294-24 Privacy and Security Enhancing Technologies

Dawn Song
dawnsong@cs.berkeley.edu

Introduction

• MW 1-2:30pm (starts at 1:10pm)
• Website: http://www.cs.berkeley.edu/~dawnsong/teaching/f07
• Prerequisite:
  – Grad students: none
  – Undergrad: check with instructor
  – Useful background knowledge: OS, PL, etc.
• Class style:
  – Lectures & in-class discussions
  – Paper reading
  – Project
• Relationship with CS261

Class Requirements & Grading

• No Midterm & Final
• 20% in-class participation
• 20% summaries
• 60% project
• Grading is not curved
Paper Reading & Summaries (I)

• Paper reading:
  – 1-3 research papers per class
• Regular paper summary (5%):
  – Contents:
    » Summarize main results of the paper
    » 3 most important technical points you learned from or liked
    » 3 most important technical points you didn’t like about the paper
      or you wished the paper had done
  – Submit in plaintext email to
    294.24.07@gmail.com midnight before class
    with subject summary-mm-dd for lecture on mm/dd
  – Optional readings no summaries required
  – Will be counted, and randomly selected for grading

Paper Reading & Summaries (II)

• Star paper summary (15%)
  – Given questions (usually open-ended)
  – Conduct thought exercise
  – Write down your thoughts/answers (usually one page)
    » Not graded on right/wrong
    » You’ll get full score as long as you’ve demonstrated you’ve
      thought carefully about the question
  – Due time specially noted

Class Project

• 1 2-person semester-long project
  – Ideally research quality
  – Will provide a candidate list
• Group sign-up: Sep 12
  – Sign-up sheet in class
• Project proposal: Oct 1
  – Two page max
  – Content
    » Problem to be addressed
    » Motivation: Why important & Why previous approaches insufficient
    » Proposed approach
    » Evaluation for success
• Project milestone report: Nov 7
  – Current status and plan for action for the remaining time
• Final project presentation & report due: Dec 10
Topics Covered in Class

• Pressing issues & state-of-the-art technologies in selected areas
• Part I: Malicious Code Defense
• Part II: OS & Web Security
• Part III: Privacy-enhancing Technologies
• Your favorites not on the list?
  – Let me know

Malicious Code---Critical Threat on the Internet

• Worms, botnets, spyware, viruses, trojan horses, etc.
  – Infiltrate/damage computer system without owner's consent

• Unpatched PC survives less than 16 min [SANS04]

• $10billion annual financial loss [ComputerEconomics05]
  – Worms
    » CodeRed: Infected 500,000 servers, $2.6billion in damage [CNET03]
    » SQL Slammer: Internet lost connectivity, affected 911, ATM, etc.
  – Botnets
    » Over 6 million bot-infected computers in 3 months [Symantec06]
    – 61% U.S. computers infected with spyware [National Cyber Security Alliance06]

A Thriving Underground Economy

• Average bot costs
  – $0.04

• Zero-day vulnerability for
  – $75K [SecurityFocus07]

• Excerpt from Underground Economy IRC Network
  – “Sell US$1$I each&UkI2$ each$ with SSN & DL105 each&land ePasspate Account with 5003 in acc05085 Hacked Host795 T7 Scam C.C
  Full in VIP-ASP $ope$195; shopadmin with 4100 order2008; Tool Calculate Drive Licence Number1055 41... I'm sleeping, MSG me and I will reply u as soon as I can !

• With one IRC channel, 24-hr period, just a few samples
  – Accounts worth $1,999.358.80 have been stolen
  – “The Underground Economy: Priceless” [login Dec06]
It's getting real---Storm Email Worm Case Study

• Clicking on email attachment/links causes malicious code installed
  – Fake news story on deadly storm
  – E-cards from family & friends
  – Links to malicious website for drive-by downloads
  – Quick change to stay ahead of AV blocking
  – Malicious code is modified every 30 minutes, undermining standard signature based AV’s ability to block this threat
• Infected machines form botnet
  – Largest botnet: 1.7 million bots by end of July
  – P2P architecture instead of centralized
• Stealth: install rootkits, etc.
• Anti-VM: detects VM and won’t infect them
• For profit:
  – Botnet sent stock-picking spam, ripping profits for risen stock price

Defense is Challenging

• Software inevitably has bugs/security vulnerabilities
  – Intrinsic complexity
  – Time-to-market pressure
  – Huge overhang of legacy code
  – Long time to produce/deploy patches
• Attackers have real incentives to exploit them
• Large scale of compromised machines being organized for malicious activities
• What can we do?

Malicious Code Defense

• Exploit & worm defense
  – How to automatically generate anti-bodies?
• Botnet analysis & defense
  – Is it hopeless? Who wins the game?
• Malware analysis & defense
  – Privacy-breaching malware (Spyware, etc.)
    ▷ How to discover GoogleDesktop sends your info home?
    ▷ Did you know that skype reads your /etc/password?
  – Stealth malware (rootkits, etc.)
    ▷ Can you design a rootkit which simply can’t be detected?
  – In-depth analysis
    ▷ How to detect hidden-behaviors in malware?
OS Security

- **Isolation**
  - New methods to achieve this classic property
- **Virtualization**
  - Myth & demythify:
    - Is virtualization the panacea?
    - What can virtualization do and not do?
- **Forensics**
  - What practical capabilities can we add to OS to support forensics?
- **Instrumentation**
  - Giving you a tool to pry inside OS, what can you do?

Web Security

- **Web is users’ window to internet**
  - On-line banking, mashup apps, etc.
- **Browser is the OS for web apps**
- **What properties should browser enforce?**
- **Web-based attacks & defenses**
  - Command injection, cross-site scripting, etc.
- **Click fraud, forum spams, etc.**
- **Trust metrics & sybil attack in social networks**

Privacy-enhancing Technologies (I)

- **How to enable rich functionalities while preserving users’ privacy?**
- **Practical cryptographic techniques for**
  - Privacy-preserving data mining & information sharing
  - Private operations on untrusted server/storage
    - Searching on encrypted data, etc.
  - Anonymous credentials
- **Note: no crypto prior knowledge required**
Privacy-enhancing Technologies (II)

- Privacy issues in practice
  - Data anonymization
    » Very much needed. What can be done? What guarantees can we offer?
  - Ubiquitous computing
    » Privacy scene looks grim. Anything can be done?
  - Web
    » Googling & web inference, etc.

Summary

- Fun class on most recent topics in security & privacy
  - Current threats & state-of-the-art technologies
    » Malicious code defense
    » OS & Web security
    » Privacy enhancing technologies
  - A nice blend of theory & systems
    » Systems + PL + crypto
    » How things should be done anyway! :-)
- Interested? Then join us!
  - May only be offered this semester
- What to do to get an A?
  - Curious about the material & do a fun project
  - Have a good time!

Questions?

- I have questions for you too :-)