Name:

Computer Security I: Grad Project Topics

For people taking the course for 4 credits, you will need to complete an extra project that will contribute 20% to your grade. This can be a reading survey paper, a implementation project, or a mini-research project.

If you have a special passion in a particular area of security, feel free to suggest a topic or a project.

Project Expectations

For survey projects, I will expect that you have read a number of papers in the area. Your report should talk about the contents of these papers, but it should not merely be a regurgitation of the contents of the papers. Your report should reflect your understanding of how the papers relate to each other. Hopefully, you will have developed your own opinions about the topic area after surveying the field, and your report should reflect this. A survey report should be on the order of 20 pages.

For implementation and other hands-on projects, you will need to write a smaller report describing the project, issues you encountered performing the project, and the results of your implementation or study. Depending on the project, I'll want access to the code or a demo of the results.

If your project is pursuing original research in your area of interest, I will expect a report that looks like a conference proceedings submission.

Project areas

Below are some topics that might be interesting. Let me know of a project interest, and I can work with you to identify additional papers to read or an interesting project to perform.

Turn in a mini-project proposal to me by the first exam (October 7), so we both know what is expected of your project, and you will still have plenty of time to complete it. I will create a final project group for you in compass.

The final projects must be submitted by reading day, December 10.

1. Biometrics – Study the strengths and weaknesses of various biometric methods. Perhaps try to trick a biometric device, e.g. a fingerprint reader.
2. Malware – Work in analyzing worm characteristics using metasploit or other frameworks. Work in detecting or preventing malware.
3. Shared Authentication techniques – What are the security characteristics of the emerging OpenID standard? How does SAML allow for sharing of identity information securely?

Name:

4. Privacy – Techniques to avoid being traced. Examine the "Veiled" darknet web browser. Work with different anonymizers. Research implication of loss of privacy with respect to data mining methods.
5. Secure Hardware and hardware insecurities – Trusted Platform Module. RFIDs. CryptoCards. Try to reproduce recently reveal security flaws on Intel or AMD architectures, e.g. SMM attack identified by Invisible Things or Kris Kaspersky's remote code execution flaws.
6. OS security – New features in VISTA such as the mandatory integrity levels or the user account control. Security features in Linux (base or SE). Comparison of various "secure" *nixes.
7. Emanations Security – Try replicating some of the soft tempest results. What is the practical range of such data leakage?
8. Intrusion detection and prevention – Examine different IDS/IPS tools.
9. Quantum cryptography – This would have to be a paper study. Don't think we have the lab space for this.
10. Random number generators – Explore how physical sources of randomness can be harnessed and how true randomness can be approximated. How is the quality of randomness evaluated?
11. Wireless security – Latest developments in WPA security. Enterprise mode 802.1X security. Research work in ad hoc or sensor networks.
12. Security of electronic money systems – PayPal, Credit card networks, electronic funds transfers.
13. DB security – Reflective database access control is a new access control model in which the access control policies, rather than being ACLs, are Datalog statements that may refer back to other parts of the database, or even modify the database. These policies must not leak information, or be vulnerable to other policies that may leak information. How can you analyze access policies to make statements about flow and safety? How can you add atomicity into the policy model?
14. Firewalls – Examine performance issues. What is a good workflow model that reflects a realistic exercising of Firewall functionality? What is used in the industry? What are strategies for filtering in a tunneled environment?
15. IPv6 – What are the security concerns as IPv6 is being rolled out? What happens in a dual IPv4 and IPv6 environment?