Data integrity and Authentication

Background Write-Up: MAC Forgery

and Length Extension Attacks

Submitted by:

Mohamed Abdelrahman Awad | ID:2205114
Mohamed Ahmed Ramdan |ID:2205043
Omar Ahmed Hemaid | ID:2205213

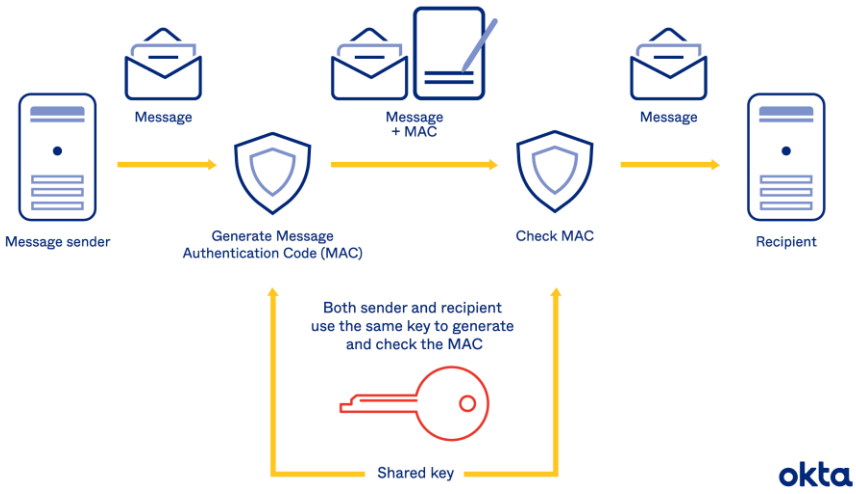
Submitted to:

Dr. Maged Abdelaty

May,2025

a. What is a MAC and why is it important?

- A **Message Authentication Code (MAC)** is a short piece of information used to verify:
  - **Data integrity** – the message hasn't been changed.
  - **Authentication** – the message really came from the expected sender.
- It's like a **digital signature** for a message, using a **secret key** and a **hash function**.
- It is generated using a secret key and a cryptographic algorithm



---

b. What is a Length Extension Attack?

- Some hash functions like **MD5 and SHA1** are vulnerable to something called a **length extension attack**.
- If an attacker knows:
  - The hash of a message, and
  - The **length** of the secret key (even if they don't know the key),
- Then they can **add new data** to the message **and calculate a valid MAC** — without knowing the key!
- This works because of how MD5/SHA1 process data in blocks — the attacker can continue hashing from where the original left off

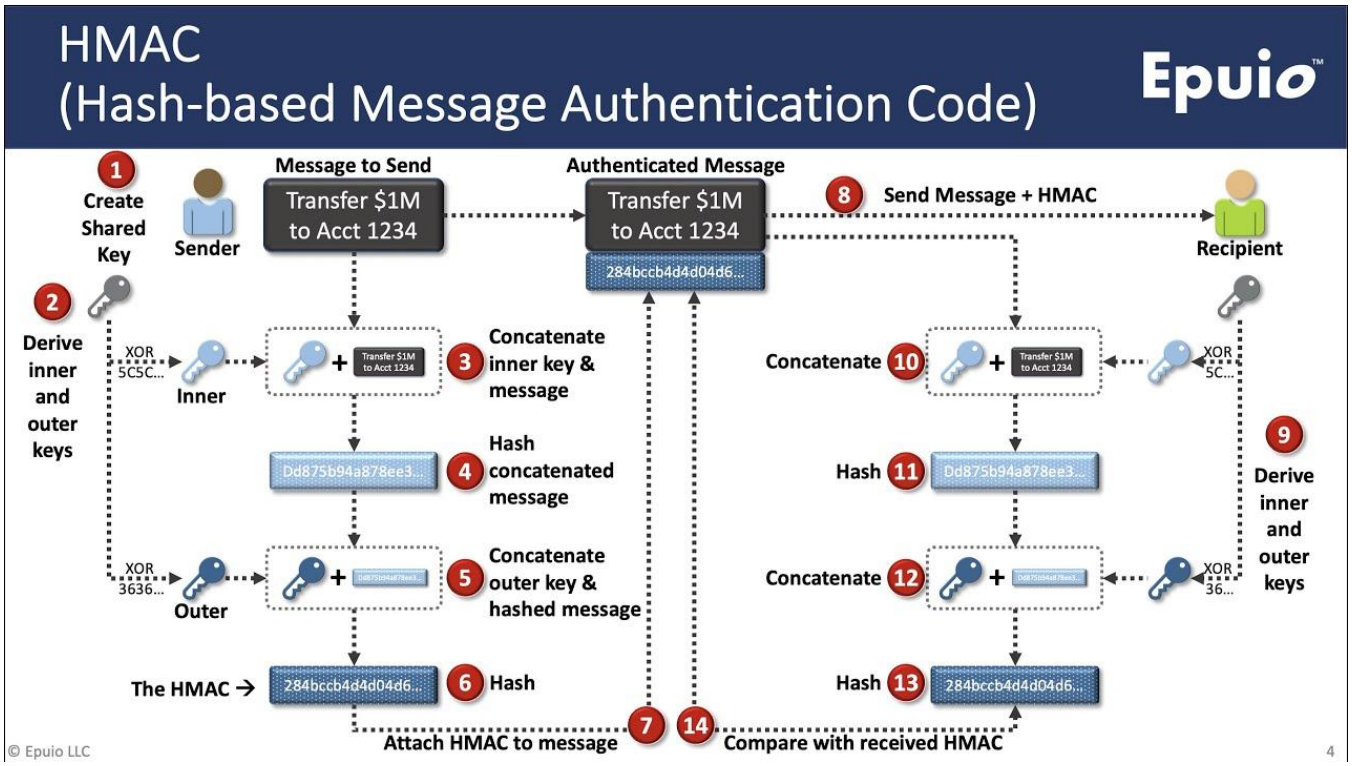
c. Why is `MAC = hash(secret || message)` insecure?

- This method puts the **secret at the beginning** of the data.
- It allows attackers to use length extension to **trick the system**:
  - Reuse the original MAC,
  - Add extra data to the message,
  - And create a new valid MAC.
- This breaks both **integrity** and **authentication**.

To Secure it use **HMAC** (Hash-based MAC) uses a cryptographic hash function along with a secret key to verify both the integrity and authenticity of a message

$$HMAC(K, m) = hash((K \oplus opad) || hash((K \oplus ipad) || m))$$

Where **opad (outer pad)** and **ipad (inner pad)** are fixed constants.



Refrences:

https://www.okta.com/identity-101/hmac/