Cyber@UC Meeting 56

WIFI

If You're New!

- Join our Slack: **ucyber.slack.com**
- **SIGN IN!** *(Slackbot will post the link in #general)*
- Feel free to get involved with one of our committees:

  Content Finance Public Affairs Outreach Recruitment
- Ongoing Projects:
  - Malware Sandboxing Lab
  - Cyber Range
  - RAPIDS Cyber Op Center

Announcements

- More headshots! cyberatuc.org/about
- **ClickUp** to manage our lab!
- **Towson University** Cyber Club Partnership
- **CAECO** NSA funding opportunity to design a cyber operations competition

Public Affairs

Useful videos and weekly livestreams on **YouTube**:

youtube.com/channel/UCWcJuk7A_1nDj4m-cHWvIFw

Follow us for club updates and cybersecurity news:

- **Twitter:** @CyberAtUC
- **Facebook:** @CyberAtUC
- **Instagram:** @CyberAtUC

For more info: cyberatuc.org

Weekly Content

New Paradigm in Cyber Security

- Most organizations focus resources on infection prevention through tools like Firewall, anti-spam, sandboxing, IPS, etc.
- Even the best companies can still be infected
- A new ideology of threat hunting is on the rise
- Proactively searching for threats that have managed to get into the network
- The movement of enterprises towards cloud-based networks has made threat hunting easier, it gives easier access to an enterprises entire network for scanning

Apple bans cryptomining apps from its app store

- Apple has banned apps and ads from performing cryptocurrency mining
- Believed to be in response to Calendar 2 app which replaced paid features with cryptomining but used far more processing power than was intended
- The limitations are that this processing cannot occur on the device, if it is occuring on a cloud or other remote device, they don't seem to care
- Wallet apps for cryptocurrency are also ok, but cryptocurrency cannot be offered as a reward for completing tasks, downloading apps, etc.
- Google made a similar ban on the chrome web store last week
- Twitter has plans to block cryptomining ads,
  Facebook already did this in January

Mac Signature Validation Bug

- A bug in Apple’s code-signing API has made it possible to bypass digital signature checks by bundling a malicious file with a legitimate apple-signed code to make malware appear to be signed by Apple
- This is not a macOS flaw, but rather third-party security tools that implement Apple’s code-signing APIs
- Requires the attacker to use Fat binary format
- Apple was notified in March but stated it was not a security issue they should directly address, as such the affected third-party developers were notified and are currently working on patches
- List of affected vendors/tools on website

Recommended Reading

https://thehackernews.com/2018/06/android-adb-hacking.html

https://thehackernews.com/2018/06/summit-fastest-supercomputer.html

https://thehackernews.com/2018/06/ethereum-geth-hacking.html

Part 11: Wifi

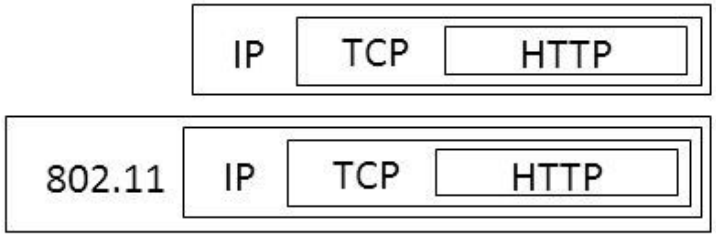
Why? Figh!

Wireless vs. Physical

Wireless	Both	Wired
Proximity Based	IP Based (MAC, IP addr, DHCP)	Physical Connection
Open Air (anyone can listen)		Limited by Cable Length
Device - AP Encryption in Standard		
Limited by Radio Power		

Adding a new layer

- When we move from wire to wireless, we need to add a new protocol to handle device connections to the router and encryption schemes.
- Most used protocol is 802.11 which originates from IEEE in 1997



802.11 Protocol Standards

IEEE Standard	Frequency/Medium	Max Speed
802.11a	5GHz	54Mbps
802.11b	2.4GHz	11Mbps
802.11g	2.4GHz	54Mbps
802.11n	2.4GHz/5GHz	600Mbps

802.11 Encryption Standards

Standard	Encryption	Vulnerability Status
WEP	RC4 40 bit	Extremely Vulnerable
WPA	RC4 124 bit	Less Vulnerable, KRACK
WPA2	AES 128 bit	Less Vulnerable, KRACK

802.11 Frame Types

Frame Type	Uses	Encryptable?
Management	Joining/Leaving Wifi Network	No, these establish encryption
Control	Controlling Data Transmissions between stations	No, must be shared between stations quickly
Data	User Data	Always Encrypted

802.11 Frame Contents

Frame Type	Contents
Management	Device MAC Addresses, Station Names, Probe Requests
Control	Station-Station Communications
Data	User Data

802.11 Exploiting Management Frames

- https://www.sparkfun.com/products/13678 Wifi chipset for IOT - direct frame level of control
- http://nodemcu.com/index_en.html That same chipset on a cheap board
- https://github.com/samdenty99/Wi-PWN Some example software
- Scanning
  - Listening to station and client management frames for MAC addresses
- Probe Request
  - device looking for a known station
- Deauthentication
  - Kick a device off a network after listening for it's MAC
  - Could also go the other way if we have a station's password and exhaust the DHCP of the network, but not in the demo software
- Beacon Advertisement
  - Listing an access point for clients to connect to

802.11 Rogue Access Points

If we can setup a router why don’t we setup a router with MITM built in?

- Wifi Pineapple: Commercial option
  - Comes with built in tools and large library of addons
  - ~$150
- AR150 Travel Router: Budget Option
  - Just a travel router with the Pineapple firmware loaded onto it
  - ~$15 and some effort
  - Also ships with OpenWRT installed (Linux for routers)
  - Can install aircrack-ng and attack routers with your router
  - Can also just use it as a router, unlike the pineapple

More Wireless tools

Software

- aircrack-ng, a collection of tools to play with wireless protocols.
  - May require certain chipsets and drivers to use
- Scapy, python library for playing with wireless protocols
  - High capability but requires development from user
  - Also requires certain hardware for certain actions

Hardware

- Raspberry Pi series
  - Powerful enough to use, cheap enough to use aggressively
  - Pumpkin Pi is a Pi based clone of the Wifi Pineapple