**Homework-4**

**MAC ATTACKS**

**What is MAC?**

MAC (Message Authentication Code) is a short piece of information used to authenticate a message. i.e, to confirm that the message came from the stated sender and has not been changed in transit.

The MAC value protects both a message’s data integrity as well as its authenticity, by allowing verifiers to detect any changes to the message content.

**How MAC Attack Works?**

Merkle-Damgard construct supports various cryptographic hash functions, such as MD5, SHA1, SHA2, etc. Using any of these hash functions, if you have a message that is concatenated with a secret, and the resulting hash of the concatenated value (the MAC), and you only know the length of the secret, you can add your own data to the message and calculate a value that will pass the MAC check without knowing the secret itself.

*Eg: Messsage + Padding + Extension*

You start by creating a new MAC to calculate the extension. To do this, message must be hashed. It’s very similar to making the SHA1 function start off at the state where the server’s hash function left off. For this attack to work, the extension must be in it’s own block when it goes into server’s hash function. The next steps to calculate padding so that key + message + padding = multiple of 512 bits. The padded and extended message its the sent to the server with the new MAC. The server hashes the attacker’s hacked message:secret + message + padding to the next block + extension + padding to the end of that block. This occurs because the attacker’s hashing operation essentially started off at the same state the server’s hash operation is at when the server has hashed half of the attack.