Chapter 12 – Hash Algorithms

Dr. Lo’ai Tawalbeh
Computer Engineering Department
Jordan University of Science and Technology
Jordan

CPE 542: CRYPTOGRAPHY & NETWORK SECURITY

Using Symmetric Ciphers for MACs

• can use any block cipher chaining mode and use final block as a MAC
• Data Authentication Algorithm (DAA) is a widely used MAC based on DES-CBC
  • using IV=0 and zero-pad of final block
  • encrypt message using DES in CBC mode
  • and send just the final block as the MAC
    • or the leftmost M bits (16 ≤ M ≤ 64) of final block

Hash Functions

• condenses arbitrary message to fixed size
• usually assume that the hash function is public and not keyed
  • different than MAC which is keyed
• hash used to detect changes to message
• can be used in various ways with message, mostly to create a digital signature
• a Hash Function produces a fingerprint of some file/message/data
  \[ h = H(M) \]

Hash Functions & Digital Signatures

Dr. Lo’ai Tawalbeh       Fall 2005

Dr. Lo’ai Tawalbeh       Fall 2005
Requirements for Hash Functions

1. can be applied to any sized message $M$
2. produces fixed-length output $h$
3. is easy to compute $h = H(M)$ for any message $M$
4. given $h$ is infeasible to find $x$ s.t. $H(x) = h$
   - one-way property
5. is infeasible to find any $x, y$ s.t. $H(y) = H(x)$
   - strong collision resistance

Simple Hash Functions

- are several proposals for simple functions
- based on XOR of message blocks
- not secure since can manipulate any message and either not change hash or change hash also
- need a stronger cryptographic function (next chapter)

Block Ciphers as Hash Functions

- can use block ciphers as hash functions
  - using $H_0 = 0$ and zero-pad of final block
  - compute: $H_i = E_{k_i} [H_{i-1}]$
  - and use final block as the hash value
  - similar to CBC but without a key
- resulting hash is too small (64-bit)

Hash Example: Secure Hash Algorithm-SHA

- Maximum length of the input is $< 2^{64}$ bits and outputs 160-bit digest
1. pad message so its length is congruent to 448 mod 512
   (first bit 1, then followed by zeros)
2. append a 64-bit integer value to the msg (contains the original msg length).
3. initialise 5-word (160-bit) buffer $(A, B, C, D, E)$ to $(67452301, efcdab89, 98badcfe, 10325476, c3d2e1f0)$
4. process message in 16-word (512-bit) blocks:
   - expand 16 words into 80 words by mixing & shifting
   - use 4 rounds of 20 bit operations on message block & buffer
   - add output to input to form new buffer value
1. output hash value is the final buffer value
Hash Example: Secure Hash Algorithm-SHA

 SHA-1 Compression Function

- each round has 20 steps which replaces the 5 buffer words thus:
  \((A, B, C, D, E) \leftarrow (E + f(t, B, C, D) + (A \ll 5) + W_t + K_t), A, (B \ll 30), C, D)\)
- \(A, B, C, D, E\) refer to the 5 words of the buffer
- \(t\) is the step number
- \(f(t, B, C, D)\) is nonlinear function for round \((t)\)
- \(W_t\) is derived from the message block
- \(K_t\) is a constant value

Wt generation

Figure 12.8 SHA-1 Processing of a Single 512-bit Block (SHA-1 Compression Function)
Revised Secure Hash Standard

• NIST have issued a revision FIPS 180-2
• adds 3 additional hash algorithms
• SHA-256, SHA-384, SHA-512
• designed for compatibility with increased security provided by the AES cipher
• structure & detail is similar to SHA-1
• hence analysis should be similar

Keyed Hash Functions as MACs

• have desire to create a MAC using a hash function rather than a block cipher
  • because hash functions are generally faster
  • Widely available
  • not limited by export controls unlike block ciphers
• hash includes a key along with the message
• Incorporation of a secret key to an existing hash function- e.g., HMAC

HMAC

• specified as Internet standard, used in IP security, SSL.
• uses hash function on the message:
  \[ \text{HMAC}_K = \text{Hash}(K' \text{ XOR opad}) || \text{Hash}(K' \text{ XOR ipad}) || M) \]
• where \( K' \) is the key padded out to size
• and opad, ipad are specified padding constants
• overhead is just 3 more hash calculations than the message needs alone
• any of MD5, SHA-1, RIPEMD-160 can be used

HMAC Overview
HMAC Security

- know that the security of HMAC relates to that of the underlying hash algorithm
- attacking HMAC requires either:
  - brute force attack on key used
  - choose hash function used based on speed versus security constraints