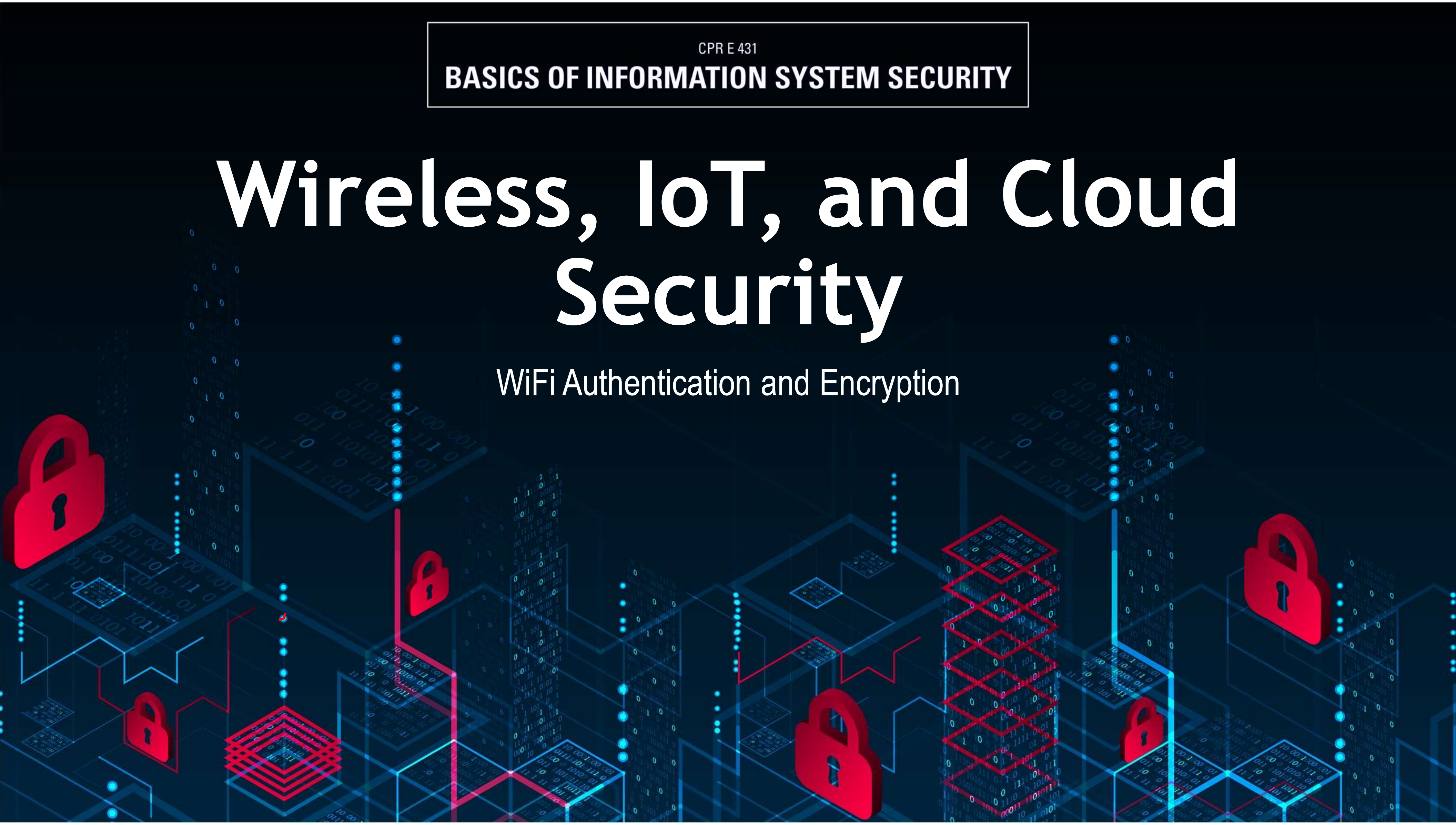
CPR E 431
BASICS OF INFORMATION SYSTEM SECURITY

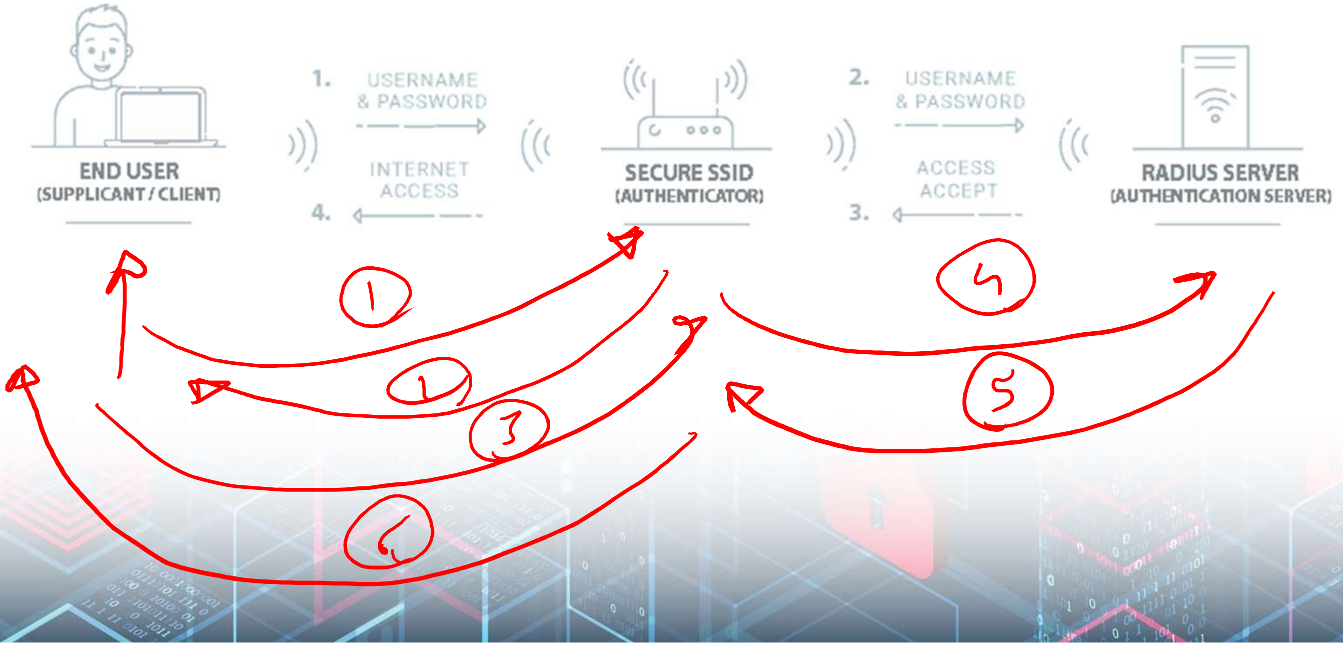
Wireless, IoT, and Cloud Security

WiFi Authentication and Encryption



Video summary

- Authentication Using IEEE 802.1X (Secure Network Authentication)



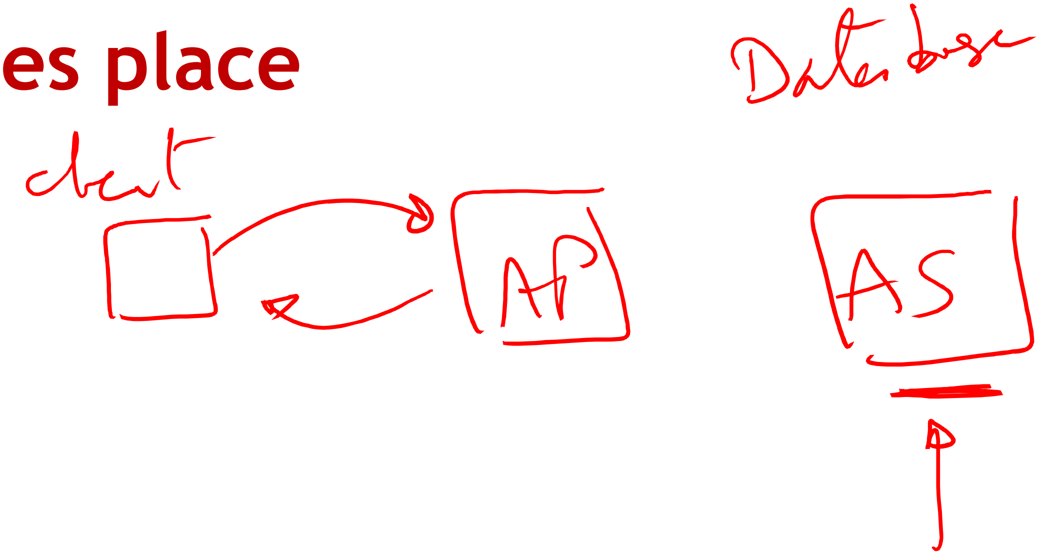
802.1X: A solution at last, maybe…

- 802.1X is an IEEE standard that enables layer 2 (MAC layer) authentication and key management on IEEE 802 LAN’s.

- Not limited or specific to 802.11 networks

- 802.1X is not an alternative to 802.11 or WEP, it works along with the 802.11 protocol to manage rotation of keys and authentication for WLAN clients

How authentication takes place



- A client requests access to the AP

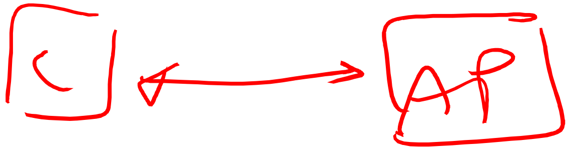
- The AP asks for a set of credentials

- The client sends the credentials to the AP which forwards them to a RADIUS (Remote Authentication Dial-in Service) server for authorization

802.1X → EAP

Extensible Authentication Protocol (EAP)

- 802.1X utilizes EAP for it's authentication framework



- EAP is a protocol for wireless networks that expands on authentication methods used by the Point-to-Point Protocol (PPP), a protocol often used when connecting a computer to the Internet.

- Developers may create their own methods to pass credentials

- There are a vary wide variety of available authentication methods: one time passwords, certificates, smartcards, etc

A few more benefits of 802.1X

- 802.1X does not use encapsulation, and thus has zero per packet overhead
- Because 802.1X integrates well with other open standards such as RADIUS, it is often easy and cost efficient to deploy
- Any RADIUS server that supports EAP can be used to manage an 802.1X network

more benefits of choosing 802.1X…

- Access points only need a firmware upgrade to enable 802.1X
- Nearly transparent setup for the client depending on the EAP you choose
- Depending on the EAP you choose, you can have a very secure wireless LAN!

A closer look at a few common EAP’s

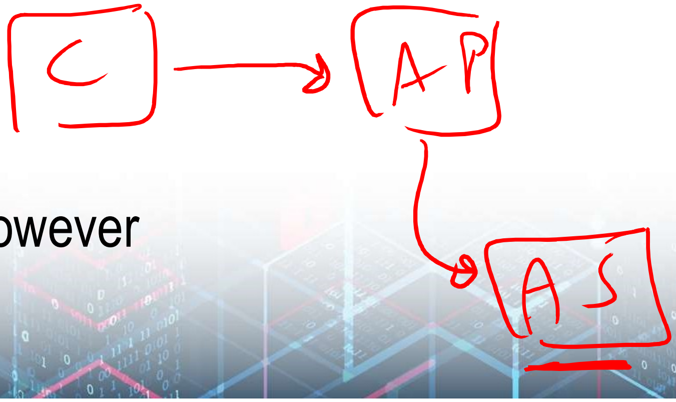
1

- EAP-MD5 is a simple EAP implementation

- Uses and MD5 hash of a username and password that is sent to the RADIUS server

- Has no dynamic key generation or key management, so the WEP key can still be found out through the methods described earlier

- Authenticates only one way



- It does keep attackers from using the network directly however

2

EAP-LEAP (Cisco Wireless)

- Like MD5-LEAP, it uses a Login/Password scheme that it sends to the RADIUS server
- Each user gets a dynamically generated one time key upon login
- Authenticates client to AP and vice versa
- Can be used along with RADIUS session time out feature, to dynamically generate keys at set intervals
- Only guaranteed to work with Cisco wireless clients

3

EAP-TLS by Microsoft

- Instead of a username/password scheme, EAP-TLS uses certificate based authentication

- Two way authentication

- Uses TLS (Transport Layer Security) to pass the PKI (Public Key Infrastructure) information to RADIUS server

- Hard to implement (exchange of public keys)

4

PEAP by Microsoft and Cisco

- A more elegant solution!

- Very similar to EAP-TLS except that the client does not have to authenticate itself with the server with a certificate, instead it **can** use a login/password based scheme

- Much easier to setup, does not necessarily require a PKI (Public Key Infrastructure)

802.1X is not perfect

- WEP is still a weakness, and only provides weak encryption and no per packet authentication

- Some EAP’s do not require mutual authentication

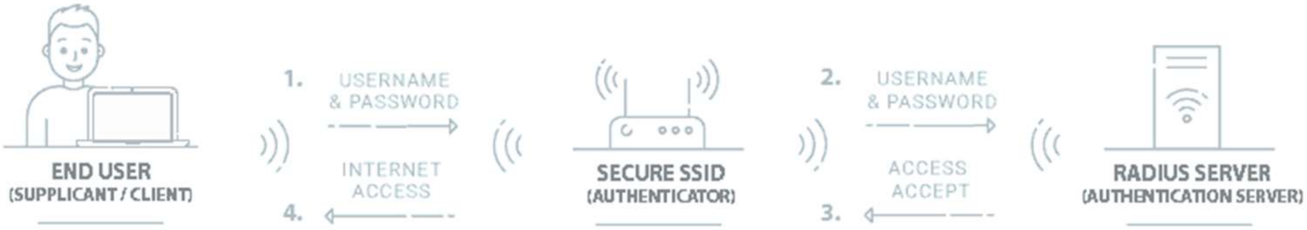
- Some EAP’s are subject to dictionary attacks

More flaws in current implementations

- 802.1X is vulnerable to many kinds of DOS attacks
- Many EAP’s are subject to man in the middle attacks. Recently these were found to include PEAP and EAP-TLS

Video summary

- Authentication Using IEEE 802.1X (Secure Network Authentication)


END USER
(SUPPLICANT / CLIENT)
1.
USERNAME
& PASSWORD
INTERNET
ACCESS
4.
SECURE SSID
(AUTHENTICATOR)
2.
USERNAME
& PASSWORD
ACCESS
ACCEPT
3.
RADIUS SERVER
(AUTHENTICATION SERVER)