CSE 543 - Computer Security

Lecture 27 - Wrapup
December 13, 2007
URL: http://www.cse.psu.edu/~tjaeger/cse543-f07/
Final

• Tuesday, December 18, 8:00am-9:50am in 102 Chemistry Building.
  – Be late at your own peril (I may lock the door at 8:00am)
  – You will have the full time to take the test, but no more
  – Closed book, closed notes

• Coverage:
  – Anything we talked about in class …
  – Or appeared in the readings
  – Focus on topics since mid-term

• Types of questions
  – Constructive (here is scenario, design X and explain it)
  – Philosophical (why does Z argue that …)
  – Explanatory (what is the key tradeoff between A and B …)
Final Project -- Due 12/20 5pm

• Should be a normal conference-style paper (limit 10 pages)-- should be written as such. (*Presentation Matters*)
  – 5 page, double spacing, etc. are signs that it is not a serious submission, and will be *seriously* penalized.
  – Citations, etc. should be made as necessary throughout the paper -- not just in related work. (must make sense)
  – Bad, unreadable or ugly presentation (e.g., Excel graphs) will not help you (hint: use gnuplot).

• The structure should be appropriate for the topic, and cover all the areas we have discussed all semester.
  – If you are not already 50-75% done with the paper, you are in real peril.

• Please submit the code that you wrote as well
  – I want to know what is necessary
More About the Final

• Short questions (12 of 14)
  – Basic items -- fundamental plus some non-trivial
  – Span the entire course
  – About half since midterm
  – Don’t spend too long on these

• Long Answer
  – 2 from second half of class
  – 2 from pre-midterm

• Constructions
  – 4 of these (2+ from second half of class)
Contents

• Basics
  – Terms
  – Cryptographic Concepts
  – Access Control Concepts
  – Network Security Concepts

• Crypto
  – Symmetric key
  – Public key
  – Hash functions

• Crypto Systems
  – Combo of above
  – PKI
  – Kerberos
Contents

• Systems Security
  – In context of SELinux/LSM
  – MLS
  – Integrity Models
  – Virtual Machine systems (that we discussed)
  – Decentralized Label Model

• Network Security
  – Homework
  – Protocols and issues
  – Firewalls -- Wool’s Configuration Errors
  – IPsec -- slides and homework (book supports)
  – DDoS -- concepts, problems, and countermeasures
  – Web Security -- Cookies, SSL, Passport
  – IDS -- Forrest and Bayes Rule
The state of security …

• … issues are in public consciousness
  – Press coverage is increasing …
  – Losses mounting … (billions and billions)
  – Affect increasing …… (ATMs, commerce)

• What are we doing?

“… sound and fury signifying nothing …”
- W. Shakespeare

(well, its not quite that bad)
The problems ...

• What is the root cause?
  – Security is not a key goal …
  – … and it never has been …

… so, we need to figure out how to change the way we do engineering (and science) …
… to make computers secure.

• Far too much misunderstanding about basic security and the use of technology
• This is also true of physical security
The current solutions ...

- Make better software
  - “we mean it” - B. Gates (2002)
  - “Linux is bad too …” - B. Gates (2005)
- CERT/SANS-based problem/event tracking
  - Experts tracking vulnerabilities
  - Patch system completely broken
- Destructive research
  - Back-pressure on product developers
  - Arms-race with bad guys
- Problem: reactive, rather than proactive
The real solutions …

• Fix the economic incentive equation …
  – Eventually, MS/Sun/Apple/*** will be in enough pain that they change the way they make software

• Education
  – Things will get better when people understand when how to use technology

• Fix engineering practices
  – Design for security

• Apply technology
  – What we have been talking about
The bottom line

• The Web/Internet and new technologies are being limited by their ability to address security and privacy concerns …

• … it is incumbent in us as scientists to meet these challenges.
  – Evangelize importance of security …
  – Provide sound technologies …
  – Define better practices …
Thank You!!!

tjaeger@cse.psu.edu