WPA Based Packet Decrypt

Lee Kyung Moon

Prologue

It is not a zero-day vulnerability at all. Let me tell you the principle of WPA protocol and how to decrypt WPA packet.

You'd better know not the specific web sites shown in a demo but also most web sites(those do not support full ssl) in the world have the same problem.

Your lan card may not support wireless packet capturing

This is why it is hard to get wireless packet information on googling.

Let's search a monitor mode supported lan card

Notebook or smart phone have its own wireless lan card, but most of them do not support “monitor mode”.

Only if the lan card is able to support monitor mode, you can capture wireless packets properly.

How to check monitor mode

Let me show you how to check if my lan card supports monitor mode.

Starting capturing wireless packets

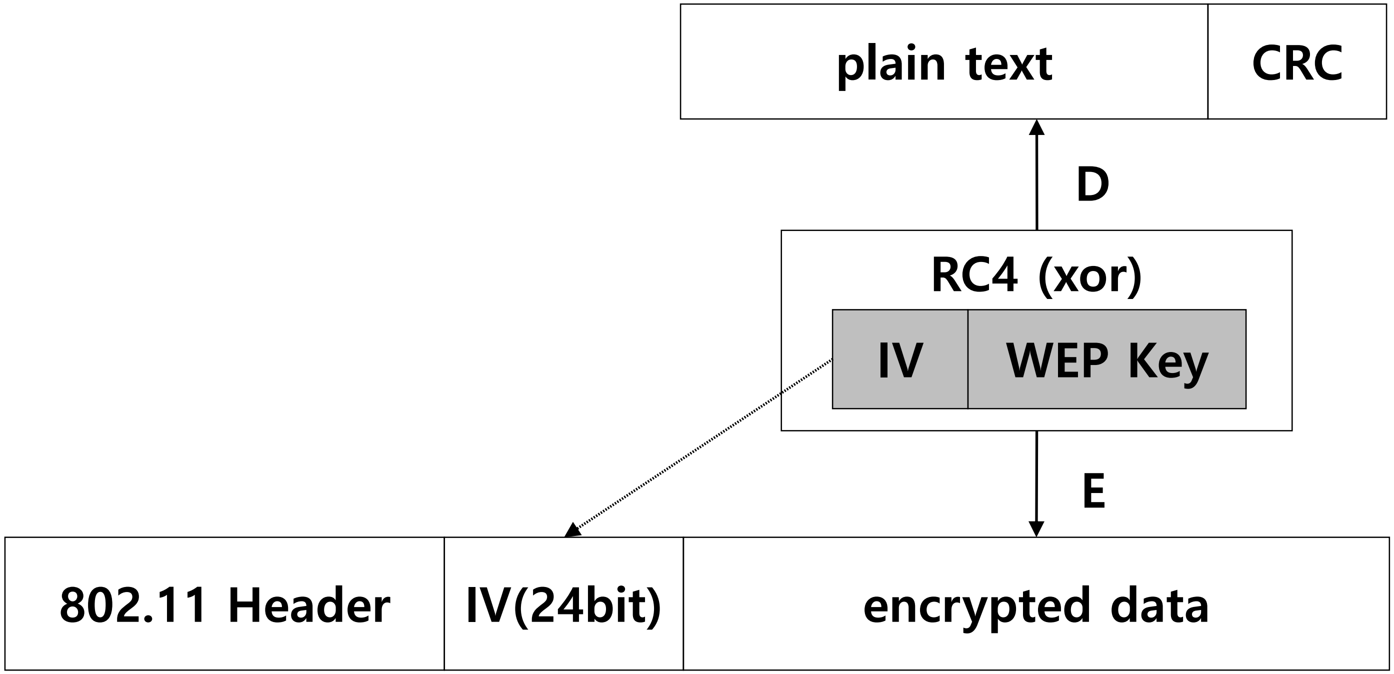
- Not encrypted
  - OPEN
- Encrypted
  - WEP
  - WPA
  - WPA2

How to decrypt wireless packet(open mode)

just capture the open AP’s packets
olleh wifi, T wifi zone, other open APs

How to decrypt wireless packet(wep mode)

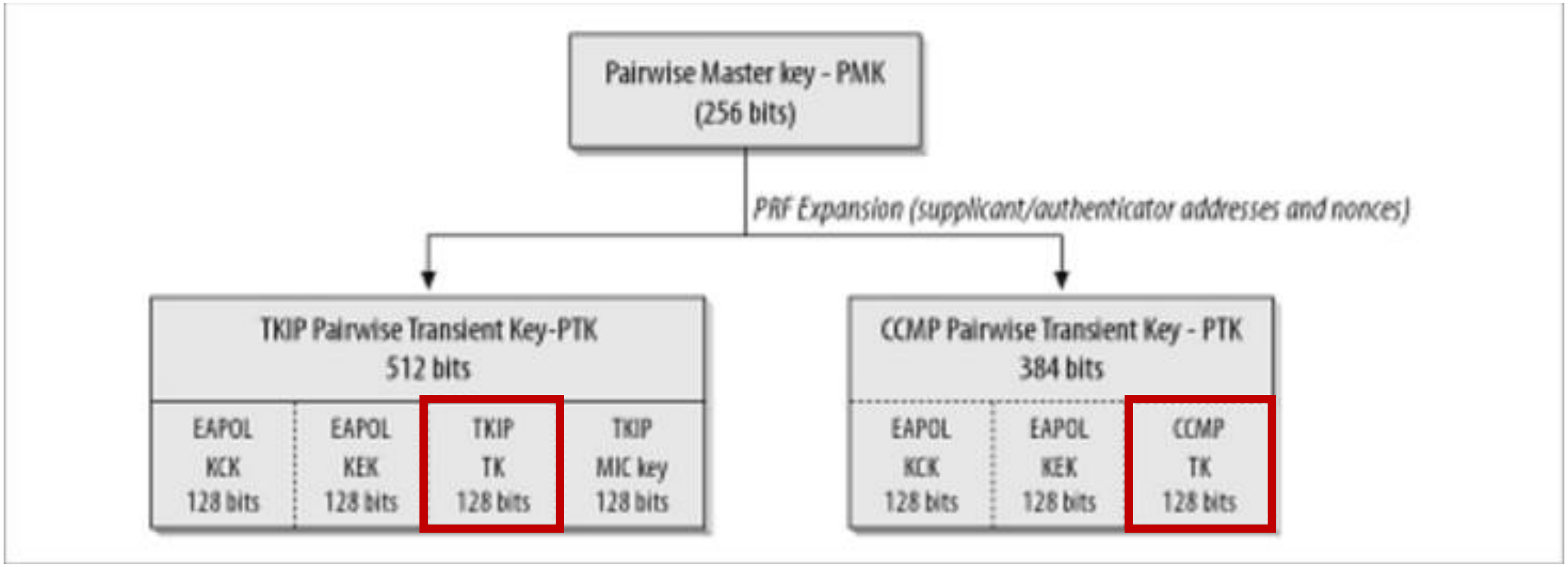
24bit IV + 40bit or 104bit shared key



wpa/wpa2 key distribution

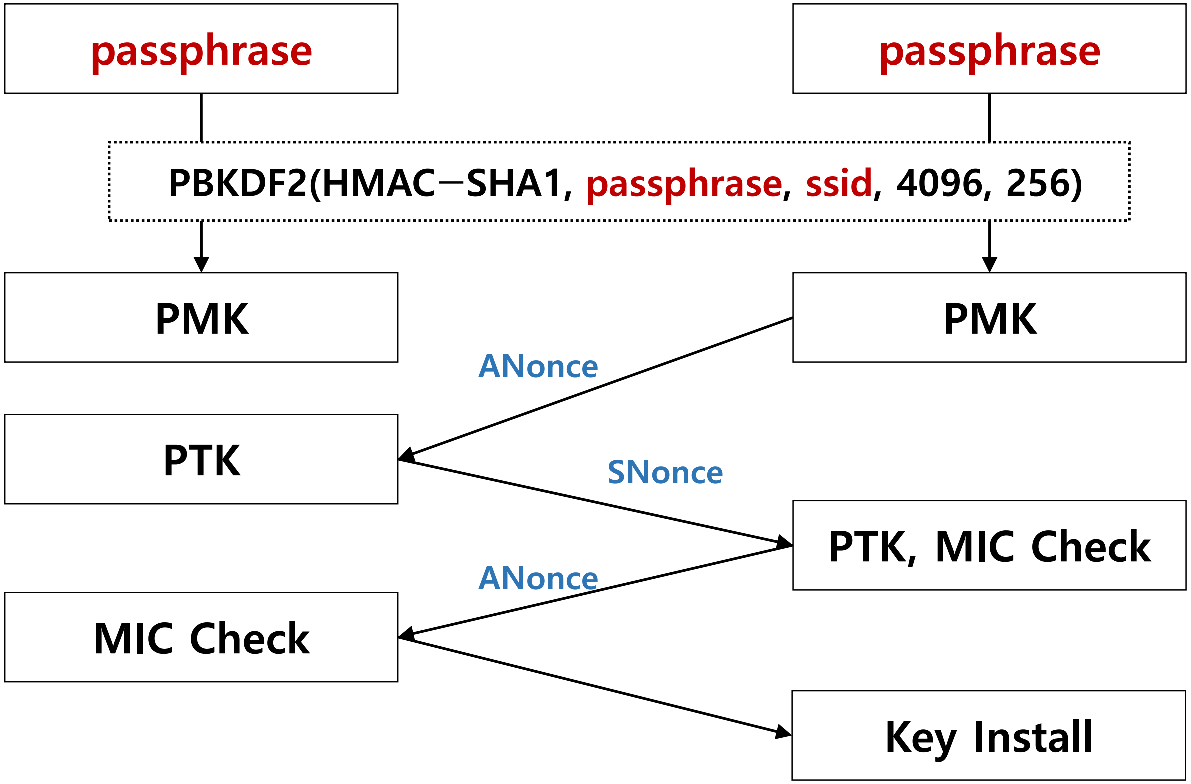
IEEE 802.11i

- Dynamic key distribution (EAPoL 4Way-HandShaking)
- We need “TK Key” for decryption


Pairwise Master key - PMK
(256 bits)
PRF Expansion (supplicant/authenticator addresses and nonces)
TKIP Pairwise Transient Key-PTK
512 bits
EAPOL
KCK
128 bits
EAPOL
KEK
128 bits
TKIP
TK
128 bits
TKIP
MIC key
128 bits
CCMP Pairwise Transient Key - PTK
384 bits
EAPOL
KCK
128 bits
EAPOL
KEK
128 bits
CCMP
TK
128 bits

wpa/wpa2 key distribution

PTK Generation

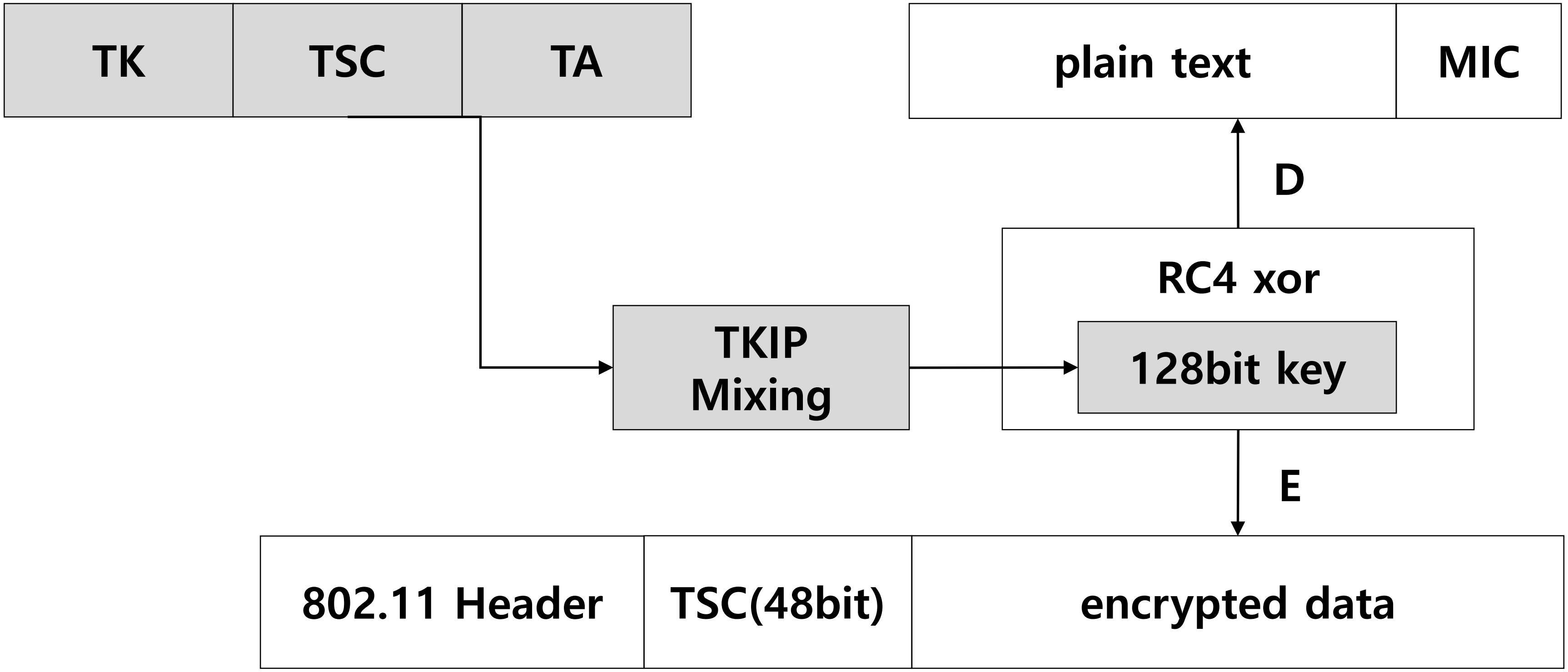


PTK = PRF-512(**PMK**, "Pair-wise Key Expansion", **AP_MAC** || **STA_MAC** || **ANonce** || **SNonce**)

How to decrypt wireless packet(wpa mode)

WPA/TKIP

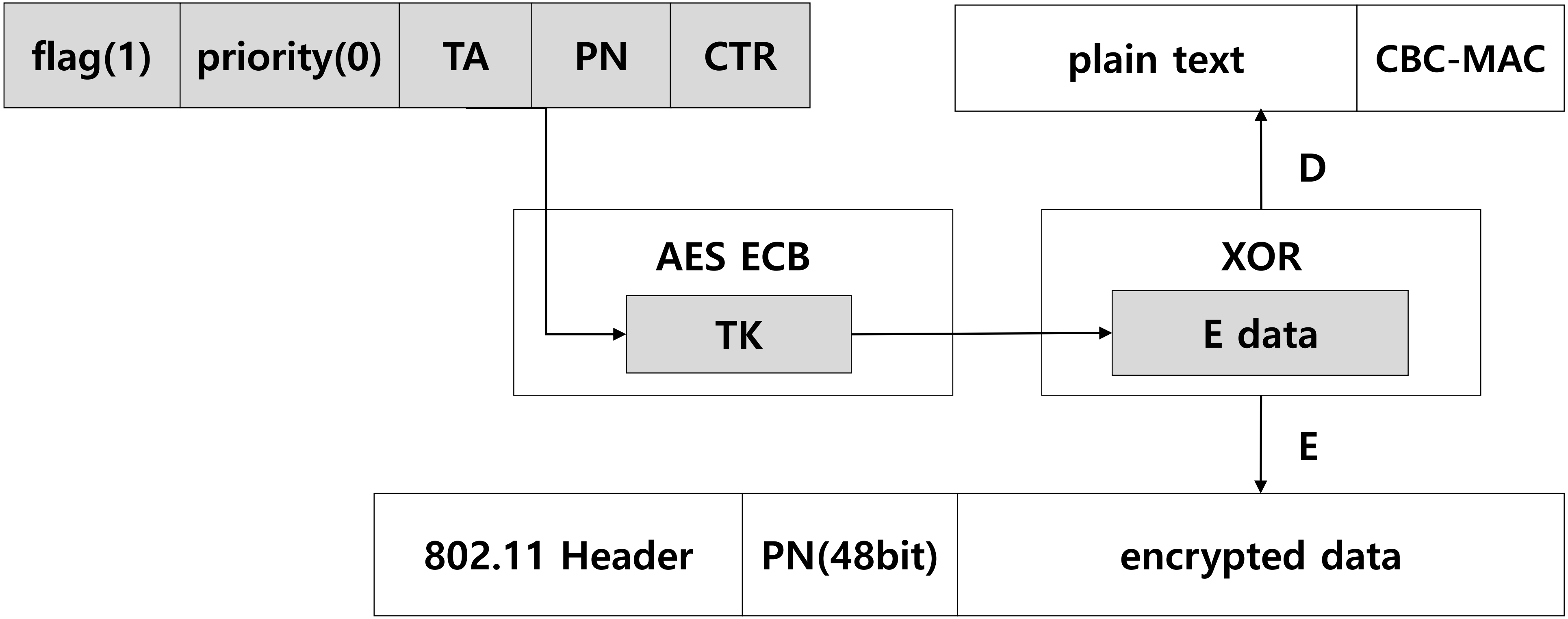
- TSC(TKIP Sequence Counter), TA(Transmitter address)



How to decrypt wireless packet(wpa 2 mode)

WPA2/CCMP

- PN(Packet Number), CTR(Counter)



Demo

It consists of 2 modules.

- Capture wireless packets and decrypt them to analyzable ethernet frames(DeSniffer).
- Figure out host and http cookie and tell the web browser them(cs).

How to protect?

- Do not use an wireless network.
  - WTF? Does it make sense?
- Use WPA Enterprise wireless environment.
- Use an web application that supports encrypted communication.
  - Use an web site encrypted over full ssl(strict) .
- State at a person who use the odd lan card in public area.
  - If he launches wireshark in his notebook?

Where can I get source code?

open source. Feel free to use my codes. :)
https://github.com/wifihack

To do list

Integrate these modules in “snoopspy” project.

Support not only ubuntu but also android, raspberry pi and arduino.

No plan on windows os.

References

https://wiki.wireshark.org/HowToDecrypt802.11

https://codebutler.github.io/firesheep

Any Question?

Thank you

gilgil (http://gilgil.net, http://snoopspy.com)
yeongsik moon (http://bbolmin.tistory.com)