Hacking Wireless Networks

Rumman Ahmed
Wasfi Momen

Cryptography

Introduction

- The data communicated can be seen by everyone in the network, so it is important to keep the communication secure
- Why hack Wi-Fi?
  - Go on the internet anonymously
  - Use someone else's bandwidth to download your own large files or torrents
  - Spy on user traffic and intercept sensitive info

Security Protocols

- There are established security protocols when dealing with the connection to wireless networks
- The reason these protocols are in place:
  - To prevent random users from connecting to your network
  - To encrypt the communication over the network
- They have changed throughout the years, mainly because major security flaws were discovered in the former

WEP (Wired Equivalent Privacy)

- Original standard developed for wireless networks
- Flawed because it allows keys to be reused in the encryption and only had a 24-bit initialization vector (IV), which is very small
  - IVs are used along with a secret key to encrypt data
- For a busy network, the same IV may be used for two clients, which allows attackers to decipher the key

How to Hack WEP…Just Use Google

how to hack wep

All | Videos | News | Images | Shopping | More | Settings | Tools

About 392,000 results (0.35 seconds)

How to Hack Wi-Fi: Cracking WEP Passwords with Aircrack-Ng « Null ...
https://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wep-passwords-with-...
Oct 20, 2013 - Let's take a look at **cracking WEP** with the best wireless hacking tool available, aircrack-ng! Hacking wireless is one of my personal favorites!

How to Crack Wi-Fi Passwords—For Beginners! « Hacks, Mods ...
https://mods-n-hacks.gadgethacks.com/how-to/crack-wi-fi-passwords-for-beginners-0...
Mar 12, 2015 - **Hacking WEP** passwords is relatively fast, so we'll focus on how to crack them for this guide. If the only networks around you use WPA ...

simple_wep_crack [Aircrack-ng]
https://www.aircrack-ng.org/doku.php?id=simple_wep_crack
Aug 29, 2010 - This tutorial walks you though a very simple case to **crack** a **WEP** key. It is intended to build your basic skills and get you familiar with the ...
Introduction · Assumptions · Equipment used · Solution

How to Crack a Wi-Fi Network's WEP Password with BackTrack
https://lifehacker.com/.../how-to-crack-a-wi-fi-networks-wep-password-with-backtrac...
Oct 28, 2011 - You already know that if you want to lock down your Wi-Fi network, you should opt for WPA encryption because **WEP** is easy to **crack**. But did ...

How To Hack Into A WEP Encrypted Wi-Fi Network (Using Windows ...
https://www.youtube.com/watch?v=P3P_s4isn2A
Aug 7, 2012 - Uploaded by Hckr
This video shows **how to hack** a wi-fi network that uses **WEP** encryption. The software I used were commview ...
▶ 2:48

How to Break WEP Encryption (with Pictures) - wikiHow
https://www.wikihow.com/Break-WEP-Encryption
How to Break **WEP** Encryption. Breaking any encryption coding or codes involves knowing a few things. First, you have to know that there is an encryption ...

How to Hack Wi-Fi (WEP) | Hacking Tutorials by Xeus - XeusHack

Applications Places Fri Jan 3, 11:11 PM root

Computer

SAM

root@kali: ~

File Edit View Search Terminal Help

```
                    Aircrack-ng 1.1

          [00:01:11] Tested 2306 keys (got 36310 IVs)

   KB    depth   byte(vote)
    0    6/  9   FE(42496) 2D(41216) 39(41216) 54(41216) 85(41216)
    1    0/  2   37(49408) 8E(46592) D2(44032) A6(43264) 69(42752)
    2    0/  3   35(47872) B0(44288) 9D(43264) 36(42752) A0(42496)
    3    0/  6   35(48384) C1(44800) 51(44032) 75(44032) 83(43776)
    4    0/  8   36(47104) 0C(45824) 83(45568) 8C(45056) 3F(44288)

              KEY FOUND! [ 39:37:35:35:36 ] (ASCII: 97556 )
      Decrypted correctly: 100%

root@kali:~#
```

[root@kali: ~] root@kali: ~

WPA (Wi-Fi Protected Access)

- This was a partial new standard implemented when the flaws of WEP were discovered
- Increased the initialization vector (48 bits) and the master key (128 bits)
- Introduces Temporal Key Integrity Protocol (TKIP), which is a set of algorithms to help with encryption (now deprecated)

WPA2

- This is the full implementation of the WPA standard, finalized in 2004
- Most important addition is the use of CCMP and AES for key encryption
- This standard was mathematically proven to be secure

How to Hack WPA/WPA2

- ARP Spoofing: used to make the access point think the attacker is the real user (man in the middle attack)
- WPA2-PSK vs WPA2-Enterprise
  - WPA2-PSK is used by home networks and places like coffee shops. Anyone who connects can observe and decrypt other's traffic because of a shared key
  - WPA2-Enterprise fixes this as every client has a unique key

GSU

Properties

SSID:	GSU
Protocol:	802.11n
Security type:	WPA2-Enterprise

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protoc	Lengt	Info
743	19…	192.168.0.103	104.25.11.6	TLS…	100	Application Data
744	19…	104.25.11.6	192.168.0.103	TCP	60	443 → 52826 [ACK] Seq=4123 Ack=559 Win=31744 Len=0
745	19…	192.168.0.103	104.25.11.6	TLS…	85	Encrypted Alert
746	19…	192.168.0.103	104.25.11.6	TCP	54	52826 → 443 [FIN, ACK] Seq=590 Ack=4123 Win=65536 Len=0
747	19…	192.168.0.103	173.236.126.226	TCP	66	52829 → 80 [SYN] Seq=0 Win=8192 Len=0 MS
748	19…	104.25.11.6	192.168.0.103	TCP	54	443 → 52826 [ACK] Seq=4123 Ack=590 Win=3
749	19…	104.25.11.6	192.168.0.103	TCP	54	443 → 52826 [FIN, ACK] Seq=4123 Ack=591
750	19…	192.168.0.103	104.25.11.6	TCP	54	52826 → 443 [ACK] Seq=591 Ack=4124 Win=6
751	20…	192.168.0.103	173.236.126.226	TCP	66	52830 → 80 [SYN] Seq=0 Win=8192 Len=0 MS
752	20…	173.236.126.226	192.168.0.103	TCP	66	80 → 52829 [SYN, ACK] Seq=0 Ack=1 Win=14
753	20…	192.168.0.103	173.236.126.226	TCP	54	52829 → 80 [ACK] Seq=1 Ack=1 Win=65536 L
754	20…	173.236.126.226	192.168.0.103	TCP	66	80 → 52830 [SYN, ACK] Seq=0 Ack=1 Win=14

```
▷ Frame 747: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▷ Ethernet II, Src: HonHaiPr_b8:c8:81 (64:27:37:b8:c8:81), Dst: TendaTec_14:c5:18 (c8:3a:35:14:c5:18)
▷ Internet Protocol Version 4, Src: 192.168.0.103, Dst: 173.236.126.226
▷ Transmission Control Protocol, Src Port: 52829 (52829), Dst Port: 80 (80), Seq: 0, Len: 0
```

```
0000  c8 3a 35 14 c5 18 64 27  37 b8 c8 81 08 00 45 00   .:5...d' 7.....E.
0010  00 34 74 12 40 00 80 06  98 d3 c0 a8 00 67 ad ec   .4t.@... .....g..
0020  7e e2 ce 5d 00 50 b6 28  0b 6f 00 00 00 00 80 02   ~..].P.( .o......
0030  20 00 d0 ec 00 00 02 04  05 b4 01 03 03 08 01 01    ....... ........
0040  04 02                                              ..
```

- Mark/Unmark Packet — Ctrl+M
- Ignore/Unignore Packet — Ctrl+D
- Set/Unset Time Reference — Ctrl+T
- Time Shift... — Ctrl+Shift+T
- Packet Comment...
- Edit Resolved Name
- Apply as Filter ▸
- Prepare a Filter ▸
- Conversation Filter ▸
- Colorize Conversation ▸
- SCTP ▸
- Follow ▸
  - TCP Stream
  - UDP Stream
  - SSL Stream
- Copy ▸
- Protocol Preferences ▸
- Decode As...
- Show Packet in New Window

How to Hack WPA/WPA2

- The former techniques require you to actually connect to the network
- You are protected if your traffic is encrypted (HTTPS)
- Up until earlier this year, these techniques were assumed the only ways to compromise wireless networks
- Now there’s a way to hack a protected WPA2 network even without the password

Key Reinstallation Attack (KRACK)

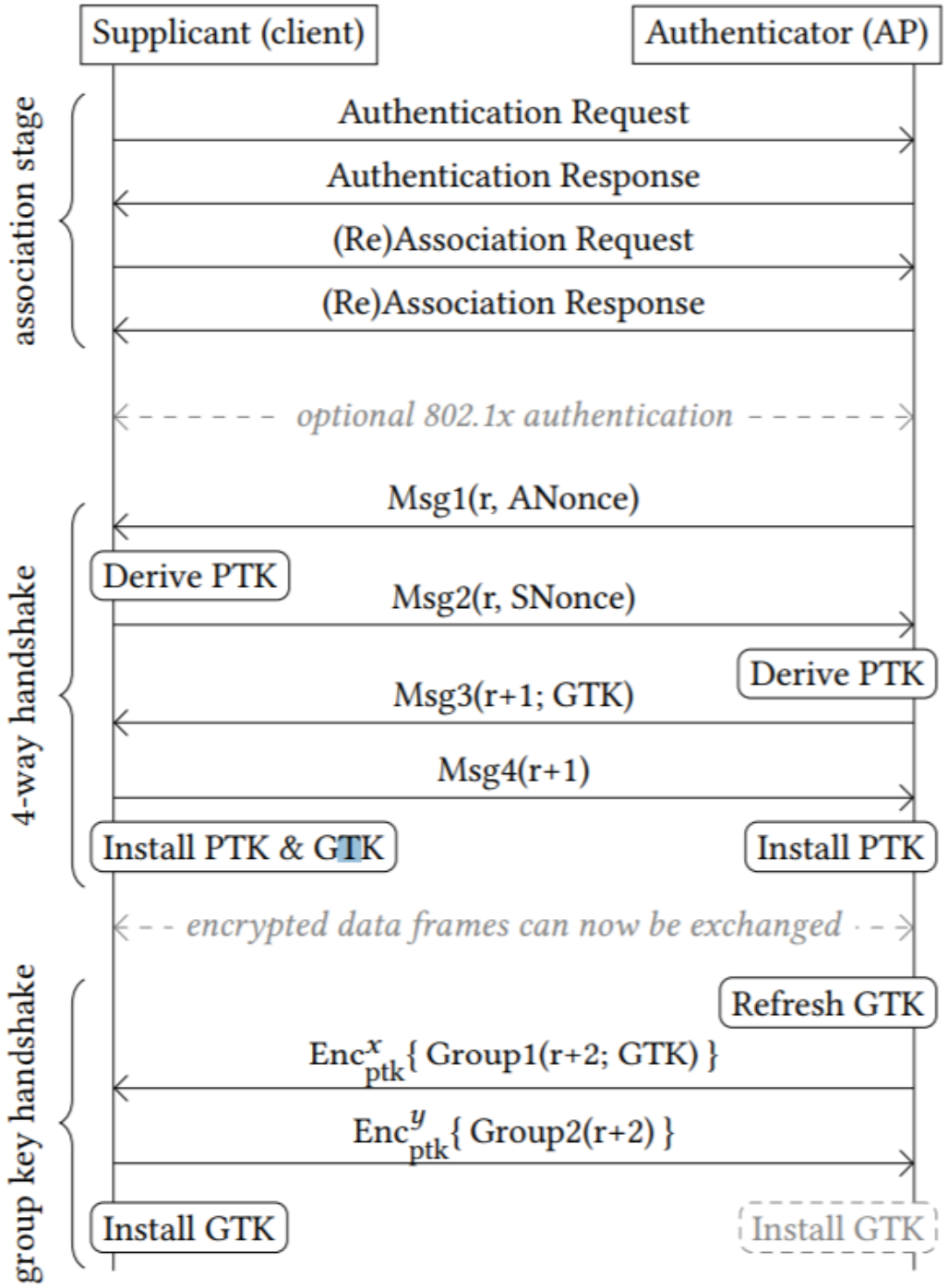
- This exploit was discovered by Mathy Vanhoef and presented at the ACM security conference in the beginning of November 2017
- The hack compromises all modern WPA2 networks, with Linux and Android devices being the most vulnerable
- Attackers, who are within range of the device or access point, can intercept data, including passwords, emails, and all other encrypted data

4-Way Handshake

- KRACK targets the 4-way handshake that occurs when a client connects to a WPA2 network
- During the handshake:
  - Verifies the client has the correct credentials
  - Generates an encryption key for the communication

4-Way Handshake (continued)

- After message 3, the key is sent from the access point to the client and installed
- However, if messages are lost (if message 3 was never received), the access point will resend and install the same key
- This prompts the IV to be reset to the same value each time
- Attackers can now use the IV to launch a replay attack to figure out what they key is


Supplicant (client)
Authenticator (AP)
association stage
Authentication Request
Authentication Response
(Re)Association Request
(Re)Association Response
optional 802.1x authentication
4-way handshake
Msg1(r, ANonce)
Derive PTK
Msg2(r, SNonce)
Derive PTK
Msg3(r+1; GTK)
Msg4(r+1)
Install PTK & GTK
Install PTK
encrypted data frames can now be exchanged
group key handshake
Refresh GTK
Enc^{x}_{ptk}{ Group1(r+2; GTK) }
Enc^{y}_{ptk}{ Group2(r+2) }
Install GTK
Install GTK

Effects

- This exploit affects all modern WPA2 networks
- Android and Linux devices are much more vulnerable, as the IV gets reset to 0 instead of what it was initially, so attackers don’t even have to figure out the IV
- Windows and iOS devices don’t allow the retransmission of message 3, so they are considered more safe

Effects

- Both the clients (our phones, laptops, and other Wi-Fi capable devices) and the access points will need to be updated
- Security patches have been rolling out since the discovery (privately told to some vendors in July)
- It is important to be kept up to date with wireless security, considering how much sensitive data we send and receive

Implementation of key exchange in WPA2 handshake

- Try to model how tools and routers compute these keys in the exchange
- Coffee shop wifi setup, we know the password
- Use Wireshark to capture the handshake
- Use Python to derive keys
- Algorithms: HMAC-SHA1, PBKDF2

Capture Handshake

Successful.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

eapol

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	Netgear_21:6e:8a	IntelCor_bd:00:f7	EAPOL	135	Key (Message 1 of 4)
2	0.000161002	IntelCor_bd:00:f7	Netgear_21:6e:8a	EAPOL	135	Key (Message 2 of 4)
3	0.024496749	Netgear_21:6e:8a	IntelCor_bd:00:f7	EAPOL	169	Key (Message 3 of 4)
4	0.024627508	IntelCor_bd:00:f7	Netgear_21:6e:8a	EAPOL	113	Key (Message 4 of 4)

Wireshark · Packet 1 · Successful

```
▸ Frame 1: 135 bytes on wire (1080 bits), 135 bytes captured (1080 bits) on interface 0
▸ Ethernet II, Src: Netgear_21:6e:8a (20:0c:c8:21:6e:8a), Dst: IntelCor_bd:00:f7 (80:86:f2:bd:00:f7)
▾ 802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: Key (3)
    Length: 117
    Key Descriptor Type: EAPOL RSN Key (2)
  ▸ Key Information: 0x008a
    Key Length: 16
    Replay Counter: 0
    WPA Key Nonce: 0d27c9ec7ad78cc4c8ccba8239af3ffe681d8cb00138d5fc...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 00000000000000000000000000000000
    WPA Key Data Length: 22
  ▾ WPA Key Data: dd14000fac048fa027f33ea89063500bebcfa4a42237
    ▾ Tag: Vendor Specific: Ieee8021: RSN
        Tag Number: Vendor Specific (221)
        Tag length: 20
        OUI: 00-0f-ac (Ieee8021)
        Vendor Specific OUI Type: 4
        RSN PMKID: 8fa027f33ea89063500bebcfa4a42237
```

Derive the PMK

```
# Change these to the network you are on.
SSID = "Circle of Hell"
password = "Inferno09"
```

```
# derive the pairwise master key
print("\nCreating Pairwise Master Key...\n");
PMK = PBKDF2(password, SSID, 4096).read(32).encode("hex") # 32 bytes max for password
                                                          # HMAC-SHA1 is included in the PBKDF2 library, default PRF
print("Pairwise Master Key: \n" + PMK)
```

Derive the PTK

```python
# need nonces, you can grab them using wireshark and filtering by the EAPOL transport protocol
# calculated using any pseudorandomfunction with 256 bits, typically HMAC
ANonce = binascii.a2b_hex("0d27c9ec7ad78cc4c8ccba8239af3ffe681d8cb00138d5fc2fad8ff003878b5c")
SNonce = binascii.a2b_hex("e9aeeff31097a2e98bb507e55d6e4870b007d7ea30a2f4e74198821aced42225")

# get these from wireshark
Auth_MAC = binascii.a2b_hex("200cc8216e8a") # Mac address of authenticator (router)
Supplicant_MAC = binascii.a2b_hex("8086f2bd00f7") # Mac address of supplicant (client/victim)
Data = "dd14000fac048fa027f33ea89063500bebcfa4a42237" # data given from authentication to supplicant in step 1
```

```python
print("\nCreating Pairwise Transient Key...\n");

# PTK is typically 512 bits and a version of HMAC
# http://etutorials.org/Networking/802.11+security.+wi-fi+protected+access+and+802.11i/Part+II+The+Design+of+Wi-Fi+Security/Chapter+10.+WPA+and+RSN+Key+Hierarchy/Computing+the+Temporal+Keys/
# input parameters are:
    # the PMK
    # a string, normally "Pairwise Key Expansion"
    # concatenation of our nonces and mac addresses of the supplicant and authenticator
def PRF(pmk, str, concat):
    numBytes = 64 # max allowed in EAPOL
    i = 0 # intial count
    R = '' # register

    while (i <= (numBytes * 8 + 159) / 160):
        hmacsha1 = hmac.new(pmk, str+chr(0x00)+concat+chr(i), hashlib.sha1) # supplied parameters are pmk, the concat string with padding and sha-1 hash
        i+=1
        R = R + hmacsha1.digest()
    return R[0:numBytes] # return bit 0 till 64th bit

str_concat = min(Auth_MAC, Supplicant_MAC) + max(Auth_MAC, Supplicant_MAC) + min(ANonce, SNonce) + max(ANonce, SNonce) # from the standard
PTK = PRF(PMK, "Pairwise Key Expansion", str_concat).encode("hex")

print("Pairwise Transient Key: \n" + PTK)
```

Conclusion

- By researching past vulnerabilities of cryptography algorithms and simulating the handshake process, we were able to understand how different attacks can compromise data transmitted between two parties via a wireless network.
- Passphrase really does matter.
- WPA3 is scheduled to be announced as a new amendment to the 802.11 standard very soon.
- There are still some issues not addressed, like deauthentication attack and coffee shop wifi sniffing

References

- https://papers.mathyvanhoef.com/ccs2017.pdf
- https://www.krackattacks.com/
- http://searchsecurity.techtarget.com
- https://www.veracode.com/security/arp-spoofing
- https://www.howtogeek.com/204335/warning-encrypted-wpa2-wi-fi-networks-are-still-vulnerable-to-snooping/

Thank you