CMSC389R

Final Lecture - WiFi

COMPUTER SCIENCE
UNIVERSITY OF MARYLAND

getting started

Any course feedback?

How did you do, how did we do?

Parting thoughts?

CourseEvals!

Final Hack

will be posted on reading day!

http://134.209.116.154/

Username and Password are your email.

PLEASE CHANGE PASSWORD ASAP!

Due 5/22 @ 11:59 PM

disclaimer

We have discussed a lot of *cool* hacking concepts this semester

Remember: you are your best lawyer.

The material presented in all slides throughout this course (including today's material) containing information such as advice, graphics, images and information is presented for general educational and information purposes and to increase overall cybersecurity awareness. It is not intended to be legal, medical or other expert advice or services, and should not be used in place of consultation with appropriate professionals. The information contained in these slides should not be considered exhaustive and the user should seek the advice of appropriate professionals. The material in these slides should not be used for nefarious purposes. The University, the course staff and the faculty facilitator are relinquish all responsibilities from your actions in practicing these skills outside of the classroom and lab environment.

WiFi

What does WiFi stand for?

WiFi

What does WiFi stand for?

Wireless Fidelity? Nope!

It doesn’t stand for anything!

In the late 1990s when WiFi was becoming mainstream, the term was invented because the industry wanted a more catchy name than “IEEE 802.11b Direct Sequence”

WiFi Security

- Only a few security protocols in use today
  - WEP - Wired Equivalent Privacy (1997)
    - Static RC4 encryption keys, *easily derived*
    - All devices share same keys
  - WPA (2003) - Wireless Protected Access
  - WPA2 (2004) - Improved successor to WPA
  - WPA3 (2018) - Not widely supported yet

WPA (2003)

- WPA - added TKIP encryption
  - Fix for easily crackable WEP
  - Network passphrase + network name are used to generate unique encryption keys for each client
  - Keys are constantly refreshed
  - Key verification added
  - 4-way handshake
  - *Encryption not good enough, quickly cracked*

WPA2 (2004)

- WPA2 - uses AES, TKIP, and EAP
  - Strengthened encryption from WPA
  - All Wifi products have been required to support WPA2 since 2008
  - WPA2 is the current global standard, ***but it is not considered to be secure today***
  - *Vulnerable to dictionary attack if weak pwd*
  - *Vulnerable to KRACK attack (2017)*

WPA3 (2018)

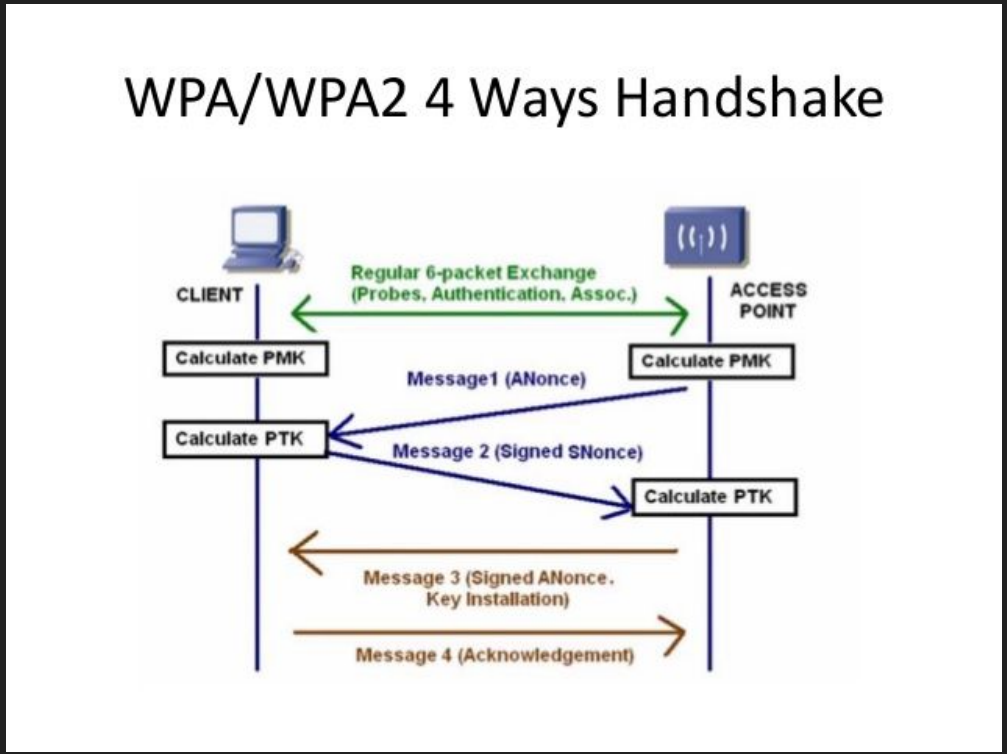
- WPA3 - New “dragonfly” handshake, forces real-time attacks
  - SAE (Simultaneous Auth of Equals) replaces PSK
    - More secure initial key exchange
  - Forward secrecy prevents recording an encrypted transmission and decoding it in the future
  - Two vulnerabilities found early on have since been patched

WiFi Cracking

- WEP is easy to crack and isn’t really used anymore
- WPA2 is the most commonly used security protocol
  - WPA2 is more secure and thus more difficult

1. Capture authentication handshake
2. Run a dictionary attack against capture

WPA2 Handshake



WiFi Cracking - WPA2

- aircrack-ng is the goto CLI suite for WiFi attacks
  - Can set your WiFi card to “monitor” mode
    - In monitor mode, your WiFi card captures *all* traffic flying through the air
  - Can send deauth requests
  - Can capture authentication handshakes
  - Can crack captured handshakes to obtain WiFi password

WiFi Cracking - WPA2

Try it out!

We’ve set up a WiFi network in this room:

Try to connect to: CMSC389R

Can you hack into our network?