

CSE 227
Computer Security

Winter 2008

Stefan Savage

Projects

- Some kind of research project in security
- Best in a group of two
 - ◆ If you can't find a partner I'll be willing to consider single person projects; but I want this to be the exception
- Form groups in the next week
 - ◆ Send me mail by next Thurs identifying who is in your group
- Project proposals due Jan 24th
 - ◆ One page
 - ◆ What you plan to do, Why is it interesting, How you'll do it, What you're not sure about (or what resources you need)
- Ultimately 6 pages and short talk (10-15mins)
- Hope: some sufficiently interesting to be real paper

Generally speaking

- Most projects will fall into the category of:
 - ◆ Analysis: evaluate the security of a system of interest
 - ◆ Attack: identify some new attack/vulnerability, develop/test it and discuss the possible ramifications, mitigations, etc
 - ◆ Measurement/analysis: measure some aspect of adversarial behavior (real or potential), characterize it, explore its limits, etc
 - ◆ Design: design and/or build a new system that addresses a problem in a new way

Random ideas

- Visual data projects
 - ◆ Remote extraction of screen data (i.e. over a distance using telescope)
 - ◆ Keyboard shoulder surfing via camera
 - ◆ Study of privacy exposure on flickr, myspace, etc (e.g. credit cards, check routing numbers, SSNs, name/address, etc)
 - ◆ Privacy issues related to GoogleEarth or StreetView
 - ◆ Automated extraction of fingerprints from currency (UV photography)

More random ideas

- Examination of security issues in Second Life
- Vulnerability of widespread “updaters” for popular software packages and computers
- Automation for “attack surface” estimation
- User authentication via singing/karaoke/pitch matching
- Analysis of Taser authentication
- Location verification via “audio-print”
- Analysis of on-line poker (fair deal or not?)

More random ideas

- Fuzz testing against popular embedded devices (e.g. cameras)
- Spam generation fingerprinting (what program?)
- Analysis of spam campaigns (size/kind)
- Something with social networking
- Security examination of iTouch/iPhone
- How to measure “relative anonymity” of different systems (e.g. ToR, etc)

Yet more random ideas

- Repeat Ozment/Schechter's Milk/Wine study on vulnerability generation w/another system
- Unique attacks on AJAX systems (e.g. GoogleMaps)
- Run-time integer-overflow protection
- Automated analysis of chat room (IRC) conversations focused on illegal transactions
- Code similarity measures to determine malware phylogeny
- Difficulty in spoofing consumer GPS

Resources

- Servers
- Lots of SPAM (we have a 200k/day Spam feed), lots of malware
- Lots of 802.11 gear (192 radios throughout the building), directional antennas, scope
- Big chunks of Internet address space
- Good DSLR and pro-am HDTV camera
- Lots of low-level stuff in the embedded lab
- Ask if you're serious and you need something