Background Writeup

Team Members

Hossam Ahmed Aldesouky	**2205097**
Omar Hossam Ahmed	**2205150**
Tarek Gamal Elkelany	**2205029**

Introduction to MAC (Message Authentication Code)

What is a MAC?

A **Message Authentication Code (MAC)** is a short piece of information used to **verify the integrity and authenticity** of a message. It ensures that the message has not been altered and that it originates from a trusted source.

Purpose of a MAC:

- **Data Integrity:** Ensures the message has not been tampered with during transmission.
- **Authentication:** Verifies the message was generated by someone who possesses the shared secret key.
- **Non-repudiation (to some extent):** Prevents the sender from denying their involvement (when combined with other methods).

How MACs Work:

A MAC is generated by computing a cryptographic function over the **message** and a **secret key**.

This MAC is then sent along with the message.

The receiver recalculates the MAC using the same key and compares it with the received MAC. If they match, the message is accepted.

Insecure MAC Construction

Naive Construction Example:

MAC = hash(secret || message)

Why it's Insecure:

Relies on appending the secret to the message before hashing.

Vulnerable to attacks like *Length Extension* due to the way hash functions process data.

Common Mistake:

Misusing general-purpose hash functions like MD5 or SHA1 directly for authentication

Understanding Length Extension Attacks

Overview:

- Exploits the internal structure of hash functions based on the Merkle–Damgård construction.

- Allows attacker to compute

hash(secret || message || extension) from hash(secret || message).

Example:

- Intercepted message: amount=100&to=alice

- Attacker appends: &admin=true

- Computes valid MAC for extended message without secret.

Hash Functions Affected: MD5, SHA1