**Chop-Chop attack**

**Definition**

A chop-chop attack is a passive attack that breaks the confidentiality and integrity of the message. In this attack, the attacker tries to obtain information about the message from its ciphertext by repeatedly manipulating and retransmitting the packet until the attacker is able to determine the pre-shared key (PSK) used to encrypt the network traffic [1]. This attack is used to exploit the weaknesses of WEP. However, it’s not effective against more secure encryption protocols like WPA and WPA2 with robust security features [2].

**Mechanism**

Let’s assume the following conditions of the network that will be attacked [3]:

* IPv4 protocol is used where the attacker knows most bytes of the IP addresses in the network (ex. 192.168.1.X).
* The network is using TKIP which is used by the client to communicate with the access point (AP).
* IEEE 802.11e QoS features are supported by the network which allows 8 different channels for data flow.
* A long re-keying interval for TKIP is being used.

These network conditions are quite realistic for most networks deployed today. For the attacker to create a chop-chop attack against a network. First, the attacker captures an encrypted ARP request/response from the network’s traffic. From this ARP packet, most of the plaintext of it is known to the attacker except the 4 bytes of the MIC, 12 bytes of the ICV (checksum), and the last byte of the source and destination IP addresses. Then, the attacker tries to guess the ICV by repeatedly manipulating the packet and sending it to the AP. When the AP receives the ARP packet it will check the last byte of the packet. If it is incorrect, it will drop it else it will send a response to the attacker where he concludes that he successfully guessed ICV. Then the attacker goes back through the rest of the bytes until he guesses the entire packet bytes [4]. With this attack, the attacker will be able to recover the MIC key, the keystream to decrypt the messages, and construct further advanced attacks.

**Tools**

Chop-chop attack can be achieved using the following tools:

* Airodump-ng
* Aireplay-ng
* Packetforge-ng: This tool is used to create encrypted packets that are used for injection. Most common use of it is to create ARP requests that will be used for an injection attack [5].
* Aircrack-ng

**Detection**

There are different techniques that can be used to detect the chop-chop attack. The following are some of the techniques:

* Packet sniffing tools: these tools are used to detect the chop-chop attack by monitoring data packets with incorrect checksum. The tool will capture and analyze data packets in the traffic to identify the chop-chop attack before it occurs.
* Wireless intrusion detection system: this system checks the anomaly behaviours in the network traffic like an unusual amount of network traffic at certain times or an unusual number of retransmissions from the client.
* Network traffic analysis: these tools are used to detect chop-chop attacks by looking for patterns in the network traffic.

**Countermeasures**

Diagram

Description automatically generatedThe following are countermeasures to prevent chop-chop attack:

* Use short rekeying time.
* Disabling the client from sending MIC failure report frame to the AP.
* Allow CCMP in the network and disable TKIP.

In addition, TKIP provides the following to prevent chop-chop attack [3]:

1. If the AP receives a correct, but it’s out of order (lower value for the TSC counter), so the AP discards it.
2. If the client receives a packet with a correct checksum however when he verifies the MIC and the verification fails, an attack is assumed, and the AP is notified by sending a MIC failure report frame.

Figure 1: Chop-chop attack mechanism

**References**

1. <https://www.aircrack-ng.org/doku.php?%20id=korek_chopchop>
2. Sheldon, F.T. & Weber, John & Yoo, Seong-Moo & Pan, W.David. (2012). The Insecurity of Wireless Networks. Security & Privacy, IEEE. 10. 54-61. 10.1109/MSP.2012.60.
3. Beck, Martin & Tews, Erik. (2008). Practical attacks against WEP and WPA. IACR Cryptology ePrint Archive. 2008. 472. 10.1145/1514274.1514286.
4. <http://wirelessnetworkssecurity.blogspot.com/2013/01/wpa-attacks.html>
5. <https://www.aircrack-ng.org/doku.php?id=packetforge-ng>