CS4630/CS6501 Defense Against the Dark Arts

Wei Wang
Defense Against the Dark Arts
Cost of Computer Crime

- 2014 CSIS survey: Computer crime cost businesses $445B/year worldwide
- Companies often cover up the worst cases
- Does not include cost of security measures
Virus Costs: Example 1

- 26-April-1999 time bomb: “Chernobyl” or “CIH”
- 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

- Large companies, CIA, The Pentagon and British Parliament, among others, shut down their mail servers
  - Ford Motor shut down their mail system for 3 days
I Love You Timeline

- 05/03/2000: Virus appears in Europe and Asia
- 05/04/2000 (0412): Anti-virus companies analyze
- 05/04/2000 (0700): Distribution of signature. Too late in U.S.
- 05/04/2000 (1300): Infection continues including Pentagon and CIA
- 05/04/2000 (1600): First variant appears (“Very funny joke”)
- 05/05/2000: Nine more variants appear
Target Data Breach

• Credit card information for 40 million customers stolen
  – Card information sales for $20 to $100 per card on the black market

• Target recently revealed that personal information for 70 million customers was stolen

• Used malware called RAM scrapers
Malware Costs: Conclusion

- Malware and other security attacks are very costly
- Computer security is a hot field today; many career and research opportunities for graduates from this course
- Knowledge of security issues is sensitive and carries an ethical responsibility with it
Computer Security is BROAD

- Computer Security
  - Viruses
  - Data storage security
  - System (OS) security

- Network Security
  - Authentication protocols
  - Encryption
  - Firewalls

- Not a complete list
What We Will Not Cover

- Access Control
- Web security model
- Authentication
- Web Content Security Policy
- Firewalls
This Course is about Real Black Magic

- System Security (viruses etc.)
  - Mechanisms (with x86 assembly basics)
  - Vulnerabilities and exploits (buffer overflow etc.)
  - Defense

- Malware (viruses etc.)
  - Infection
  - Disguise
  - Defense: prevent, detect and repair

- Network Security
  - Cryptography basics
  - Web Security
  - Web Attacks (SQL injection etc.)

- Ethic issues
What I hope You Will Know in the End

- Understand the nature and types of malware
  - You will be able to write malware, but DO NOT DO IT
- Understand system vulnerabilities and exploits
  - You will be able to hack, but DO NOT DO IT
- Be able to prevent, detect, repair and defend malware
- Understand computer security ethic issues
- Get a Wizard title
Extra Benefits for Graduate Students

- Two goals for a graduate course
  - Study the latest works in a field—computer security
  - Learn how to do research or scientific methods
- Hopefully after this course, you will know:
  - How to properly define a research problem
  - How to do a solid background survey
  - How to conduct a project with feasible but sound methodology, and rigorous evaluation
  - How to present your work and convince others
Class Information – CS4630

- Prerequisites: CS 2150 and CS 3330 or equivalent
- Three exams (15% each, low score dropped)
- Final exam (25%)
- Assignments, including programming assignments (40%)
- Class participation, in class quizzes, special and extra credit events (5%)
- The percentages may be adjusted depending on the number of assignments and quizzes
Class Information – CS6501

- Prerequisites: CS 2150 and CS 3330 or equivalent
- Research Proposal (30%)
- Final exam (25%)
- Normal assignments, including programming assignments (30%)
- Paper reading assignments (10%)
- Class participation, in class quizzes, special and extra credit events (5%)
- The percentages may be adjusted depending on the number of assignments and quizzes
Class Information cont'd

- No textbook required. The Art of Computer Virus Research and Defense — Peter Szor is useful

- Late homework is docked 10%
  - If it is more than one week late, the assignment will not be accepted

- Office Hours – Rice Hall 409 TuWe 3:00 p.m. – 4:30 p.m. and by appointment
Class Information cont'd

• Class site:
  - I post my slides, supplement materials, class schedules and syllabus on the class site
  - Collab for assignments and extra materials
  - Piazza for questions

• Graduate TA: None

• Undergrad TA: many~
Syllabus — It is your friend

"What did we cover in class last week?"
"It's in the syllabus."

"What's your late homework policy?"
"It's in the syllabus."

"When are your office hours?"
"It's in the syllabus."

"How will my grade be computed?"
"It's in the syllabus."

"It's in the syllabus."
This message brought to you by every instructor that ever lived.
About Me

- Just got my Arch Mage (PhD) title 5 mouths ago
- Dr. Davidson is my advisor
- Research area: system software (OS, compiler, run-time etc.), cloud computing, computer architecture, software engineering
- Research interest: large-scale system design and optimization
With Great Power Comes Great Responsibility

- Knowledge of security issues is sensitive and carries an ethical responsibility with it.
- 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
• Scan the signed pledge and submit through collab
• 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
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?
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
• Aaron Schwartz (see web story).
Ethics Violations

- Violations by students endanger our ability to offer this course
- As a result, they will be treated severely
  - UJC (University Judiciary Committee)
  - Course grades
  - Criminal prosecution
ACM Code of Ethics

- ACM is the primary professional organization for computer scientists
- The entire code is available online
  - https://www.acm.org/about/code-of-ethics
Student Participation

• Attendance (I know it is hard)
• In-class discussion
• Ask questions
• Let me know what do you think about this course
• Any feedback is welcome