COMP90043 Cryptography and Security

Semester 2, 2021, Workshop Week 7 Solutions

1. **What are the advantages of using Hash functions in digital signatures?**

   - You can sign arbitrary long messages.
   - Can be used to build authentication mechanisms (see textbook / slides).
   - Assuring integrity of messages.

2. **What characteristics are needed in a secure hash function?**

   1. H can be applied to a block of data of any size.
   2. H produces a fixed-length output.
   3. H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical.
   4. For any given value h, it is computationally infeasible to find x such that H(x) = h. This is sometimes referred to in the literature as the one-way property.
   5. For any given block x, it is computationally infeasible to find y ≠ x with H(y) = H(x).
   6. It is computationally infeasible to find any pair (x, y) such that H(x) = H(y).

3. **What is the difference between weak and strong collision resistance?**

   Weak collision resistance: Property 5 of answer in previous question;

   Strong collision resistance: Property 6 of answer in previous question.

4. **Is it possible to use a hash function to construct a DES like block cipher?**

   If you examine the structure of a single round of DES, you see that the round includes a one-way function, f, and an XOR: $R_i = L_{i-1} f(R_{i-1}, K_i)$

   For DES, the function f maps a 32-bit R and a 48-bit K into a 32-bit output (see the slides/text for details). That is, it maps an 80-bit input into a 32-bit output. This is clearly a one-way function. Any hash function that produces a 32-bit output could be used for f. The demonstration in the text that decryption works is still valid for any one-way function f.

5. **Explain the birthday paradox. What is the main implication of this for hash function?**

   The problem for adversary in collision resistant attack is to produce two messages x and y which give same hash value, i.e. H(x) = H(y).

   Birthday paradox is not a paradox! If we choose random variables from a uniform distribution in the range 0 to N-1, then the probability that a repeated element is encountered exceeds 0.5 after about $\sqrt{n}$ choices have been made.

   You can see Appendix 1A of Chapter 11 of the textbook for precise derivation of this result.

   Hence for m-bit hash, if we pick messages at random, we can expect to find two messages with the same hash value with about $\sqrt{2^m}$ = $2^{m/2}$ attempts. Hence to break the collision resistant property of an m bit hash function, the effort for adversary is upper bounded by a quantity approximately $2^{m/2}$.

This implies that m should be chosen reasonably high.

6. **List two disputes that can arise in the context of message authentication.**

Suppose that John sends an authenticated message to Mary. The following disputes that could arise:

- Mary may forge a different message and claim that it came from John. Mary would simply have to create a message and append an authentication code using the key that John and Mary share.
- John can deny sending the message. Because it is possible for Mary to forge a message, there is no way to prove that John did in fact send the message.

7. **What are some threats associated with a direct digital signature scheme?**

- The validity of the scheme depends on the security of the sender's private key. If a sender later wishes to deny sending a particular message, the sender can claim that the private key was lost or stolen and that someone else forged his or her signature.
- Another threat is that some private key might actually be stolen from X at time T. The opponent can then send a message signed with X's signature and stamped with a time before or equal to T.

Homework:

1. **Explain how you can use RSA encryption function to construct a digital signature scheme.**

Public Key Parameters: (n, e)

Private Key parameter: (n, d)

Hash Function: (H)

Signature is generated as S = $(H(M)^d)$ mod n; [M, s] form message signature pair.

Verification logic: If H(M) == $((s^d)$ mod n) then accept the signature otherwise declare verification failure.

2. **Name three important hash functions used in practice.**

MD4, MD5, SHA-1/2/3.

3. **Discuss how the security of the hash functions depends on the length of the hash.**

(Discuss Brute force attack and birthday attacks and show how they influence the decision on length of the hash.) 32-bit hash is trivial to break. The length of the hash should be at least 160 bits or more.

4. **Why CRC checksum cannot be used as a secure hash function?**

Collisions are easy to find and does not satisfy one-way property requirement of hash functions.

5. **What is a message authentication code?**

It is an authenticator that is a cryptographic function of both the data to be authenticated and a secret key.

6. **What is a Timing Attack? How can Timing Attacks be prevented?**

This is a very dangerous attack side channel attack, as it factors in the time complexity involved in deciphering a message by the intended receiver in order to be able to recover the private key.

The following are examples of approaches which can be used to prevent timing attacks:

- Constant Exponentiation Time: Requires the modifications of algorithms so as to ensure that all exponentiation operations take a fixed amount of time to execute before producing a result. This can be detrimental on performance however.

- Random Delay: Furthers on the exponentiation time problem by introducing random delay periods during each exponentiation operation to throw off an attacker from knowing how long the operation actually took. Offers better performance than constant exponentiation time operations.

- Blinding: Involves the multiplication of the plaintext by a random integer prior to performing any exponentiation operations on it.

7. **What types of attacks are addressed by message authentication?**

Masquerade: Insertion of messages into the network from a fraudulent source. This includes the creation of messages by an opponent that are purported to come from an authorized entity. Also included are fraudulent acknowledgments of message receipt or non-receipt by someone other than the message recipient.

Content modification: Changes to the contents of a message, including insertion, deletion, transposition, and modification.

Sequence modification: Any modification to a sequence of messages between parties, including insertion, deletion, and reordering.

Timing modification: Delay or replay of messages. In a connection-oriented application, an entire session or sequence of messages could be a replay of some previous valid session, or individual messages in the sequence could be delayed or replayed. In a connectionless application, an individual message (e.g., datagram) could be delayed or replayed.

8. **What are the properties a digital signature should have?**

- It must be able to verify the author and the date and time of the signature.
- It must be able to authenticate the contents at the time of the signature
- The signature must be verifiable by third parties, to resolve disputes.