The Power of Security Policy Modeling

1. Message authentication code (MAC)-- data integrity mechanism that provides integrity, but no confidentiality.
2. Chosen plaintext secure encryption (CPA-secure encryption) provides confidentiality against eavesdropping, but is not secure against an active attacker who tampers with traffic.
3. Intuitively, combining the two primitives should provide both confidentiality and integrity against an active adversary.
   – How to do this integration?

Integrating Confidentiality and Integrity

- k_e and k_m denote the encryption and MAC keys, respectively
  - X| | y denotes concatenation of x and y

TLS: First, compute a checksum over the message, append it to the message, and encrypt the result. In symbols, compute

$$t := MAC(k_m, m) \text{ and output } c := E(k_e, m \| t).$$

IPsec: First, encrypt the message and then output the resulting ciphertext followed by a checksum computed over the ciphertext. In symbols, compute

$$c_0 := E(k_e, m) \text{ and output } c := c_0 \| MAC(k_m, c_0).$$

SSH: Send the concatenation of the separately computed encryption and checksum. In symbols, compute and output

$$c := E(k_e, m) \| MAC(k_m, m).$$

During decryption, if the relevant integrity tag fails to verify, the decryption algorithm outputs a distinguished symbol ($) to indicate error

Which method is Right and which is better?

Threat Model

- Threat model associated with authenticated encryption:
  - the attacker is able to obtain the encryption of arbitrary messages of its choice
  - Attacker's goal :
    - Learn information about the decryption of a well-formed challenge ciphertext (thereby defeating confidentiality),
    - or generate a new well-formed ciphertext different from all ciphertexts previously given to the attacker (thereby defeating integrity).
- **If the attacker cannot do either then we say that the system provides authenticated encryption**

Choice: TLS

- Not generically secure:
  - there are specific instances of encryption and MAC such that the TLS combination does not provide authenticated encryption.
  - However, for specific encryption systems, such as randomized counter mode encryption, TLS method provides authenticated encryption even if the MAC is only weakly secure (so called, one-time secure). The reason is that the MAC is protected by the encryption and therefore need not be a fully secure MAC; weak MAC security is sufficient.

Choice: IPSEC

- The IPsec construction can be shown to provide authenticated encryption for any MAC and CPAsecure encryption.
- The basic reason is that the MAC locks the ciphertext so that any modification of the ciphertext en-route will be detected by the decryptor.

Choice: SSH

- The SSH construction is known to be secure when a very specific MAC is used, but may not be secure for a general purpose MAC. To see why, recall that a MAC need not preserve confidentiality and therefore MAC (km, m) may leak information about the encrypted plaintext.

Choices

- Based on these comparisons, a designer can choose the appropriate method for the application at hand.
  - When countermode encryption is used, the TLS construction is adequate even if a simple MAC is used.
  - Otherwise, one should use the IPsec construction.
- This clear understanding is only made possible thanks to the precise formulation of authenticated encryption

What do we learn

- Using the definition of authenticated encryption, the National Institute of Standards and Technology (NIST) was able to publish precise encryption modes, called CCM and GCM, designed to meet the definition
- Once the goals of authenticated encryption were clearly spelled out, it turned out that authenticated encryption can be built far more efficiently than by combining encryption and MAC algorithms

Reference: Privacy and Cybersecurity: the next 100 years
Carl Landwehr et al., Vol 100, Proceedings IEEE 2012, 13 May 2012