Final Exam Review

Leslie Hwang
University of Illinois
CS461 / ECE422 Spring 2016

Date, Time and Format

- May 9 (Monday) 7-10PM @ Tentative location
- Exam Format
  - True/False questions
  - Multiple choice questions
  - Short answer questions
  - Long questions

Materials Covered

- ~ Midterm (~10%)
  - Lecture: Operating System Security ~ Cryptography
  - MP: MP1. Application Security, MP2. Web Security
- Midterm ~ (~90%)
  - Lecture: Networking and Distributed System Security ~ Forensics Study
  - MP: MP3. Cryptography, MP4. Networking Security, MP5. Forensics
- No U-Pick-ems lectures are covered on exam

Outline

- MP5 Forensics
- Distribution system security
- MP4 Network security
- Network security
- MP3 Cryptography
- Cryptography
- Web security, OS security and Security Basics
- Note: These slides are not a complete set of all the materials, but general guide for key concepts and where you can start.

MP5. Forensics

- Live vs. Dead Analysis: what are the consequences? what is the benefit of drawback?
- Verify checksum: ensures that the downloaded file hasn't been altered
- Investigator mode: which files to look for? where would files be located? What time did this action happen?
- Understand what kind of information can be found on Unix system files
  - E.g. */var/log/auth.log* contains the log of all authentication attempts.
- Username vs. Display name
- OS distribution number vs. kernel version number
- Password cracking: search space (number of combinations), runtime
- File metadata: what kind of information can be found?

Distribution System and Other Security

- Worm vs. Virus vs. Trojan horse…
  - How to differentiate from one another?
  - How does the machine get infected?
  - How does it propagate? Does it require human intervention?
- DDoS attack: how the attack get executed? what does it affect, confidentiality, integrity or availability?
- Botnets: techniques and measurements
- Privacy
- Anonymity
- Off-the-Record: Tor (The onion routing)

MP4. Network Security

- PCAP analysis
  - Identify types of network attack
  - TCP, SYN, ACK packets, etc.
  - FTP, HTTP traffics, etc.
- IP address/MAC address, gateway
- Port scan
- WEP key cracking: how does it work? what information does it need?
- Network eavesdrop
- Decrypt SSL communication w/ server’s private key

Network Security Terminologies

- Authentication
- Digital signature
- Certificate (authority)
- SMTP server
- Spoofing
- Man-in-the-Middle
- Replay attack
- HUB, switch
- Heartbeat protocol
- ...

Network Security Basics

- Network/Internet layer
  - Application
  - Transport
  - Network
  - Data Link
  - Physical
- For any network security protocol and attack, identify which layer it targets
  - SSL/TLS
  - TCP
  - IP
  - ...
- DNS spoofing, IP spoofing, ARP spoofing, TCP/SYN flood, TCP/IP hijacking
- OpenSSL, hostname
- HTTPS protocol, Firewall

MP3. Cryptography

- AES, RSA encryption: no need to memorize the math, but understand the benefit/drawback and the application
- Hash function
  - Avalanche effect
  - Weak hash
- Length extension attack: how does it work?
  - m + padding(len(m)*8) + suffix: understand the big picture of where padding gets appended and how does this work to make into an attack
  - padding bits = (len(m) + len(padding(len(m)*8)))*8
- Collision attack: how does it work? when to use this attack?

Cryptography

- Categories each cryptographic algorithm and understand the similarities/differences between each other
- Symmetric/Asymmetric encryption
- Block cipher: what kind of attack can use the block cipher structure?
- One-time pad
- Cryptographic hash function
- RSA (Wiener’s attack)
- Public key crypto: public/private key pair

Security Basic and OS, Web Security

- Web security
  - SQL injection
  - XSS, CSRF, Cookies
- OS security
  - Buffer overflow
  - Authentication and password cracking
- Confidentiality, Integrity, Availability (CIA)
  - In any security context, identify why security aspect is being addressed