Final Review

Dawn Song
dawnsong@cs.berkeley.edu

Outline

- **Summary of semester**
- **Course evaluation**
- **Final review**

What we have covered so far

- **Introduction to cryptography**
- **Software security**
- **OS security**
- **Web security**
- **Networking security**

Three Things to Remeber

- **Attacker's mindset**
- **Security is tricky**
- **How to do security evaluation?**
  - **Security goal**
  - **Threat model**
  - **Analysis**

Field of Security Is Unique

- **The security field is unlike any others**
  - **Extremely broad**
  - **Extremely creative**
    - » **Think out-of-the box**
  - **Game with intelligent attackers**
- **If you want to be celeb over-night ☺**

If You'd Like to Learn More

- **Classes**
  - **CS294: Networking Security**
  - **CS276: Foundations of Cryptography**
- **Seminar**
  - **TRUST security seminar**
- **Security research project**

Hope You've Enjoyed the Class ☺

- Diverse background for students
  - Students have different backgrounds in math/programming
  - Students have different interests
- Broad field, a lot of material to cover

Thank You for Your Support!

- I really enjoyed having you in the class ☺
- You all did a great job!
- Write down your comments
  - Particularly if you like the class ☺

Final Review

- OS Security
- Web Security
- Networking Security

OS Security (I)

- Principle of least privilege
- How to ensure principle of least privilege?
  - Should only grant privilege necessary
  - Privilege separation
  - Drop privilege when possible
    - Least privilege with Setuid

OS Security (II)

- Reference monitor
  - Properties of reference monitor
    - Complete mediation
    - Tamperproof
    - Small
  - Properties it enforces:
    - safety properties
    - E.g., cannot prevent covert channels
  - Examples
    - System call interposition
    - JVM
    - SFI
    - VM

OS Security (III)

- SFI
  - Insert checks to ensure certain properties
  - Make sure that checks are not by-passed or certain invariants should still hold even when checks are by-passed
  - Verification
- Trusted computing
  - TCB
    - Security design principle: minimize TCB
  - Trusted path
  - Trusted/authenticated boot
    - Remote attestation
  - Secure boot

Web Security

- Common vulnerabilities
  - Input validation vulnerabilities
    - » SQL injection
    - » XSS
    - » HTTP response splitting
  - CSRF
- Same origin policy

Networking Security (I)

- Design has wrong trust model
- TCP session hijacking
- Distributed denial-of-service attacks
  - SYN flooding
  - IP spoofing
  - Reflector attacks
- Worms & botnets
  - How worms propagate
  - C&C botnets
- Measurements: Internet telescope, backscatter

Networking Security (II)

- DNS security issues
- Firewalls
  - Stateless firewalls
  - Stateful firewalls
- Attacks & defenses on NIDS

- Guest lecture Mon