

# Week 11

# Wireless Security

Generic Template



# Announcements

**CSAW 21 Grand Finals:** Second Place GLOBALLY!!!

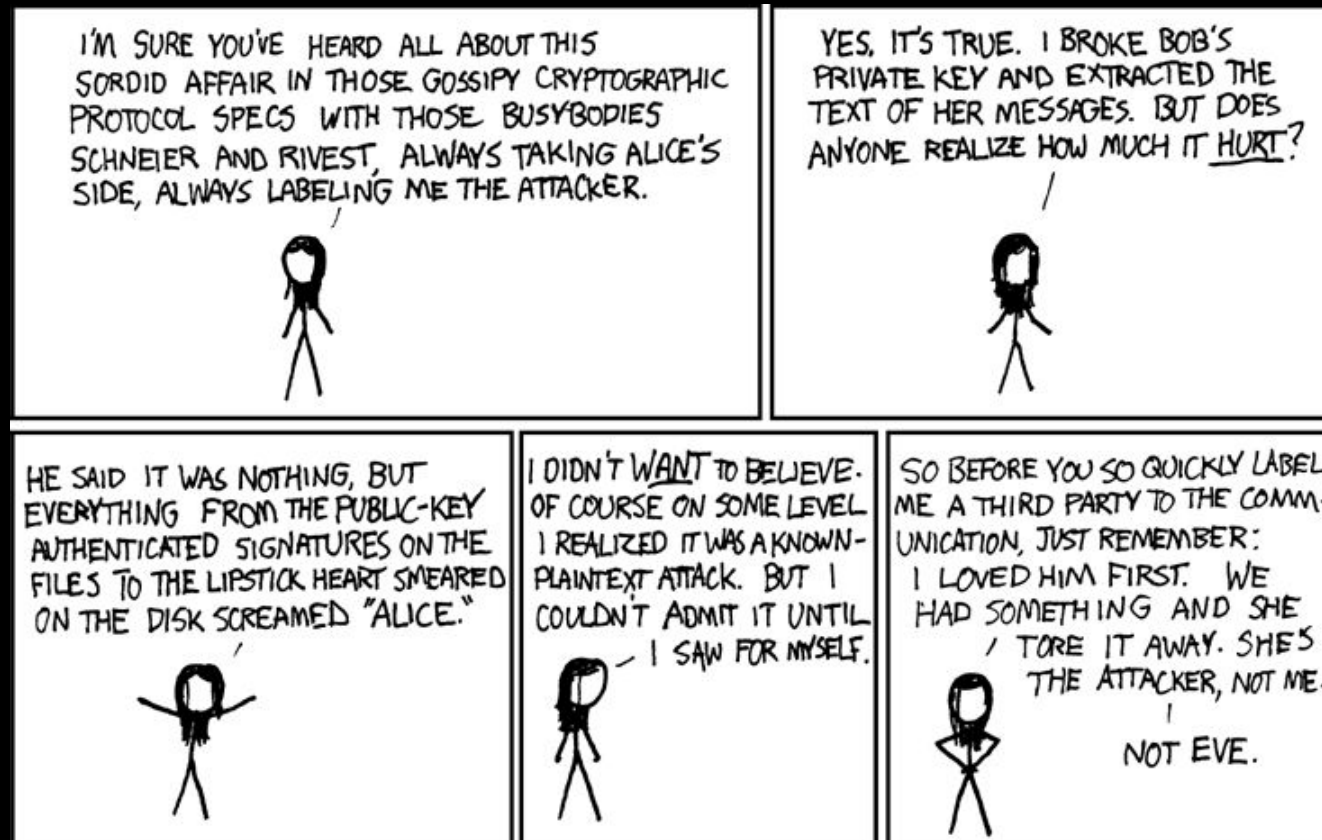
**Shib auth and Infra:** We need people (Sophomores and younger) to learn the things.

**Spray Paint Social:**



# Meeting Flag

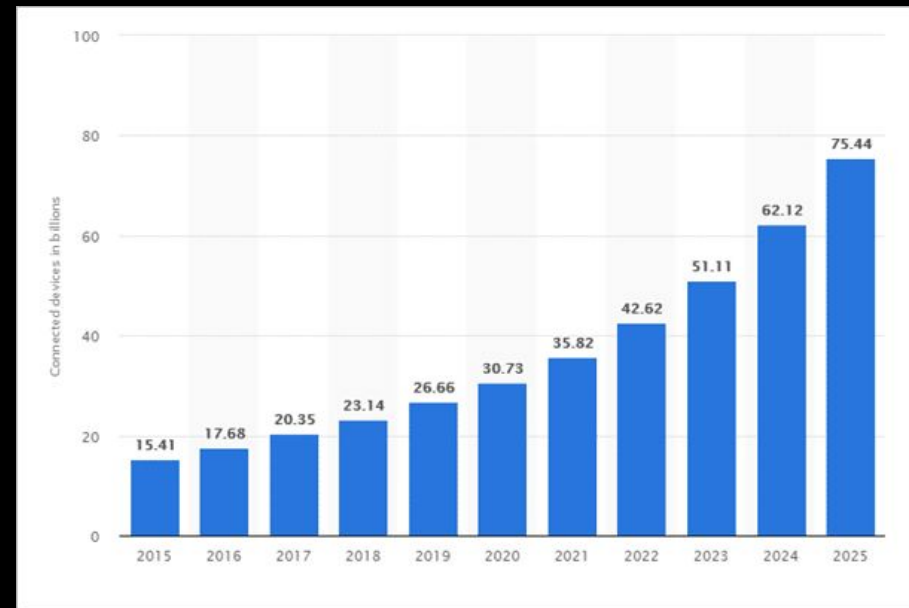
sigpwny{networking\_but\_wireless}



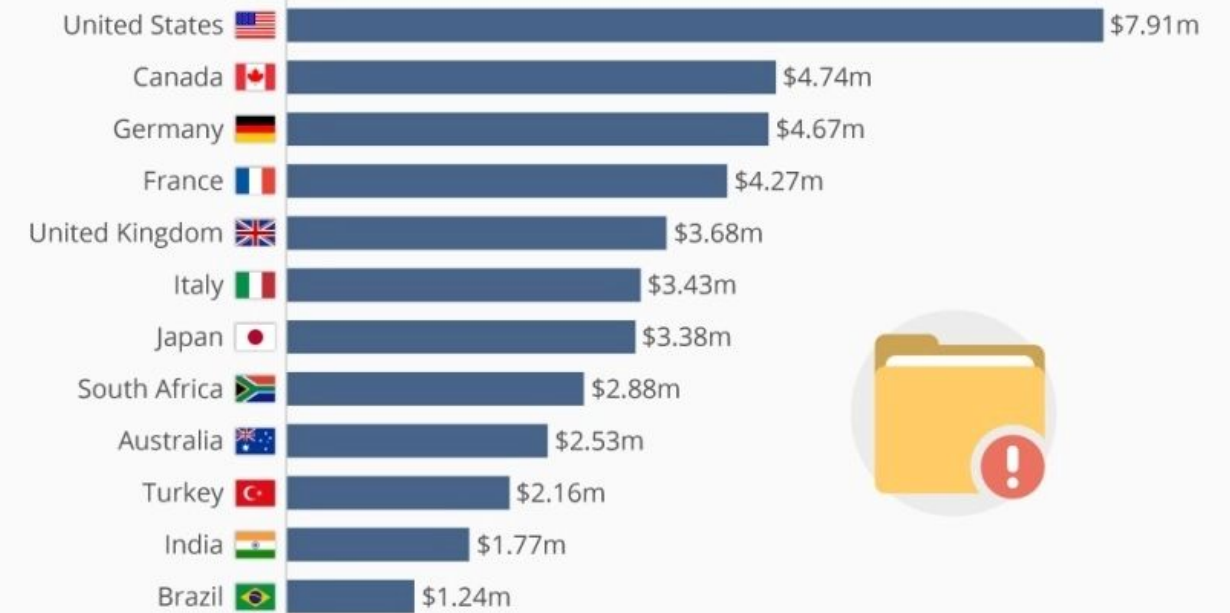
# Overview

Wireless network security is critically important.

I am **not** a lawyer

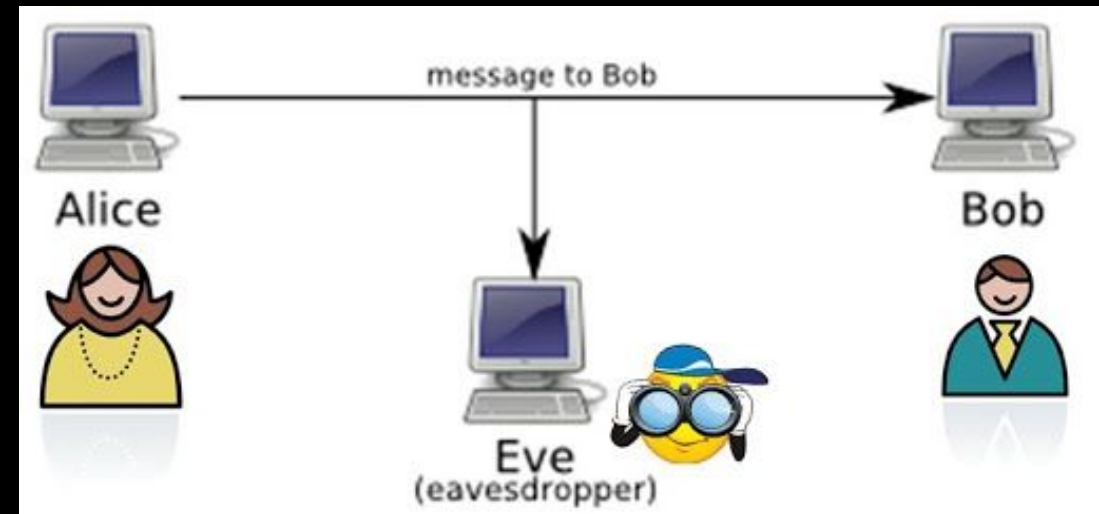


Average total cost of a data breach by country in 2018



# A story of Alice and Bob

- Alice and Bob want to send each other some secret gossip
  - Eve wants to know the gossip
- What can eve do?
  - Eavesdrop
  - Send messages to Bob / Alice
  - Place themselves in between Alice & Bob
- Ultimate Goal
  - Man-In-The-Middle
  - Takeover



# The CIA(A) Security Model



# Confidentiality, Integrity, Availability (2)



## Confidentiality

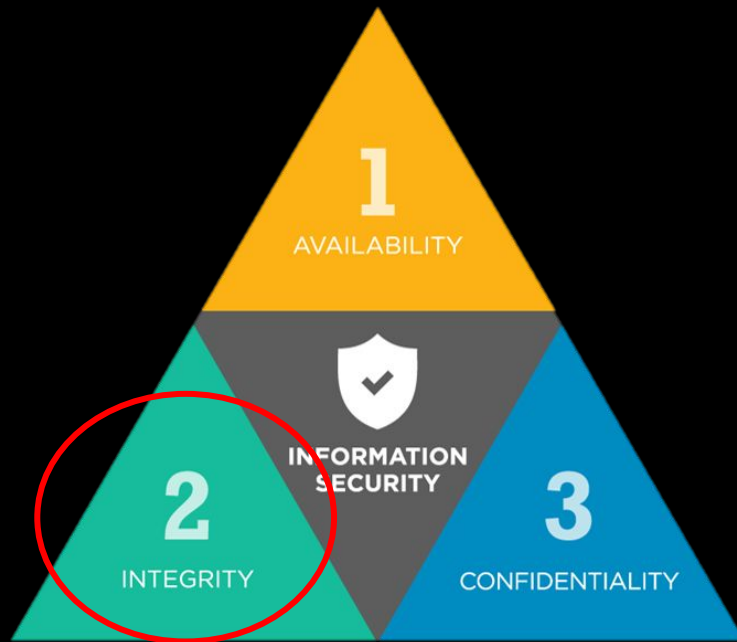
If a system has confidentiality,  
then the messages you send \*\*\*

\*\*\* \*\*\*\*\* \*\* \*\*\*\*\* \*\*\*

- Sniffing
- Implications
  - Data
  - Secrets
  - Material for other attacks



# Confidentiality, Integrity, Availability (2)



## Integrity

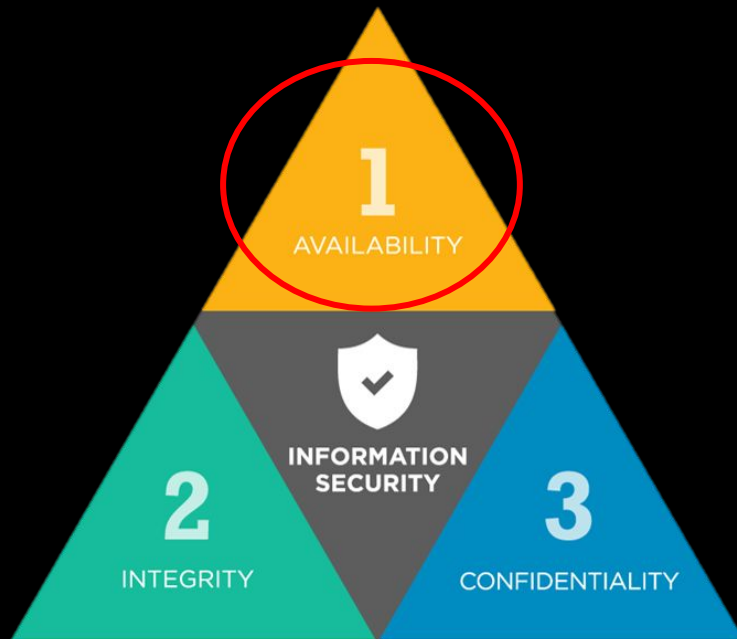
Data transmitted is correct, and has not been modified intentionally or unintentionally.

- Unintentional Modification
  - Bitflips
  - Error Bytestreams
- Intentional Modification
  - Off path attacker
  - MITM attack





# Confidentiality, Integrity, Availability (2)



## Availability

Are my services available, can my data actually be transmitted.

- Hard to stop
  - Very difficult to prevent this
- Law yet to catch up
  - I am not a Lawyer



# Confidentiality, Integrity, Availability (2)



## Authenticity

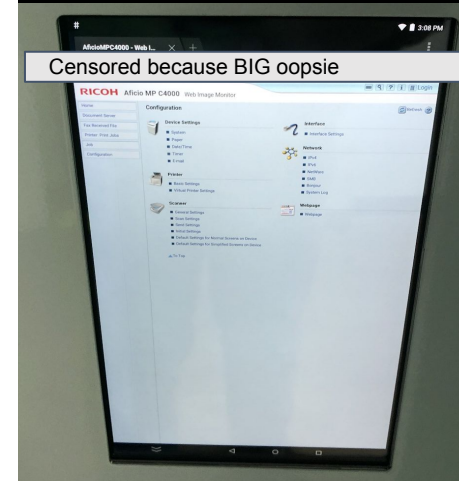
Is the data being transmitted genuine, are both parties who they claim to be.

- Extension of integrity
  - Will be lumped in with integrity.
- Examples
  - Passwords
  - 2 Factor Authentication
  - PKs
  - Zero Knowledge Proofs



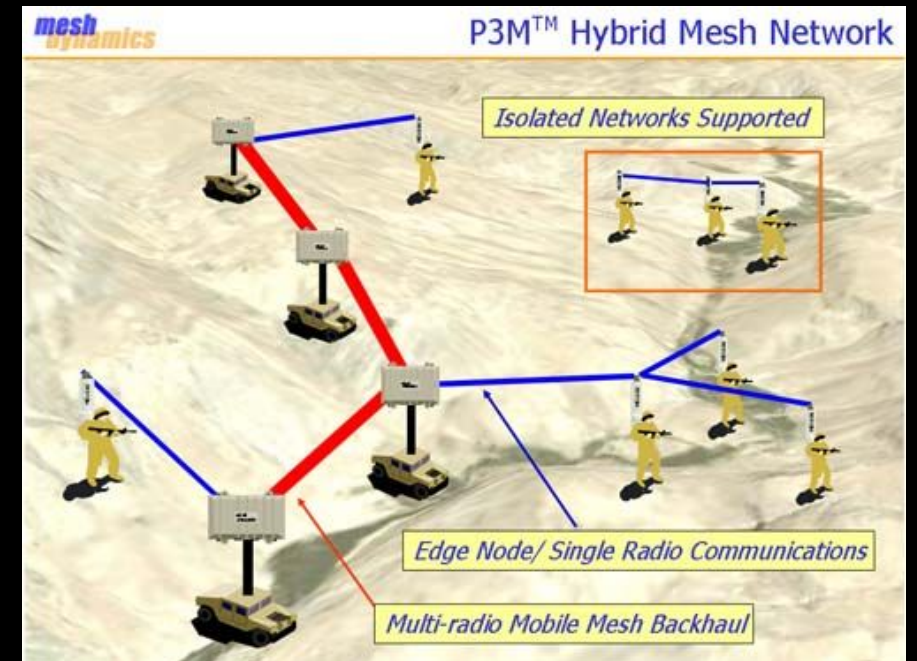
# What can go wrong

- Node integrity
  - Subvert one node → access to entire network
  - Smart Soda Machine... total network compromise
- Human Error
  - Mike will always click on free cruise tickets on a Sunday night on his work laptop, then bring it into the network the next day.
- System misconfiguration
  - IOT device takeover → network access → network takeover
- Impact
  - 14 Million Dollars
  - Cost of recent wireless based breaches



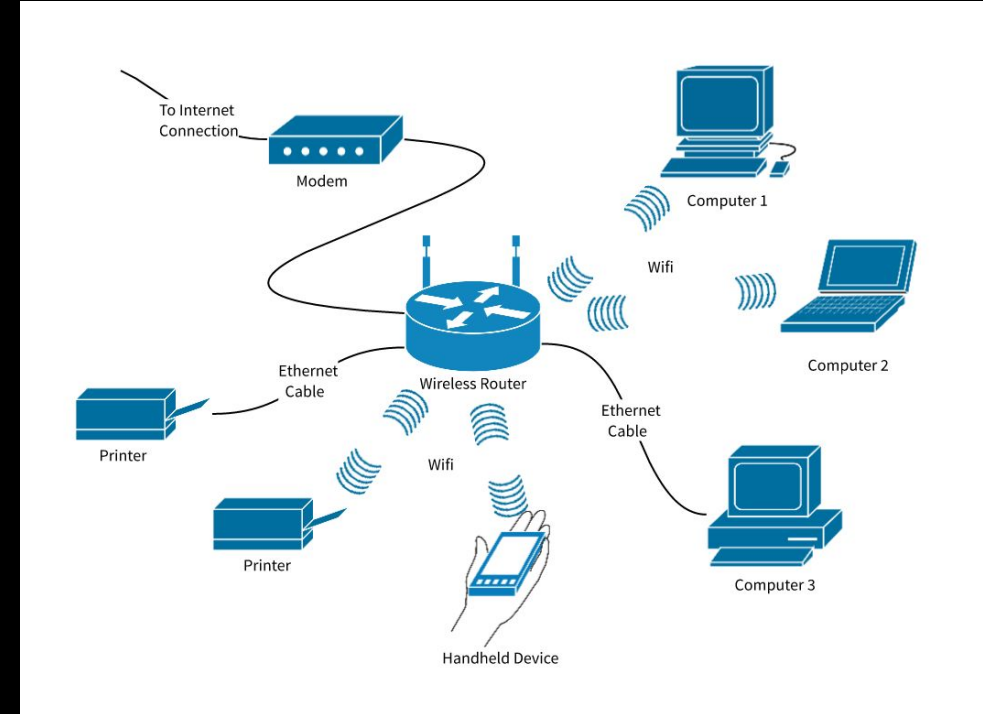
# Two Security Contexts

- Military and Non-Military
  - Wildly different threat models
  - Wildly different implementations
- Military Wireless Networking
  - Able to operate under physically strenuous conditions
  - E2E encryption, jamming resilience, etc.
  - **Adheres to a detailed security standard**
    - [Approved Networking Products List For US Military](#)
    - [Army Wireless Security Standard](#)
  - Highly secured, but out of date
  - Not perfect
    - [Wearable Fitness Devices](#)
- Non-Military Wireless Networking



# Two Security Contexts

- Military and Non-Military
  - Wildly different threat models
  - Wildly different implementations
- Military Wireless Networking
- Non-Military Wireless Networking
  - Does not legally have to adhere to any security standards
  - Large variety of vulnerabilities
  - Types of wireless networking
    - Star topology
    - P2P (ad-hoc)



# Confidentiality Attacks



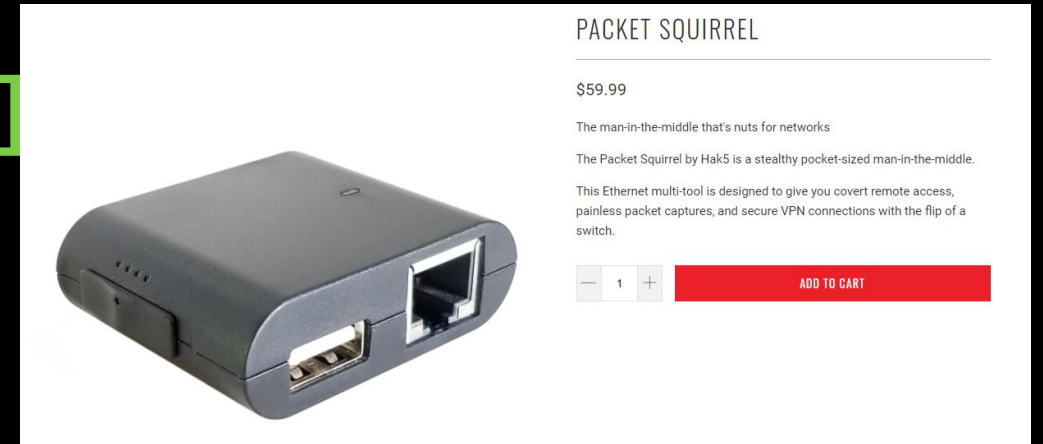


# Wireless Confidential

Your messages are \*\*\* \*\*\*\*\* \*\*\*\*\*  
\*\*\*\*\*, and only the intended recipient can read them.

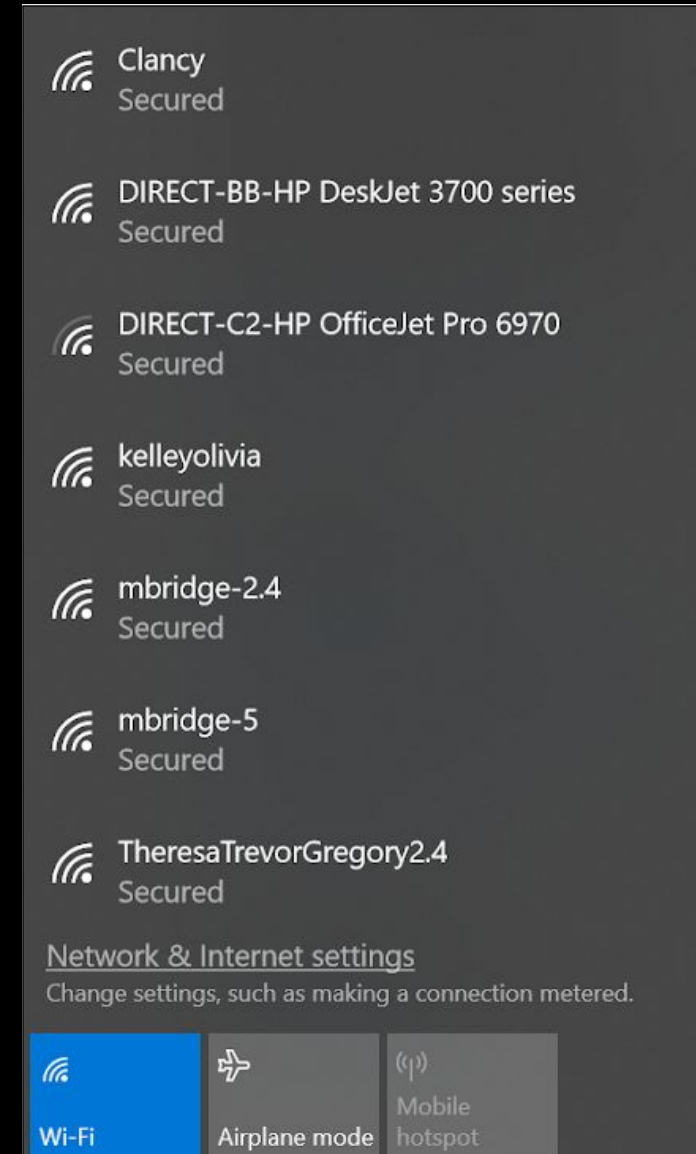
In all networks, sniffing affects confidentiality.  
Wireless communication travels through open space, which means several things.

1. No authentication
2. No network connectivity
3. No physical access →→→→



# Exposure

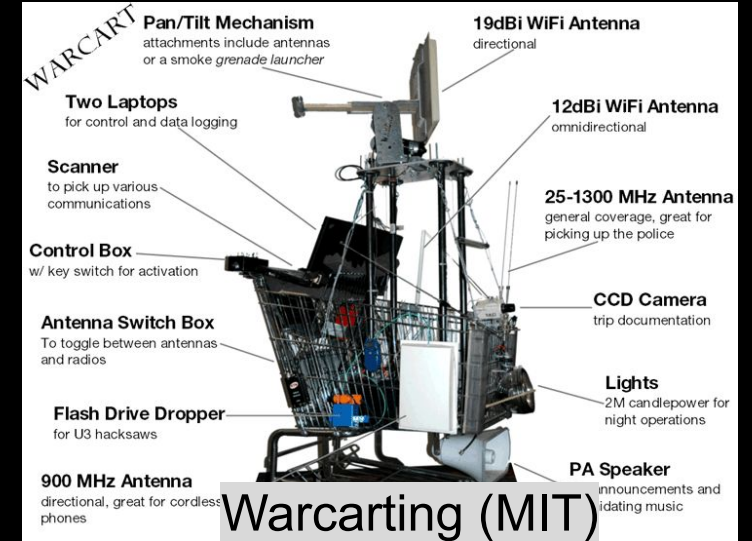
- Range and decipherability depend solely on network configuration and location.
  - Thus, effectiveness varies wildly over a wireless network.
- Works on BLE, Thermal, VLC, almost all forms of communication.
- Monitor Mode, compatible with many NIC's
- Tools Used
  - tcpdump, wireshark





# Wardriving: sniffing to the extreme

- Car full of WiFi antennas, laptops, and various sensors.
- Drive around picking up signals
- Create datasets of wifi strength and configuration.
  - Not necessarily hostile
- Malicious wardriving
  - Find weakest access point
  - Google Wardriving Lawsuit



[Back to results](#)



Roll over image to zoom in

## WiOpsy - 802.11ac USB Windows Wi-Fi Sniffer by Intelligraphics Inc

Brand: Intelligraphics Inc

Price: **\$399.00** ✓prime & FREE Returns

Get \$100 off instantly: Pay **\$299.00** ~~\$399.00~~ upon approval for the Amazon Prime Rewards Visa Card. No annual fee.

- Enterprise Grade 802.11ac Dual Band Windows WiFi Sniffer Product
- USB 2.0 WLAN adapter that support for both 2.4GHz and 5GHz bands with 20MHz, 40MHz and 80MHz wide channel widths
- Support for Windows 7/8/8.1/10 OS (both x86 and x64)
- Easy-to-use configuration GUI with deep inspection of hundreds of protocols, live capture and offline analysis
- Guaranteed packet capture performance in par with all the existing WiFi sniffer solutions

[Compare with similar items](#)

[Report incorrect product information.](#)

**\$399.00**

✓prime & FREE Returns ▾

FREE delivery: **Saturday, Nov 21**  
[Details](#)

**Only 4 left in stock -  
order soon.**

Qty: 1 ▾



Add to Cart



Buy Now



Secure transaction

Ships from Amazon

Sold by Intelligraphics

Return policy: Returnable until  
Jan 31, 2021 ▾

**Add a Protection Plan:**

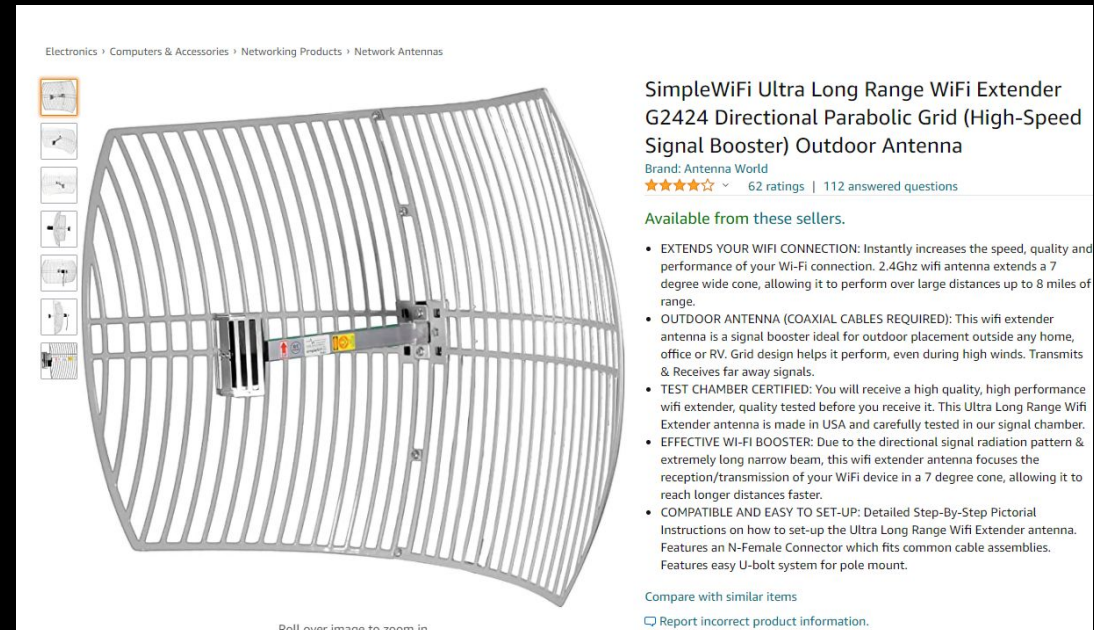
☐ 4-Year Protection for **\$44.99**

☐ 3-Year Protection for **\$33.99**



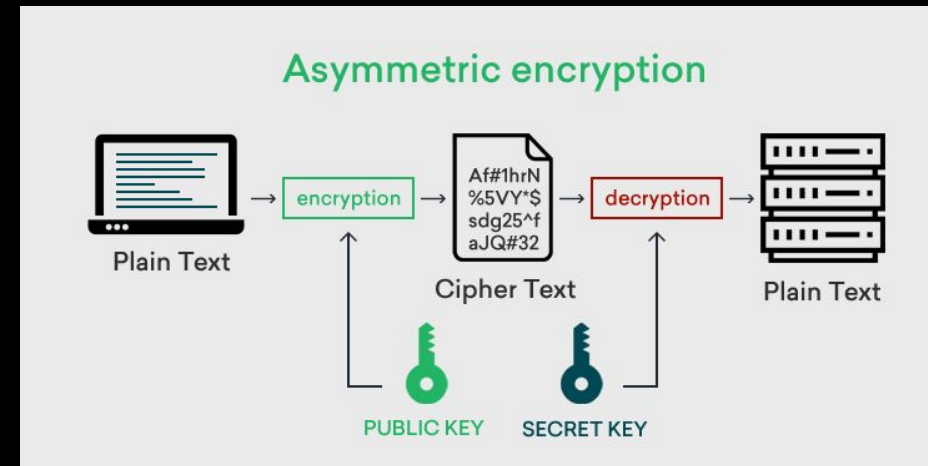
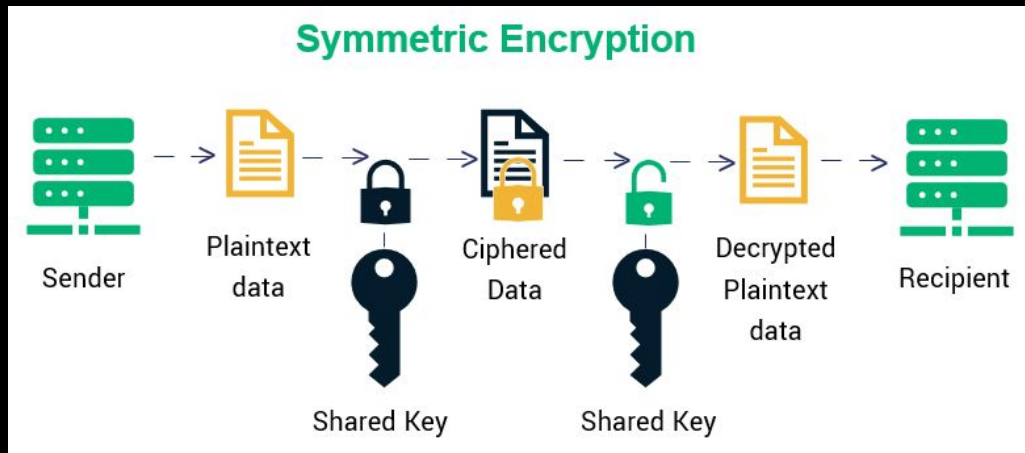
# Packet Sniffing Countermeasures

- Require authentication
  - The packets are still in open air, if bad actors are in monitor mode, they can be sniffed.
- ... Hide your SSID ???
  - Doesn't make a difference, provides false sense of security
    - The packets are **still** in open air, many frames still contain the SSID information.
  - Bad actors can send out various requests to find hidden networks.
- Send packets directionally
  - Can still be sniffed
  - Directionality has a cone of dispersion
    - You can read from that cone.
    - WokFi as a receiver
      - 3-5 km typically in decent conditions
      - With a 7° cone (at 4km), you could be
      - At 4km, you could be 200m away!
- Encryption



# Encryption solutions confidentiality attacks

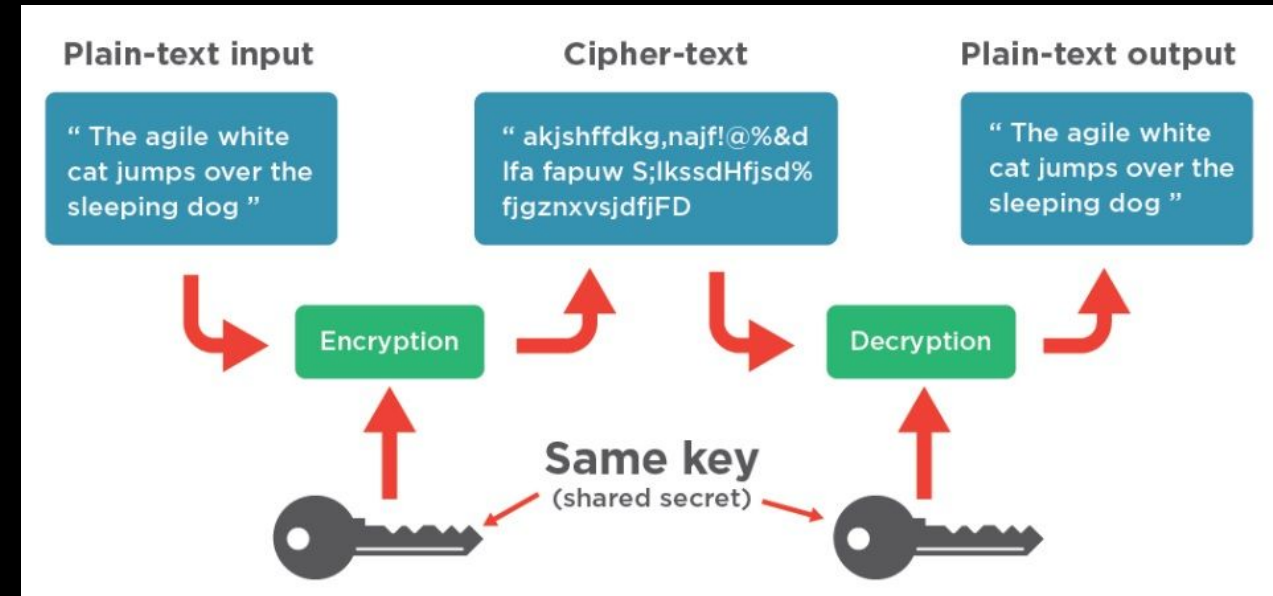
- Two main types of encryption
  - Symmetric key encryption
    - AES
    - Diffie Hellman Key Exchange
  - Asymmetric key encryption
    - RSA
- Other networking specific solutions
  - TKIP, EAP, SAE, 802.1x (EAP)

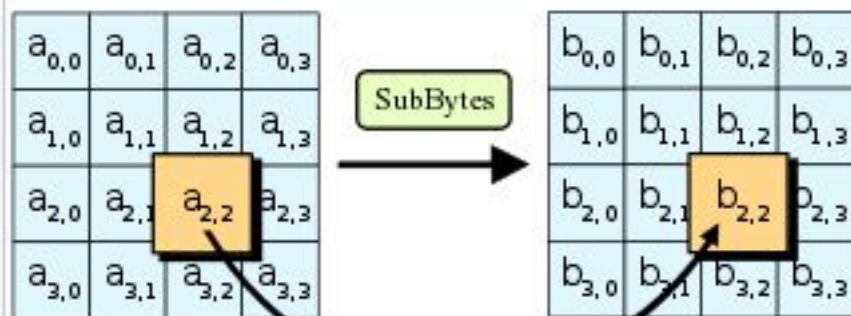




# AES (256 Bit)

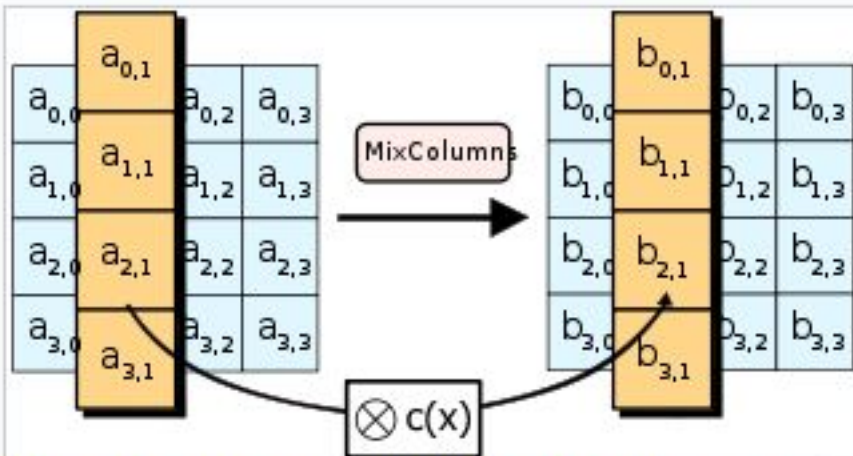
- Advanced Encryption Standard
- Block based encryption
- Symmetric Key Encryption
- Extremely fast
- Known vulnerabilities
  - Known plaintext attack
  - Not extremely effective
- Wireless makes shared secret complicated
  - Has to generate shared key somehow.





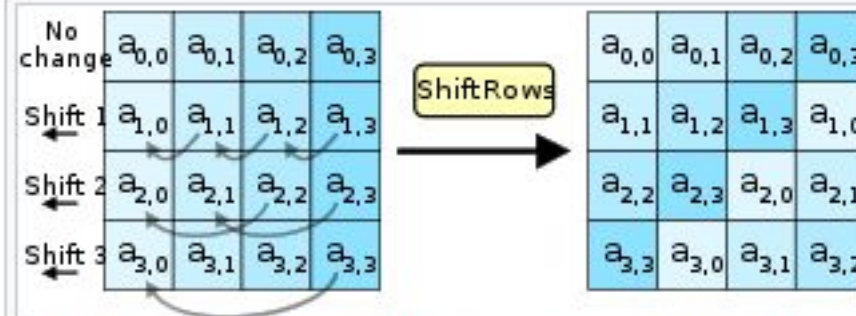
In the SubBytes step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table,  $S$ ;  $b_{ij} = S(a_{ij})$ .

### STEP 1, SubBytes



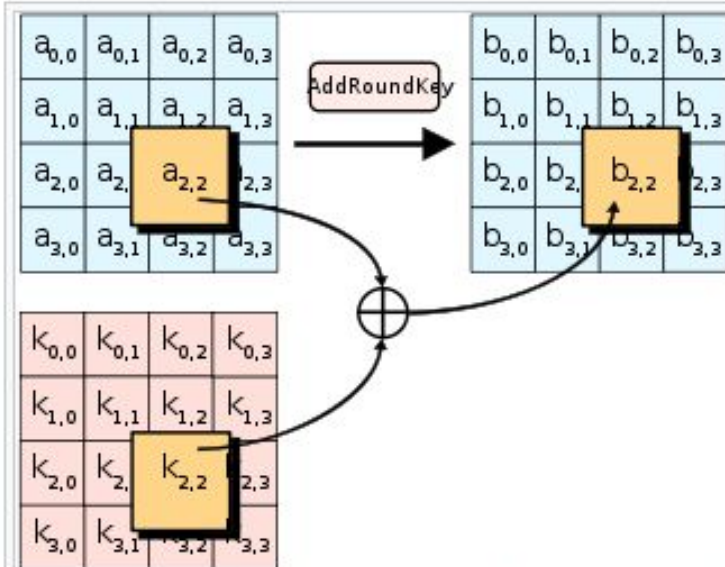
In the MixColumns step, each column of the state is multiplied with

### STEP 3, MixColumns



In the ShiftRows step, bytes in each row of the state are shifted cyclically to the left. The number of places each byte is shifted differs incrementally for each row.

### STEP 2, ShiftRows

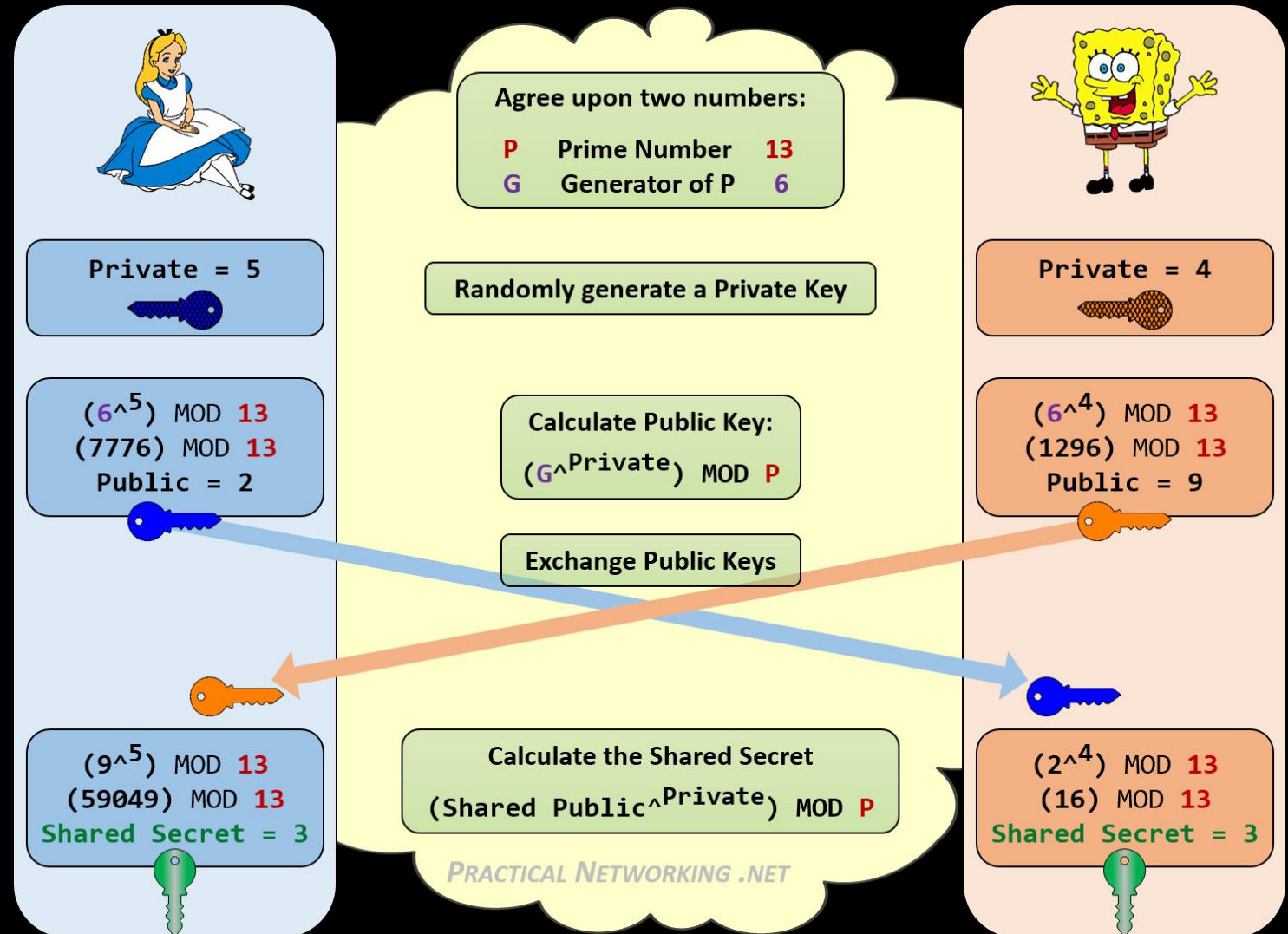
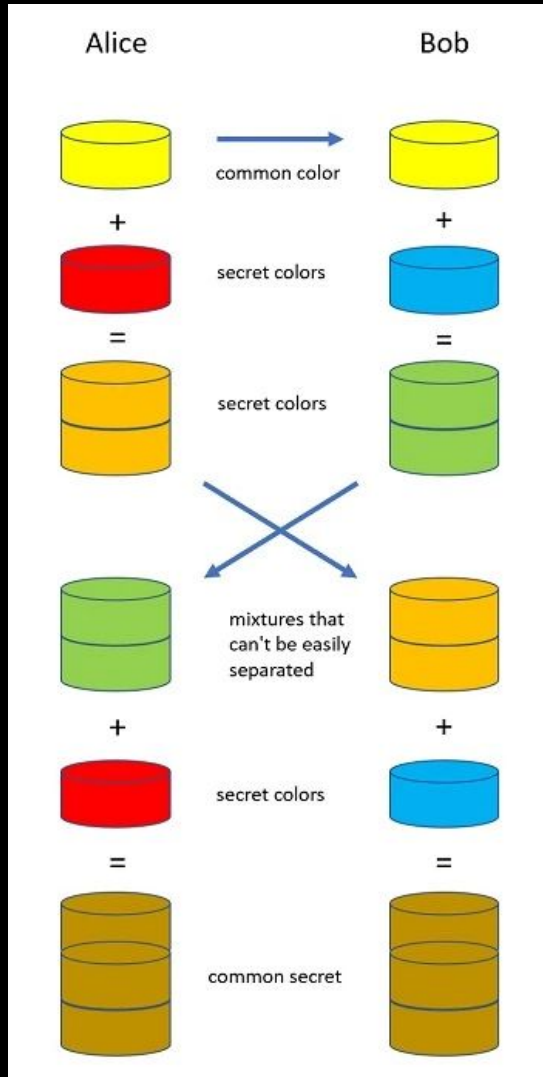


In the AddRoundKey step, each byte of the state is combined with the round key using the XOR operation ( $\oplus$ )

### STEP 4, AddRoundKey

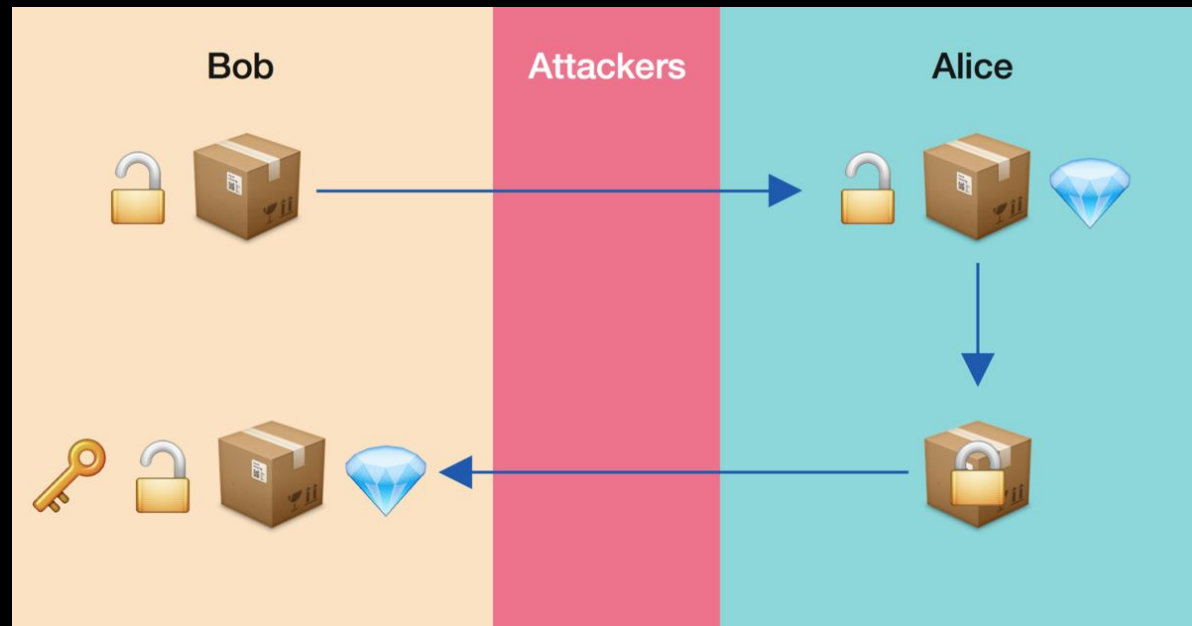


# Diffie Hellman Key Exchange



# RSA (2048 Bit)

- RSA (Ron Rivest, Adi Shamir, and Leonard Adleman)
- Two keys, one public key, one private key
  - Large prime numbers
  - $23 * 11 = 253$
  - What are 253's factors?
- ssh-keygen
  - Try it out yourself



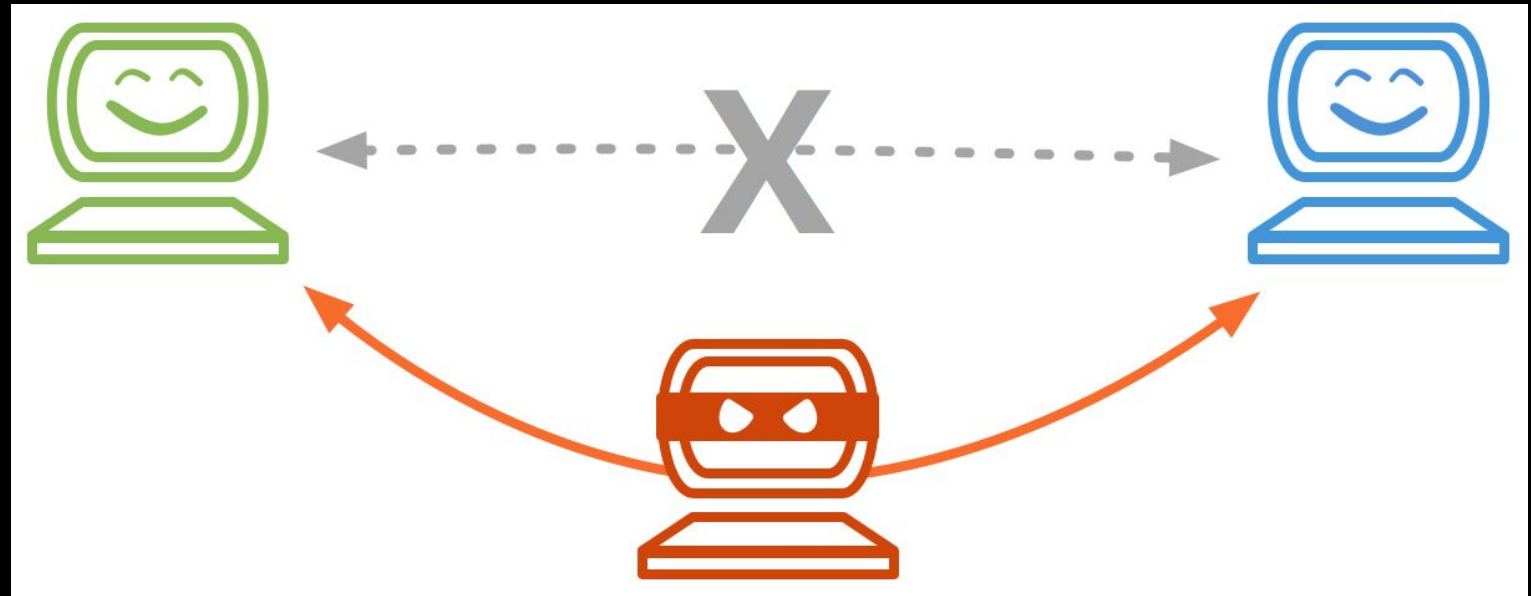


# Integrity Attacks



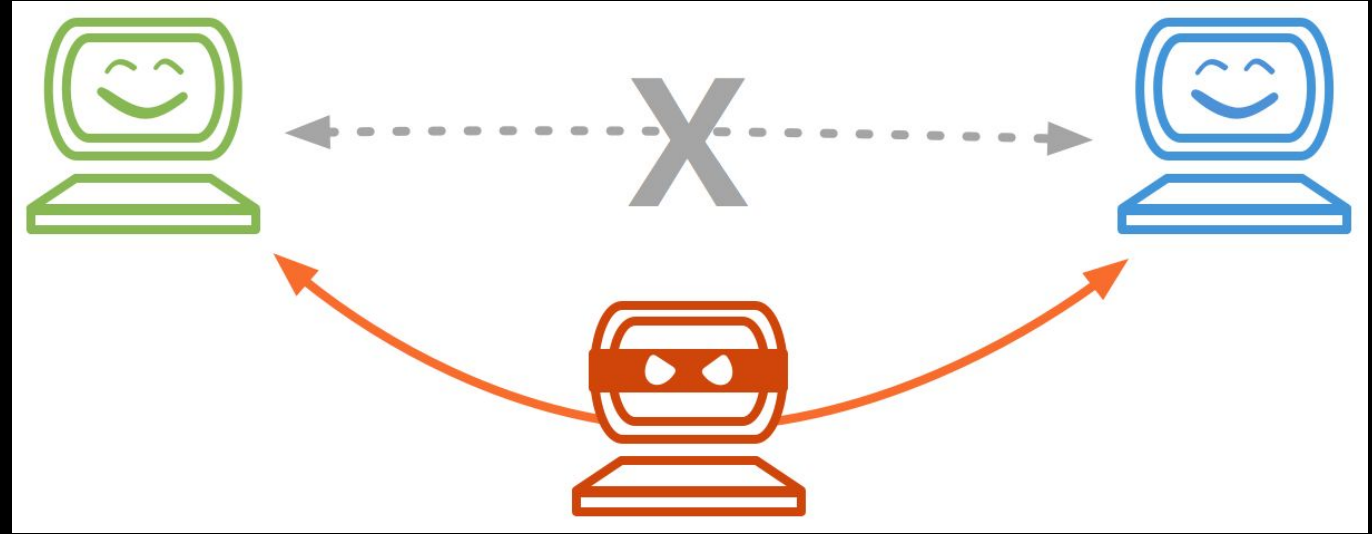
# General network integrity attacks

- Integrity assures your data is not tampered, and is from the correct person.
- Off path attacker
  - Can sniff and send, but can't tamper.
- Man-In-The-Middle
  - Put yourself in-between Alice and Bob
- Replay attacks (common)
  - Alice sends key to router
  - Use same key with your information.
  - <https://www.youtube.com/watch?v=ZoG5jJ3E8rg>



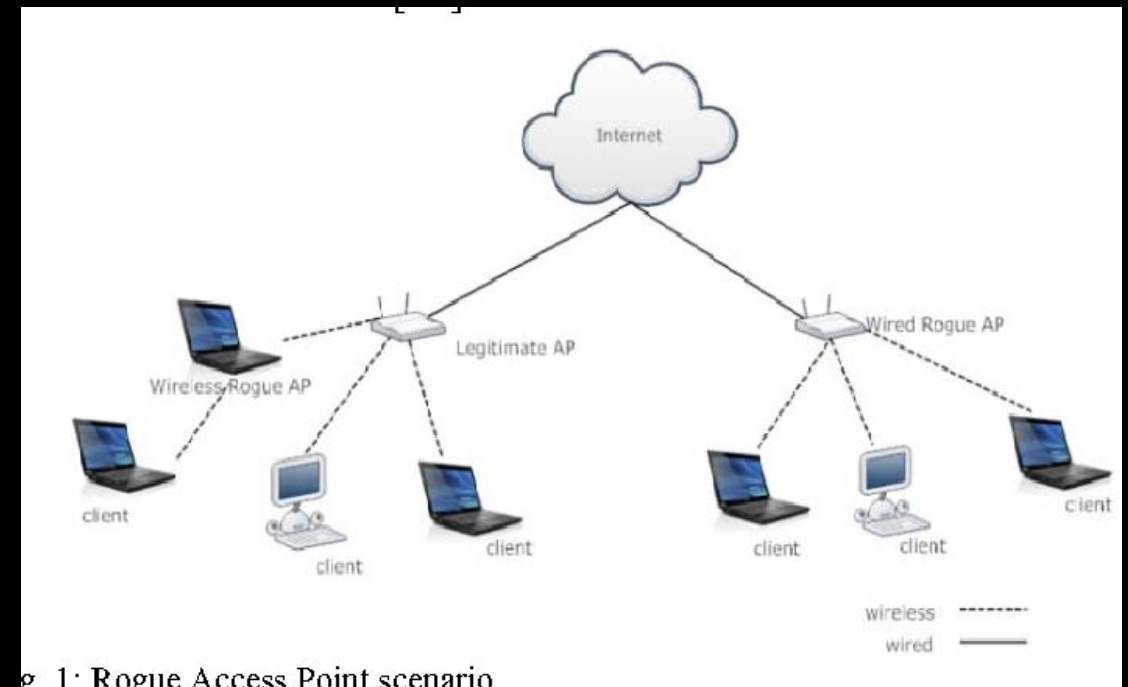
# Wireless Integrity Attacks

- Evil twin attack
  - KARMA attack
- Rogue Femtocells
  - Cellular
- Deauthentication Attack
- Replay Attack
- Cracking WiFi security protocols.



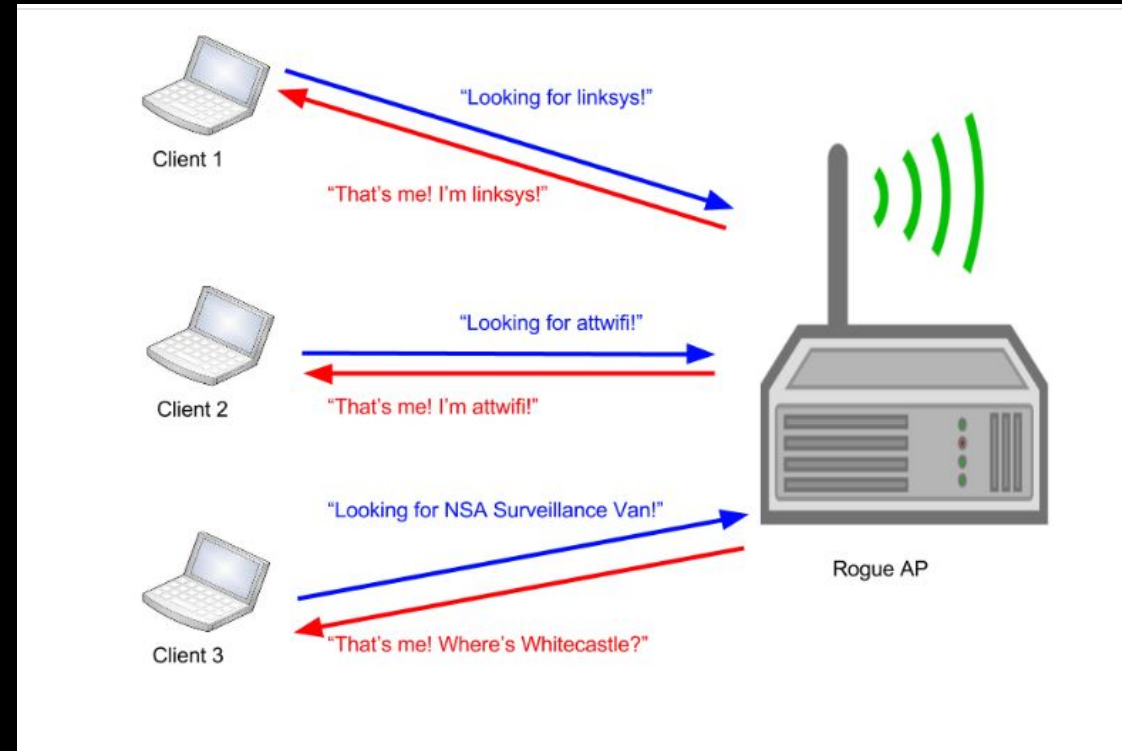
# RAP

- Rogue Access Points
  - Anything that isn't yours
- Not necessarily malicious
  - Could just be someone else's wifi.
- 2nd Definition
  - Any way to get into a secured network without consent
  - Backdoor




# Evil Twin (KARMA attack)

- Evil Twin Attack
  - First come, first serve
- KARMA Attack
  - Applied evil twin attack
- Wireless makes this easy
  - First come first serve
  - Sniffing



# Rogue Femtocell

- Rogue Femtocell
  - Cellular
  - As seen in Mr. Robot S2
- Wifi Pineapple
  - <https://shop.hak5.org/products/wifi-pineapple>



### WIFI PINEAPPLE

\$99.99

The industry standard pentest platform has evolved. Equip your red team with the WiFi Pineapple® Mark VII. Newly refined. Enterprise ready.

Automate WiFi auditing with all new campaigns and get actionable results from vulnerability assessment reports. Command the airspace with a new interactive recon dashboard, and stay on-target and in-scope with the leading rogue access point suite for advanced man-in-the-middle attacks.

Next-gen network processors combine with multiple role-based radios and the Hak5 patented PineAP suite to deliver impressive results. Hardened and stress tested for the most challenging environments.

The new WiFi Pineapple Mark VII features incredible performance from a simple web interface with an expansive ecosystem of apps, automated pentest campaigns, and Cloud C2 for remote access from anywhere.

MARK VII BASIC \$99.99	MARK VII TACTICAL \$119.99
KISMET CASE MOD \$49.99	KISMET LED MODULE \$14.99
<del>MK7AC MODULE \$39.99</del>	<del>ENTERPRISE \$349.99</del>

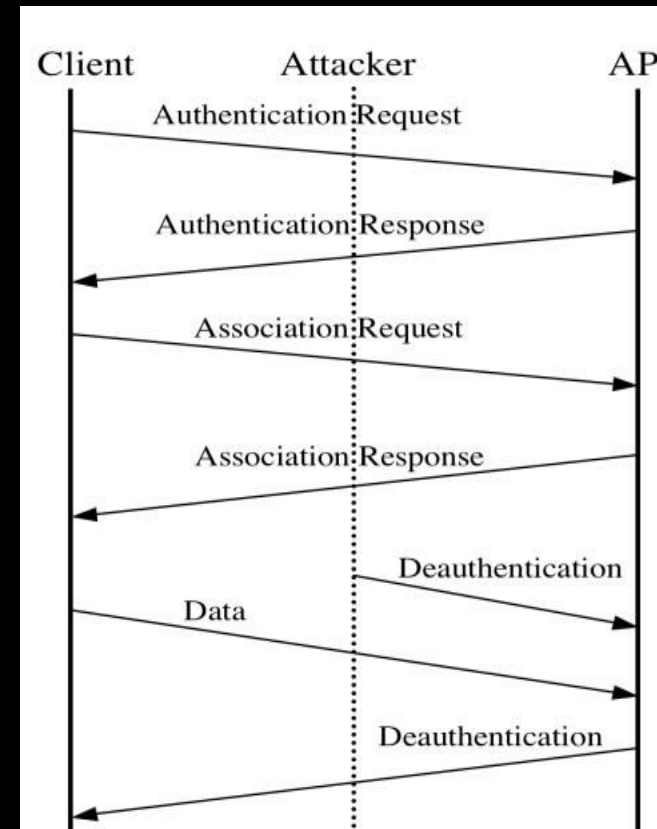
1

ADD TO CART



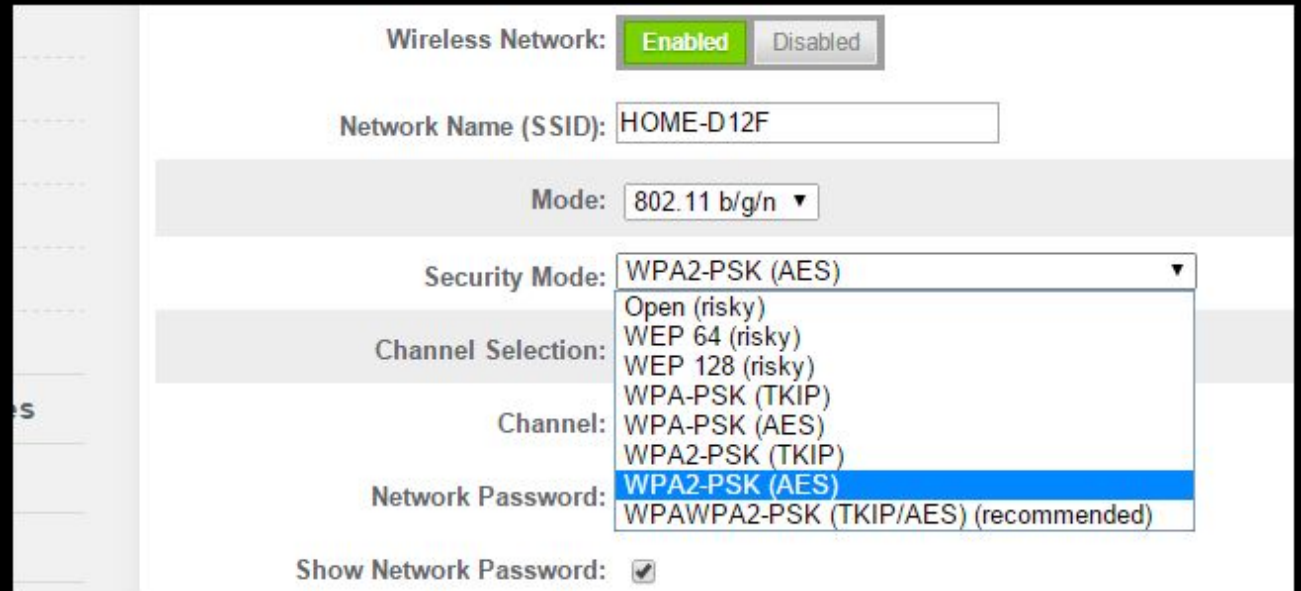
# Other Integrity Attacks

- Deauthentication attack
  - Boot users off whatever wifi they are using.
- Replay attacks
  - Made easier by wireless sniffing.
- Protocol Cracking



# WiFi Security Protocols

- WEP
  - Wired Equivalent Privacy
  - Encrypts with **RC4**
  - No key management
- WPA
  - Wi-Fi Protected Access
  - 4 Way key handshake
  - Built upon WEP
- WPA 2 Handshake (4 Way)
  - PBKDF2-SHA1 hash
  - **This is what we currently use**
- WPA 3
  - Currently being implemented worldwide



The screenshot shows a wireless network configuration window. At the top, there are two buttons: "Enabled" (highlighted in green) and "Disabled". Below this, the "Network Name (SSID)" is set to "HOME-D12F". The "Mode" is set to "802.11 b/g/n". The "Security Mode" dropdown menu is open, showing a list of options: "Open (risky)", "WEP 64 (risky)", "WEP 128 (risky)", "WPA-PSK (TKIP)", "WPA-PSK (AES)", "WPA2-PSK (TKIP)", "WPA2-PSK (AES)" (which is highlighted in blue), and "WPAWPA2-PSK (TKIP/AES) (recommended)". The "Channel Selection" and "Channel" fields are empty. The "Network Password" field is empty. At the bottom, there is a "Show Network Password" checkbox which is checked.





	WEP	WPA	WPA2	WPA3
Brief description	Ensure wired-like privacy in wireless	Based on 802.11i without requirement for new hardware	All mandatory 802.11i features and a new hardware	Announced by Wi-Fi Alliance
Encryption	RC4	TKIP + RC4	CCMP/AES	GCMP-256
Authentication	WEP-Open WEP-Shared	WPA-PSK WPA-Enterprise	WPA2-Personal WPA2-Enterprise	WPA3-Personal WPA3-Enterprise
Data integrity	CRC-32	MIC algorithm	Cipher Block Chaining Message Authentication Code (based on AES)	256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)
Key management	none	4-way handshake	4-way handshake	Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA)

# aircrack-ng (WEP, WPA, WPA 2-PSK, RC4)

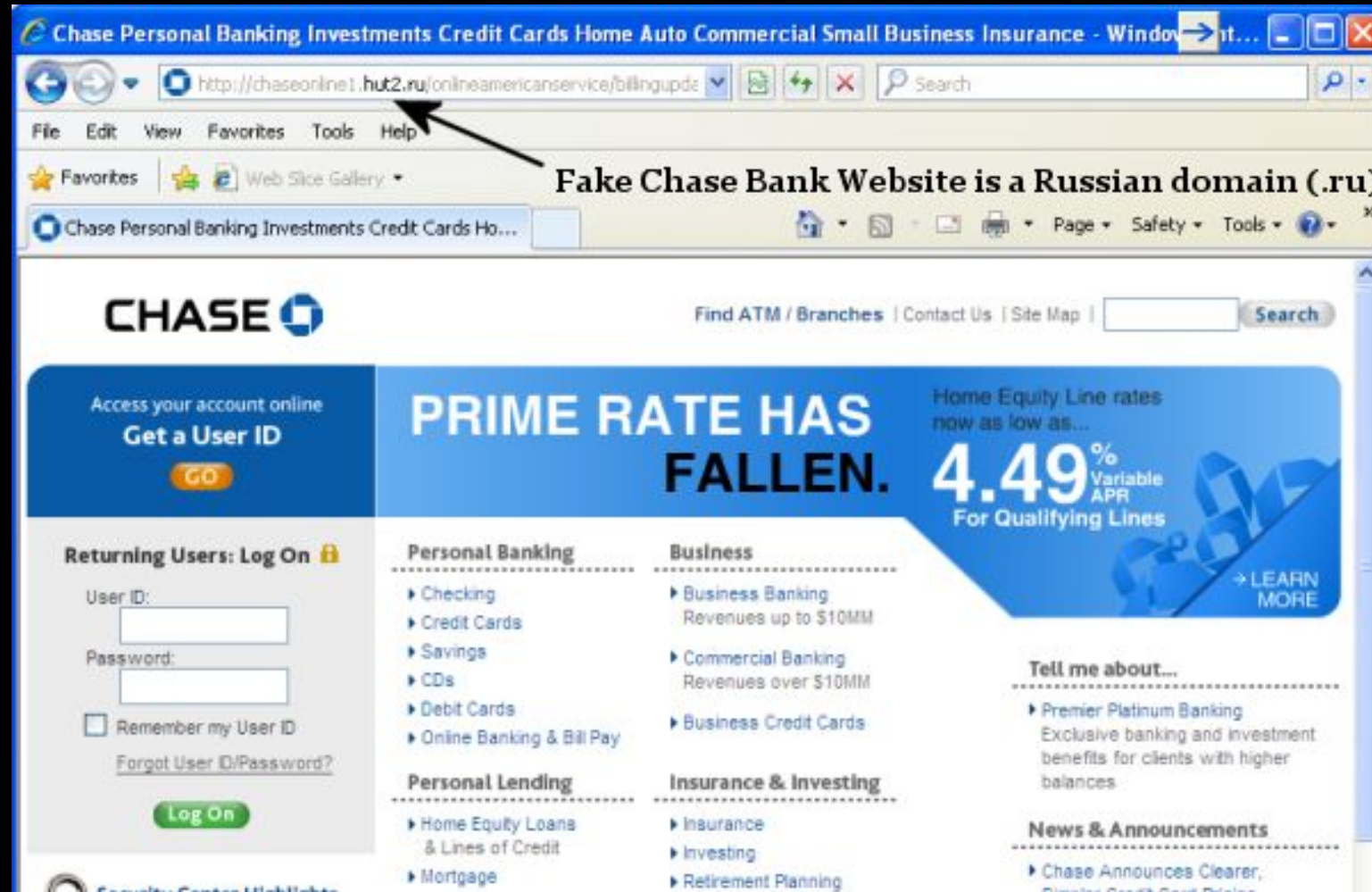
- All in 1 key cracking program
- Many of these protocols are built upon RC4
  - RC4 is provably insecure.
- Crack time
  - WEP: any in a few minutes
  - WPA, as fast as WEP
  - WPA 2 Handshake (4 Way)
    - PBKDF2-SHA1 hash
  - WPA2 cracked in as little as 10 minutes. Avg a few days
  - This is what most of you use **right now.**

```
Aircrack-ng 0.5
E00:00:15:1 Tested 451275 keys (got 566683 IVs)
1 2 3 4
KB depth byte(vote)
0 0/ 1 AE< 50> 11< 20> 71< 20> 10< 12> 84< 12> 68< 12>
1 1/ 2 5B< 31> BD< 18> F8< 17> E6< 16> 35< 15> CF< 13>
2 0/ 3 7F< 31> 74< 24> 54< 17> 1C< 13> 73< 13> 86< 12>
3 0/ 1 3A< 148> EC< 20> EB< 16> FB< 13> F9< 12> 81< 12>
4 0/ 1 03< 140> 90< 31> 4A< 15> 8F< 14> E9< 13> AD< 12>
5 0/ 1 D0< 69> 04< 27> C8< 24> 60< 24> A1< 20> 26< 20>
6 0/ 1 AF< 124> D4< 29> C8< 20> EE< 18> 54< 12> 3F< 12>
7 0/ 1 9B< 168> 90< 24> 72< 22> F5< 21> 11< 20> F1< 20>
8 0/ 1 F6< 157> EE< 24> 66< 20> EA< 18> DA< 18> E0< 18>
9 0/ 2 8D< 82> 7B< 44> E2< 30> 11< 27> DE< 23> A4< 20>
10 0/ 1 A5< 176> 44< 30> 95< 22> 4E< 21> 94< 21> 4D< 19>

KEY FOUND! [ AE:5B:7F:3A:03:D0:AF:9B:F6:8D:A5:E2:C7 ]
```

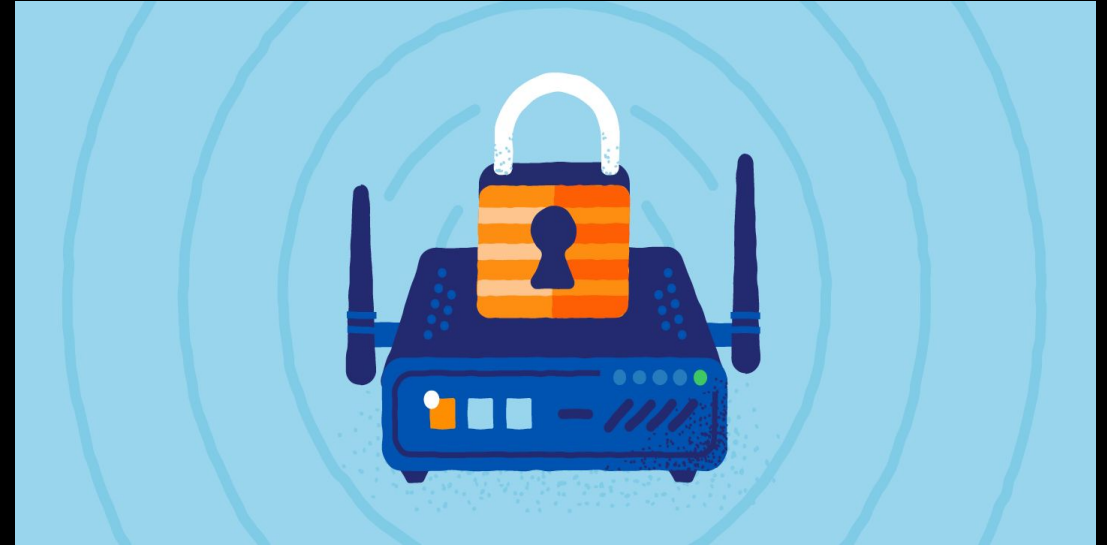
# What can you do with this?

If you are a man-in-the-middle, you have almost full control over the system.



# Countermeasures to Integrity attacks

- Proper authentication procedures
  - WPA3, PIKs
- Make it harder for the attacker
  - Spray out lots of fake WiFi Access Points
  - More complex passwords on your wifi
- Use stronger version of 802.11i
- Again, **Encrypt your data.**
  - TKIP (Temporal Key Integrity Protocol)
    - Wrapped around WEP
    - Insecure
- Message authentication codes.



# Availability Attacks





# Attacks on Availability

- DOS (Denial of service)
  - Send out garbage packets
  - Turn on the microwave
  - Frequency blasting ([Qualcomm Atheros C](#))
- Deauthentication attacks
  - Force people off the network.
  - Can be used
- Mitnick Attack
  - Application of a DOS
  - Stop server from connecting so the client would give information to Mitnick
    - Ultimately gained root access

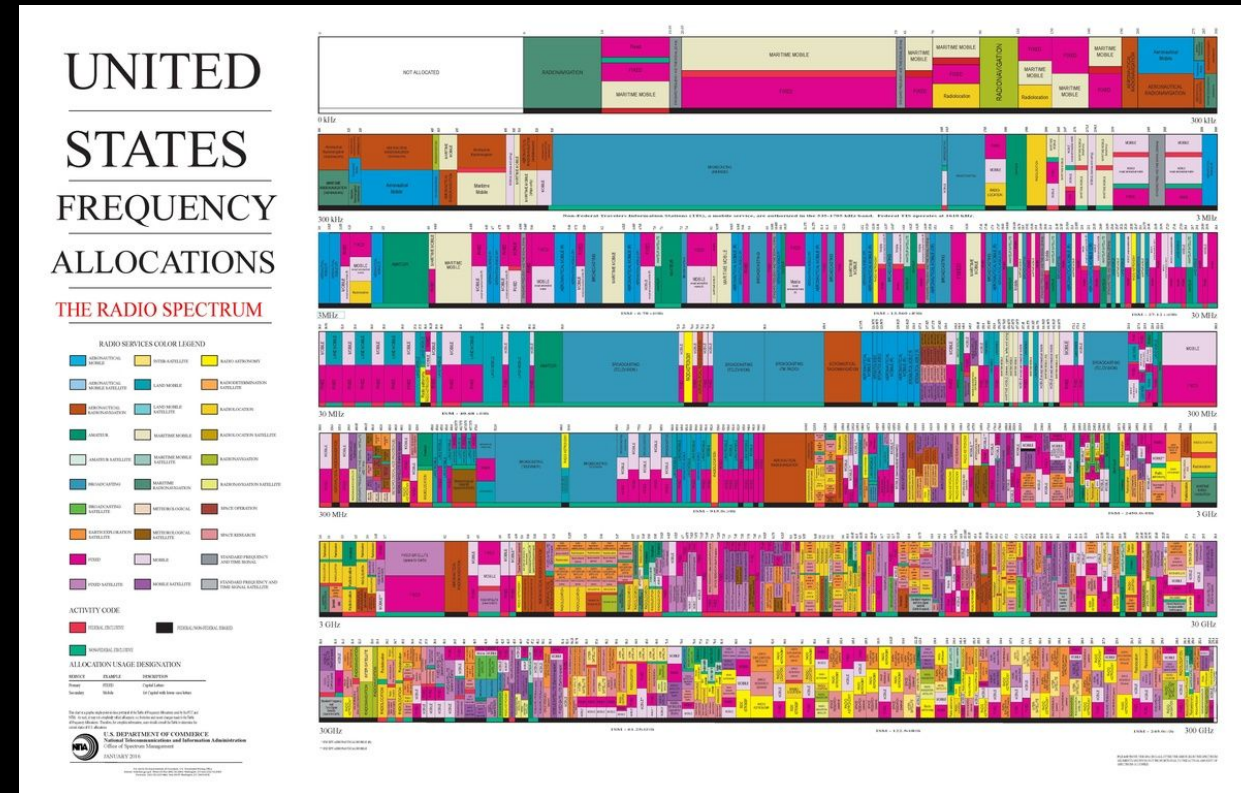


# Solutions to availability

... Not really any

# Use illegal bandwidths?

(This is where the law has not caught up)



# Remember the Human

- Wireless technical solutions only go so far
  - Human error and gullibility will always be the weakest link.
- Training
  - Teach employees and partners about Social Engineering
  - Phishing awareness, general security awareness
- Common Sense Security Measures
  - 2FA
  - Enforce HTTPS
  - Adblock, Scriptblock
  - Only connect to things you trust
  - Update to latest security standards
    - WPA 3 enforced as of July 2020.
  - Have an appropriate threat model
- **Never connect to open WiFi**



Isn't this just the worst stock photo ever?



# Sources

[https://courses.cs.washington.edu/courses/csep590/05au/whitepaper\\_turnin/WiFi%20-%20final.pdf](https://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/WiFi%20-%20final.pdf)

<https://www.networkworld.com/article/2303872/wireless-attacks--damage-and-costs.html>

<https://www.afcea.org/content/secure-wi-fi-enters-battlefield>

[https://armypubs.army.mil/epubs/DR\\_pubs/DR\\_a/pdf/web/ARN4771\\_Pam25-2-9\\_Final\\_Web.pdf](https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN4771_Pam25-2-9_Final_Web.pdf)

<https://aplits.disa.mil/processAPList.action>

<https://www.bbc.com/news/technology-42853072>

<https://www.statista.com/statistics/471264/iiot-number-of-connected-devices-worldwide/>

<https://www.pcmag.com/news/how-much-does-a-data-breach-cost>

<https://www.solarwinds.com/network-performance-monitor/use-cases/wifi-packet-sniffer>

<https://www.youtube.com/watch?v=JqQn6OD5rno>

[https://wiki.wireshark.org/CaptureSetup/WLAN#Turning\\_on\\_monitor\\_mode](https://wiki.wireshark.org/CaptureSetup/WLAN#Turning_on_monitor_mode)

[https://en.wikipedia.org/wiki/Monitor\\_mode](https://en.wikipedia.org/wiki/Monitor_mode)

<https://en.m.wikipedia.org/wiki/WoWiFi>

<https://www.amazon.com/WiOpsy-802-11ac-Windows-Sniffer-IntelliGraphics/dp/B0821JWP9K/>

<https://www.youtube.com/watch?v=JqQn6OD5rno>

<https://www.amazon.com/SimpleWiFi-G2424-Directional-High-Speed-Antenna/dp/B00NQGVMSF>

<https://media.defcon.org/DEF%20CON%2026/DEF%20CON%2026%20presentations/DEFCON-26-Damien-Cauquil-Secure-Your-BLE-Devices-Updated.pdf>

<https://fmdx.pl/5ghz-wardriving/>



# Next Meetings

## Thursday Meeting: Windows Environments

- Learn about the most common environments in the world
- Topics Covered: SMB, Active Directory, Ldap, DC, Windows Vulns

## Weekend Seminar: None

- Go home
- It is fall break

