Final Review

ENGG5105/CSCI5470 Computer and Network Security

Spring 2014

Patrick P. C. Lee

Threat Model

- A threat model defines the scope of security that we consider
- Understand:
  - the threat model of each proposed attack
  - the corresponding defense solutions

Applied Cryptography

- Security properties:
  - Confidentiality
    - via encryption/decryption
  - Integrity
    - via message authentication (or hashing)
  - Authentication and non-repudiation
    - via digital signatures and certificates

Applied Cryptography

- Cryptographic primitives: building blocks of cryptosystems
  - Symmetric key cryptography (e.g., AES)
  - Public key cryptography (e.g., RSA, Diffie-Hellman)
  - Digital signatures (e.g., DSA)
  - Hashing (e.g., MD5, SHA-1)
  - Certificates (e.g., X.509)

Applied Cryptography

- How AES works?
  - Symmetric-key crypto algorithm, assuming a secret key has been agreed by two parties
  - AES is a 128-bit block cipher scheme
  - Key size is 128, 192, or 256 bits
  - Compatible with cipher block chaining (CBC) mode to add dependency to ciphertext block
    - i.e., c(i+1) = Enc(c(i) + m(i))

Applied Cryptography

- How RSA works?
  - n = pq, for two secret prime numbers p, q
  - public key: e, private key: d
    - How to form e and d?
  - Encryption: $c = m^e \bmod n$
  - Decryption: $m' = c^d = m \bmod n$
- How Diffie-Hellman works?
  - For key agreement between two parties
  - A → B: $g^x \bmod p$, B → A: $g^y \bmod p$,
  - Secret key = $g^{xy} \bmod p$

Applied Cryptography

- How a public-key certificate works?
  - The certificate is authenticated by a Certificate Authority (CA)
  - The certificate is used to authenticate a user
  - Use the public key inside the certificate to verify the signature of the certificate owner
  - How to form a CA hierarchy?

Applied Cryptography

- How A and B communicate securely?
  - A and B set up a communication channel (e.g., via socket programming)
  - A and B exchange their certificates
    - They will sign the digests of all messages that they exchange later
  - A and B carry out the key agreement procedure (e.g., via public key crypto) to agree on a comment secret key
  - A and B communicate through symmetric key crypto

Applied Cryptography

- OpenSSL:
  - How to call different cryptographic primitives?
  - How to integrate these primitives into a cryptosystem?
  - How to use OpenSSL to do SSL programming?
- Assuming you are familiar with Assignment 1

Network Security

- Network attacks exploit the fundamental weaknesses of network protocols
- Sniffing:
  - exploits the fact that message payload (in application layer) is not protected
  - Use Wireshark or your own libpcap-based sniffer tool

Network Security

- ARP Spoofing:
  - Exploits the weakness of ARP (in link layer) that ARP requests/responses are spoofable
- TCP Exploits:
  - Exploits the weakness of TCP (in transport layer) that sequence numbers are spoofable
- Attack tools:
  - Hunt, Netcat

Network Security

- Port scanning:
  - identifies any active network processes, and tries to exploit weaknesses in those active processes
- Denial-of-service (DoS) attacks
  - One attack point, overwhelm resources of a victim (e.g., via flooding of traffic)
- Distributed DoS attacks
  - Launch DoS attacks from multiple attack points

Network Security

- Worms:
  - How worms propagate?
- Botnets:
  - How botnets launch attacks?

Network Security

- Defenses: firewall or intrusion detection sytems
- Firewall
  - To block attacks
  - How to configure iptables?
- Intrusion detection systems
  - To detect attacks
  - How to configure Snort?
  - How to add user-defined modules to Snort?

Web Security

- Exploits the weaknesses in HTTP
- How HTTP works?
  - By default, no encryption
- Cookies
  - maintain state of users
  - can be easily read/modified by attackers
- Same origin policy (SOP)
  - Security measure enforced by browsers
  - Attackers can find ways to bypass SOP

Web Security

- HTTPS encrypts every HTTP request/response messages
  - including cookies, HTTP header, HTTP message content
- Is HTTPS perfectly secure?

Web Security

- Cross-site attacks
  - XSS: leaks state to attacker websites via client-side scripting
  - CSRF: triggers HTTP requests to vulnerable website by attacker websites
  - Clickjacking: special case of CSRF
- SQL injection
  - Inject malicious SQL commands

System Security

- Buffer overflow
  - How buffer overflow is feasible?
  - Examples of exploit programs:
    - how do they attack a vulnerable program and gain root accesses?
  - Countermeasures
    - Use C libraries with bound checking
    - Compiler-level and OS-level protection

System Security

- Password
  - How to crack passwords?
    - Besides brute-force, attackers can use dictionary attacks to make attackers easier
  - How to come up with secure passwords?
    - A password is secure if the only feasible attack to the password is via brute-force

Storage Security

- FADE:
  - How to apply cryptography in cloud storage?
  - How does blind RSA work?
- AONT-RS:
  - How to achieve keyless security?
  - What are the implications of different configurations of (K,N) in real deployment?

Final Exam

- 3-hour exam
- Cover lecture notes, tutorials, assignments
- Open books, open notes
- No notebooks nor electronic equipment
- Computer-based exam
  - Some programming questions (I try to keep them minimal)
  - Some written questions
    - Short questions – give answers with limited number of words

Final Exam

- Scope – covers everything except:
  - DeRef
  - WiFi and cellular network security
  - Mobile botnets

Final Exam

- How to prepare?
  - Understand everything in class notes and assignments
    - Not required to read all readings, so long as you understand what the concepts mean
  - Do past exams
    - http://library.cuhk.edu.hk/
    - Ignore questions that we didn’t cover
  - Ask via facebook