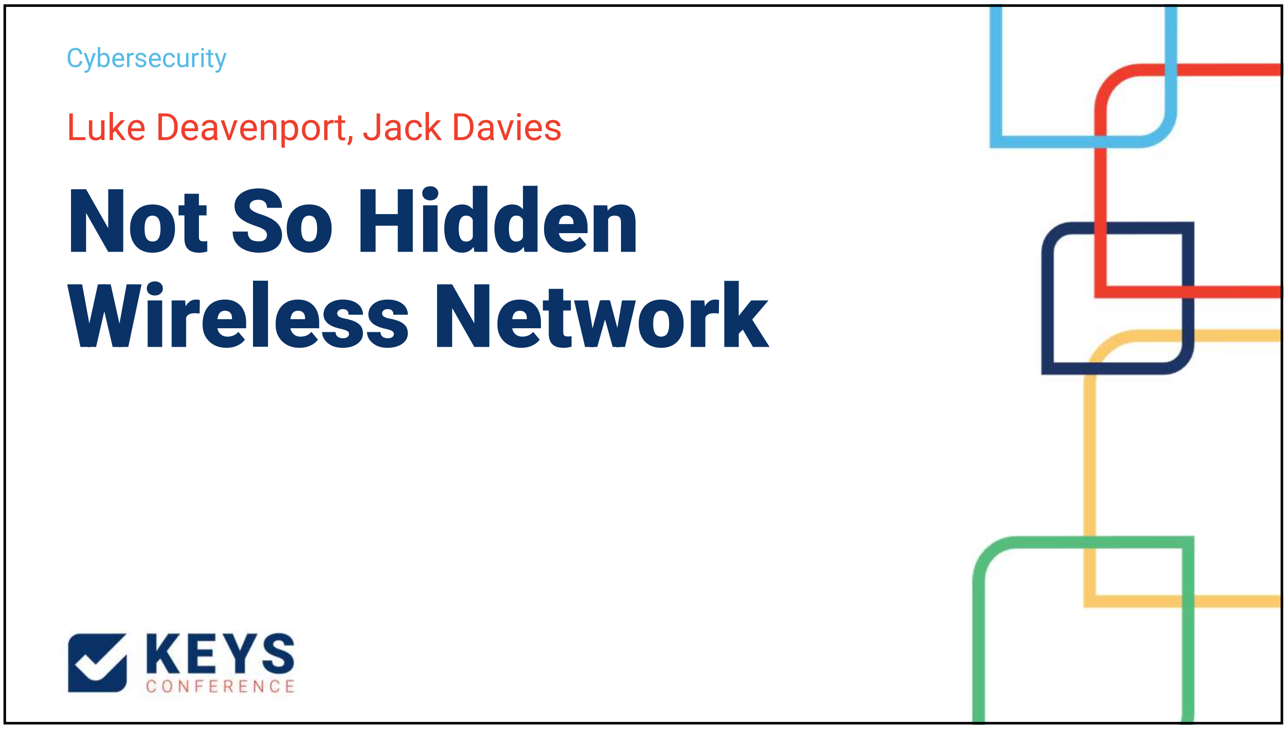


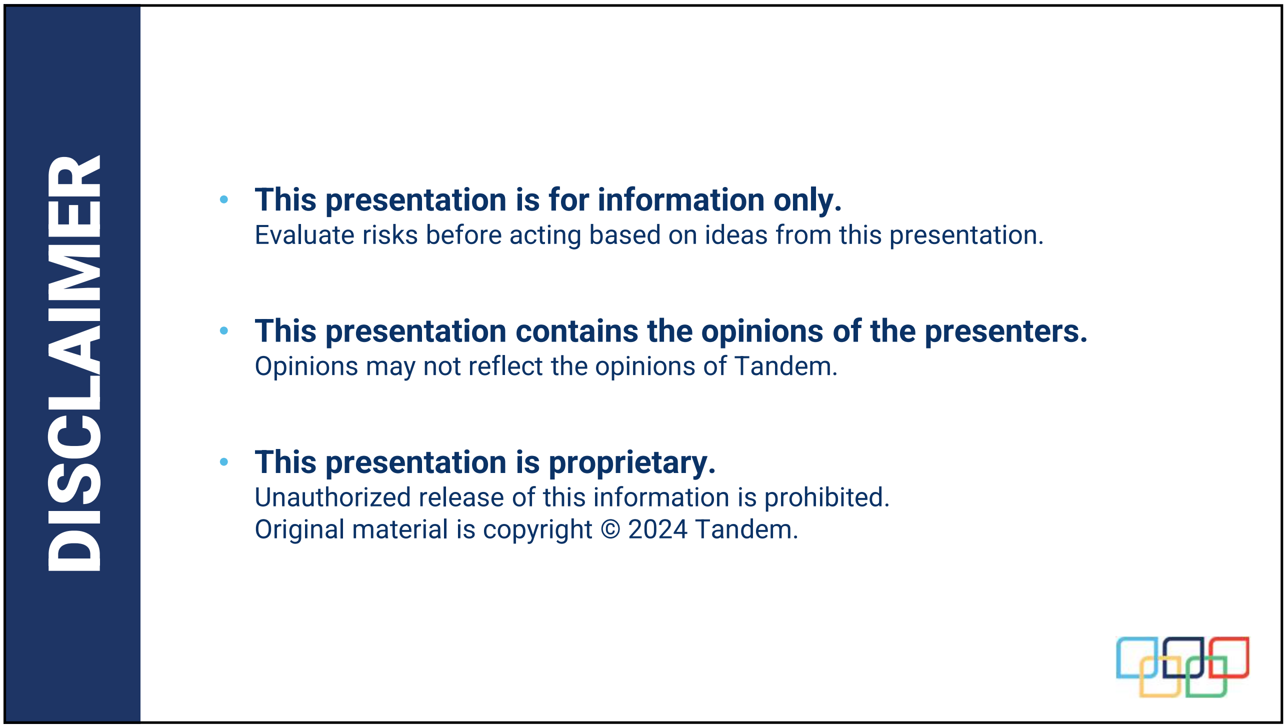
Cybersecurity

Luke Deavenport, Jack Davies

Not So Hidden Wireless Network

KEYS CONFERENCE

1



DISCLAIMER

- **This presentation is for information only.**
  Evaluate risks before acting based on ideas from this presentation.
- **This presentation contains the opinions of the presenters.**
  Opinions may not reflect the opinions of Tandem.
- **This presentation is proprietary.**
  Unauthorized release of this information is prohibited.
  Original material is copyright © 2024 Tandem.

2

Luke Deavenport

CISSP, CISA

IT Audit and Consultant

Jack Davies

eWPT, eJPT, Security+

Security Engineer

3

DISC GOLF!

4

Coffee Shop?

Speakeasy?

5

Outline

1 Terms

2 WPA2 Attack

3 Rogue Access Points

4 WPA2-Enterprise Attack

5 Take Aways

6

Terms

Access Point

An Access Point provides a wireless signal (SSID)

Client

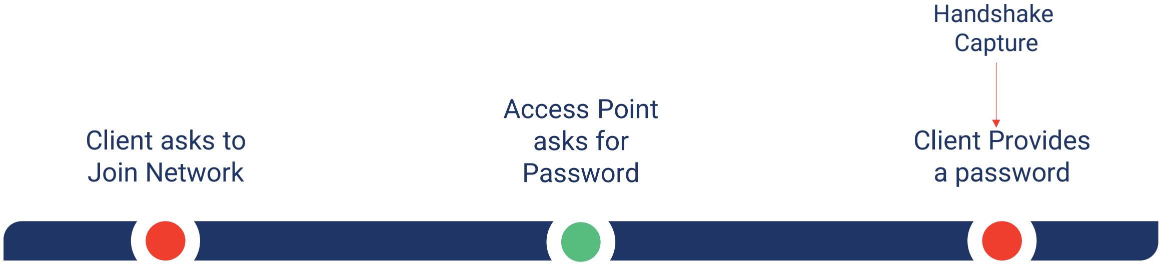
A Client is a device looking to connect to the Access Points

Handshake

The process for a client to authenticate to an access point

7

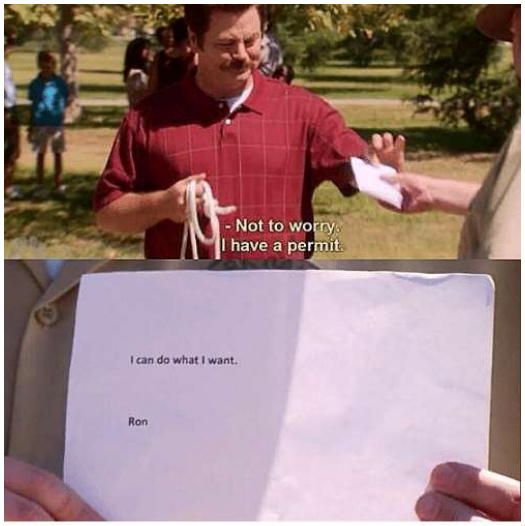
Wireless Handshake


Handshake Capture
Client asks to Join Network
Access Point asks for Password
Client Provides a password

8

Legal?

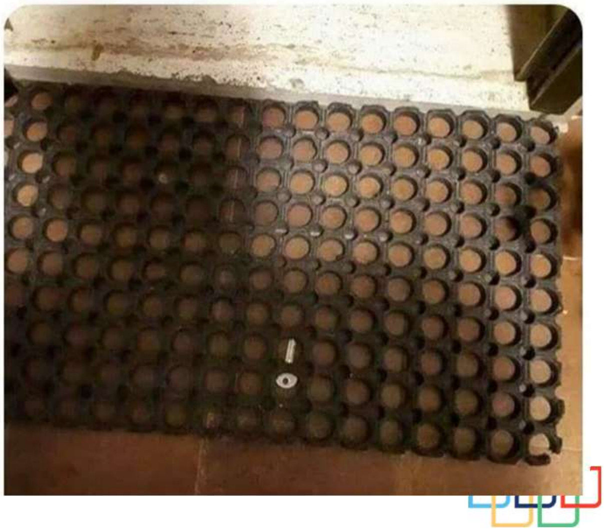
1. Permission is required.
2. The only part that is illegal (without permission) is saving the traffic that is captured.
3. If you connect to our test routers, you give us permission to store the data.



Passwords

1. Encrypted, only as strong as the password
2. Dictionary is used for password cracking
3. Password captured is what the client provides

Login: admin
Password: admin



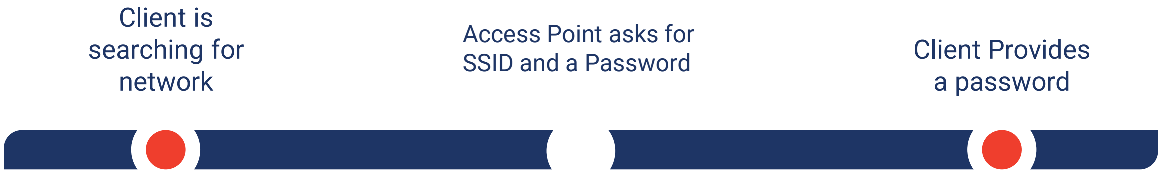
WPA2 ATTACK

11

A hidden network keeps me safe, right?

12

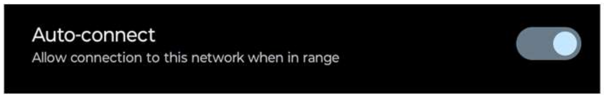
Wireless Handshake (Hidden)



Client is searching for network

Access Point asks for SSID and a Password

Client Provides a password



Auto-connect

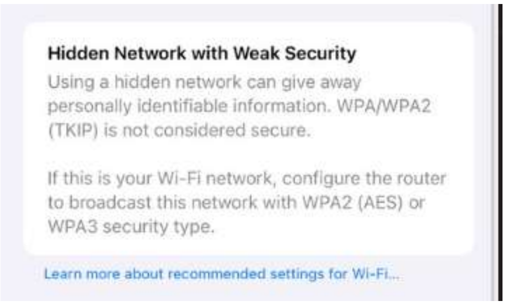
Allow connection to this network when in range

13

Are you my Network?

14

iOS and Android warnings:

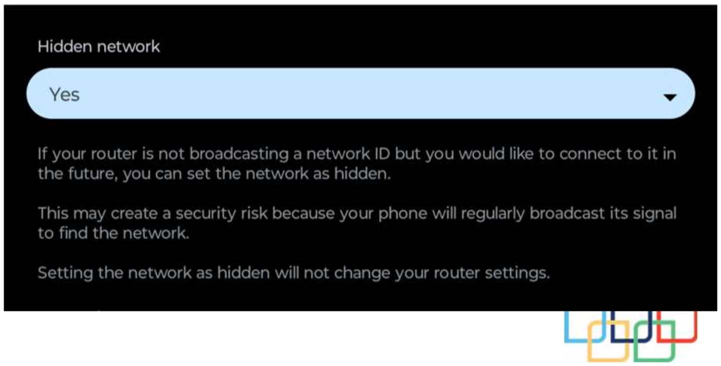


Hidden Network with Weak Security

Using a hidden network can give away personally identifiable information. WPA/WPA2 (TKIP) is not considered secure.

If this is your Wi-Fi network, configure the router to broadcast this network with WPA2 (AES) or WPA3 security type.

Learn more about recommended settings for Wi-Fi...



Hidden network

Yes

If your router is not broadcasting a network ID but you would like to connect to it in the future, you can set the network as hidden.

This may create a security risk because your phone will regularly broadcast its signal to find the network.

Setting the network as hidden will not change your router settings.

15

Avenues of Attack

Proximity

- Near the original wireless network
- Can be conducted if the SSID is hidden or seen
- Wait for someone to connect

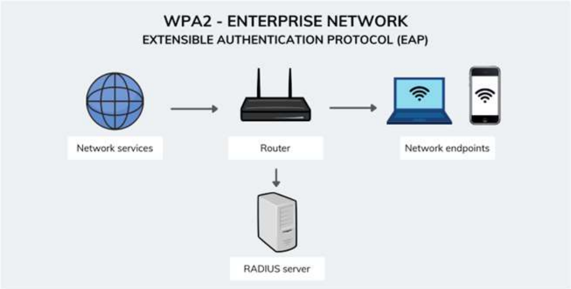
Away from the Network

- Anywhere
- Original wireless network is likely hidden
- Rely on clients automatically connecting

16

WPA2-Enterprise

- WPA2-E utilizes a RADIUS server for authentication
- Most commonly the RADIUS server is associated to Active Directory
- Credentials will be sent to any familiar network

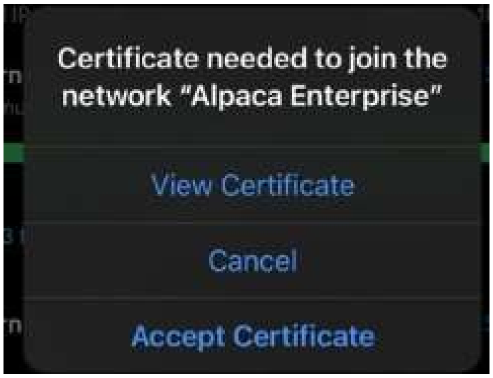

WPA2 - ENTERPRISE NETWORK
EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)
Network services
Router
Network endpoints
RADIUS server

17

Radius Certificate

For a device to trust a RADIUS server,
a certificate needs to be available.

If that certificate is self-signed,
a ‘speedbump’ is presented to the user.



Certificate needed to join the network “Alpaca Enterprise”

18

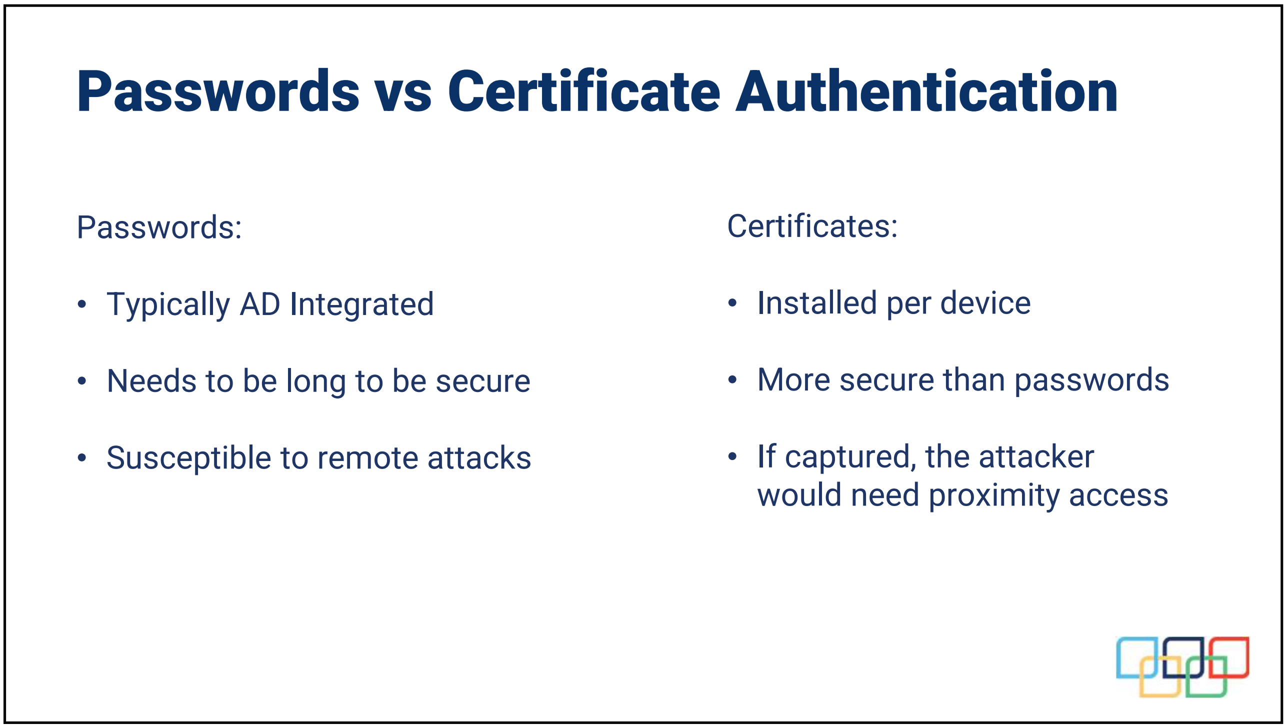
Going Rogue

- Fake Access Point
- Easy to setup
- Can be set up anywhere!

19

WPA2-Enterprise Attack

20



Passwords vs Certificate Authentication

Passwords:

- Typically AD Integrated
- Needs to be long to be secure
- Susceptible to remote attacks

Certificates:

- Installed per device
- More secure than passwords
- If captured, the attacker would need proximity access

21

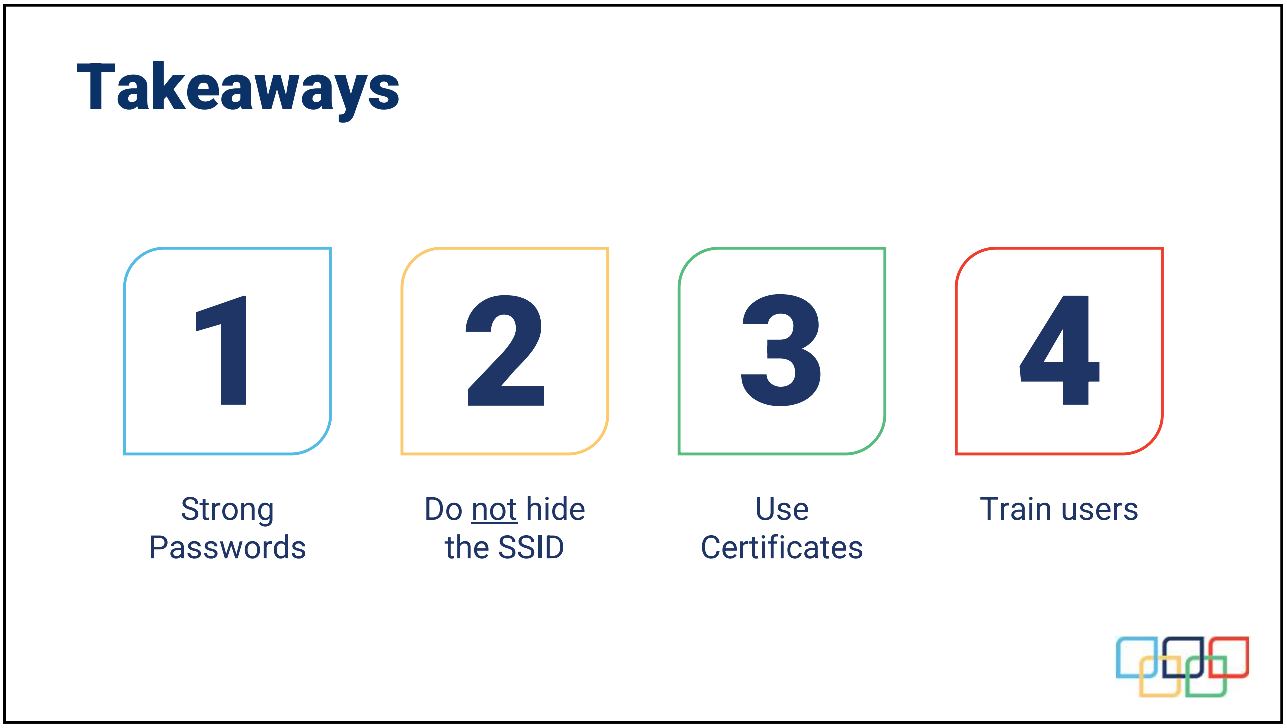
WPA2-Enterprise Threat Summary

IF:

- WPA2-E network SSID is hidden
- Uses Active Directory credentials
- Device are set to automatically connect

AD credentials are susceptible to being captured anywhere users go.

22



Takeaways

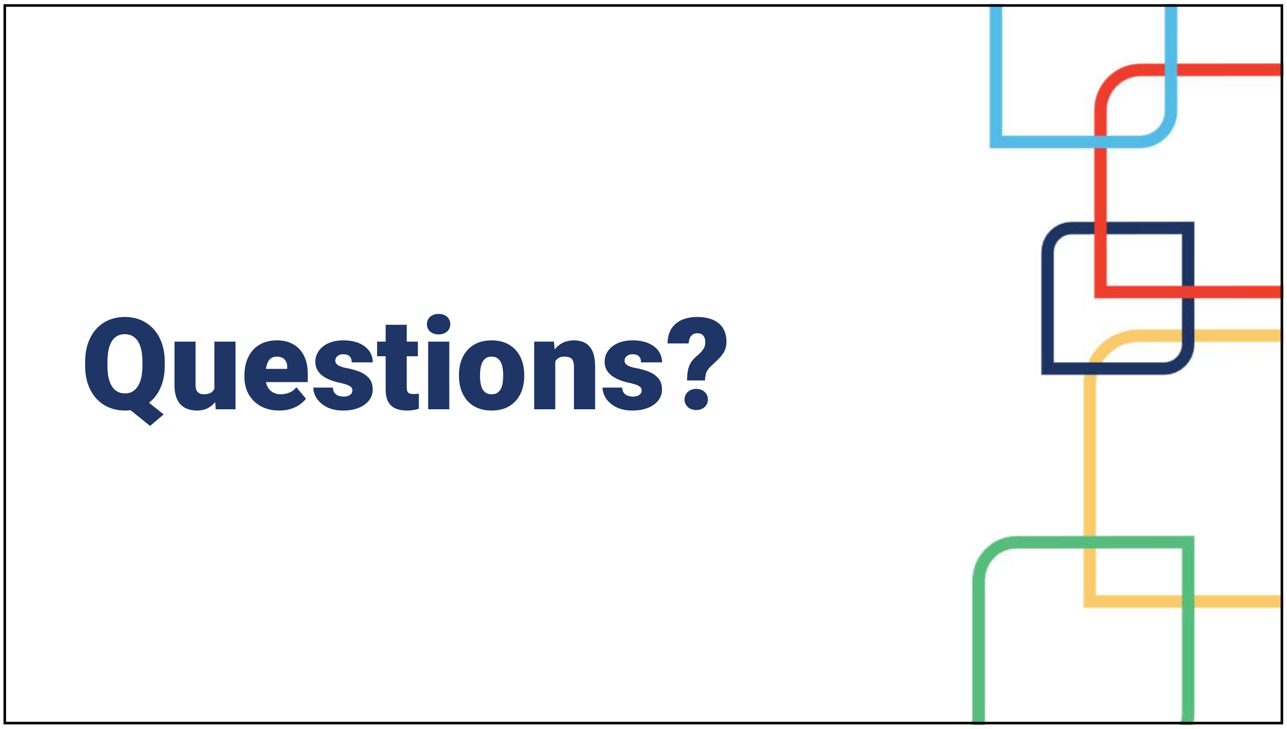
1 Strong Passwords

2 Do not hide the SSID

3 Use Certificates

4 Train users

23



Questions?

24

THANKS FOR JOINING!

Not so Hidden Wireless Networks

Luke Deavenport

CISSP, CISA
IT Audit and Consultant

Jack Davies

eWPT, eJPT, Security+
Security Engineer

KEYS CONFERENCE