OWASP
Open Web Application Security Project

Wireless De-auth attacks and Handshake Captures

Mike Warner BSc (Hons) CRISC

@minimike86

Disclaimer: The demonstrations in this talk are for educational purposes only! Obtaining access to networks that you do have authorization to access, and unauthorised acts is illegal under the Computer Misuse Act 1990. Summary convictions can result in up to life imprisonment and/or the statutory maximum fine (£5000).

[~]$ whoami

Mike Warner BSc (Hons) CRISC

- Software Developer / Information Risk Manager
- 6 years in Risk, Cyber & SE roles
- Currently studying towards CISSP

// TODO

Passive Attack Vector

- Manual capture of WPA-2 handshake
- Brute force WPA-2 passphrase

WPA/WPA2 4-Way Handshake

Out of band passphrase generation and distribution

PMK

PMK

1 ANonce

STA constructs the PTK

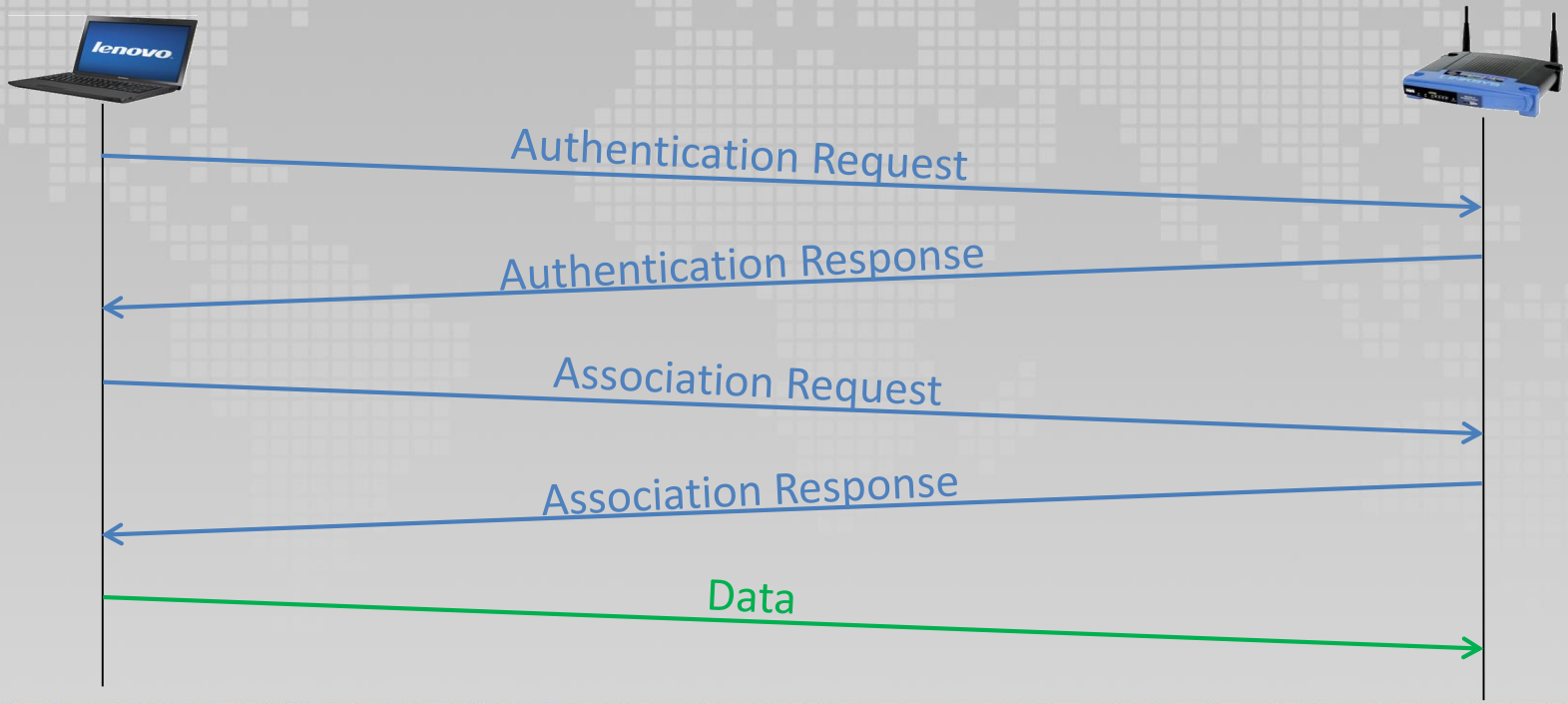
2 SNonce + Message Integrity Code (MIC)

AP constructs the PTK

3 Group Temporal Key (GTK) + another MIC

4 Acknowledge

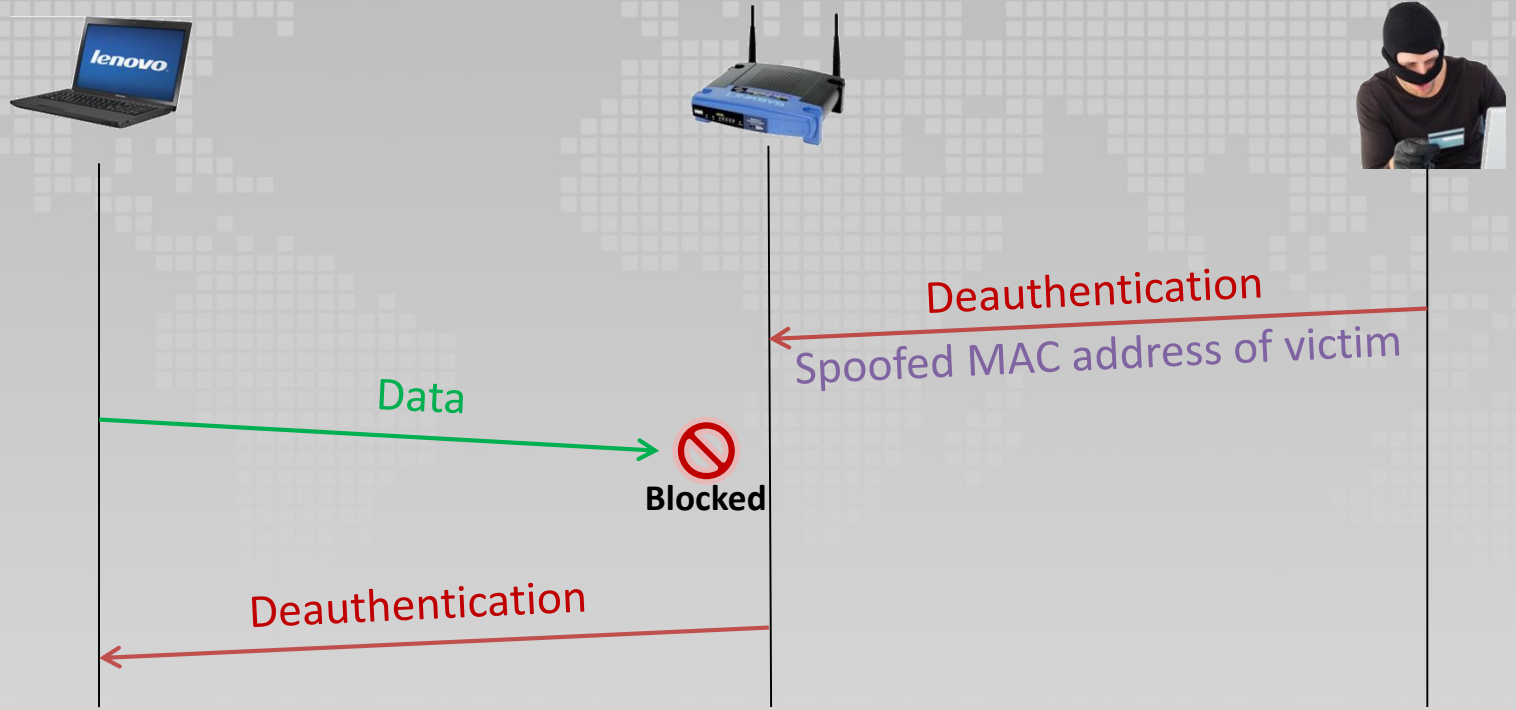
WPA/WPA2 Data Transfer



Capture WPA2 handshake

1. Grab a Wi-Fi adapter that supports "*promiscuous*" packet capture
2. Start monitoring Wi-Fi traffic (airmon-ng)
3. Send "deauthentication frames" to active Wi-Fi users - *forces station to initiate a new 4-way handshake (aireplay-ng)*
4. Capture handshake *(airodump-ng)*

Deauthentication Frames



Cracking WPA2 handshake

- Now we can brute force the passphrase by generating a "Pairwise Master Key (PMK)" for all possible passwords.
- By running our test PMK through the WPA2 algorithm we can then derive its "Pairwise Transient Key (PTK)" and "EAPOL HMAC";
- Finally we compare our result against the actual keys in the handshake captured.

WPA2 Cracking Demo

KEY FOUND! [h4xx0r]

WiFi Vendor Passwords

Vendor SSID	Len	Format	Combinations	Time*
3Wireless-Modem-XXXX	8	0-9 A-F	(First 4 digits = SSID) 65,536	1 sec
belkin.xxxx	8	0-9 A-F	4,294,967,296	7.5 hrs
TP-LINK_XXXXXX	8	0-9	100,000,000	1 wks
SKYXXXXX	8	A-Z	208,827,064,576	2 wks
BTHomeHub2-XXXX	10	2-9 a-f	289,254,654,976	3 wks
TALKTALK-XXXXXX	8	3-9 [!5] A-Y [!LOS]	282,429,536,481	3 wks
Cisco	26	0-9 a-f	43,608,742,899,428,874,059,776	Never

Mitigation #1

- ~~Use WPA3!~~ (New standards are more broken than old ones!)
- Use WPA2 with good passwords!
- Don't use WEP! (Even worse than WPA2)
- Don't connect to "Open" access points!
- Change the default passphrase!
  - Length: Must have at least 12 characters (16+ better)
  - Complexity: Include upper/lowercase and special characters ("ASCII Printable Characters" only)

Mitigation #2

- Change network name (SSID) from the default
  - Disable SSID broadcast
- Disable Wi-Fi Protected Setup “WPS”
  - Susceptible to PixieDust attacks
- Disable auto-connect to known Wi-Fi networks

Questions?