NC-EXPERT
CREATING EXPERTS

Conundrums and Enigmas in Wi-Fi Security

Phil Morgan
CTO NC-Expert

Presented at: Ekahau Day

Thursday, 21 March, 2024

About NC-Expert

NC-Expert was founded in 2011 in Silicon Valley, California, USA

- NC-Expert is a consortium of industry experts in multiple fields, including wireless, security/cybersecurity, networking, and collaboration
- NC-Expert is a trusted Learning Partner of Cisco, CompTIA, ISC^2, CWNP, CertNexus and EC-Council (Cyber Security)
- NC-Expert is a partner and member of the Wireless Broadband Alliance (WBA)
- NC-Expert consults and trains for Fortune 50 companies, military, government departments, and enterprise customers worldwide
- NC-Expert has helped thousands of students gain industry certifications and enhance their careers

About Phil Morgan

CCIEx2 #5224, CWNE #322, CWISE #4

- Also: CEH, N+, S+, etc.
- Spent too much time doing exams and certs
- Has worked with computers and networks for >30 years
- Working with wireless since late 1990's, remembers "b" being the new thing in town! ☺
- When not working with wireless, Phil is usually found entertaining his German Shepherd dog "Max"

Contacts

Presenter

- Email: philmorgan@nc-expert.com
- LinkedIn: https://www.linkedin.com/in/morganphil
- Twitter: @CCIE5224

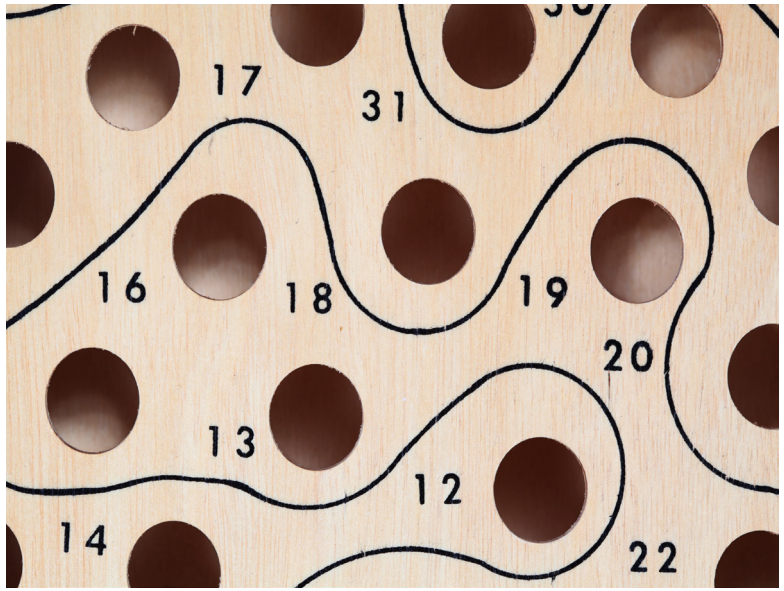
Blogs

- https://tinyurl.com/ncxphilblog
- https://wizardofwifi.com (link to 3 of my blogs: Wi-Fi 6E, 7, and security)

Outline: Conundrums and Enigmas in Wi-Fi Security

Webster's dictionary...

- Conundrum: an intricate and difficult problem
- Enigma: something hard to understand or explain



Outline (Cont.)

Some of the biggest conundrums we have today:

- How do we stay safe in an ever-evolving world?
- How do we balance security with convenience?
- How do we remain secure without annoying our users?

Because combining Wi-Fi and Security is difficult (the Enigma)

Security is Important

Security is important to us

- or, at least, it should be

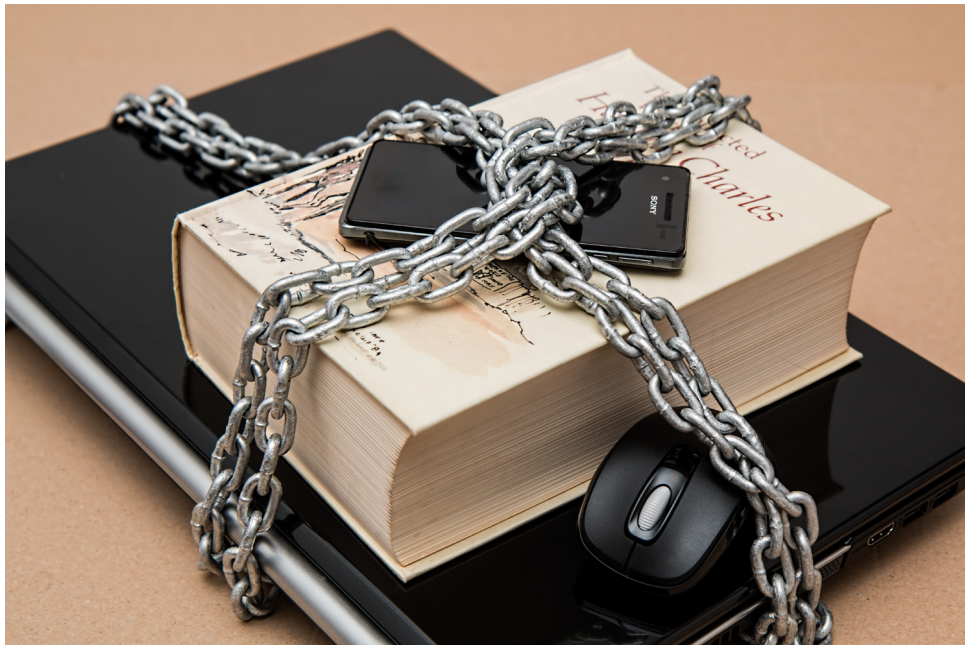
Basic Security Premise

“Inconvenience is a hacker’s best friend” – Phil Morgan

- **Every time I say the word “Inconvenient”, feel free to shout this back at me!**

We are not paranoid enough

Longer is generally better than complex



Security Terms (Defined Simply!)

Vulnerability
- a weakness, or flaw or error

Threat
- a potential use of vulnerability to cause damage

Attacker or Threat Agent
- the bad guy

Exploit
- an attacker using a threat (exploiting a vulnerability)

Risk
- likelihood of success, compared to damage caused
- the potential for loss

Loss
- how much it costs us

Top Threats

US Cybersecurity & Infrastructure Security Agency

UK National Crime Agency

UK National Cyber Security Centre

- Malware, Phishing and Ransomware
- DOS (DDOS)
- Inadequately securing your company (and network)
- Lack of proper information sharing and reporting
- Criminal Organizations – organized crime
- Nation State Threat Actors
- Rogues/Shadow IT
- Out-of-date software and firmware

Other Threats

US Cybersecurity & Infrastructure Security Agency

- Spoofing
- Social Engineering
- Configuration errors
- Poor cyber hygiene
- Identity Stealing
- Vulnerabilities Clients and Cloud
- Unprepared
- Insider Threats

UK National Crime Agency

UK National Cyber Security Centre

- Identify Crown jewels
- Phishing
- Giving users too much power

  (We need to be like parents, keep them safe)
- Tailgating
- USB attacks
- MITM/PITM
- 0Day
- Physical Security

Recent Threats

Within the last month or so...

Recent Outage

- Facebook/Meta/Instagram, Comcast, LinkedIn

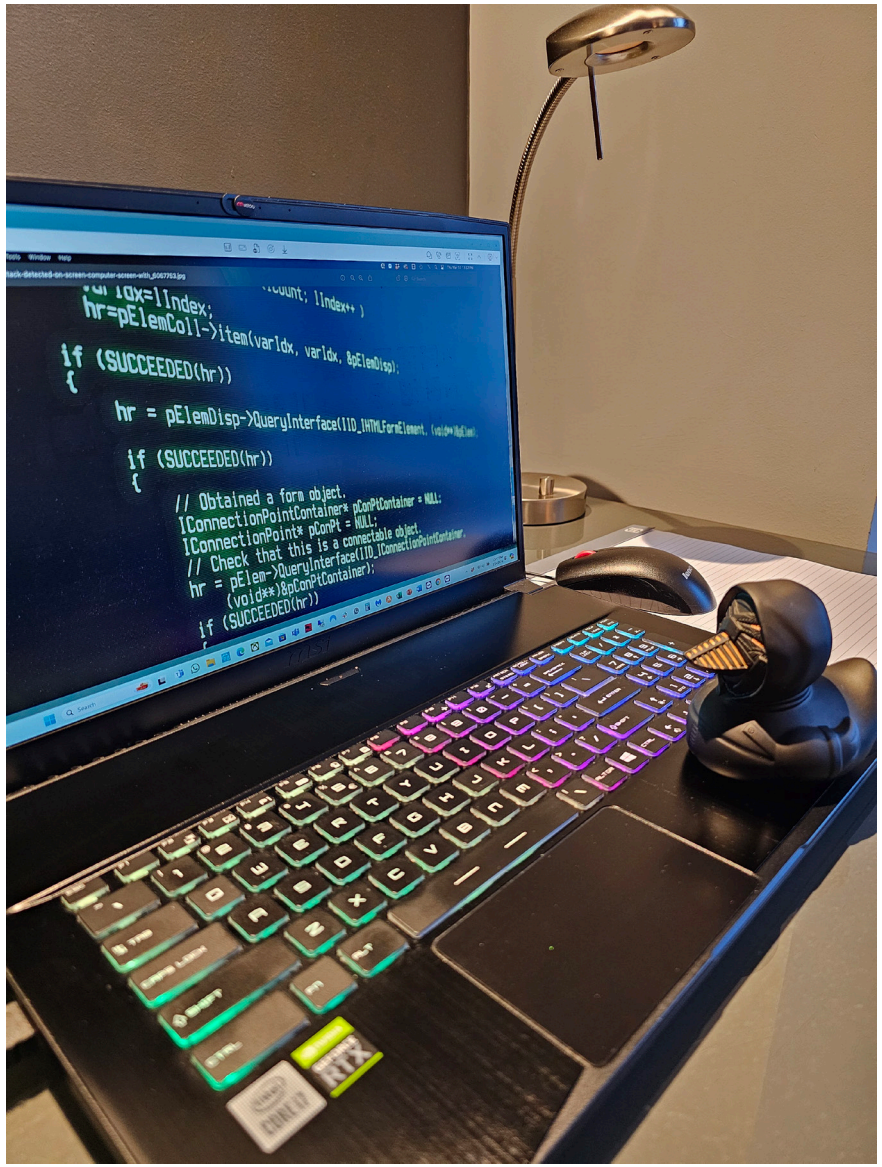
Cronos

- Feb 24 Lockbit Ransomware takedown
- https://cybersixgill.com/behind-the-headlines/march-2024/Operation-Cronos-v-LockBit-The-battle-rages-on

WPA supplicant flaw

- Bypasses 2nd phase of PEAP

Others?



Threats: the Reality

Online marketplace

RAAS

What do “they” want

To steal your:

- technology
- money
- data
- customers
- bitcoin!

Cyber Health

We need Security

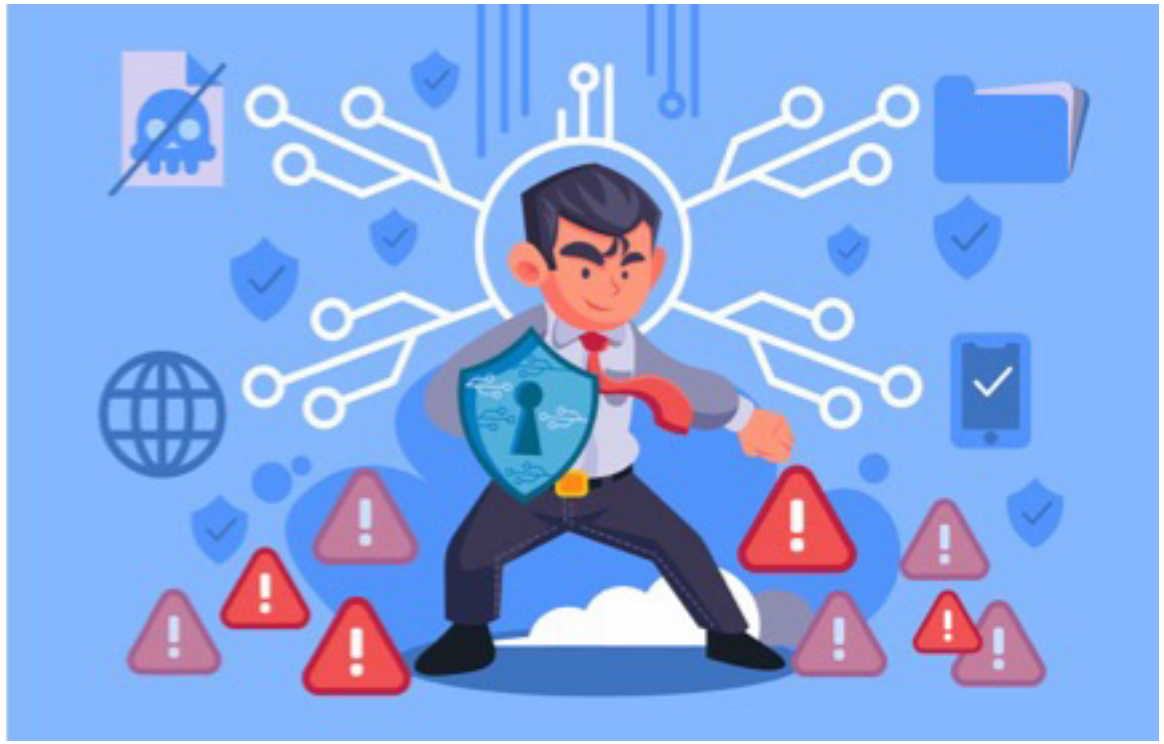
We need to Test our security

- Pentesting
- Audit

VPNs

Safe Guest Networking

- OpenRoaming



Trojan Devices

NEW

O.MG CABLE

$119.99

FEATURE TIER

BASIC | PLUS | ELITE (EARLY ACCESS)

ACTIVE END

USB-A | USB-C | DIRECTIONAL C TO C

PASSTHROUGH END & BLACK OR WHITE

LIGHTNING (WHITE) | USB-C (BLACK) | USB-C (WHITE) | MICRO (BLACK)

1 ADD TO CART

Pay in 4 interest-free installments of $29.99 with shop Pay Learn more

Ships in 1-3 business day worldwide • Free US Shipping on orders >$250

All orders protected against loss, damage & theft

USB Ethernet adapters with covert backdoors

These seemingly innocent USB Ethernet adapters are discrete remote access toolkits and man-in-the-middles for penetration testers and systems administrators.

NO, NO, NO, NO, NO, NO, NO!
Mama Mia, Mama Mia, Mama Mia let me go…

Be careful plugging in anyone else's USB

- Be afraid!
- Be paranoid!
- Trust, but verify

Don't trust coffee shops and airports!

- Use a protector
  - or a battery pack!

Number 1 Threat

Uninformed Users

- Train them!
- Don’t write down password and leave around office
- Don’t give password out unnecessarily
- Establish a Security Policy
  - Enforce it
  - Review and keep up-to-date

Good Cyber Hygiene

PNL/Preferred Network List

*Note: only recent feature on iPhone

Examples:

MyHouse
Hotel_net
Airline
Coffee_shop
That_vacation_place_you_stayed_at_3years_ago
Your_friend_daves_house
MerGuest

Alert!

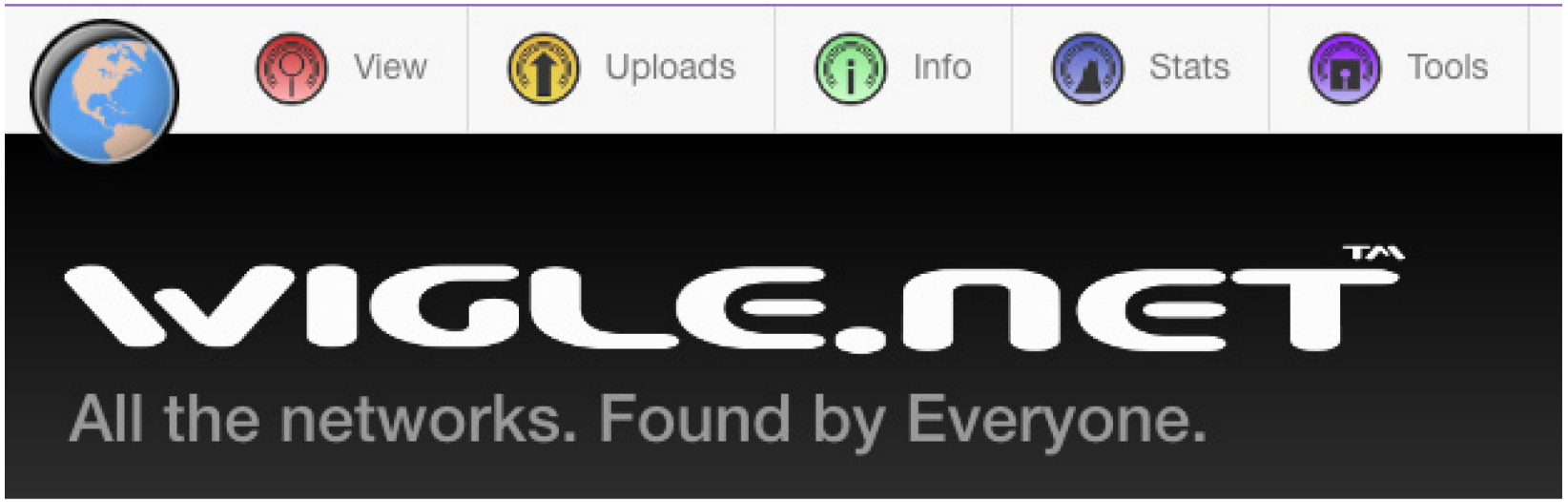
Do you know who knows your home Wi-Fi password?

- Friends?
- Family?
  - How many of you have kids?
    - All your kids' friends - they likely know it!

What security do you have at home?

- Me?...

Wiggle it, just a little bit…
and get in the Groove



Wi-Fi: Is it Secure?

Wi-Fi is Safe

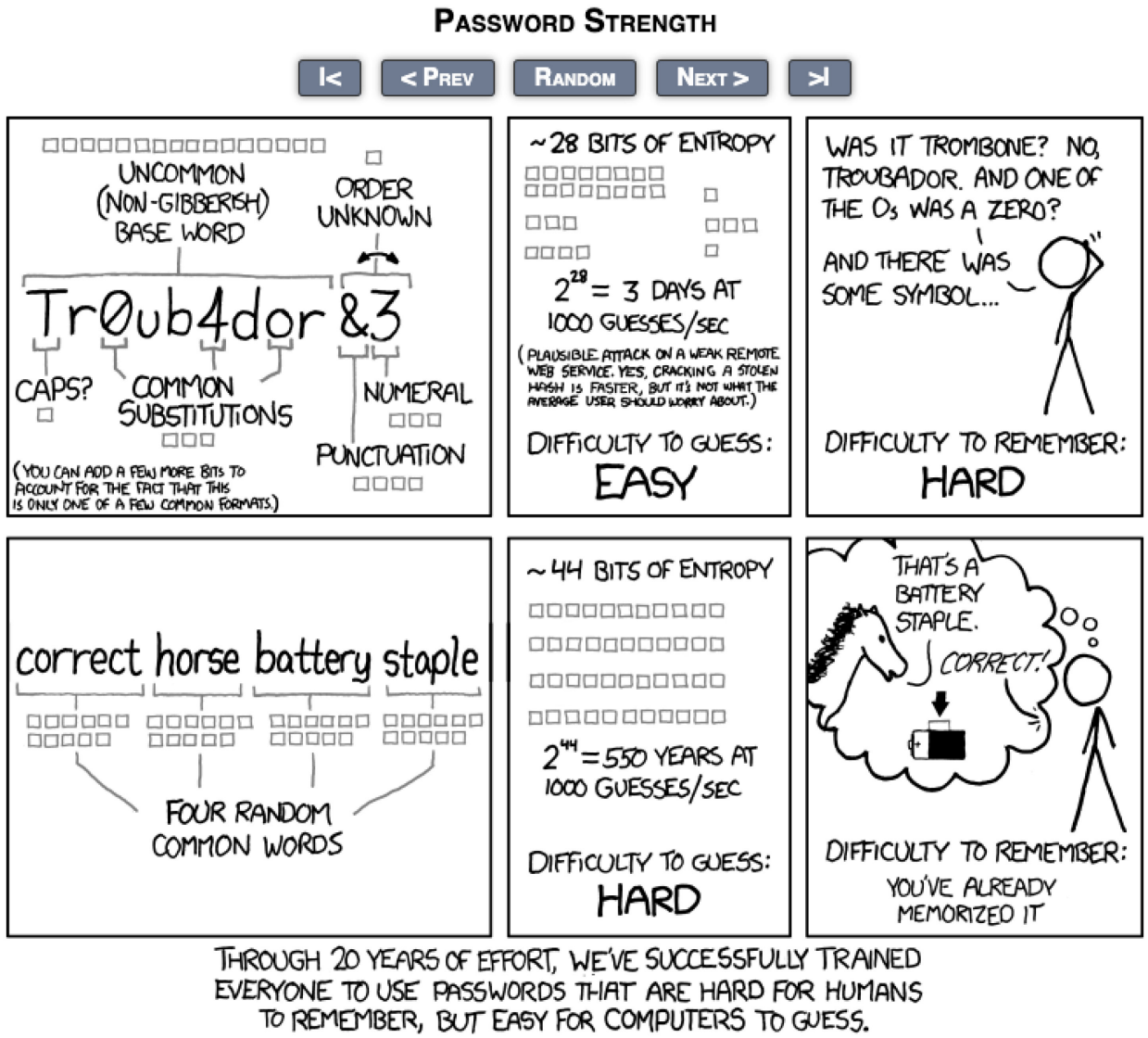
Wireless (**when configured correctly**) is as safe as ethernet

- Some would argue that it is safer

Famous Cartoon

https://xkcd.com/936/

Length vs Complexity



Longer is Better than Complex

https://www.sans.org/blog/nist-has-spoken-death-to-complexity-long-live-the-passphrase/ (2017)

https://www.zdnet.com/article/fbi-recommends-passphrases-over-password-complexity/ (2020)

https://resources.infosecinstitute.com/topic/password-security-complexity-vs-length/ (2021-update)

Perform the search **Is a longer password better than a complex one?** and see how many sites give you a “Yes” response.

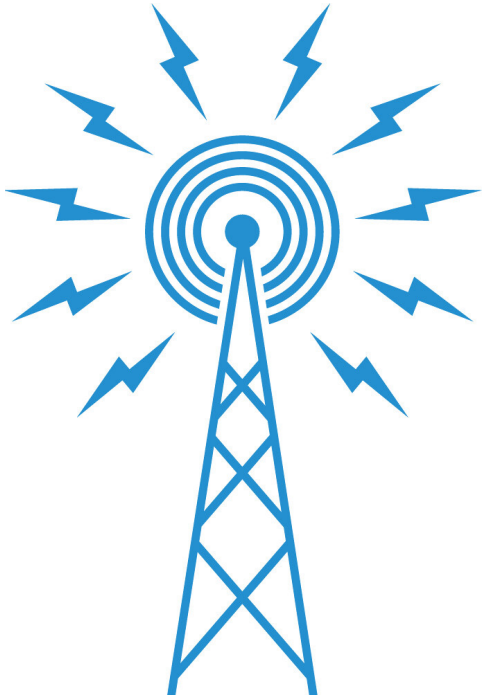
My search while preparing for this talk:

- Gov’t of Singapore “yes”, FBI ”yes”, NIST “yes”, gov.uk “yes”
- Daily Mail “yes”, The Guardian “yes”
- NCSC (GCHQ):

  https://www.ncsc.gov.uk/news/ncsc-lifts-lid-on-three-random-words-password-logic

Wi-Fi Security:
History and Theory

Wi-Fi is Broadcast Radio



Wi-Fi frames are broadcast, so anyone can hear

- NOT broadcast frames, broadcast as in TV and Radio

Scary fact: if I can increase my antenna gain, I can hear you from further away

- This means “distance away” should never be used as a security mechanism
- “It’s OK. The boundary of the network is too far away for anyone to pick up the signal” is NOT a valid security mechanism!

Clarity and Emphasis

Just because you cannot hear the signal outside an area with your device…

...does <u>not</u> mean I cannot hear it with my device!

Distance should NEVER be used as a security method

https://null-byte.wonderhowto.com/how-to/pick-antenna-for-wi-fi-hacking-0202742/

The Bogey Man IS out There!

There ***are*** monsters in the world

from whom we need to be protected!

A Favorite Quote

"Dance like nobody's watching,
encrypt like *everyone* is."

Werner Vogels

CTO@Amazon

Wi-Fi Foundations: Connecting to the Network

Finding the network:

- Beacons
- Probes
- 802.11k & 802.11v

Joining the network:

- Authenticate
- Associate

Security Options

Wi-Fi Security: History

WEP

- Easy to break

WPA

- Short term fix to WEP, while we worked on something better

WPA2

- The solution to WEP and WPA

WPA3

- Our hero!

Ekahau can help Decode the Complexities of Wi-Fi

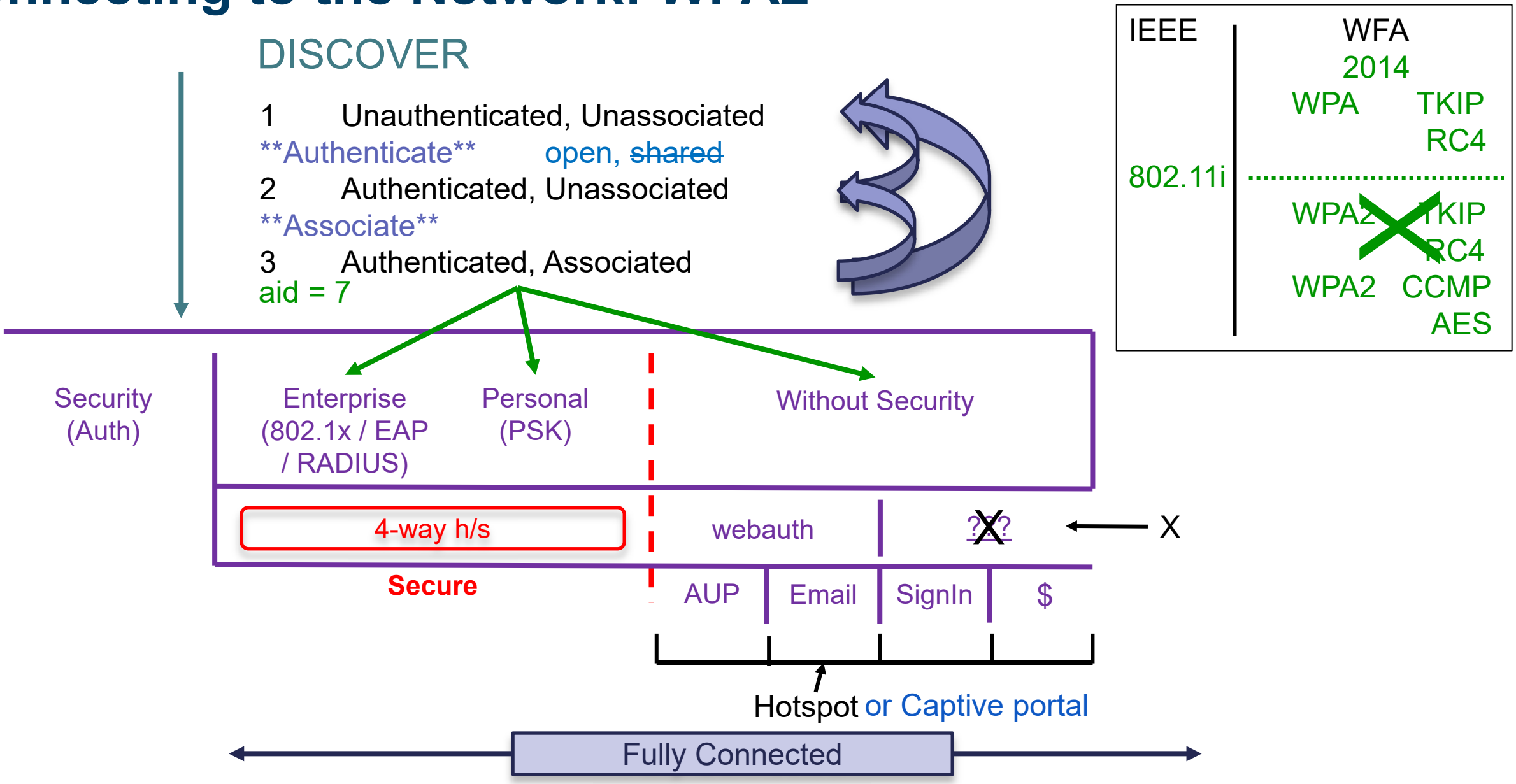
ekahau

12:14 Tue 1 Nov 81%

Scanning | All Networks | 2.4 | 5 | 6 | All | Open | Secure

SSID	SECURITY	MFP	MIN RATE	AMEND	GEN	BAND	CH	UTIL	BSS UTIL
WiFi-Ninjas-2 5C:5B:35:68:73:01	WPA2	Not Required	6 Mbps	k, v	4	2.4 GHz ISM	6	16.7%	20.0%
WiFi-Ninjas-Corp 5C:5B:35:68:72:E1	WPA2	Not Required	24 Mbps	k, v	6	5 GHz UNII-...	100(40)	6.2%	2.4%
WiFi-Ninjas-2 5C:5B:35:C9:A7:A1	WPA2	Not Required	6 Mbps	k, v	4	2.4 GHz ISM	11	6.4%	64.3%
WiFi-Ninjas-5 5C:5B:35:C9:A7:B1	WPA2	Not Required	12 Mbps	k, v	5	5 GHz UNII-1	44(40)	8.0%	7.5%
BTWifi-X 7A:86:20:35:B4:85	802.1X	Not Required	6 Mbps	v	5	5 GHz UNII-1	44(80)	8.0%	8.2%
[Hidden]-62:86:20:35:B4:80 62:86:20:35:B4:80	WPA2	Not Required	1 Mbps	v	4	2.4 GHz ISM	6	16.7%	18.0%
BTWi-fi 62:86:20:35:B4:85	Open	NA	1 Mbps	v	4	2.4 GHz ISM	6	16.7%	18.0%
Ekahau-Analyzer B4:A2:5C:04:CE:A0	802.1X	Required	1 Mbps	v	6	2.4 GHz ISM	6(40)	16.7%	22.4%
Ekahau-Analyzer B4:A2:5C:04:BA:A0	802.1X	Required	6 Mbps	v	6	5 GHz UNII-...	104(80)	4.4%	2.0%
SKYTPWL4 80:72:15:50:E1:12	WPA2	Not Required	1 Mbps	k, v	4	2.4 GHz ISM	11	6.4%	22.0%
SKYTPWL4 D0:58:FC:20:A8:0E	WPA2	Not Required	1 Mbps	k, v	4	2.4 GHz ISM	6	16.7%	NA
WN-Cambium-6 B4:A2:5C:04:C4:A0	WPA3	Required	574 Mbps	k	6	6 GHz UNII-5	5	19.3%	2.4%
BT-N8CPZ9 C0:D7:AA:81:24:A4	WPA2	Not Required	1 Mbps	v	4	2.4 GHz ISM	11	6.4%	54.9%
SKYYGHRD 00:A3:88:4A:52:BA	WPA2	Not Required	1 Mbps	k, v	4	2.4 GHz ISM	11	6.4%	36.9%
SKYYGHRD 0C:F9:C0:D0:4C:AE	WPA2	Not Required	1 Mbps	k, v	4	2.4 GHz ISM	11	6.4%	NA
SKYI1V1I 9C:31:C3:7E:E9:EA	WPA2	Not Required	1 Mbps	k, v	4	2.4 GHz ISM	11	6.4%	36.5%

Connecting to the Network: WPA2



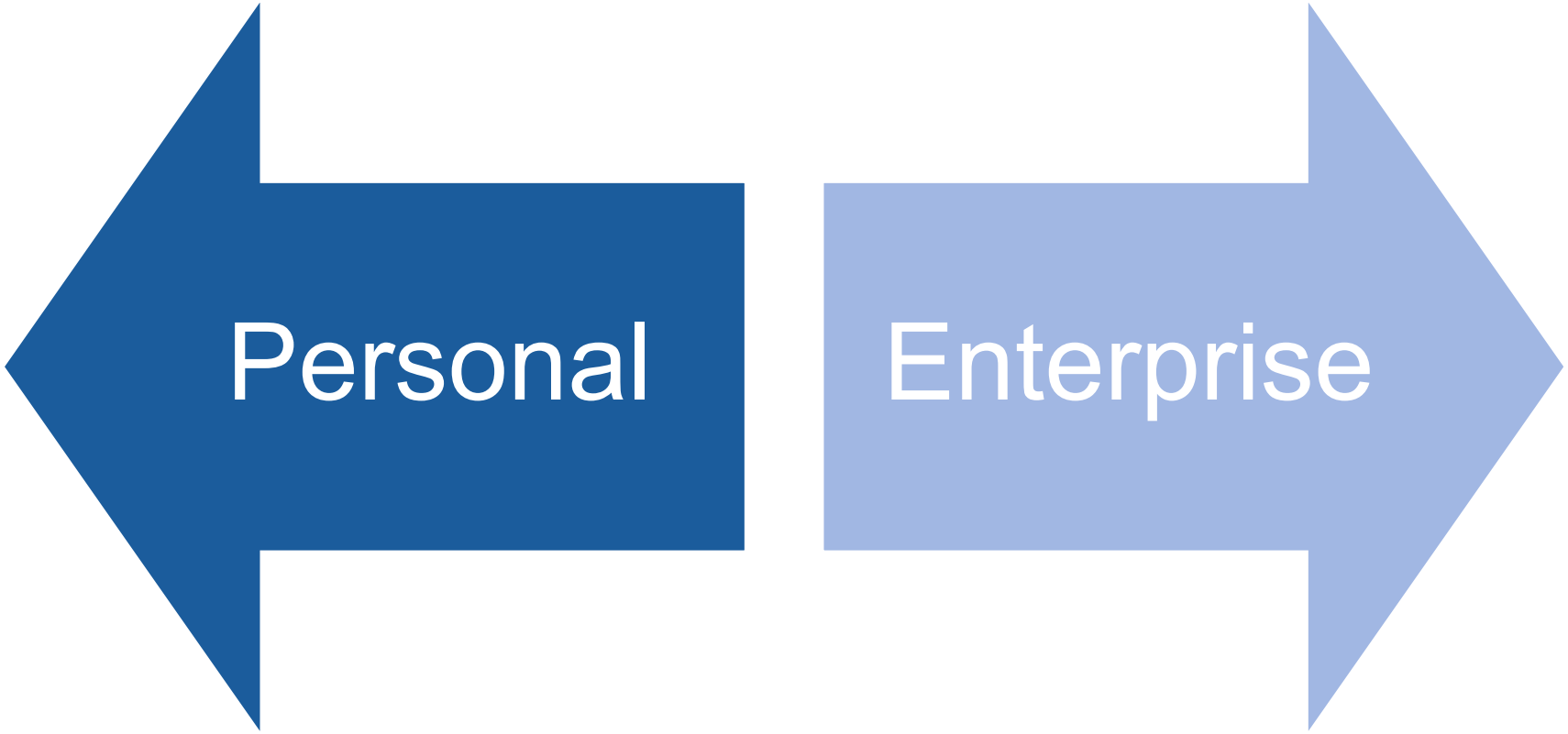
What do You Mean, “Without Security”?!?!?!

Without Security:

- Guest networks
- Should never be left open
- Should always restrict traffic that can be allowed
- Can use a Captive Portal
- Isolate properly with VLANs and Firewalls

Wi-Fi Security (WPA2)

There are two ways to use Wi-Fi with security (according to the WFA):



Personal

Personal

- Also known as PSK
- The wireless infrastructure and the clients share a common password
- This password is entered manually or calculated from an entered common passphrase
  - Everyone who knows the passphrase can access the network, and de-encrypt traffic

This is perfectly safe

As long as…

- You change the password every so often (maybe every 30 days)
- Change the password when someone leaves the company
- Use a serious level of length/complexity
  - Remember - length is better than complex
- These are very inconvenient

Enterprise

Problems with Enterprise:

Users can simply click “continue” or “OK” when presented with an invalid certificate

- This is quite possibly the dumbest thing to ever be allowed!

Don’t allow it

- Group Policy
- MDM control
  - These two can be quite inconvenient

Enterprise (Cont.)

Enterprise

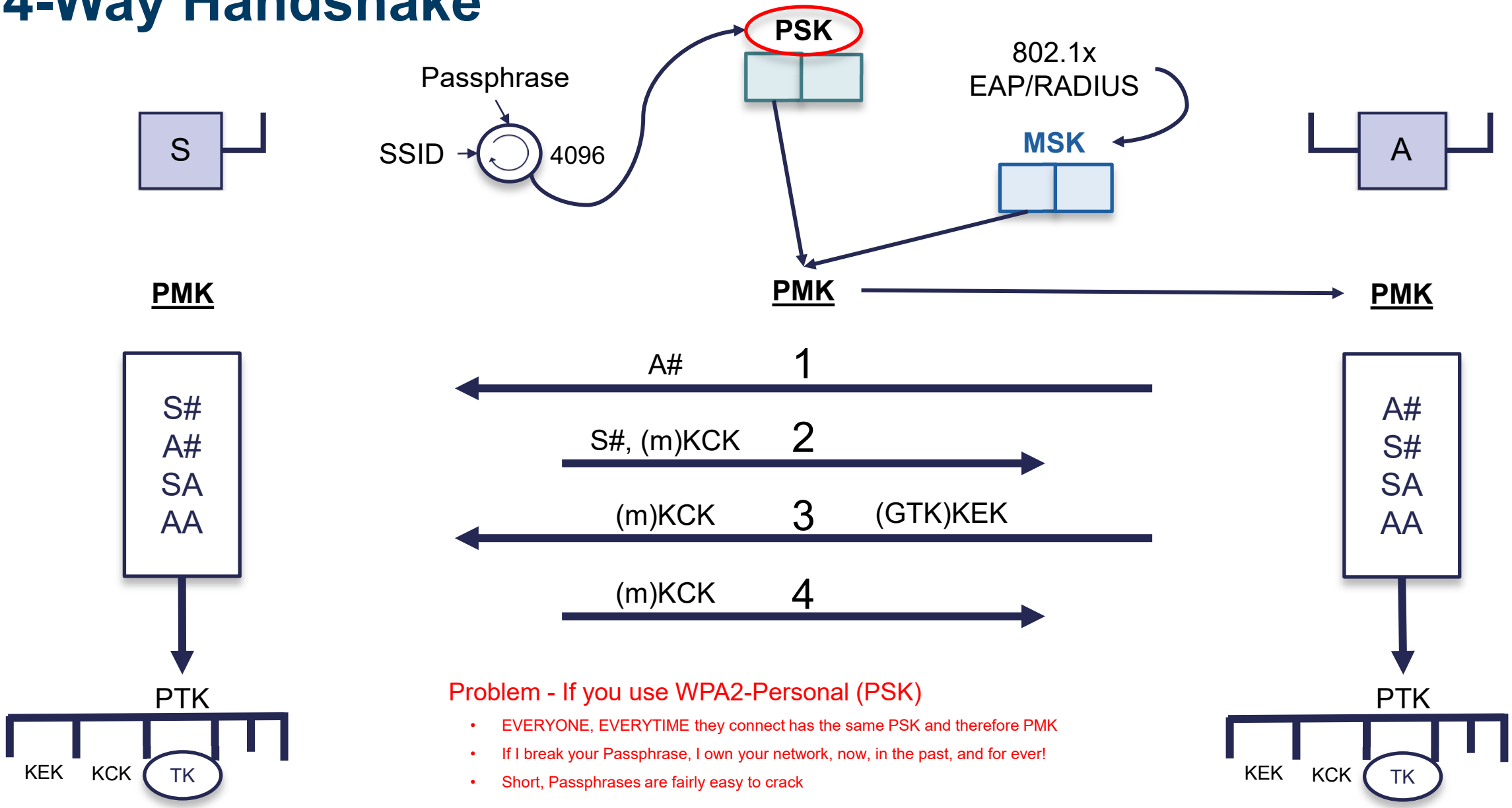
- Requires the use of EAP and RADIUS
- Will need to use Certificates (or Cisco variant EAP-FAST)
- Devices will need to be onboarded
- Can be very inconvenient

if if if if

Arguably the safest mode of Wi-Fi security today…

When configured <u>correctly</u>

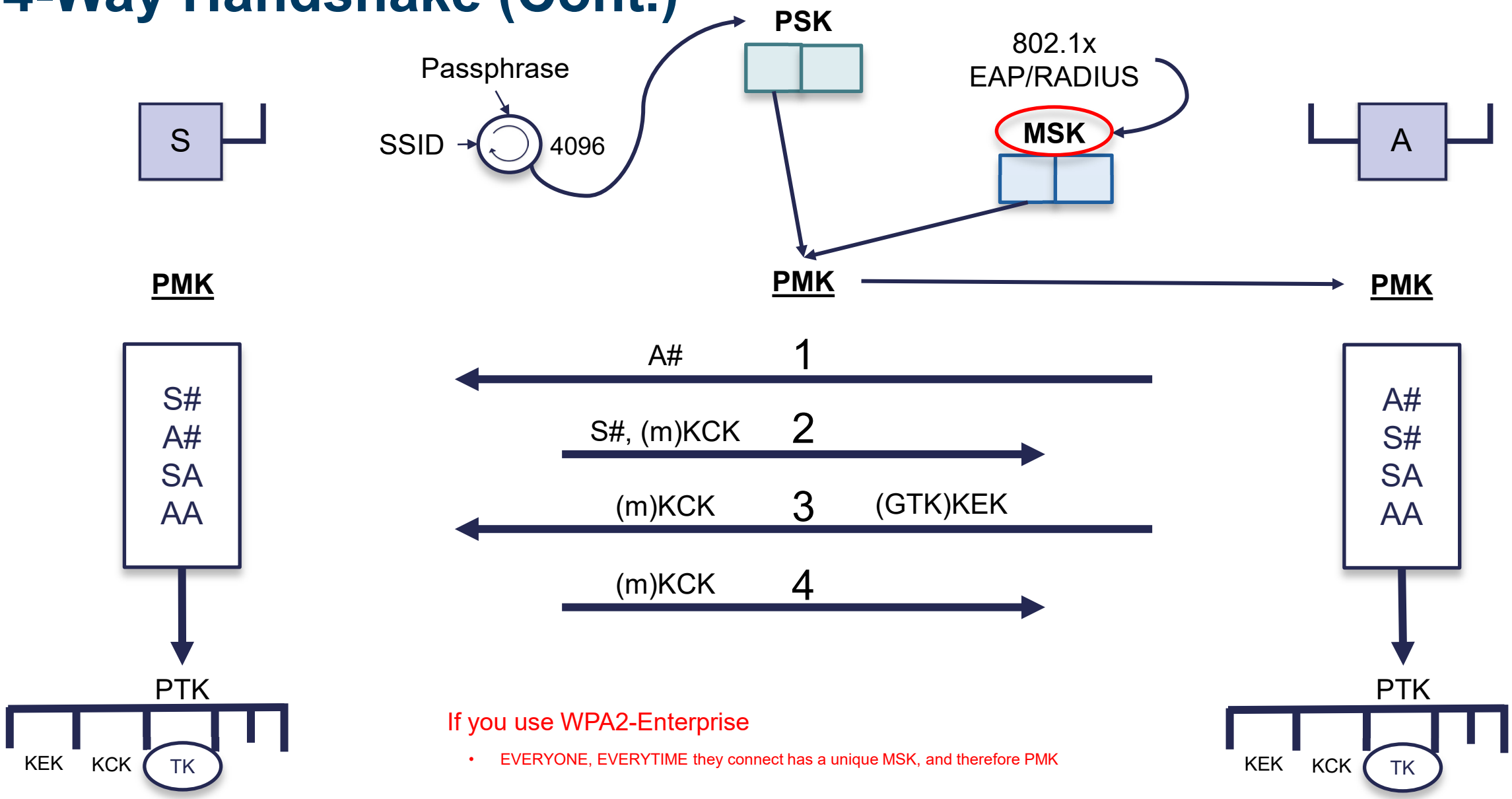
4-Way Handshake



Problem - If you use WPA2-Personal (PSK)

- EVERYONE, EVERYTIME they connect has the same PSK and therefore PMK
- If I break your Passphrase, I own your network, now, in the past, and for ever!
- Short, Passphrases are fairly easy to crack

4-Way Handshake (Cont.)



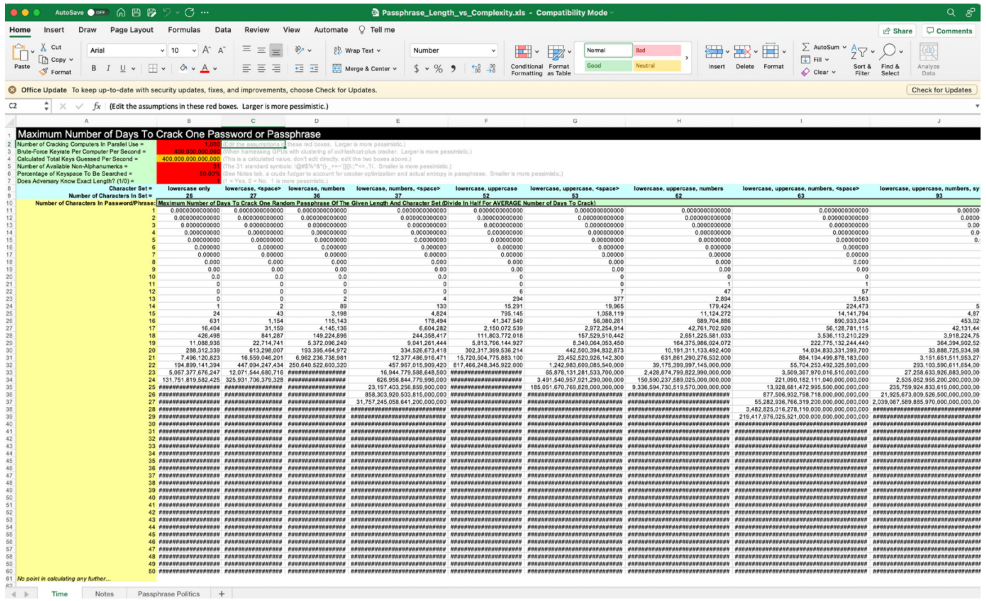
If you use WPA2-Enterprise

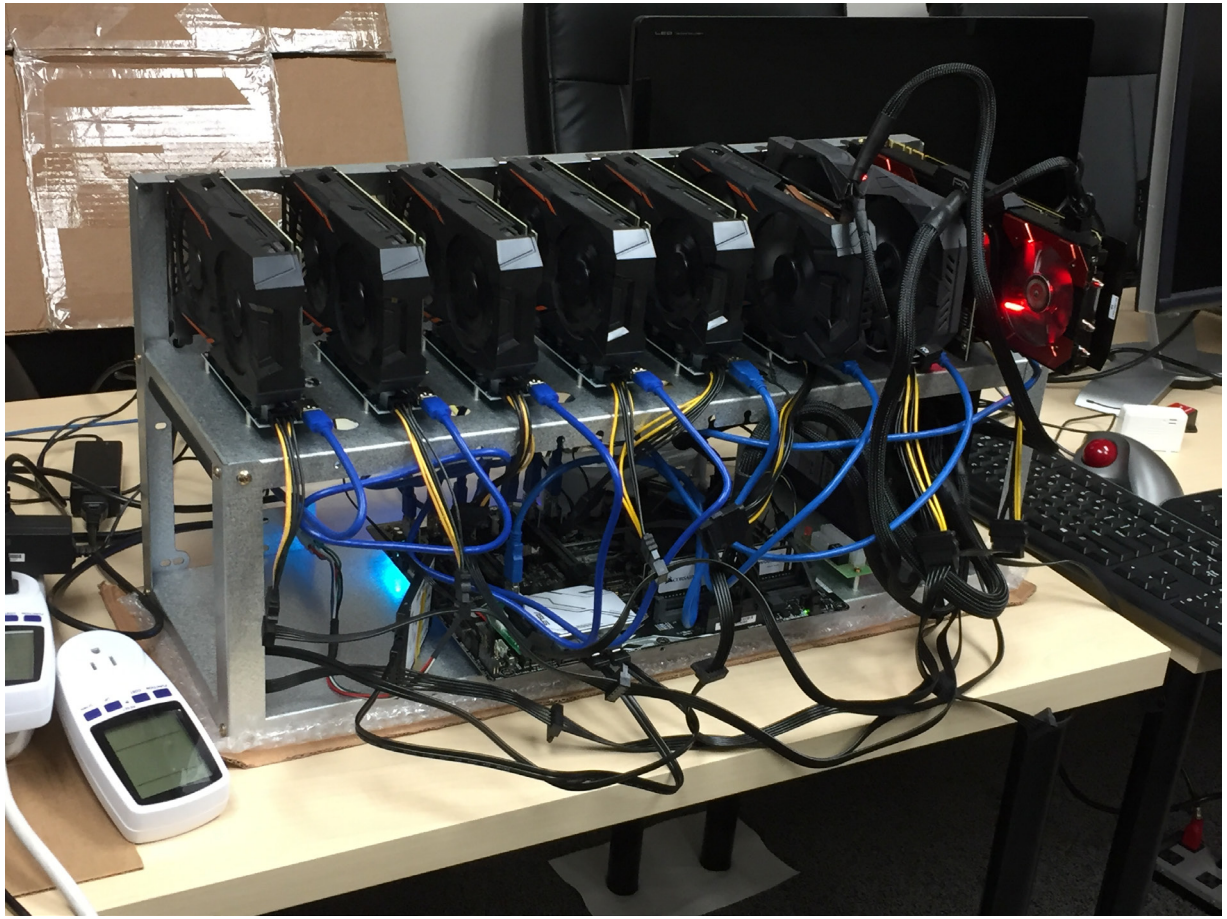
- EVERYONE, EVERYTIME they connect has a unique MSK, and therefore PMK

Surely, it’s not *That* Easy to Break?

But it Takes *Years* to Break, Right…?

Nope…





OK, but it’s Difficult to Capture Traffic, Right?

Nope…

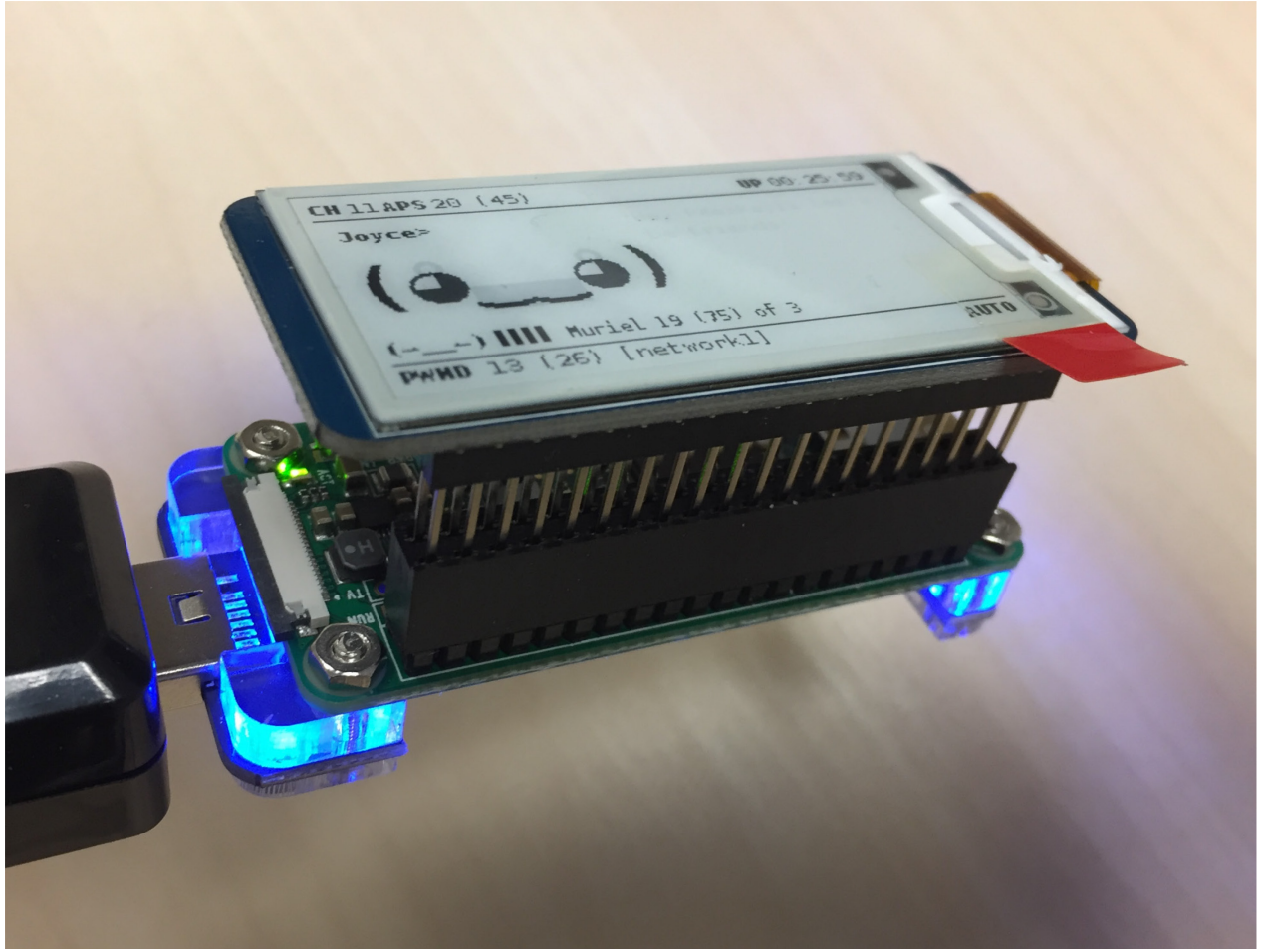
aircrack-ng suite - the heart and soul of Kali and Wi-Fi Hacking/Pentesting

- airmon-ng configures devices in monitor mode
- airodump-ng displays wireless SSIDs, APs, Clients, etc.
- aircrack-ng key cracking program
- aireplay-ng packet injection
- airbase-ng simulate an AP
- airdecap-ng decrypts packets

Pwnagotchi

Based on Tamagotchi:

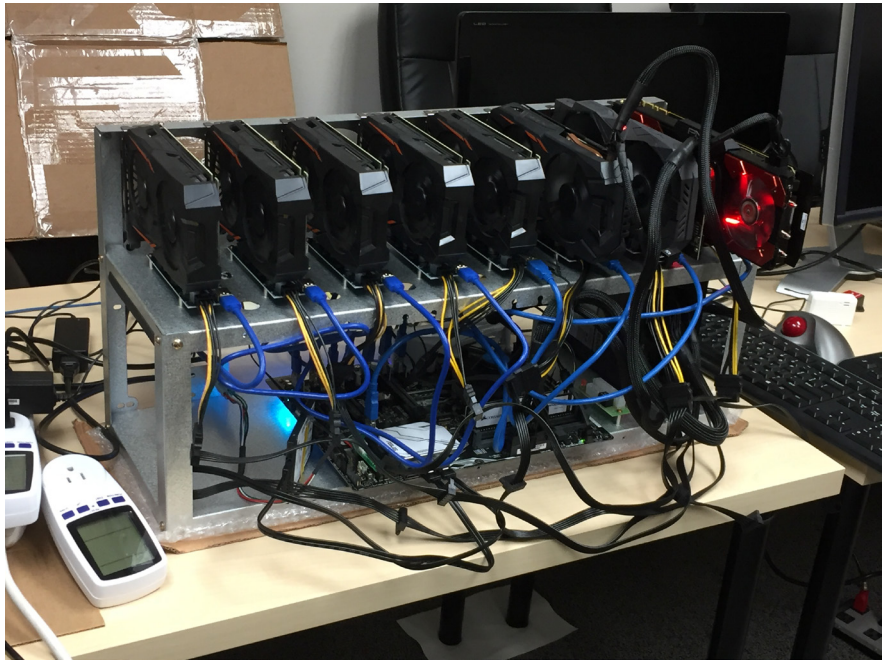
- “That game” from 90’s
  - You had to keep the thing alive
  - Apparently, it’s back!
- Captures WPA/WPA2 handshakes and PMKIDs
- Stored as PCAP
- Will try to associate to SSIDs
- Will de-authenticate
- Uses AI to learn how to get better



Flipper

Now banned in Canada!

So, What’s Wrong with WPA2?



- 2004: nearly 20 years old
- DeAuth spoof
- 4-Way handshake capture attacks
- Password can be cracked offline
- Once you know the PSK, you’re the king!
- It happily lets you NOT use Security
  - No Security = no Encryption
    - “Noooooooooooo!” (Think: “Luke, I am your father.”)
- Krack and other attacks

Is There Hope?

How Do We Fix the Problems with WPA2?

There *must* be a solution?

- This is 2024
- We are planning to send people to Mars
- We have self-driving cars
- Our phones have more raw power than 1960 supercomputers
- We have robots
  - Ok, they entertain our kids and vacuum our floors, but it's a start…
- We have AI and Machine Learning (for reference see Cyberdyne Systems)
  - Note, there is a *real* company called Cyberdyne (Terminator: Sci-Fi or prophetic warning!!!)
  - I'll just leave you with that thought…

How Do We Fix the Problems with WPA2? (Cont.)

USE STRONGER (LONGER) PASSWORDS

Yup, that’s all, folks!

Image credit: http://clipart-library.com/bunny-cartoon-images.html

WPA3

Magical Unicorns and stuff

WPA3 (Cont.)

- Next Generation Wi-Fi security from WFA
- Simplify and enhance Wi-Fi security
- Robust authentication, increased cryptographic strength
- Disallows legacy protocols, like TKIP
- Requires PMF (ends WPA2 DeAuth attacks)

WPA3-Personal: Summary

- Fixes the problems with WPA2
- Super-duper-mega-awesome
- Separates PSK and PMK generation
  - This one step makes WPA3 Personal infinitely more secure

WPA3-Personal: Summary (Cont.)

- Resistance to offline dictionary attacks
- Stronger protection against password guessing attempts
- Protection for users using ~~(stupidly)~~ easy-to-guess passwords
- Changes are invisible to users
  - Needs device support

WPA3-Personal: Summary (Cont.)

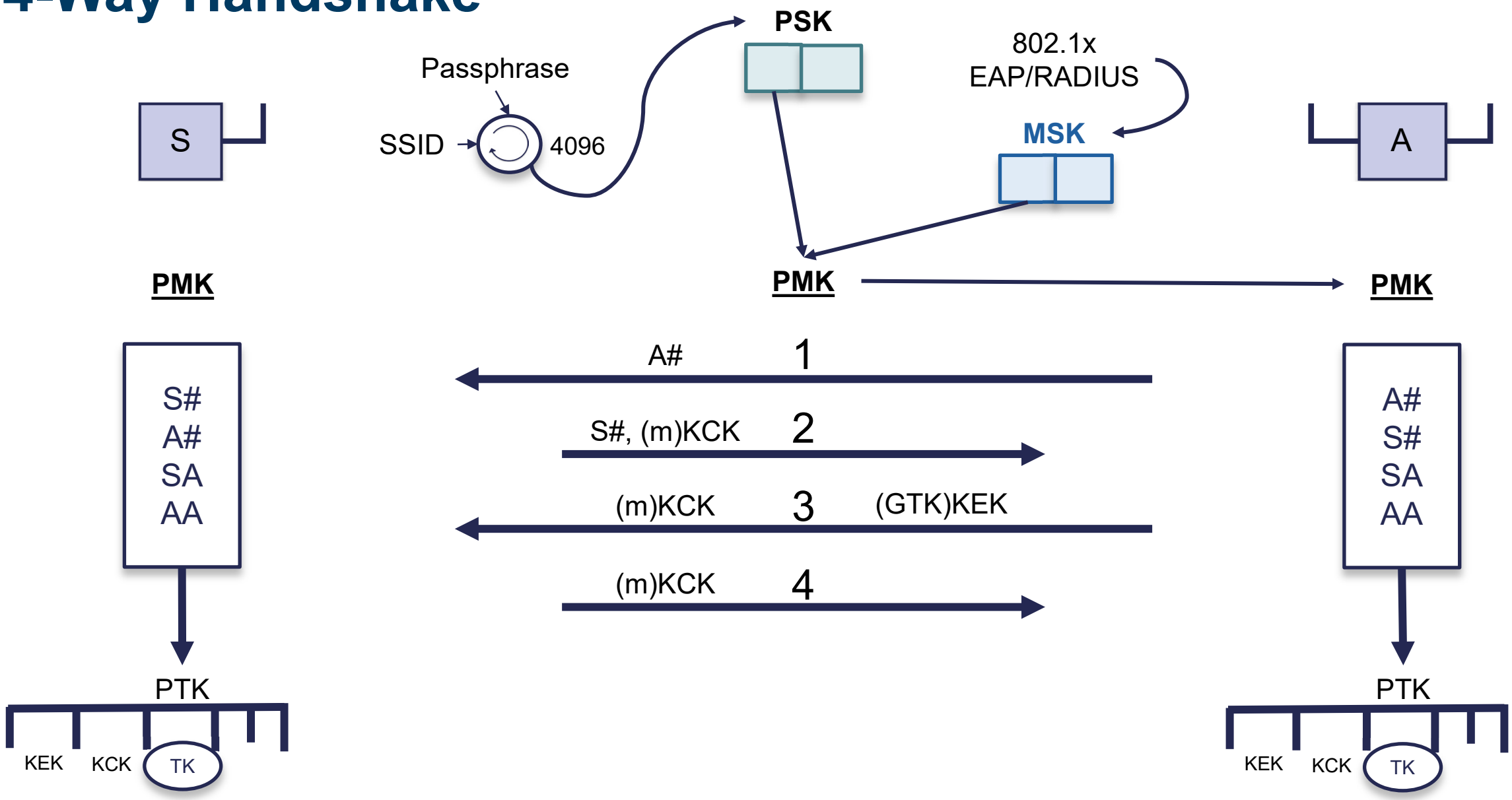
Forward secrecy provided, as SAE handshake assures that PMK cannot be recovered if password becomes known

Update, as of July 2022:

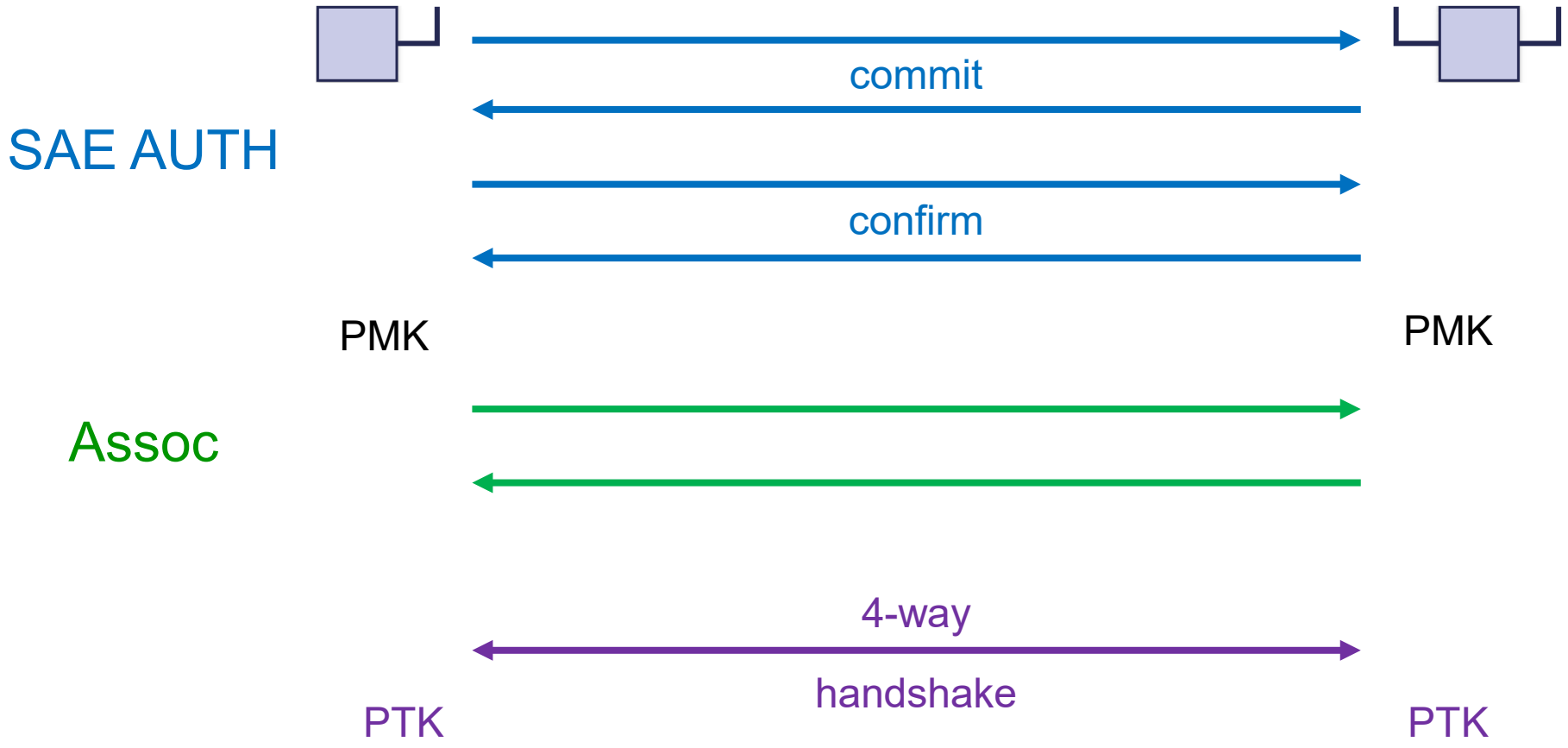
WPA3 support was mandated for Wi-Fi 6 certification (802.11ax)

WPA3 only option in Wi-Fi 6E (802.11ax in 6GHz)

4-Way Handshake



WPA3-Personal: SAE Process

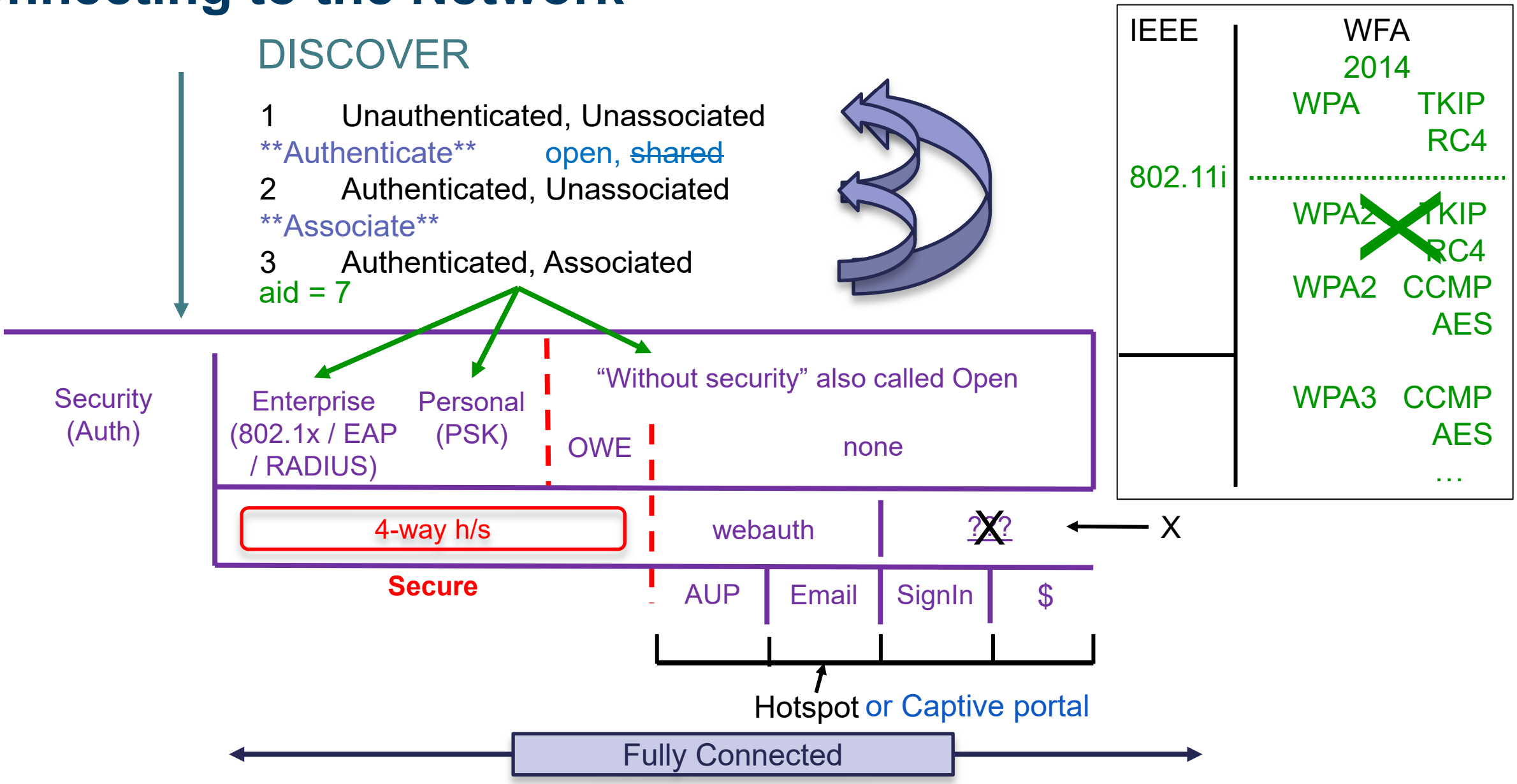


- Now…
  - EVERYONE, EVERYTIME they connect have a unique PMK

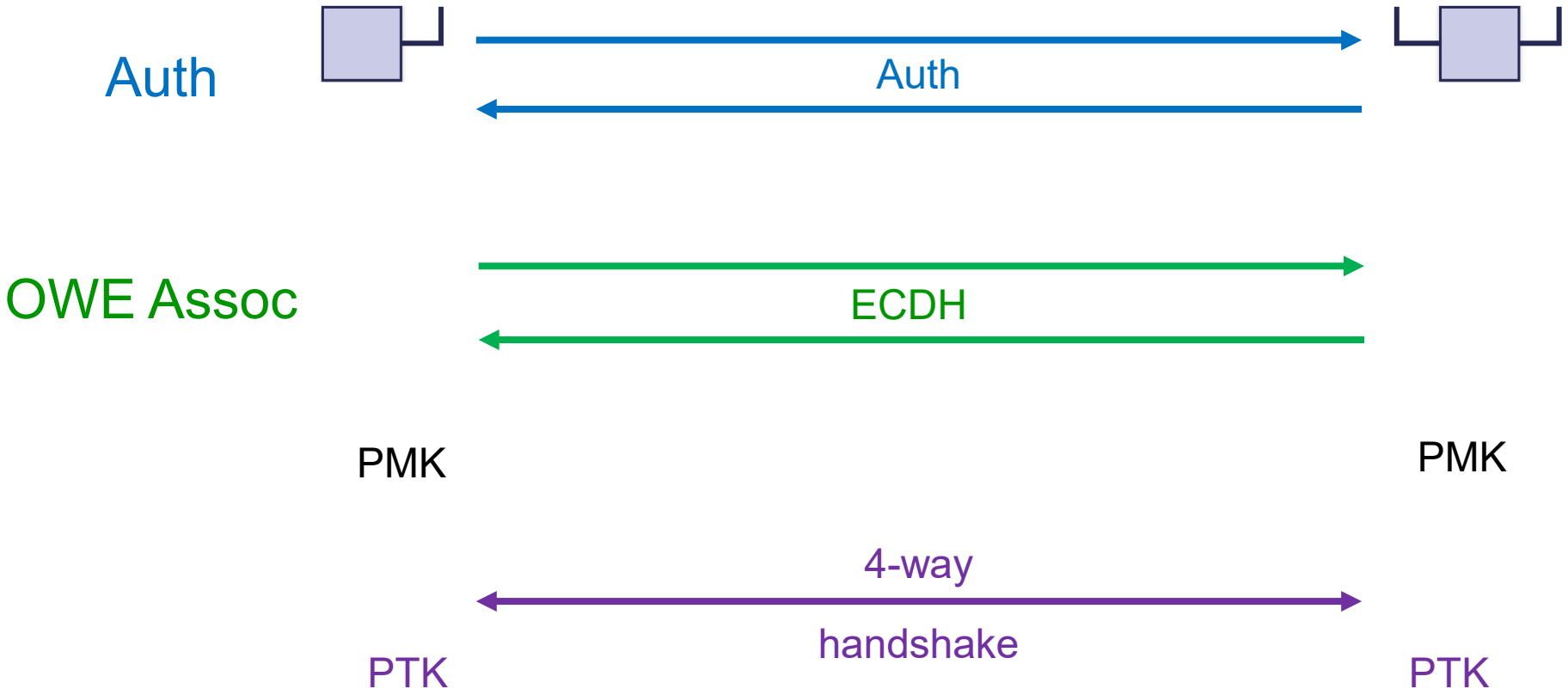
WPA3-Enterprise

- Invisible to users, no fundamental change to WPA2-Enterprise
  - Needs device support
- Optional 192-bit cryptographic strength
  - Essential for government, military, healthcare, and finance
- PMF cannot be disabled

Connecting to the Network



OWE Process



- Now…
  - EVERYONE, EVERYTIME they connect has a unique PMK
    - Even if they are connected to an open network, and even if they didn't want one!

WPA3

Turn it on

Use it

The End!

WPA3 Realities

- Not all clients support it
  - Phil’s story
- We may need to have the same SSID on 5GHz and 6GHz
  (for the foreseeable future)
- 6GHz mandates WPA3/PMF, 5GHz allows transition mode for both
  - If you run transition mode it can really mess things up, especially roaming
- Clients really don’t like to roam between different security configurations
  - Especially Fast Roams (each client is different)

Know your Vendor!

WPA3 Enterprise

- Fairly easy!
- Fast roaming may give you some problems
- Vendor specific, but generally works whether 2, 3, or transition

WPA3 Personal

- !$%@^#&, and other bad words
  (Yeah, give it up!)
- May work, or it may not, is vendor dependent, is client dependent
- Depends on which way you are roaming
- You will get stressed and spend hours troubleshooting!

WPA3-Personal: Solutions

We have spent years fixing Wi-Fi basic rules:

1. In 2.4GHz use only channels 1,6,11
2. Don’t do channel bonding in 2.4GHz
3. Use 20/40 not 80MHz bonding in 5GHz
4. Don’t have the same SSID available in 2.4 and 5 GHz
5. Reduce your number of SSIDs

Now it seems the solution to all our WPA3 problems are simple, either:

1. Don’t use 6GHz!
   - Totally rad bro!
2. Consider - use 6GHz, and have two SSIDs
   - One on 5GHz only, one on 5+6GHz
     - WPA2 (or Transition mode if you need it) on 5GHz only
     - WPA3 only on 5+6GHz
   - Migrate clients over to WPA3 SSID as needed

Security Strategy that May not Work as Expected!

MAC address filtering

- Limited benefits
- Easy to bypass

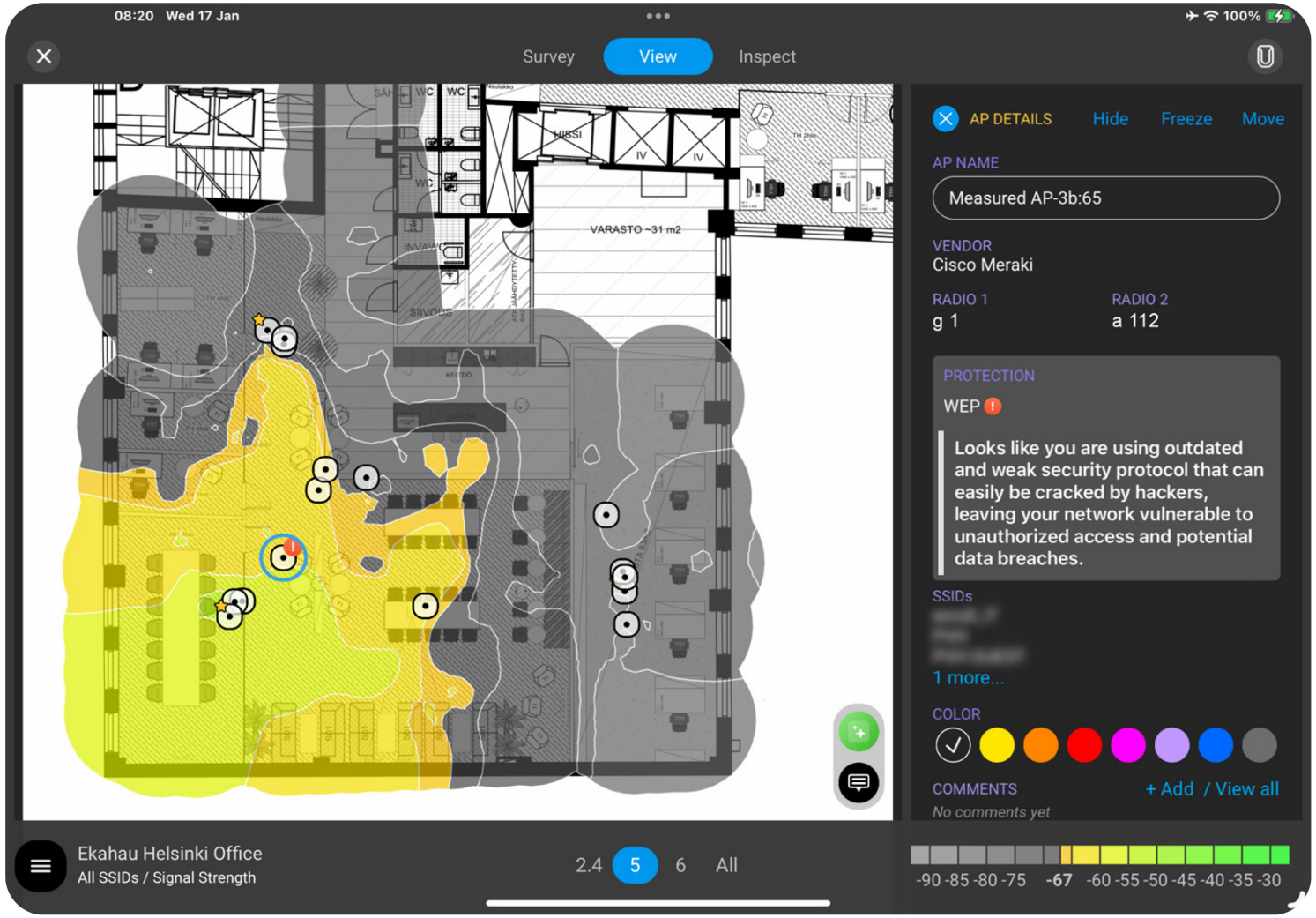
SSID Hiding

- Actually, makes your network more unsafe
- Easy to bypass

Old security WEP/WPA

- Easy to bypass

Easily Identify Outdated Security



ekahau

PROTECTION

WEP

Looks like you are using outdated and weak security protocol that can easily be cracked by hackers, leaving your network vulnerable to unauthorized access and potential data breaches.

Top Tips

Use a WIPS

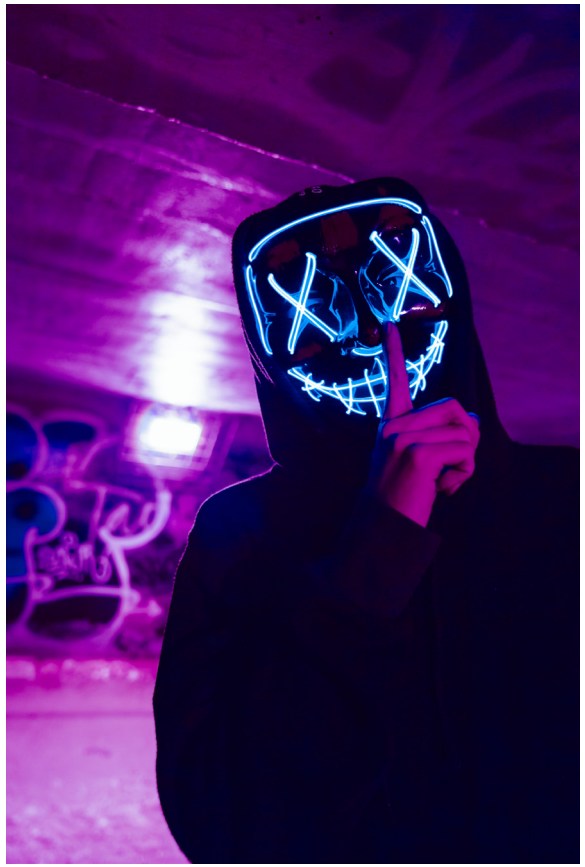
- Really - use one
- Know your environment
- Know what is normal
- Know what is abnormal

WIPS

Use DNS security

- e.g., Cisco Umbrella
- Meraki//Umbrella integration

DNS!



Use PMF/MFP

- Needs client support
- Again, use transition mode, with care

PMF

How can Ekahau Help make Your Network more Secure?

Use Ekahau to:

- Audit, view and Review your networks
  - Look for Security Type used WPA2/WPA3
  - Look for PMF Support
  - Look for outdated protocols
- Search for Rogues
- Search for Interferers
- Know your Environment – Scan with Ekahau
  - Know what is Normal
  - Know what is Abnormal

Ekahau: Easy Security Visualizations

“Your fastest path to a secure wireless network”

Protect Your Network

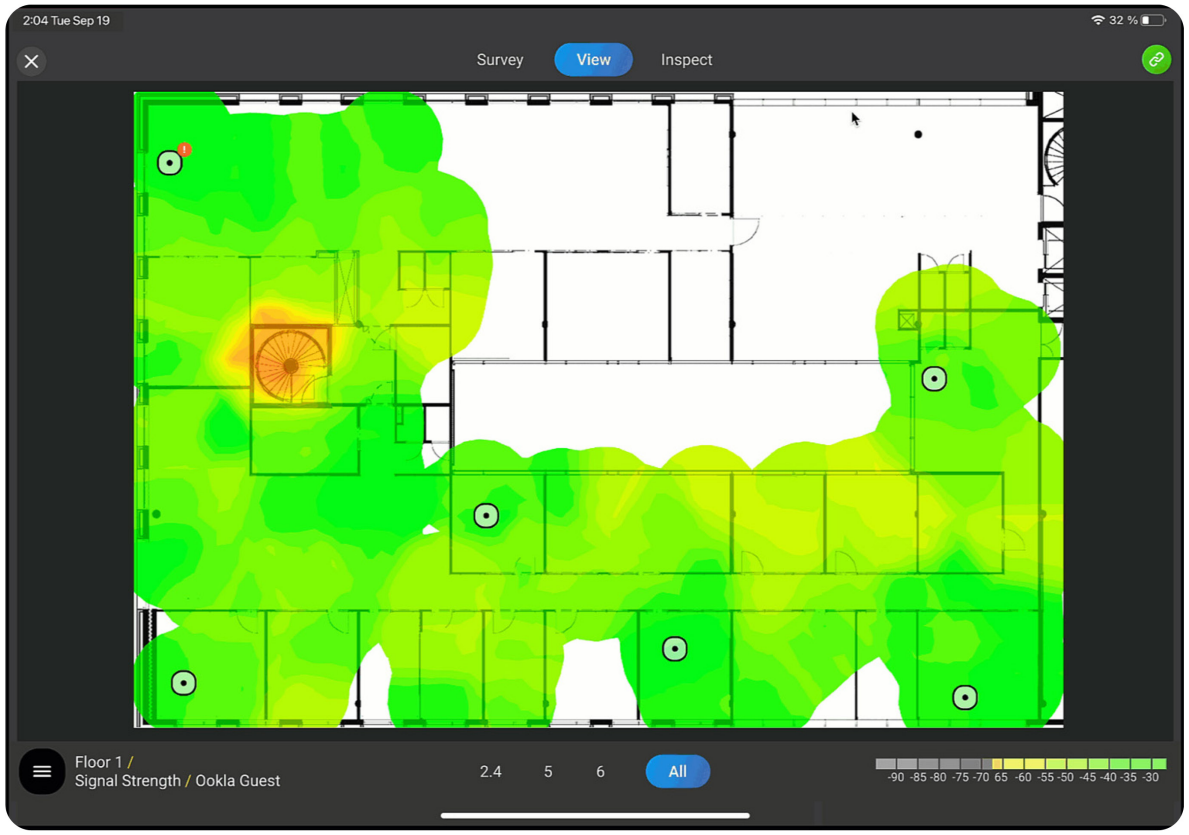
Identify weak security encryption protocols that leave your network vulnerable to attacks

Lock It Down From Rogue Threats

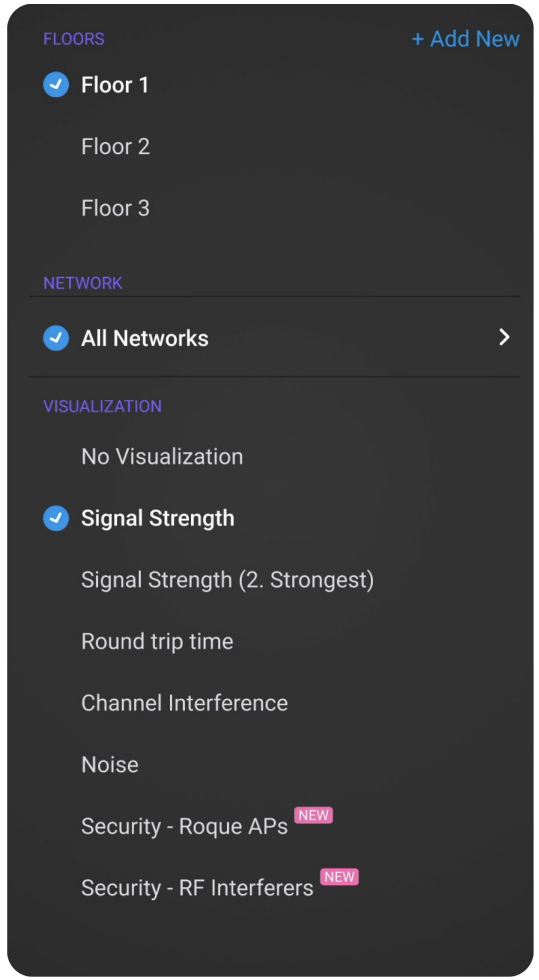
Detect and locate RF interference impacting network performance and data throughput

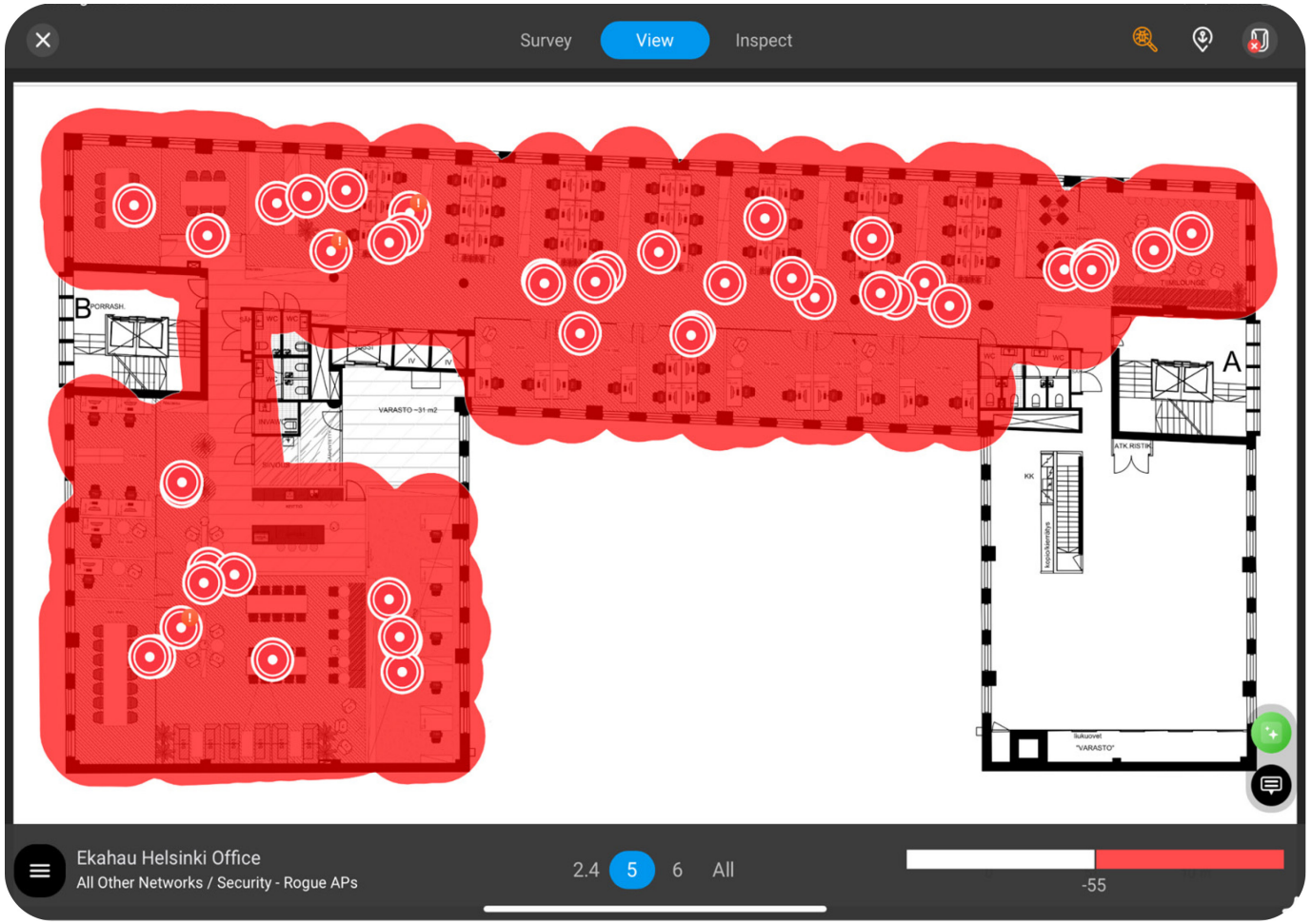
Instantly Update Encryption in Optimizer

Click to deploy powerful security improvements to your cloud controller

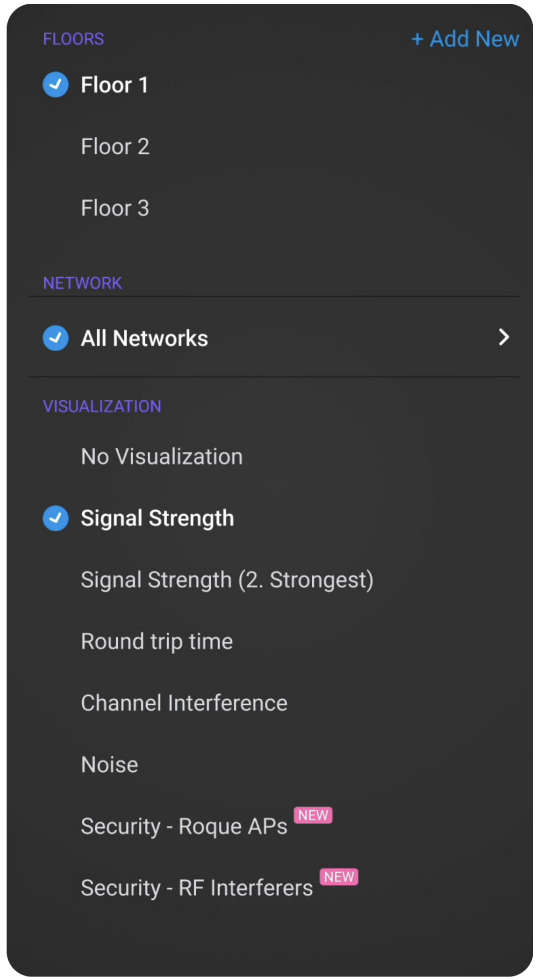


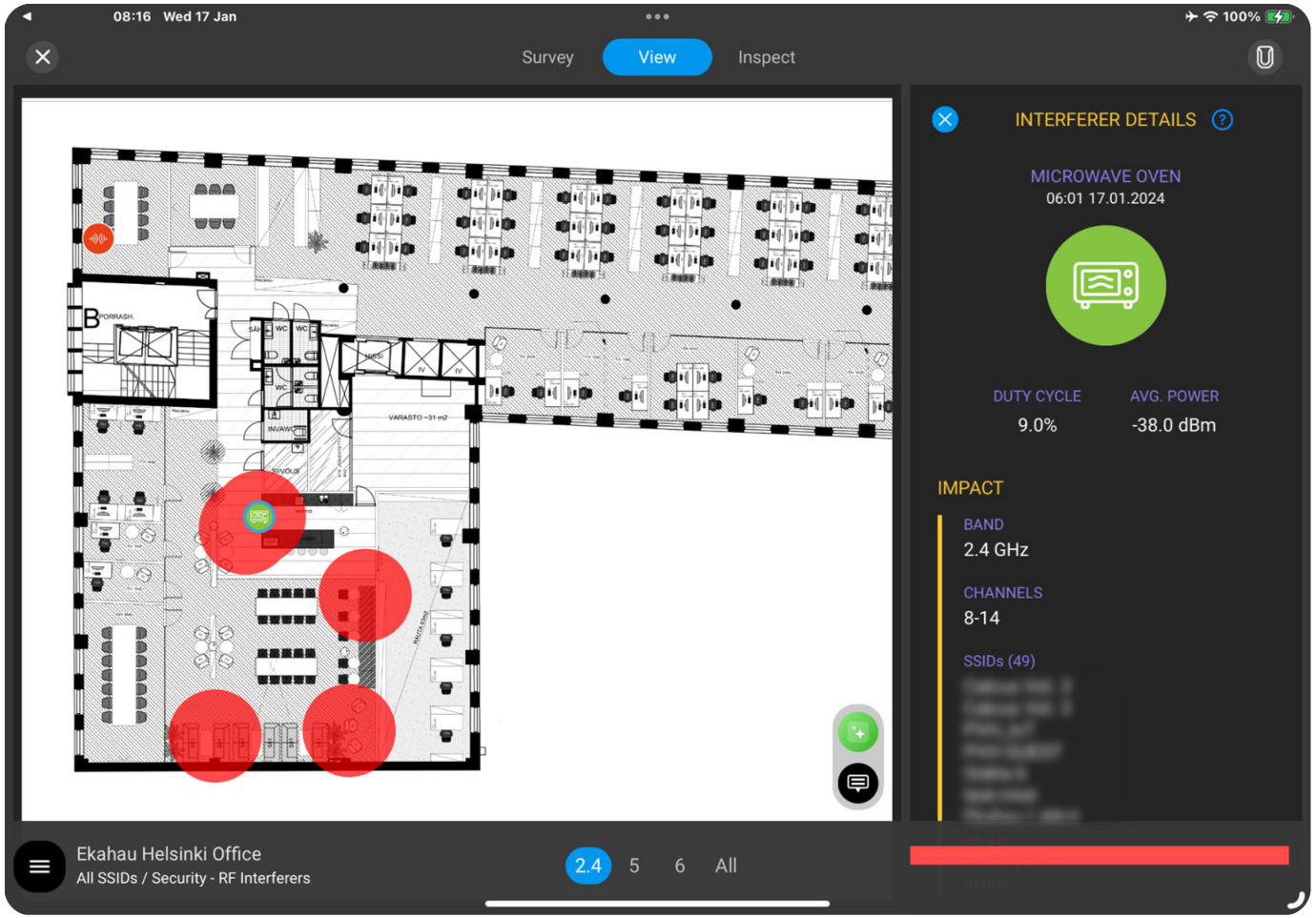
Easily Locate Rogue APs





Easily Identify and Locate RF Interferers





Key Lessons/Takeaways

What are the WPA3 lessons / takeaways?

Use WPA3 ASAP

Reality: it is difficult to not use “Personal”

Be wary of WPA3 Transition Mode

- It effectively makes everything be WPA2
- It can cause roaming problems

Use multiple SSIDs for each frequency

- Separate 2.4 and 5/6Ghz
- 5+6 may need to be same SSID
- Consider using a different SSID for WPA2 and WPA3 personal clients

Don’t use the same PSK on your WPA2 and WPA3 SSIDs

Isolate your guest networks

Keep software/firmware up-to-date

If you a serious about security:

- **Seriously** consider TLS based options

But Phil, these are so inconvenient…

Key Lessons/Takeaways

What are the WPA3 lessons / takeaways?

Use WPA3 ASAP

Reality: it is difficult to not use “Personal”

Be wary of WPA3 Transition Mode

- It effectively makes everything be WPA2
- It can cause roaming problems

Use multiple SSIDs for each frequency

- Separate 2.4 and 5/6Ghz
- 5+6 may need to be same SSID
- Consider using a different SSID for WPA2 and WPA3 personal clients

Don’t use the same PSK on your WPA2 and WPA3 SSIDs

Isolate your guest networks

Keep software/firmware up-to-date

If you a serious about security:

- **Seriously** consider TLS based options

But Phil, these are so inconvenient… **Ekahau can make your job easier!**

ekahau

Contacts

Presenter

- Email: philmorgan@nc-expert.com
- LinkedIn: https://www.linkedin.com/in/morganphil
- Twitter: @CCIE5224

Blogs

- https://tinyurl.com/ncxphilblog
- https://6ewi-fi.com/
- https://wizardofwifi.com (link to 3 of my blogs: Wi-Fi 6E, 7, and security)

Thank you

NC-EXPERT

CREATING EXPERTS