

Wireless Encryption



Dale Meredith

MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: [@dalemeredith](https://twitter.com/dalemeredith) | LinkedIn: [dalemeredith](https://www.linkedin.com/in/dalemeredith)

Identifying our weaknesses gives us strength and that's when we get dangerous.

Dale Meredith

Knowing is half the battle

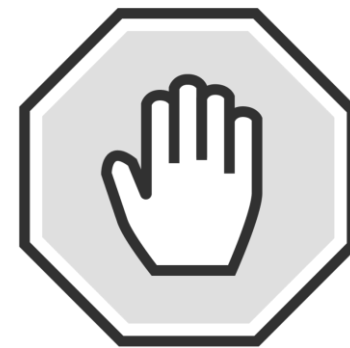
WEP Encryption

WEP

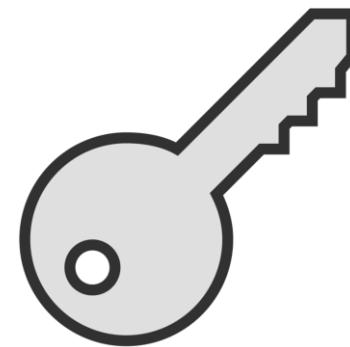
Wired Equivalent Privacy



Protects against digital eavesdropping



Disallows network access



Utilizes an inefficient key

Intended Purpose

Control access

Confidentiality

Data integrity

Efficiency





Wasn't reviewed by academia

Did not receive input from cryptologists

Was ratified in 1999

Restriction of exporting cryptography technologies led to manufacturers restricting their devices which impacted WEP's functionality

Utilized RC4 algorithm which is designed for encrypting randomized keys and WEP didn't allow for randomizing

Can be cracked if enough traffic can be intercepted

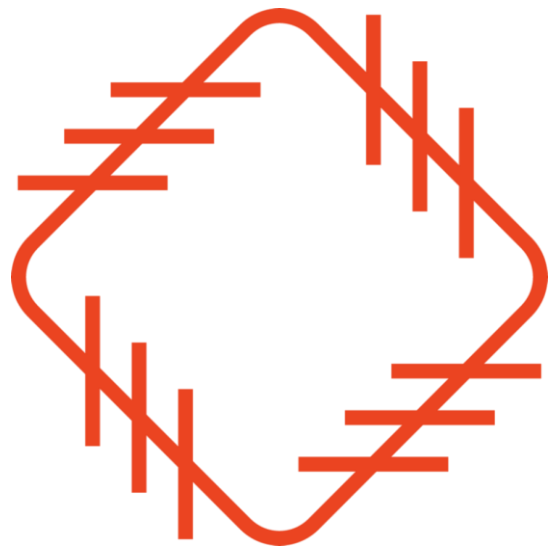
Its 104-bit WEP key provides no significant practical advantage



WPA and WPA2 Encryption

WPA

The TKIP creates unique encryption keys for each wireless frame, which creates a more secure network connection



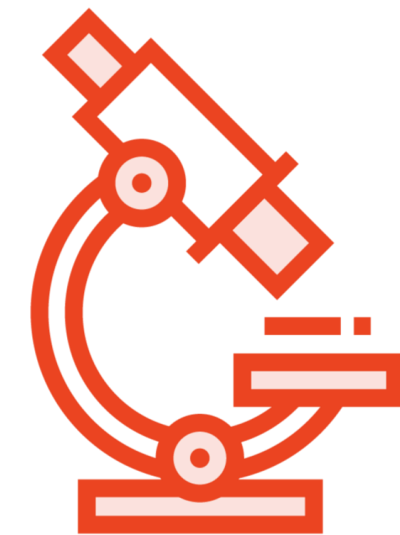
Adopted in 2003

**Designed to patch WEP
issues**



**Utilizes a pre-shared
key (PSK)**

**Operates with a stronger
256-bit key**



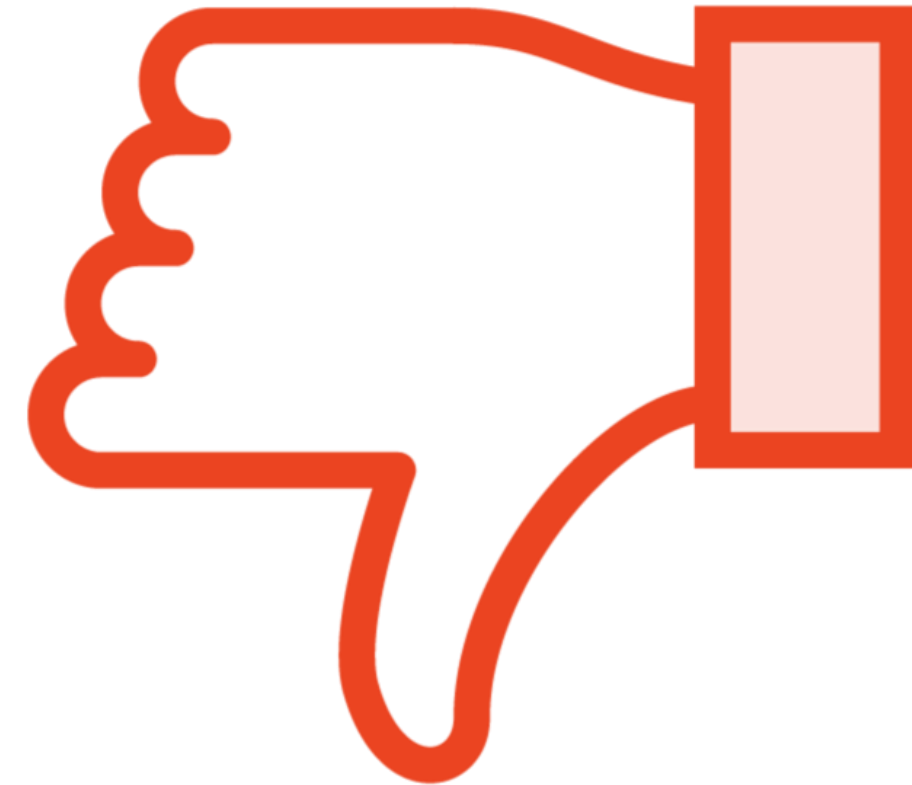
**Includes message
integrity**

**Checks to see if packets
have been captured or
altered**

WPA



Did not require a hardware purchase due to its ability to run a firmware upgrade



Creates exploits making it almost as insecure as WEP



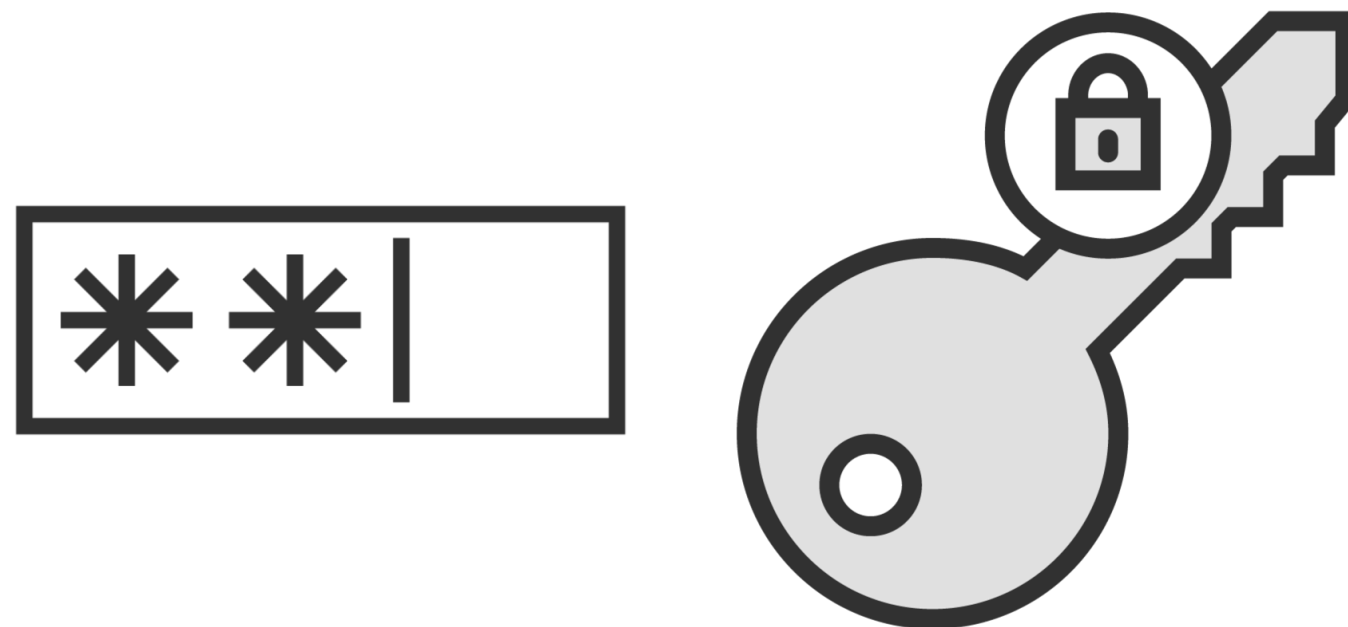
WPA2

WPA Personal

Uses a pre-shared key

Encrypts using a 256-bit key

Requires eight to 63 ASCII characters

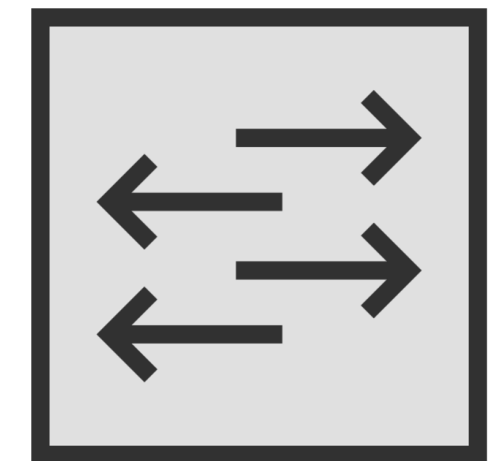


WPA2 Enterprise

Addresses distribution concerns and manages static passphrases

Uses EAP or RADIUS

Requires credentials

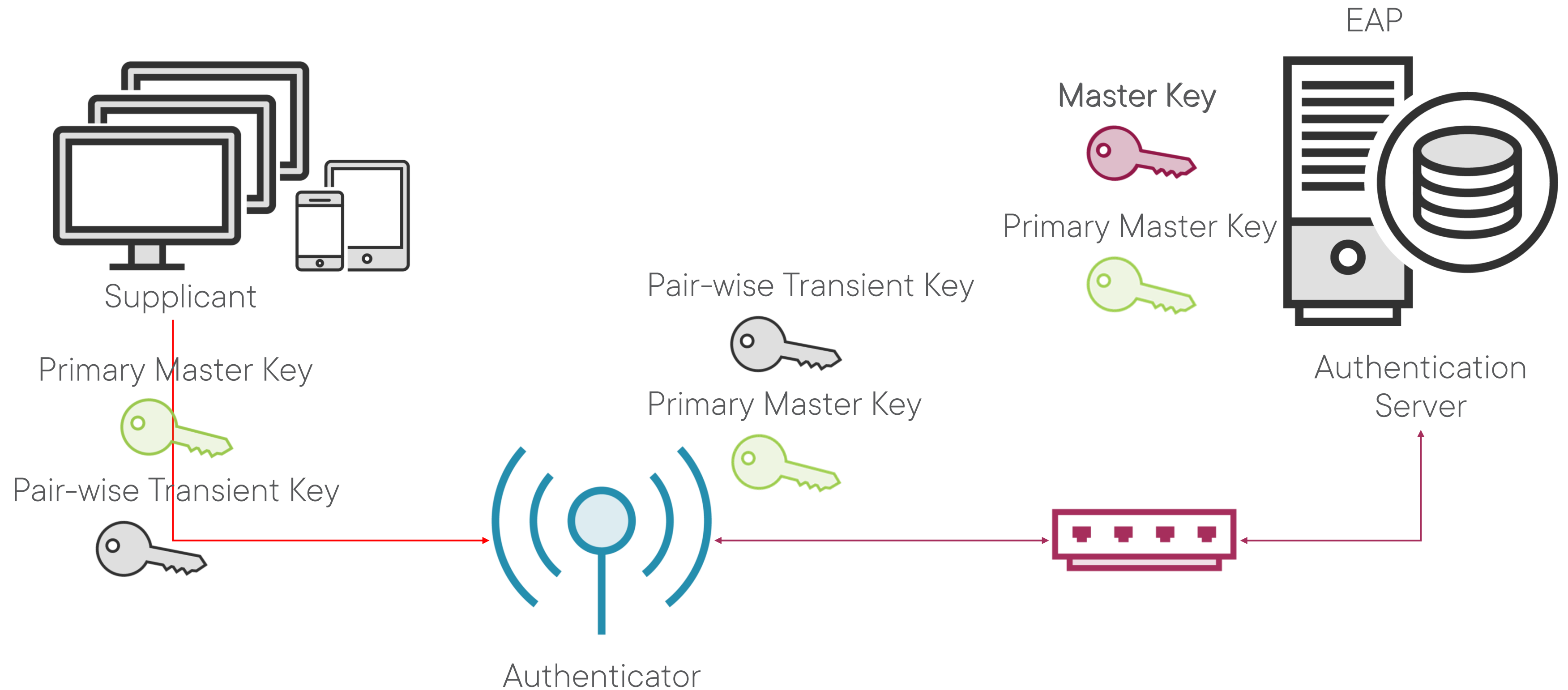


802.1x

Supports both user and machine authentication with port-based controls

Supports both wired switches and wireless access points

How 802.1x Works





Security Issues Found in WPA



Vulnerable to password-cracking attacks



All packets are vulnerable to encryption



Vulnerable to packet spoofing and decryption that allows attackers to hijack TCP connections



GTK predictability which allows malicious traffic to be injected into the network



IP addresses of the subnet can easily be identified or guessed

Security Issues Found in WPA2



Vulnerable to both man-in-the-middle (MiTM) and denial-of-service (DoS) attacks



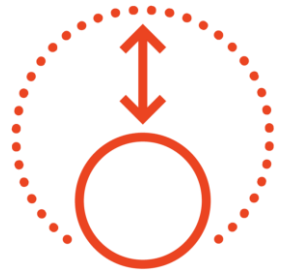
Vulnerable to an exploit known as key reinstallation attack (KRACK)



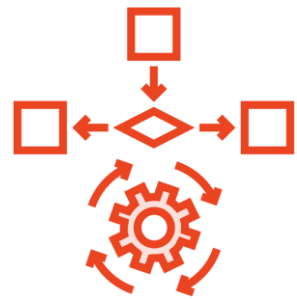
It's WPA2 key can be disclosed by determining the WPS's PIN through simple steps

WPA3 Encryption

WPA3



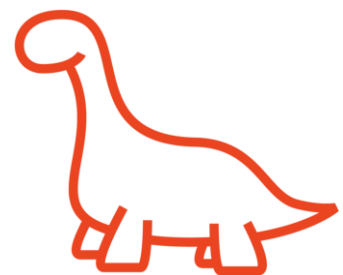
Supports both large and small deployments



Utilizes encryption algorithms like AES and TKIP



Includes enhanced network resilience to deliver a stronger defense against eavesdropping and forging attacks



Rejects outdated legacy protocols

WPA2 Compared to WPA3



WPA2 Compared to WPA3



Layered security strategy



Improved protocol to protect passwords



Specifies standards



Modes of Operation

WPA3 Personal

Resistant to offline dictionary attacks

Resistant to key recovery

Provides users password choices

Easy accessibility

WPA3 Enterprise

Authenticated encryption

Key derivation and validation

Key establishment and verification

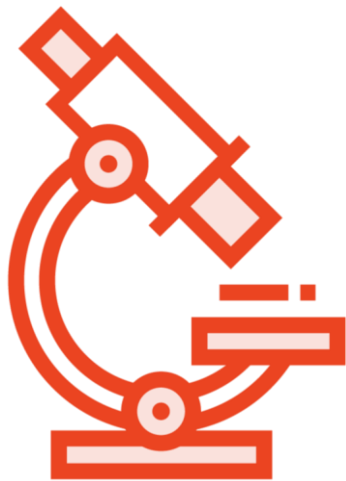
Frame protection

Breaking Encryption

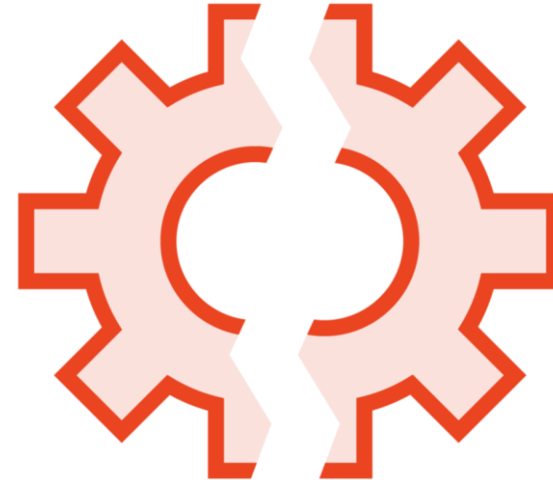
IV Vulnerabilities



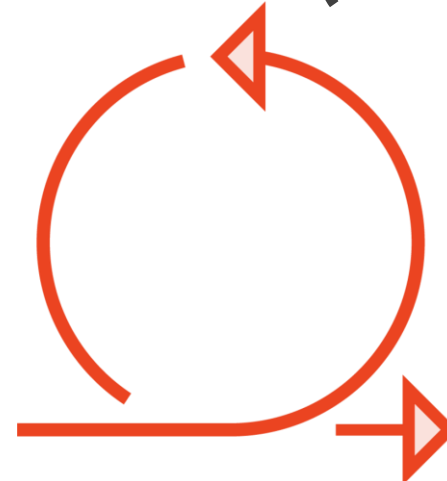
**How to break
encryption**



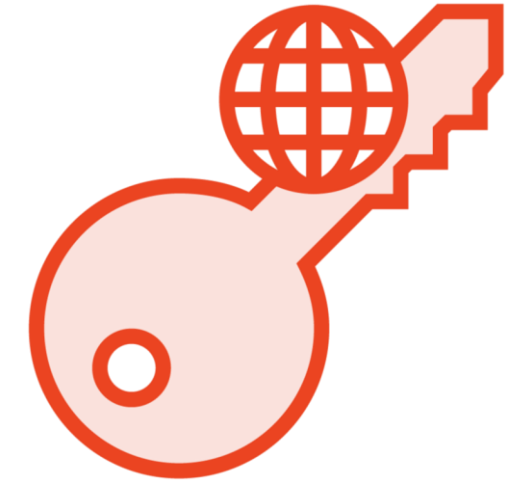
Predictable



**Feeble
initialization
vectors (IVs)**



**Reused
many times**

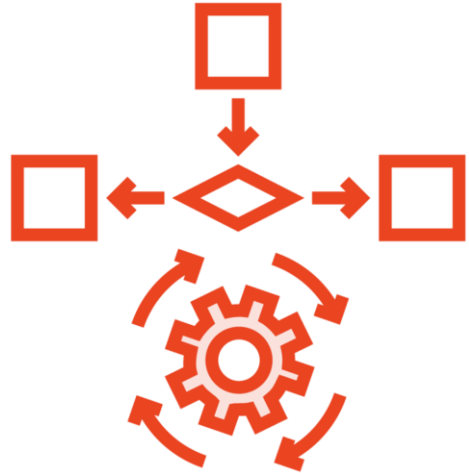


**WEP uses a key
scheduling
algorithm**



**Vulnerable to
FMS attacks**

IV Vulnerabilities



**Takes advantage
of RC4 algorithms**



**Simple tools
exploit its
weakness**



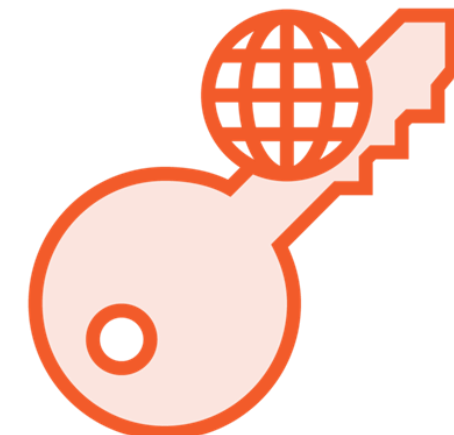
**Tampering is hard
to identify**



**Can be detected
quickly**



**Sniffing tools
capture its
packets**

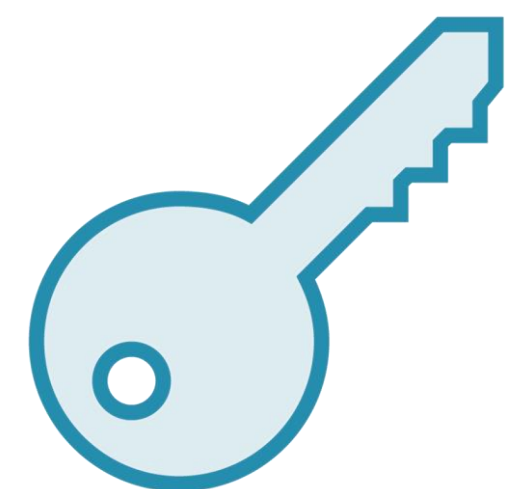
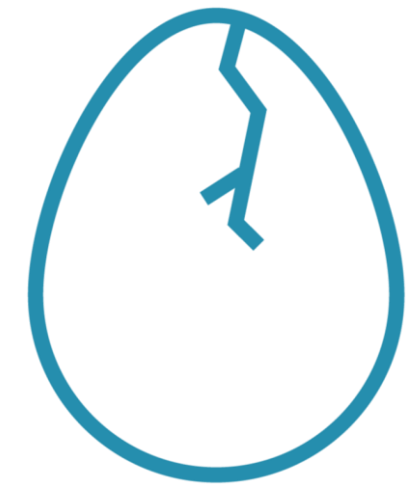
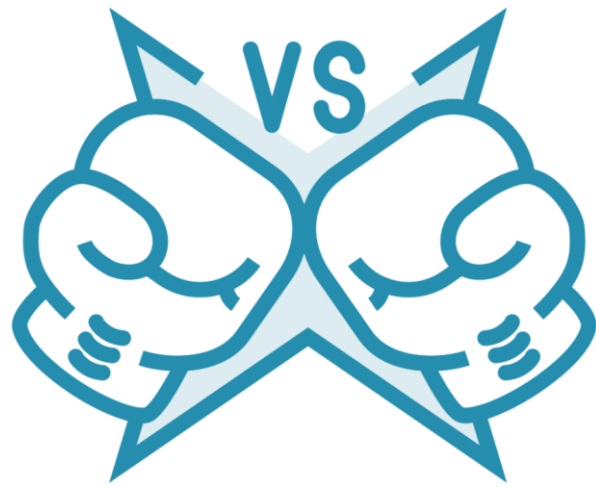


**Base key is easily
accessed**



**Initialization vectors are what makes
WEP vulnerable and easy to crack**

Breaking WPA's Encryption



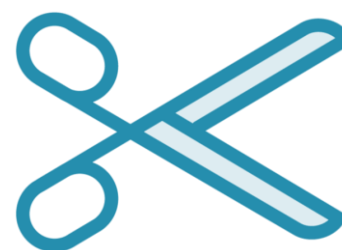
Crackin' Tools



Aircrack-ng



KisMAC



Reaver

Breaking Encryption

WPA PSK

De-authentication attack

Guessing of IP addresses

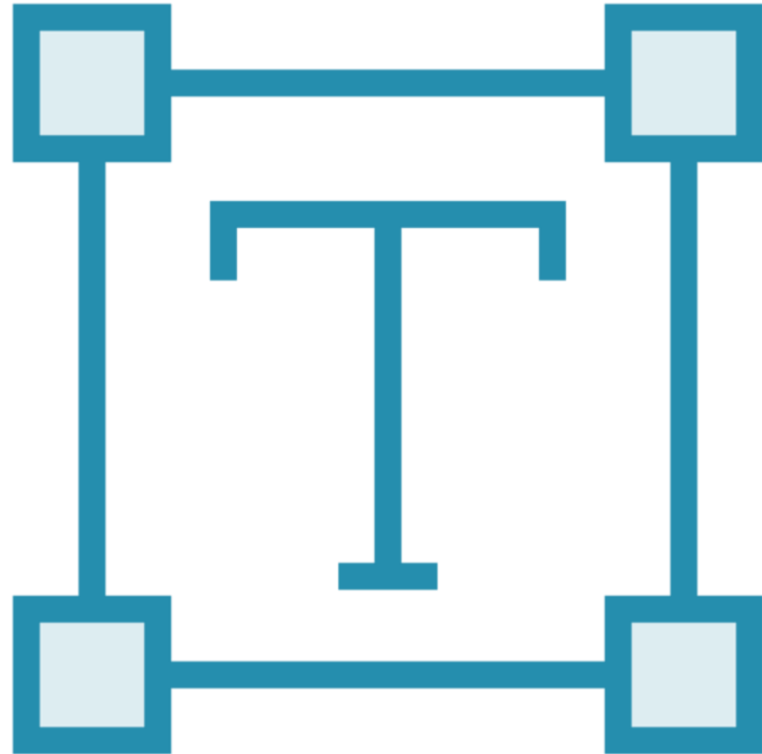
WPS



Defense Measures

Knowing risks will help us and
our networks become stronger
and safer

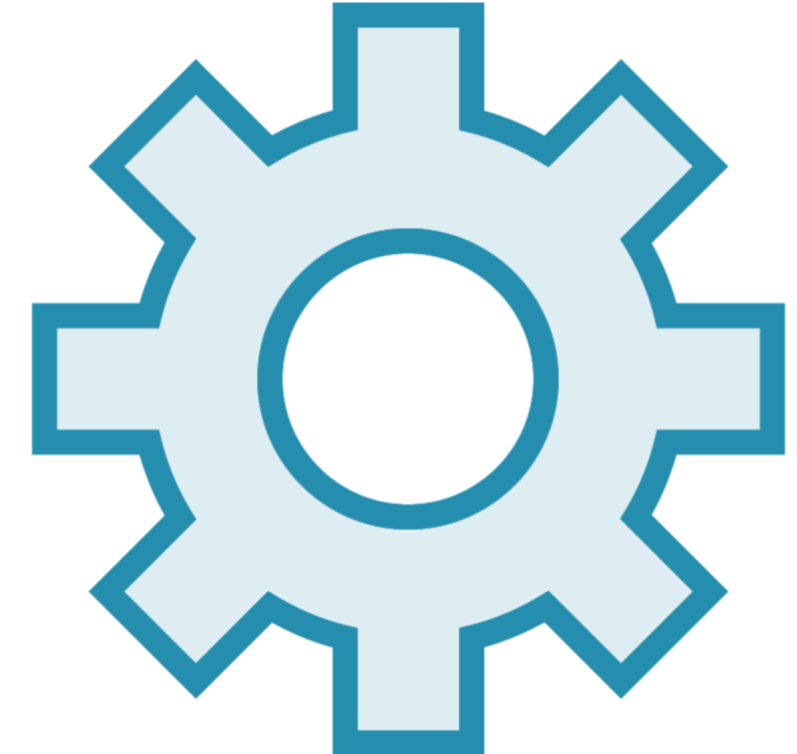
Securing Networks



Passphrases

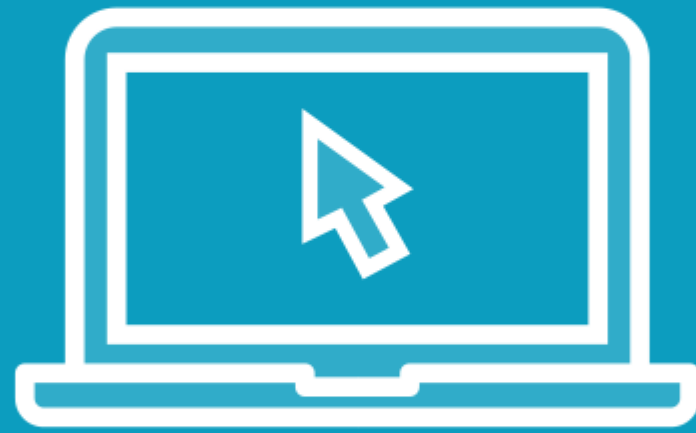


Added Controls



Client Settings

Demo



Cracking WPA-PSK Using Aircrack-ng

Demo



Examining the encryption options

Demo



Find WPS-Enabled APs

Demo



Find Normally and Hidden APs

Learning Check

Learning Check



Pre-shared keys / Same key



Enterprise



Dragonfly Key Exchange



104-bits



TKIP



Up Next:
Appraising Wireless Threats
