Course Title: Data Integrity & Authentication

Instructor: Dr. Maged Abdelaty

Team Members:

- Maryam Waheed Zamel - 2205154
- Amina Ahmed Ferra - 2205225
- Mayssoune Hussein Elmasry - 2205251

Mitigation Writeup

Why HMAC Mitigates the Length Extension Attack?

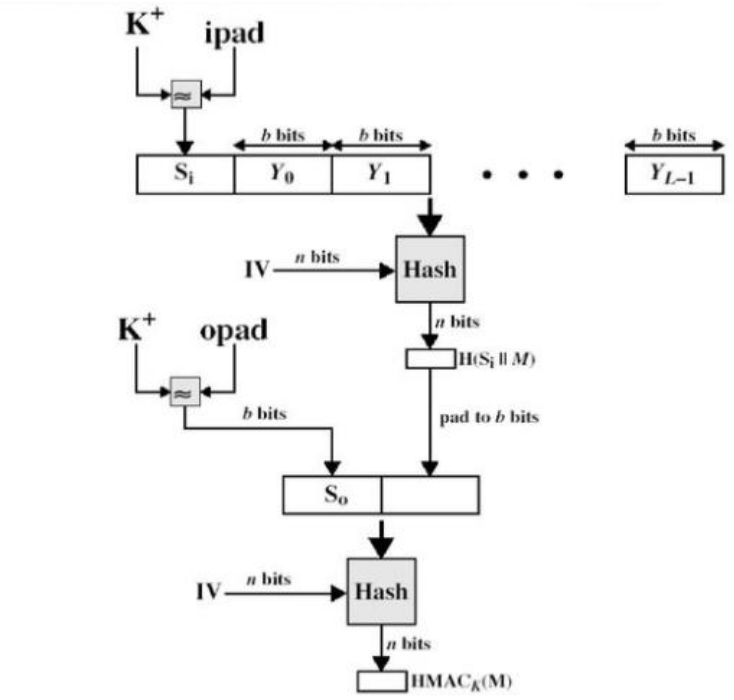
HMAC (Hash-based Message Authentication Code) is a secure method for generating message authentication codes using hash functions like MD5 or SHA1. Unlike the insecure method MAC = hash (secret || message), HMAC protects against length extension attacks by structuring the use of the secret key in a completely different and safer way.

1. How HMAC Works?

HMAC uses two hashing passes, and two padding values called ipad and opad:

HMAC (key, message) = hash ((key ⊕ opad) || hash ((key ⊕ ipad) || message))

The key is XORed with the inner pad (ipad) and hashed together with the message. That result is then hashed again after XORing the key with the outer pad (opad). This double hashing hides the internal state of the hash and prevents attackers from continuing the hash process, unlike in basic hash (secret || message).\



Mitigation Writeup

2. Why is HMAC Secure Against Length Extension?

HMAC does not expose the internal hash state to the attacker. Even if the attacker sees the output of HMAC, they cannot continue or extend the hashing process because:

- The key is hashed with padding in both inner and outer layers.
- The structure makes the final MAC independent of intermediate hash states.
- The original message length and secret are both fully hidden.

So, even if the attacker knows HMAC (key, message), they cannot append new data and generate a valid HMAC for the modified message.