# Packet Injection Attack

## Definition

Packet injection attack on Wi-Fi WEP is a sort of attack in which an attacker injects packets within a Wi-Fi network protected by Wired Equivalent Privacy (WEP) encryption. The objective of this attack is to compromise the confidentiality, integrity, and availability of wireless networks.

The packet injection attack can be used specially against WEP encryption because it utilizes a shared key to encrypt the entire data packet, where it is easy to crack this key using the appropriate tools. Here, when the key is compromised then the attacker is able now to apply the packet injection attack on the target network. [1][2]

## Mechanism

There are five basic phases in the packet injection attack, and it is described in the below figure.

Timeline

Description automatically generated

*Figure 1 : Mechanism of Packet Injection Attack*

Repeating these actions will allow an attacker to access the wireless network without authorization and might compromise sensitive data. [1][2][3][4][5]

## Tools

Packet injection attacks on Wi-Fi WEP networks can be implemented by the use of a variety of tools. the most commonly used tools for this kind of attack:

* Aircrack-ng
* Wireshark
* Aireplay-ng
* WepAttack
* Airdecap-ng

## Detection techniques

The detection of packet injection attacks on WiFi WEP may be done using a variety of detection methods:

Graphical user interface, text

Description automatically generated

*Figure 2 : Detection Techniques of Packet Injection Attack*

## Countermeasures

Packet injection attacks are a serious threat to the security of WEP-secured Wi-Fi networks, and it is important to take steps to protect against them. Some ways to protect against packet injection attacks on Wi-Fi WEP:

* Upgrade to WPA/WPA2.
* Use stronger encryption keys.
* Implement MAC address filtering.
* Use intrusion detection and prevention systems.
* Limit network access.
* Regularly update network devices.

These countermeasures are all designed to reduce the risk of successful packet injection attacks on WiFi WEP-encrypted networks. Implementing the combination of the above countermeasures will obviously increase the security and reduce the risk of thee attack.[1][6][7]

## References

1. "Wireless Network Security: A Beginner's Guide" by Tyler Wrightson (2011).
2. "Hacking Exposed Wireless, Third Edition: Wireless Security Secrets & Solutions" by Joshua Wright, Johnny Cache, and Vincent Liu (2015).
3. "Mastering Wireless Penetration Testing for Highly Secured Environments" by Ali A. Al-Shemery,‎ Aditya Gupta,‎ and Vijay Kumar Velu (2015).
4. Bhattacharya, S., Kalita, J. K., & Kar, S. (2012). A survey of security issues in wireless networks. Journal of Network and Computer Applications, 35(2), 534-552.
5. Thakur, N., & Jindal, A. (2018). Packet Injection Attacks on Wi-Fi Security Protocols. In Advances in Wireless Communications and Networks (pp. 375-388). Springer.
6. "Security+ Guide to Network Security Fundamentals, 5th Edition" by Mark Ciampa (2015)
7. "Computer Security Handbook, 6th Edition" by Seymour Bosworth, Michel E. Kabay, and Eric Whyne (2014)