raspberry pi computer
   - Biometric scanner
   - Oculus rift
   - Google daydream
   - Talkies – internet connected toys
   - Wifi Baby monitor – iBaby monitor