MAC Forgery and Length Extension Attack

Mohamed Ahmed Ali Mubarak

Mariam Waleed

Amr Khaled

May 16, 2025

What is a MAC and Its Purpose?

A Message Authentication Code (MAC) is a cryptographic checksum used to ensure data integrity and authentication. It is computed using a secret key and a cryptographic hash function, then appended to the message. The purpose of the MAC is to allow the recipient to verify that the message was not altered and that it was sent by a trusted source possessing the shared secret key.

How Does a Length Extension Attack Work?

Certain hash functions such as MD5 and SHA-1 are susceptible to a cryptographic exploit known as a **Length Extension Attack**. In cases where the MAC is computed as:

$$\text{MAC} = \text{hash}(secret||message)$$

an attacker, knowing the original message and its corresponding MAC, can exploit the structure of the hash function. By extending the message with additional data, and using the hash function's internal state, the attacker can compute a valid MAC for the forged message — all without knowing the secret key.

This vulnerability arises because hash functions process input in blocks and apply padding in a predictable way. The internal state after processing `secret || message`

can be reused to hash extra content, which leads to unauthorized message extensions being accepted as valid.

Why is `MAC = hash(secret || message)` Insecure?

The construction `MAC = hash(secret || message)` is considered insecure due to its vulnerability to length extension attacks. This occurs because the hash function:

- Does not differentiate between the secret key and the message when applying padding.
- Processes the data in a way that exposes intermediate states, enabling partial forgery.

An attacker can use these properties to craft a new message and generate a valid MAC, thus compromising both integrity and authenticity.

Secure Alternative: HMAC

The secure and recommended alternative is HMAC (Hash-based Message Authentication Code), which is designed to protect against length extension and similar attacks. HMAC ensures that:

- The key and message are handled separately and securely.
- The structure includes inner and outer hash operations that prevent exposure of internal states.

With HMAC, even if the attacker knows the message and its HMAC value, they cannot forge a new message or valid MAC without the original secret key.

Team Members

- Mohamed Ahmed Ali Mubarak
- Mariam Waleed
- Amr Khaled