CS 4440/7440 Malware Analysis & Defense

Bill Harrison

Class Information

- Prerequisite:
  - CS3280 or the ECE equivalent
  - knowledge of C/C++ are essential
- Two Midterms (20% + 20%)
  - Dates TBA
- Final exam (35%)
- Programming & Homework Assignments (15%)
- Class participation, pop quizzes (10%)
- Graduate Students: 25 minute presentation on malware related publication at end of class. More information later.

Class Information

- Textbooks:
  - The Art of Computer Virus Research and Defense, Peter Szor.
  - (Recommended) Gray Hack Python, Justin Seitz
- Resources listed in the syllabus could prove useful
  - http://www.immunityinc.com/products-immdbg.shtml
  - http://www.exploit-db.com/
    - See the author `corelanc0d3r`
- Office Hours (318 EBN) – **by appointment only**.
  - the "drop in" visit should be avoided at all costs.

Malicious Software (Malware)

- Economic Cost: $15B-$150B yearly
- 5-6 Million Varieties "in the wild" [Szor]
- "Black Hat" Malware Education is too good
  - Many resources for aspiring hacker on the web
  - Incl. Foreign Governments [Paller09]

- "White Hat" Education should be high priority
  - …but it is **not** in US Academia
- ACM Computing Curricula pay lip service to security
  - But not to "next generation" critical to malware defense
    - Vulnerability Analysis
    - Computer Forensics
    - Reverse Engineering
    - …

Who are the Black Hats?

Three types of highly-motivated and well organized groups are behind the current proliferation of malware:

1. nation states looking for strategic information and advantage,
2. organized crime groups looking for profits, and
3. terrorist groups looking for political and economic gain.

One Country's Example

***China**, as just one example, runs a **national competition** for college and grad school students who may currently be hacking illegally, but who could be effectively employed in creating and using new attack techniques. In 2005, for example, Tan Dailin, a*

Estimated number "Patriotic Hackers" working for the PRC: **50K ~ 100K**

Source: ***A Giant, Armed for Cyber War***, Josh Rogin, CQ Weekly in Focus, May 2, 2009

DoD. tens of thousands of documents. The PLA's competition continues to recruit and develop ever improving talent.

Alan Paller, Director of Research, SANS Institute

2009 Testimony, US Senate Committee on Homeland Security and Government Affairs

Misinformation

It's impossible for our students to hack Google and US companies, they are just high school graduates and not at an advanced level.

Dean Shao (Lanxiang University)
NY Times, 5/19/10

Costs of Computer Viruses

- 2000 FBI survey: Large corporations placed annual losses from attacks above $1 million per company
- Thousands of large corporations nationwide in the U.S.A.
- Companies often cover up the worst cases
- Does not include cost of security measures

Virus Costs: Example 1

- 26-April-1999 time bomb: “Chernobyl”
- Wrote random garbage all over the hard disk until the PC crashed
- $250 million lost in one day in Korea alone; widespread across Asia
- Hard to quantify cost of lost files, time spent reinstalling OS and applications, etc.

Virus Costs: Example 2

- 4-May-2000 mass mailer: “LoveLetter”
- Visual Basic script attached to email
- Re-mailed itself to first 500 addresses in Outlook address book
- Also spread itself through chat software
- Also installed password-stealing software
- Finally, copied itself over numerous existing files, destroying them
- Ford Motor Company, among others, shut down all email for three days

Virus Costs: Conclusion

- Computer viruses and other security attacks are very costly
- Computer security is a hot field today; many career and research opportunities
- Knowledge of security issues is sensitive and carries an ethical responsibility with it

Computer Ethics

- We must teach attacks upon computer systems in order to teach defenses against attacks
- Information about attacks must NEVER be used to attack any computer system in any way

Ethics Pledge

- Read and sign ethics pledge (available at the course website)
- Should not be difficult to follow
- Ethics will be covered in more detail later
- You cannot continue in the course without signing the ethics pledge!

Ethics Pledge Points

- Unauthorized use of computer resources is forbidden
- Even a virus or worm that does nothing but copy itself uses resources
- Don't ever rationalize that a system owner won't object to your actions; ask permission
  - If you are afraid to ask permission, it must be forbidden!

Example: 1988 Morris Worm

- Creator rationalized that the worm did no damage; it only copied itself from system to system over the internet
- BUT: Copying monopolized system resources until they had to be shut down
- Worm reached 10% of entire internet
- Creator did not realize it would be that resource-intensive
- Creator was convicted of felonies!

Morris Worm Lessons

- Consequences of a virus or worm cannot always be foreseen
- Severe damage can be done without destroying data
- Excessive resource usage is destructive enough to be criminal

Criminal Prosecution

- Attackers have been prosecuted for:
  - Stealing passwords, even if never used
  - Copying copyrighted materials
  - Accessing confidential data, even if it was never used for harmful purposes
  - Entering a system without permission, causing sys admins to spend time tracking them and securing the system, even without otherwise causing harm
- Moral: Don't assume it is legally safe to do any of the above

Ethics Violations

- Violations by students endanger our ability to offer this course
- As a result, they will be treated severely
  - Reported to Provost's office
    - Dr. Michael Prewitt, Associate Vice Provost and Director of the Office of Student Rights & Responsibilities
  - Course grades
  - Criminal prosecution

ACM Code of Ethics

- ACM is the primary professional organization for computer scientists
- The entire code is available online
- Portions most applicable to students are excerpted in the course website

Ethics Questions

- Scenario: John Doe attempts to guess the password of a user of a system on which John Doe has no account. After a few guesses, he succeeds, but finds nothing of interest on the system and logs off.
- Q1: Has he committed a crime?
- Q2: Are his actions analogous to any common crime not involving computers?

My Expectations

- You are able to accomplish such tasks as installing software completely on your own.
- If I make a reading assignment, you will read it carefully.
- If I make a programming assignment, that you will complete it.

My Expectations

- There will be neither trails of bread crumbs nor spoon feeding of material
- Some of the material we read will not be in text books
  - research papers, websites,…
- If you are not willing and able to meet these expectations, then you should find another class

Reading Assignment*

- Szor, pp. 23-38 (terminology)

* In about a week.