Final Project

A list of project suggestions has been added to the end of the document.

Overview

This course culminates in a final project in which you work on a security-related project that you choose. You are encouraged to work in pairs, but you do have the option to work alone, if you prefer. The project should have the following properties:

- It must be in the area of computer security.
- Since projects are intended to be both instructive and fun, you should choose a topic that you are passionate about. You will be using your creativity, your knowledge, your intuition, and your energy to grapple with some aspect of computer security that interests you. You are encouraged to take chances: failure is OK as long as you fail well and deservedly.
- The project should involve more than just becoming familiar with the literature on a topic. It should have some sort of hands-on technical component in which you implement programs, write exploits, experiment with software, design a protocol, evaluate the security of a system, collect/analyze/visualize security-related data, etc.
- Ideally, you should choose a topic that has some sort of client or stakeholder that cares about the results.
- It would be nice to choose a topic that you could imagine continuing to work on in the Spring as an Independent Study project (if you are so inclined).

Calendar

The final project has several components, which are described in more detail below. Here are the due dates for the components:

1. **Mon. Nov. 1**: Submit a proposal explaining your choice of topic and what you plan to do in your project. You should meet with Tyler and/or me in person at least once before submitting your proposal to talk about ideas. We will get you feedback on your proposal by Mon. Nov 8.

2. **Fri. Nov. 19**: Submit a progress report on your project, summarizing the work you have done so far. We will give you feedback on your report by Tue. Nov 23. **Note**: you will have two more problem sets in November, so will have to balance work on your project with the final two problem sets.

3. **Last two classes meetings (Mon. Dec. 6 & Thu. Dec. 9)** Give a presentation on your project in class.

4. **Mon. Dec. 13**: Submit a draft of your final report. We will get you feedback by Thu. Dec. 16.

5. **Mon. Dec. 20**: Final reports due by 4:30pm.
Proposal

You should submit a project proposal both in email and in hardcopy on Mon. Nov. 1. It should be one to two pages long and include the following sections:

Introduction and Motivation: What you want to do and why it is worthwhile doing.

Deliverables: What will be the result(s) of your project (research paper, survey paper, computer program, proof-of-concept, data results, step-by-step guide, etc.)?

Methodology: How are you going to produce the deliverables (implement something, design the prototype, do a survey, test functionality, evaluate system security, collect/analyze/visualize security related data, etc.)?

Resources: Where you will find the resources that you need to complete your project?

Milestones List a sequence of milestones (including the final deliverables) in your project. This will allow you to track your progress, and serves an an insurance policy if your project fails (which can happen). That is, if you aim high and make significant progress toward your goal, you can still succeed on some milestones.

Progress Report

You should submit a project progress report both in email and in hardcopy on Fri. Nov. 19. It should be one to two pages long and include the following sections:

Summary: What have you done on the project so far?

Sources: By this point, you should have consulted all the resources you need for your project. List these and describe how you’re using them.

Outline: Give a (not-yet-fleshed out) skeleton of your final report.

Presentation

On Mon. Dec. 6 or Thu. Dec. 9 you will give a class presentation on your project. The length of the presentation will depend on how many projects we have (somewhere between 15 and 30 minutes).

You may not be done with your project on this point, but should describe the work you’ve done so far. You can incorporate feedback from your presentation into your final report.

Final Report

A draft of your project report is due on Mon. Dec. 13. We will get you feedback on this draft by Thu. Dec. 16. The final version of your report is due on Mon. Dec. 20 at 4:30pm. Both for the draft and the final version, you should submit a softcopy and a hardcopy.

Your report should have the following sections;

Introduction: Explain what your project is about.

Background: Summarize the state of the art of research in this area.

Statement of Work: Explain what you did and how you did it.

Results: What are the result of your work? If you have negative results, discuss them, too.
Conclusions: Summarize your work and explain how you would continue the work if you had more time. Based on what you’ve learned, what recommendations do you have for others working in this area?

How-to Guide: If others want to do what you did or wanted to reproduce your work, how would they go about it? Include tips/caveats.

Suggested Topics

The choice of project topic is completely up to you. Below are a few ideas, but don’t be limited by these. You are strongly encouraged to discuss project ideas in one or more meetings with Tyler and/or me.

- **Wall of Sheep (Lyn):** The Defcon security conference features a “Wall of Sheep” that sniffs unencrypted wireless network traffic and publicly displays information about it to make people aware of the dangers of unencrypted communication (http://www.wallosheep.com/). The goal of this project would be to develop something like the Wall of Sheep for public spaces at Wellesley, like the Sage lounge or the Pendleton Atrium. An alternative to a public display is a private tool that makes users aware which information they’re communicating is unencrypted.

- **Security visualization (Lyn):** Servers like the CS dept server puma log information that can be used to detect suspicious activities that could indicate attempted attacks. But logs typically contain so much information that it’s hard to determine what constitutes suspicious activity. How can information visualization tools be used to address this problem? An example is NetGrok, a tool developed in Ben Schneiderman’s Information Visualization course (http://www.cs.umd.edu/projects/netgrok/). This project would involve using using existing visualization tools or developing new ones to present information from puma logs.

- **Information privacy on the Wellesley Web (Lyn):** Personal information about students, faculty, and staff is stored in Wellesley College web pages, directories, Banner, FirstClass, etc. How private is this information? How easy is it for those inside and outside the college network to mine this information?

- **ballroom forensics (Lyn):** The security lab machine ballroom was recently found to be launching an attack on computers in Germany. How was ballroom compromised? What could have been done to prevent this attack?

- **OneCard study (Lyn):** What information does a OneCard magnetic strip contain, and how is that information used to control access to Wellesley College buildings?

- **Shoe knockoffs (Tyler):** A Google search for mbt kaya shoes returns top hits that include both legitimate resellers and sites for cheap knockoffs. Can you automatically distinguish between the two kinds of sites for products like these?

- **Herdict (Tyler):** Herdict (http://www.herdict.org/web/) crowd sources information about web site censorship. The current version is very simple. Can it be improved by (1) developing better assessments of blockage, (2) devising a “reputation” for for reporters and (3) comparing Herdict reports to news and twitter reports?

- **Privacy breach reports (Tyler):** The DataLossDB web site (http://datalossdb.org/) tracks privacy breaches. What can you determine about privacy breaches from analyzing this data?

- **High-yield investment programs (Tyler):** High-yield investment programs (e.g., http://www.hyip.com/) are post-modern Ponzi schemes in which investors are tempted to make high short-term profits before the bottom falls out. What can you determined about these programs from analyzing web data (e.g., examining meta-data, cross-correlating information from different sites). Can any of the information about these programs be trusted?