

Computer Security

CS 426

Lecture 24

Review of Cryptography

Review of Cryptography: Symmetric Encryption

- Classical ciphers are broken under ciphertext-only attacks
- One-time pad has perfect secrecy, but is difficult to use in practice
- Stream ciphers (RC5) approximate one-time pad
 - fast, but difficult to use correctly
 - avoid reusing the same key stream
- Block ciphers: DES, AES
- Block cipher encryption modes
 - ECB is deterministic
 - should use CBC with random IV

Review of Cryptography: Asymmetric Encryption and Hash

- RSA: $C=M^e \bmod n$. $M=C^d \bmod n$.
 - security relies on factoring,
 - 700-bit n broken today, 1024 likely crackable by 2010, at least 2048 to be kept secure for 2030
- Hybrid encryption
 - To encrypt M , get $(k^e \bmod n, \text{AES-CBC}_k[M])$
- Cryptographic hash functions
 - preimage resistant, second preimage resistant, collision resistant
 - birthday attack
 - MD5 (128, broken), SHA-1 (160, partially broken), SHA-2 (256, 384, 512)

Review of Cryptography: Message Authentication and Key Agreement

- $MAC = C_K(M)$, can be computed only when knowing k
 - can be constructed using hash function or block cipher
- Digital signatures:
 - to sign M using RSA, computes $h(M)^d \bmod n$
- Public key certificates
- Entity authentication: storing passwords (salts), hash-chain based one-time passwords, challenge response
- Diffie-Hellman key agreement
- Needham-Schroeder shared-key and public-key protocol
 - trusted third party (online and offline)

HW3: Problem 1

- Substitution cipher
 - ciphertext-only: frequency analysis
 - known-plaintext: recover the substitution
- Chosen plaintext attack against DES
 - for each key k
 - add $\langle E_k[M_0], k \rangle$ to a table sorted based on the first element
 - end
 - when given C , a ciphertext of M_0 under unknown key
 - search for C in the table, and find the corresponding key(s)

HW3: Problem 1 (continued)

- Effectiveness
 - known-plaintext:
 - depending on whether common strings are encrypted and the mode
 - known-plaintext with common strings
 - vulnerable under ECB mode
 - not vulnerable under CBC mode with random IV

HW3: Problem 2: Life of AES

- Weakness of algorithm
 - likely no weakness in 50 years and more
 - no weakness of DES in 30 years, AES designed with much better understanding of block cipher
- Vulnerability to exhaustive search
 - assumes that 70-bit can be broken today
 - assumes every year can break 2 more bits, then 128 can last 28 years and 256 can last 93 years
 - Moore's law says every year can break 2/3 more bits
- Quantum computers
 - takes $2^{n/2}$ to search 2^n
 - unlikely to be of threat in next 50 years

HW3: Problem 3

- Alice poses math problem to Bob
 - known as cryptography commitment
 - requires two security requirements (hiding and binding)
- Stealing password file
 - preimage resistance
- Hashing system binary files
 - second preimage resistance
- Coming up with new messages for old signatures
 - second preimage resistance
- New signatures
 - collision resistance (which implies the other two)

HW3:

- Problem 4
 - Replace both Alice and Bob's public keys with the attacker's public key
- Problem 5:
 - create an account and use the cookie to try to log into another account, using your own password
 - how to store correctly?

HW3: Problem 7

- Separation of privilege:
 - can use statically mutually exclusive roles
 - can be violated when permissions are incorrectly assigned
- Least privilege
 - roles help assign only the minimal needed permissions
 - hierarchy and constraints on role activation help limit permission sin each session
 - require correct configuration
 - allow multiple role activation means constraints are explicitly needed to support least privilege

HW3: Problem 7

- Economy of mechanism: RBAC is simple, but can require a lot of extensions to support desirable properties
- Fail-safe defaults: in RBAC default is no access
- Complete mediation: an **enforcement** issue, RBAC is about policy **specification**
- Open design: yes
- Least common mechanism: not relevant
- Psychological acceptability: basic RBAC matches how one thinks about permission management

Coming Attractions ...

- November 20:
 - Web browser security issues

