Herzlich Willkommen

Bern Beer-Talk

13.03.2019, Bern, Patrick Vananti @ Compass Security

Beer-Talk

Bier

Selbstgebrautes Know-How

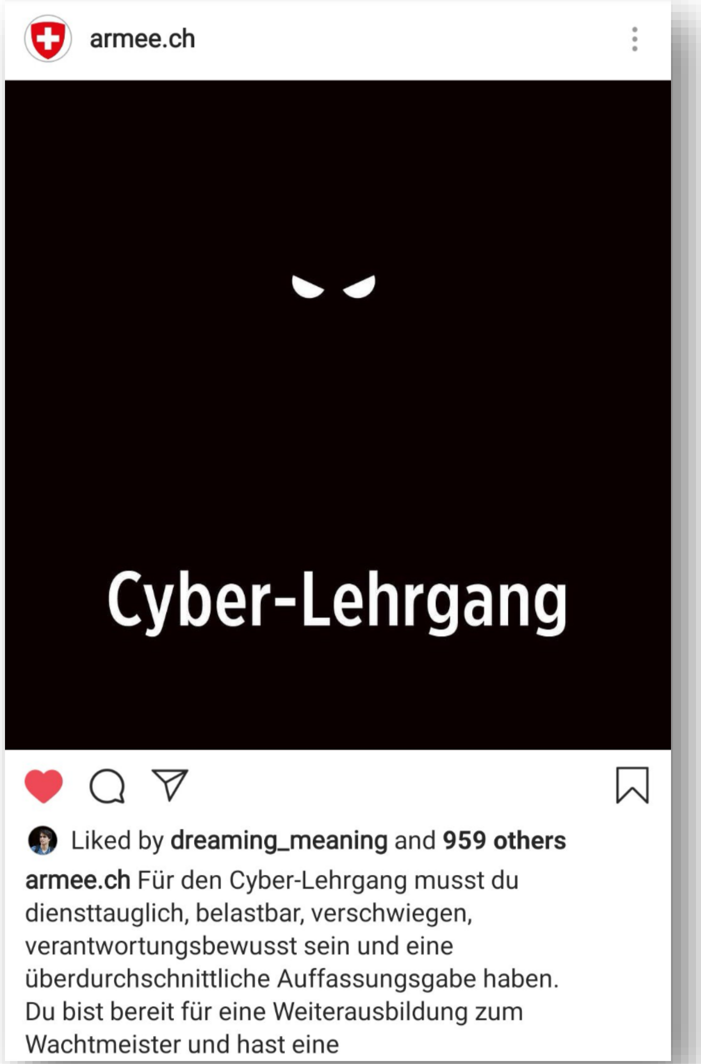
Talk

Bier + Essen

Save the Date!

COMPASS SECURITY
June 7th, 2019

Cyber-Lehrgang



Liked by **dreaming_meaning** and **959 others**

armee.ch Für den Cyber-Lehrgang musst du diensttauglich, belastbar, verschwiegen, verantwortungsbewusst sein und eine überdurchschnittliche Auffassungsgabe haben. Du bist bereit für eine Weiterausbildung zum Wachtmeister und hast eine

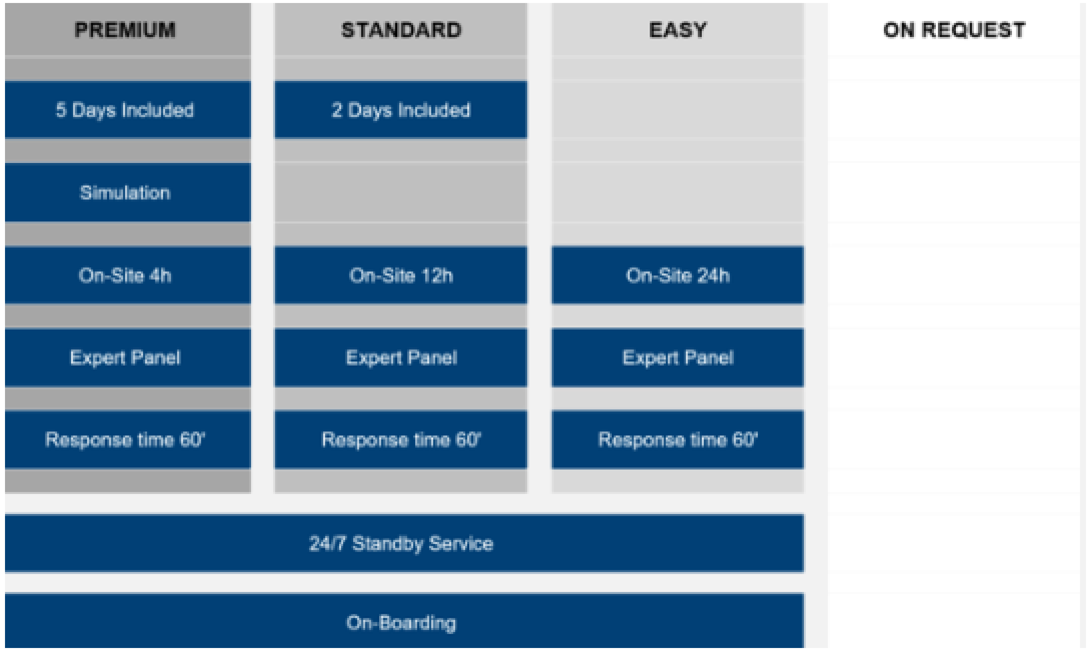
Powered by Hacking-Lab

Kurse

12./13. November 2019
Social Engineering

Erhöhte Nachfrage für

24/7 Incident Service



PREMIUM	STANDARD	EASY	ON REQUEST
5 Days Included	2 Days Included		
Simulation			
On-Site 4h	On-Site 12h	On-Site 24h	
Expert Panel	Expert Panel	Expert Panel	
Response time 60'	Response time 60'	Response time 60'	
24/7 Standby Service			
On-Boarding			

Heutiges Thema

Freibier
Free WiFi spot
Passwort: Biergarten

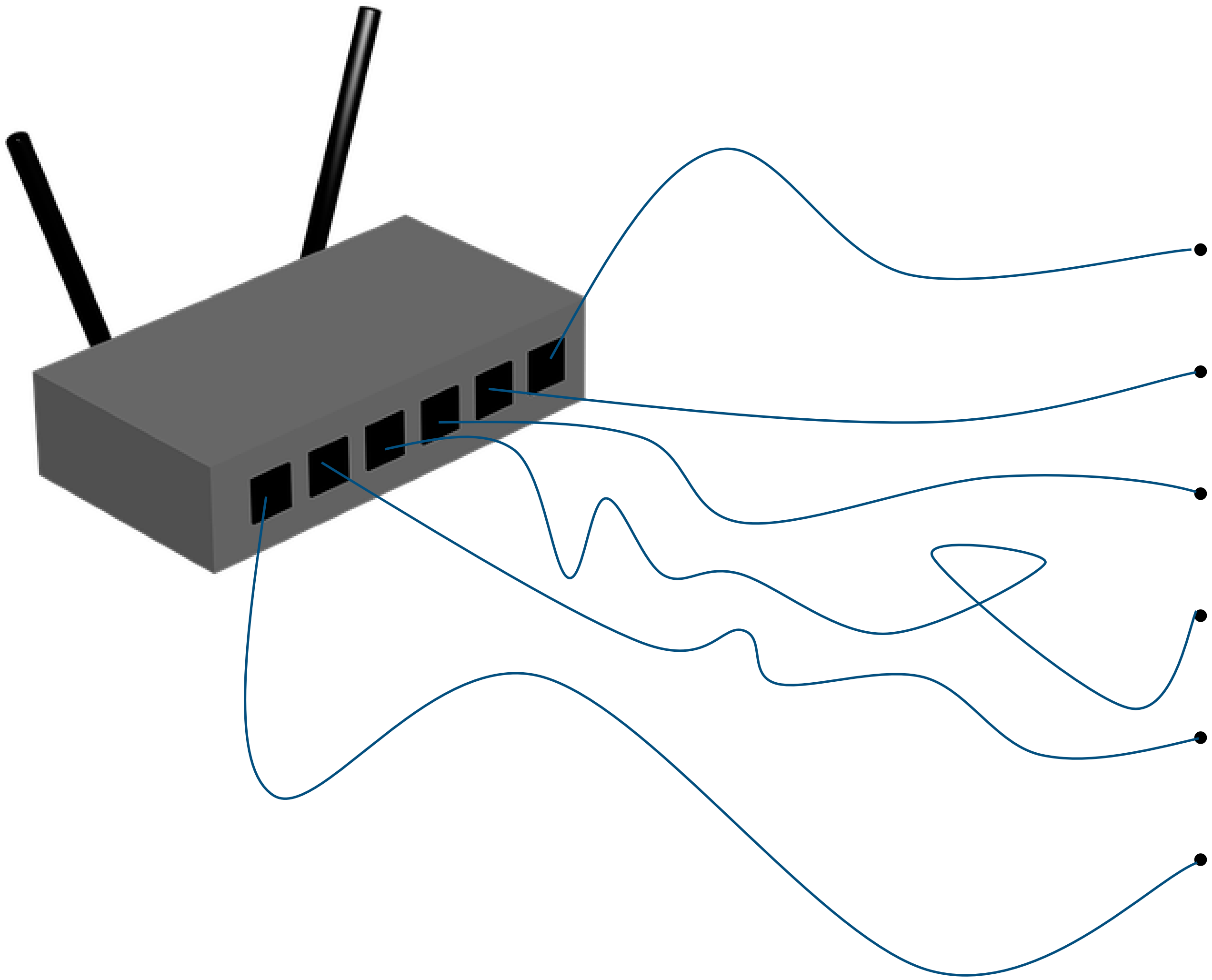
Proscht und
Viel Spass

WiFi from Open to WPA3

Beer-Talk #18

13th March, Bern, Felix Sieges

Agenda



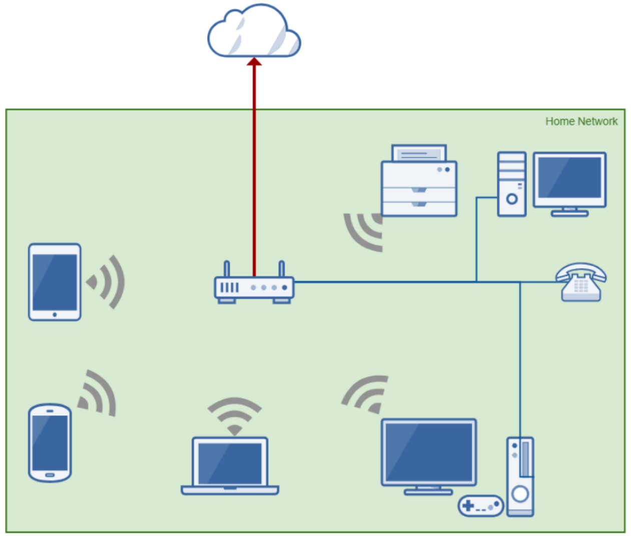
- Introduction
- Authentication
- Preamble
- Attacks
- Defenses
- Questions?

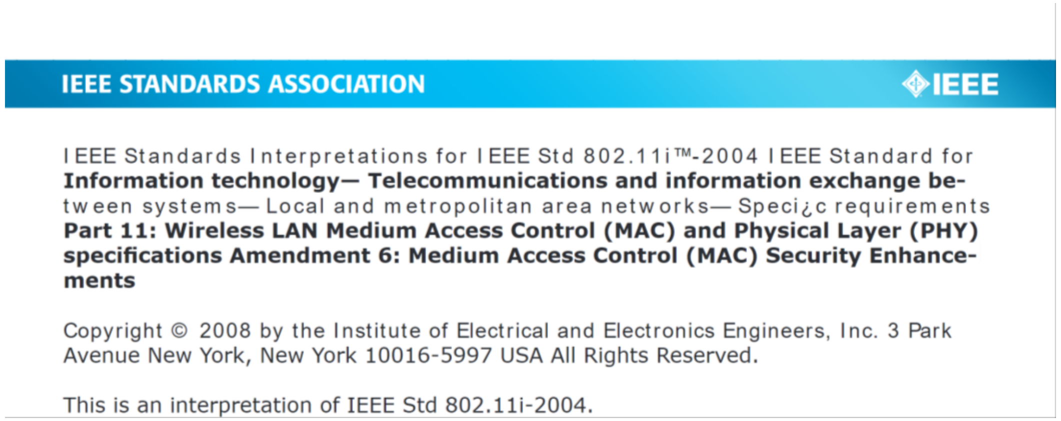
Introduction to WiFi

IEEE 802.11 Standards

WLAN

Wi-Fi




IEEE STANDARDS ASSOCIATION

IEEE

IEEE Standards Interpretations for IEEE Std 802.11i™-2004 IEEE Standard for **Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks— Speci¿c requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements**

Copyright © 2008 by the Institute of Electrical and Electronics Engineers, Inc. 3 Park Avenue New York, New York 10016-5997 USA All Rights Reserved.

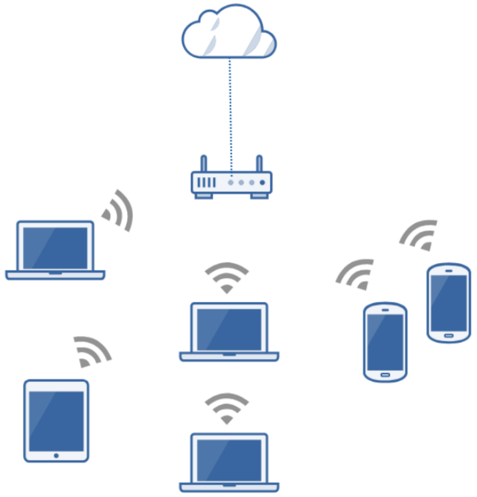
This is an interpretation of IEEE Std 802.11i-2004.

Wi Fi®

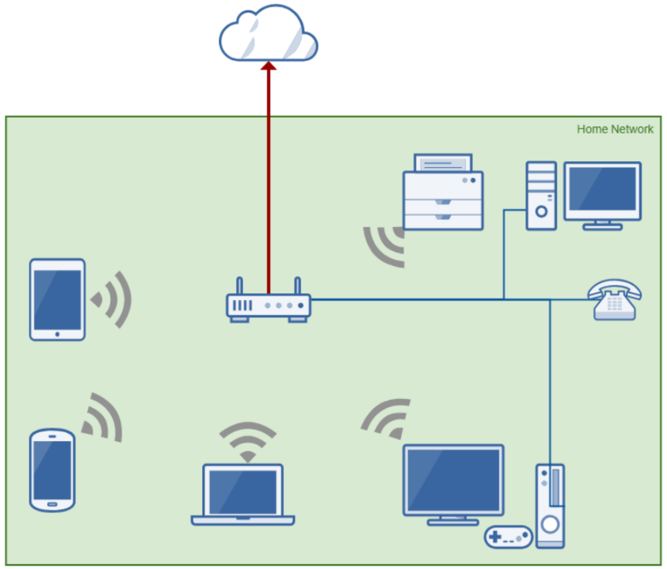
CERTIFIED

Architectures

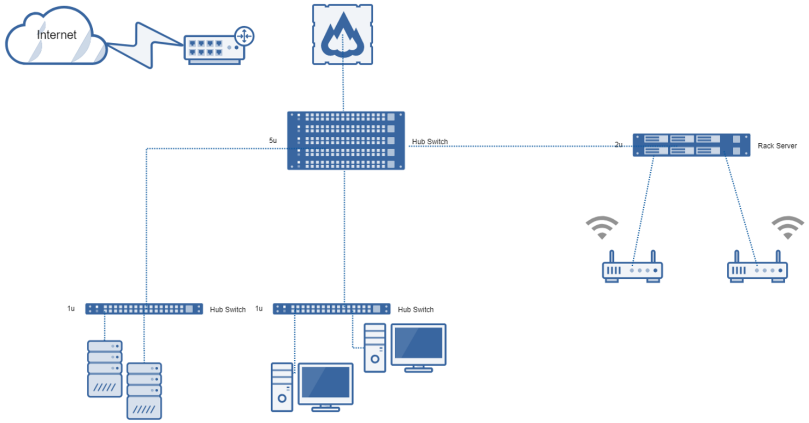
Open Hotspots



Home Networks



Corporate Networks

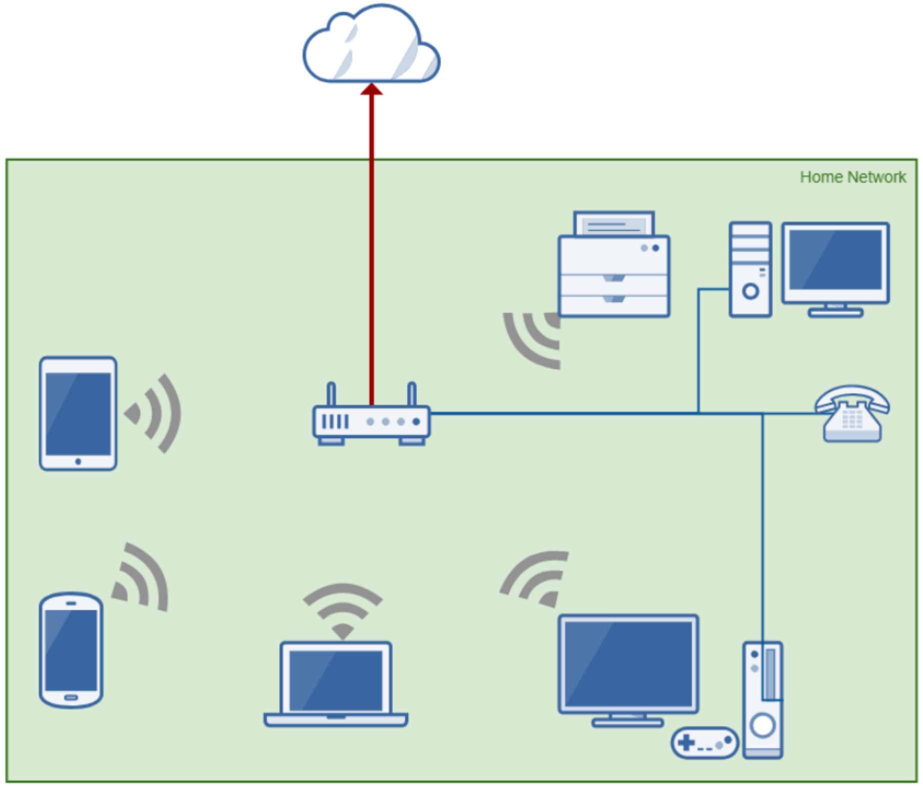


Authentication and Encryption

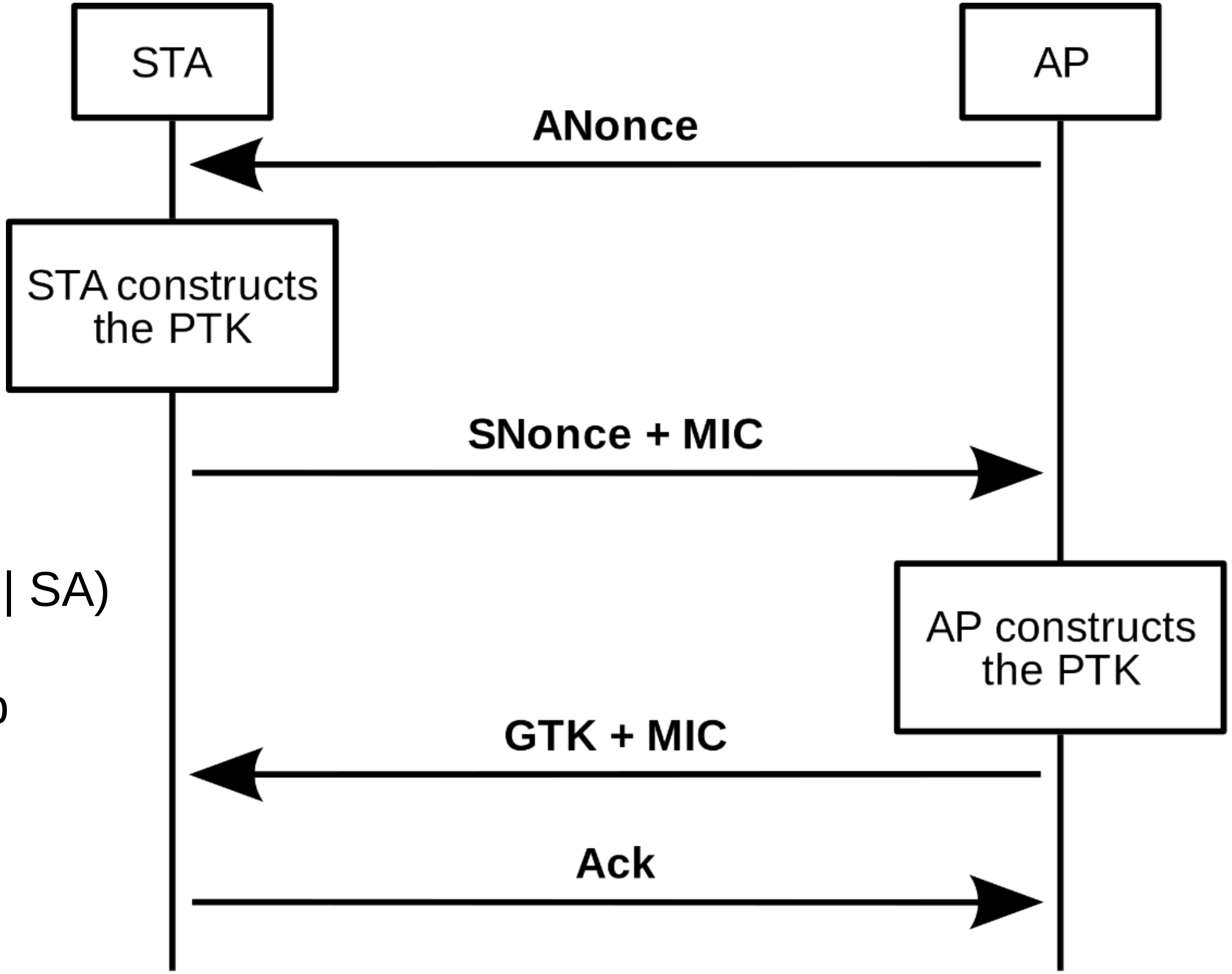
The Attack Surface

WiFi Protected Access 2 (WPA2-PSK)

- Superseeded WEP and WPA
- Also called RSN (Robust Security Network)
- Must be compliant to (802.11i)
- Mandates CCMP (AES)
- Still supports TKIP (RC4)!
- PMF (802.11w)
- KRACK mitigations



four-way handshake

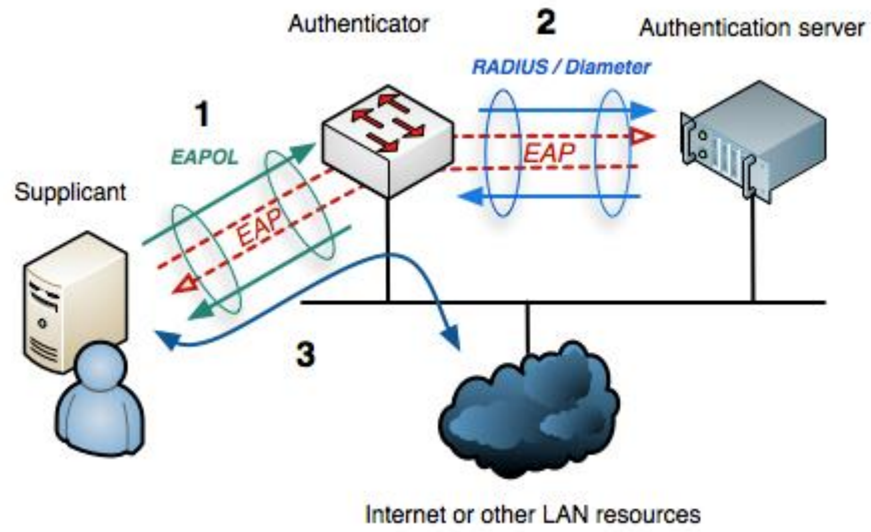


1. Prove the knowledge of PSK/PMK
2. Generate PTK (Pairwise Transient Key)
   - PTK = PRF(PMK | ANonce | SNonce | AA | SA)
3. Generate GTK (Group Temporal Key)
4. GTK is updated if a device leaves the group

Extensible Authentication Protocol (EAP)

- PEAPv1/MSCHAPv2 Authenticates with the Windows User and Passwort against an Authentication Server such as Radius.
- Access Point are 802.1X enabled NAS
- Uses the traditional four-way handshake
- The PMK is a key derived from EAP/WPA-802.1X

- EAP-TLS Authenticates with client side X.509 Certificates



- Supplicant = Station (client)
- Authenticator = AP (access point)
- Authentication Server = Radius

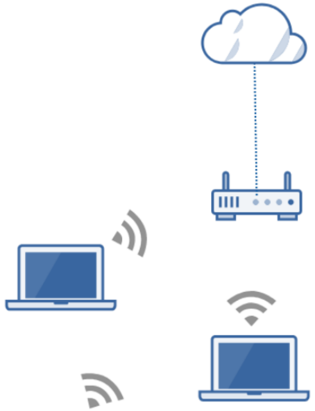
Opportunistic Wireless Encryption (OWE)

Replaces „Open Networks“ and Networks with PSK known to the public.

- No authentication
- It is encrypted
- PFS is used

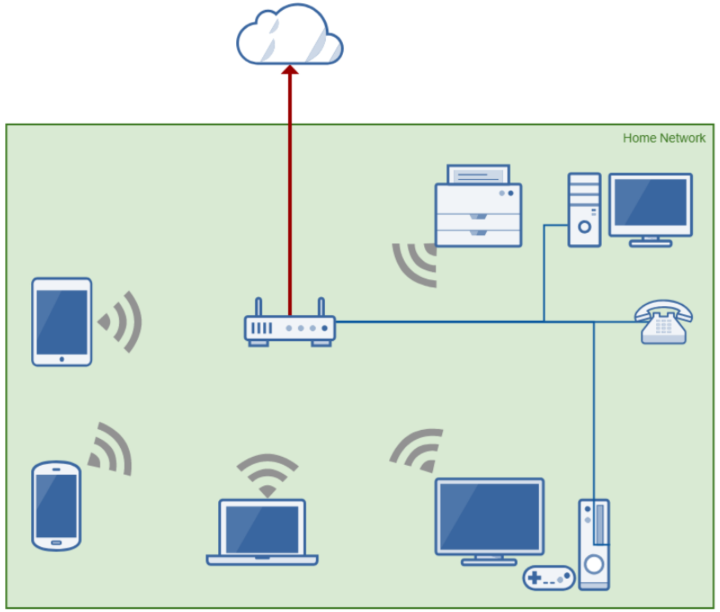
OWE = DH + four-way handshake:

1. Performs a DiffieHellman key exchange
2. Resulting pairwise secret is used as PMK
3. Is doing the traditional four-way handshake

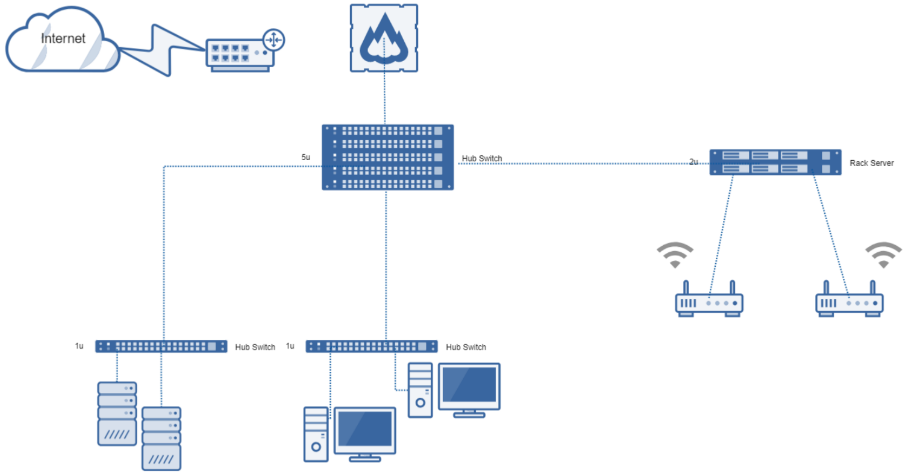


WPA3

WPA3-Personal



WPA3-Enterprise

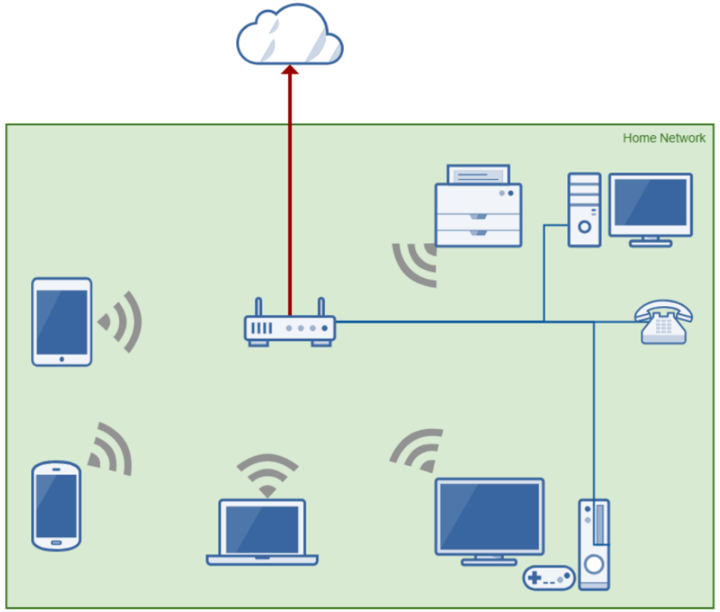


WiFi Protected Access 3 (WPA3-PSK)

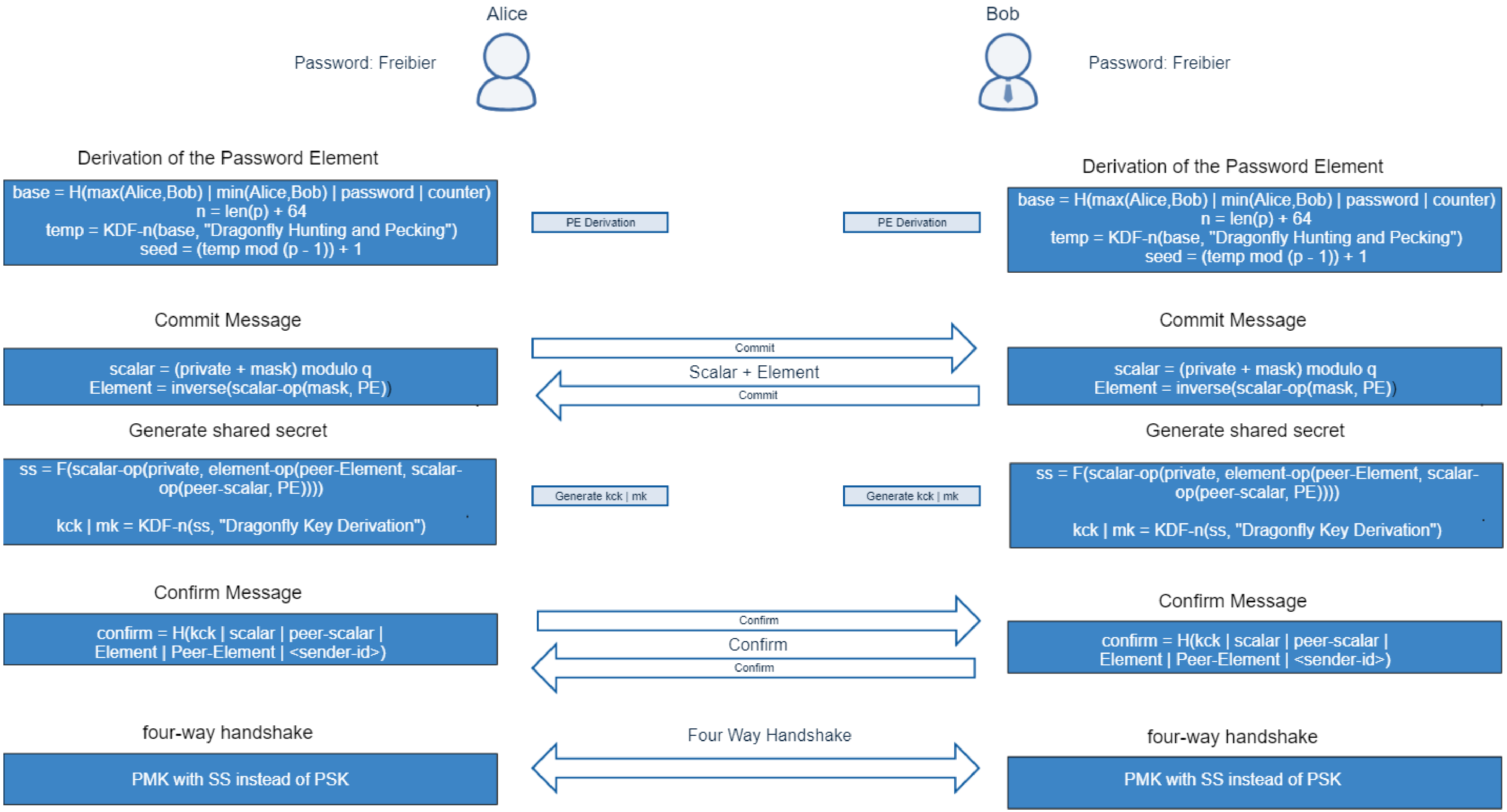
- Superseeds WPA2
- NSA Suite B 128-bit
- Makes use of PFS (Perfect Forward Secrecy)

SAE (Simultaneous Authentication of Equals):

- A Password is used as a shared credential
- SAE is used to generate the PMK
- The PMK is used in the traditional four-way handshake
- The four-way handshake ist used for GTK/PTK



SAE



Alice

Password: Freibier

Bob

Password: Freibier

Derivation of the Password Element

base = H(max(Alice,Bob) | min(Alice,Bob) | password | counter)
n = len(p) + 64
temp = KDF-n(base, "Dragonfly Hunting and Pecking")
seed = (temp mod (p - 1)) + 1

PE Derivation

PE Derivation

Derivation of the Password Element

base = H(max(Alice,Bob) | min(Alice,Bob) | password | counter)
n = len(p) + 64
temp = KDF-n(base, "Dragonfly Hunting and Pecking")
seed = (temp mod (p - 1)) + 1

Commit Message

scalar = (private + mask) modulo q
Element = inverse(scalar-op(mask, PE))

Commit

Scalar + Element

Commit

Commit Message

scalar = (private + mask) modulo q
Element = inverse(scalar-op(mask, PE))

Generate shared secret

ss = F(scalar-op(private, element-op(peer-Element, scalar-op(peer-scalar, PE))))

kck | mk = KDF-n(ss, "Dragonfly Key Derivation")

Generate kck | mk

Generate kck | mk

Generate shared secret

ss = F(scalar-op(private, element-op(peer-Element, scalar-op(peer-scalar, PE))))

kck | mk = KDF-n(ss, "Dragonfly Key Derivation")

Confirm Message

confirm = H(kck | scalar | peer-scalar | Element | Peer-Element | <sender-id>)

Confirm

Confirm

Confirm

Confirm Message

confirm = H(kck | scalar | peer-scalar | Element | Peer-Element | <sender-id>)

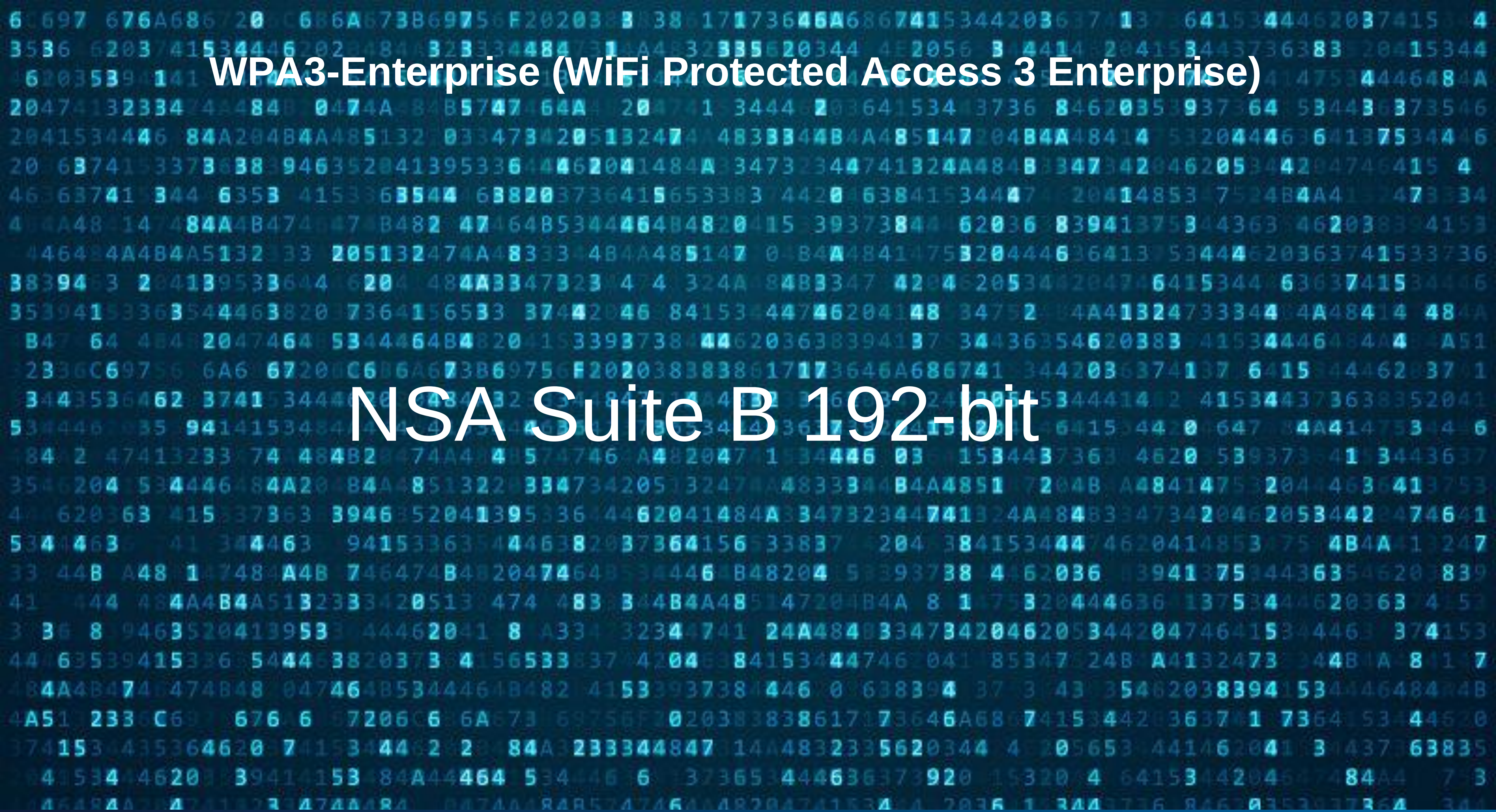
four-way handshake

PMK with SS instead of PSK

Four Way Handshake

four-way handshake

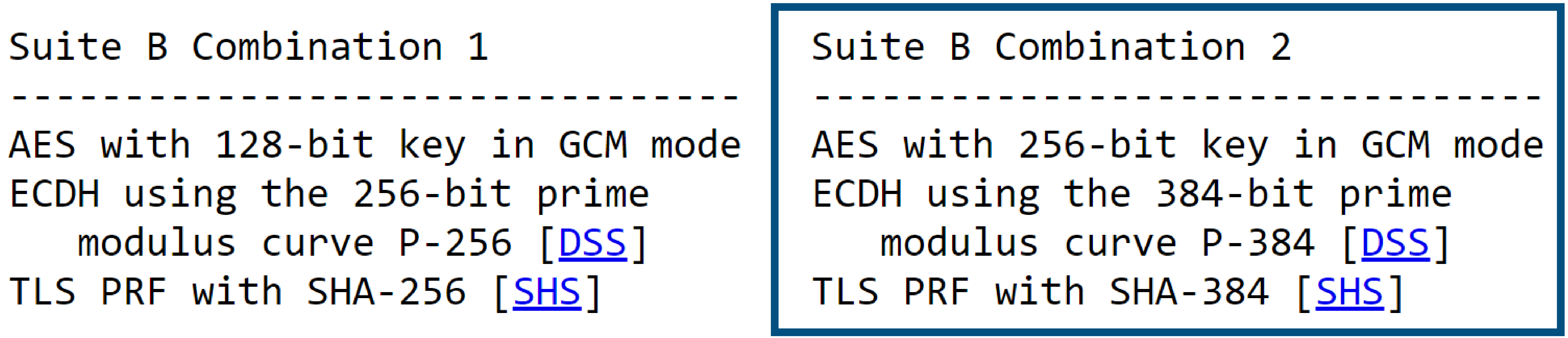
PMK with SS instead of PSK



WPA3-Enterprise (WiFi Protected Access 3 Enterprise)

NSA Suite B 192-bit

WPA3-Enterprise (WiFi Protected Access 3 Enterprise)



```
Suite B Combination 1
--------------------------------
AES with 128-bit key in GCM mode
ECDH using the 256-bit prime
   modulus curve P-256 [DSS]
TLS PRF with SHA-256 [SHS]
```

```
Suite B Combination 2
--------------------------------
AES with 256-bit key in GCM mode
ECDH using the 384-bit prime
   modulus curve P-384 [DSS]
TLS PRF with SHA-384 [SHS]
```

Preamble

Tales from war and espionage

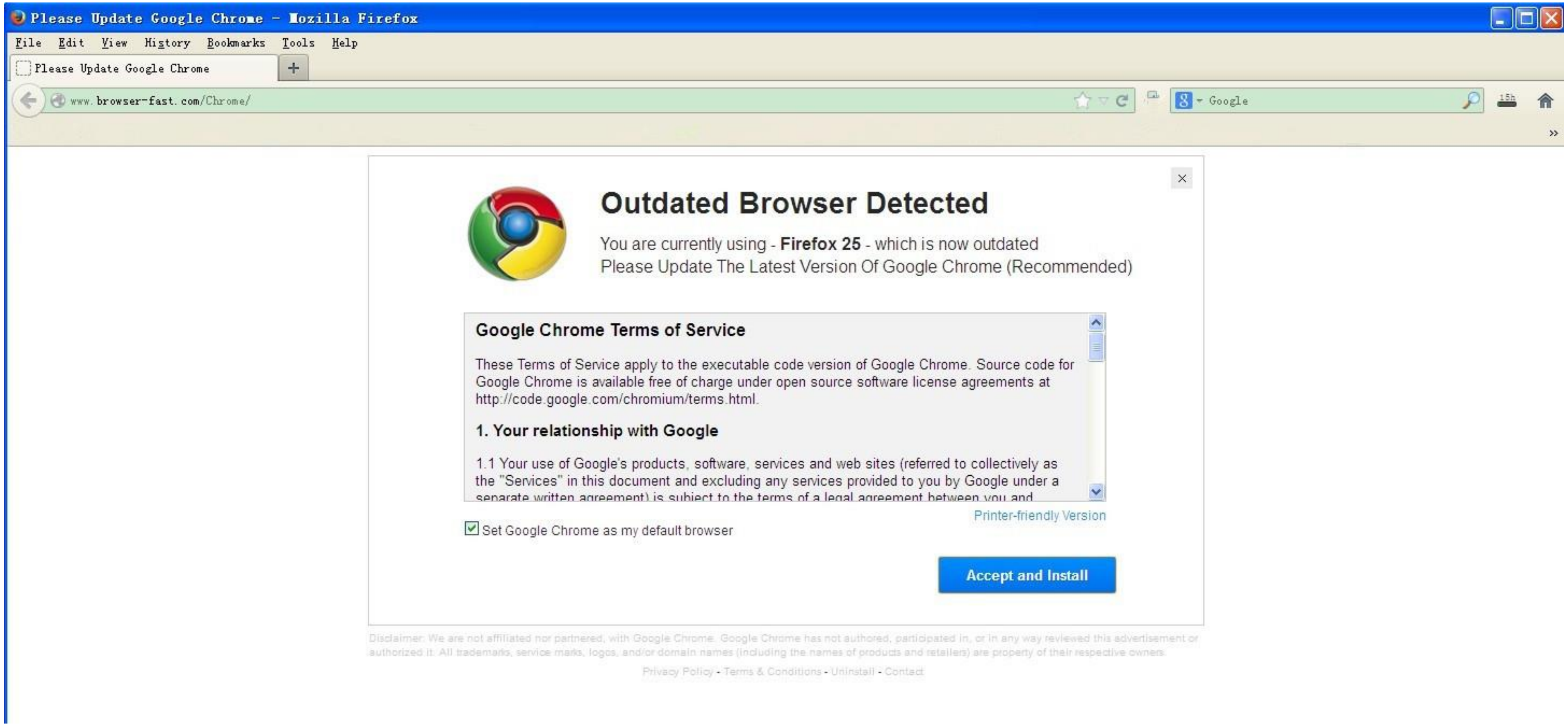
Dark Hotel APT

When some managers checked in to the Hotel, they connected to the Hotel WiFi…

2014: https://securelist.com/the-darkhotel-apt/66779/ by Kaspersky Inc.

Dark Hotel APT

they surfed the Internet. Some Pop-Ups appeared to coerce them into installing malware.


Please Update Google Chrome - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Please Update Google Chrome
www.browser-fast.com/Chrome/
Google

Outdated Browser Detected

You are currently using - **Firefox 25** - which is now outdated
Please Update The Latest Version Of Google Chrome (Recommended)

Google Chrome Terms of Service

These Terms of Service apply to the executable code version of Google Chrome. Source code for Google Chrome is available free of charge under open source software license agreements at http://code.google.com/chromium/terms.html.

1. Your relationship with Google

1.1 Your use of Google's products, software, services and web sites (referred to collectively as the "Services" in this document and excluding any services provided to you by Google under a separate written agreement) is subject to the terms of a legal agreement between you and

Printer-friendly Version

☑ Set Google Chrome as my default browser

Accept and Install

Disclaimer: We are not affiliated nor partnered, with Google Chrome. Google Chrome has not authored, participated in, or in any way reviewed this advertisement or authorized it. All trademarks, service marks, logos, and/or domain names (including the names of products and retailers) are property of their respective owners.

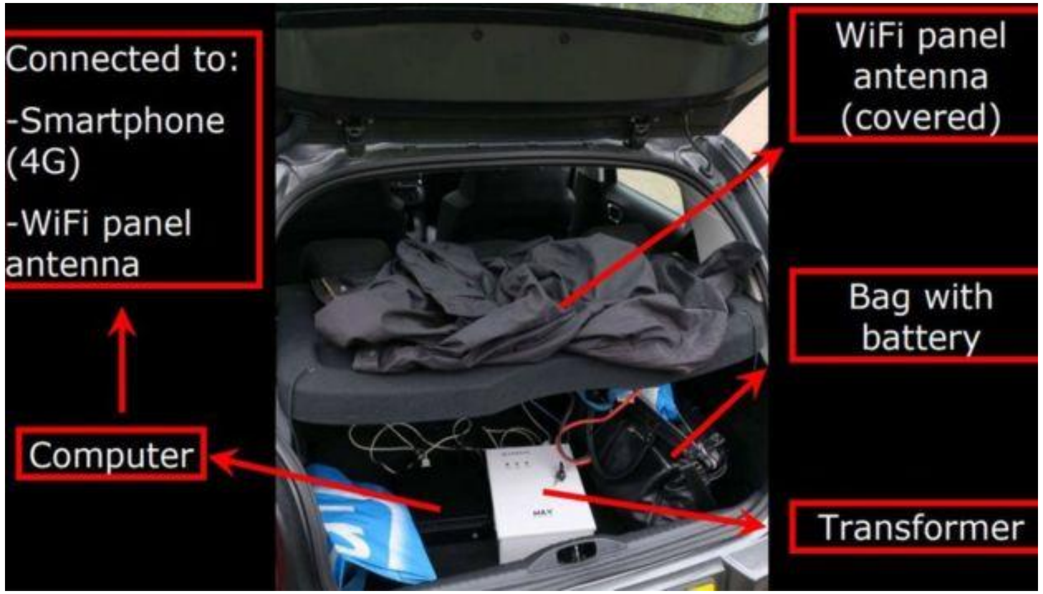
Privacy Policy - Terms & Conditions - Uninstall - Contact

It is believed that South Korean authorities are behind this act of economical espionage.

G.U World Tour

Canceled

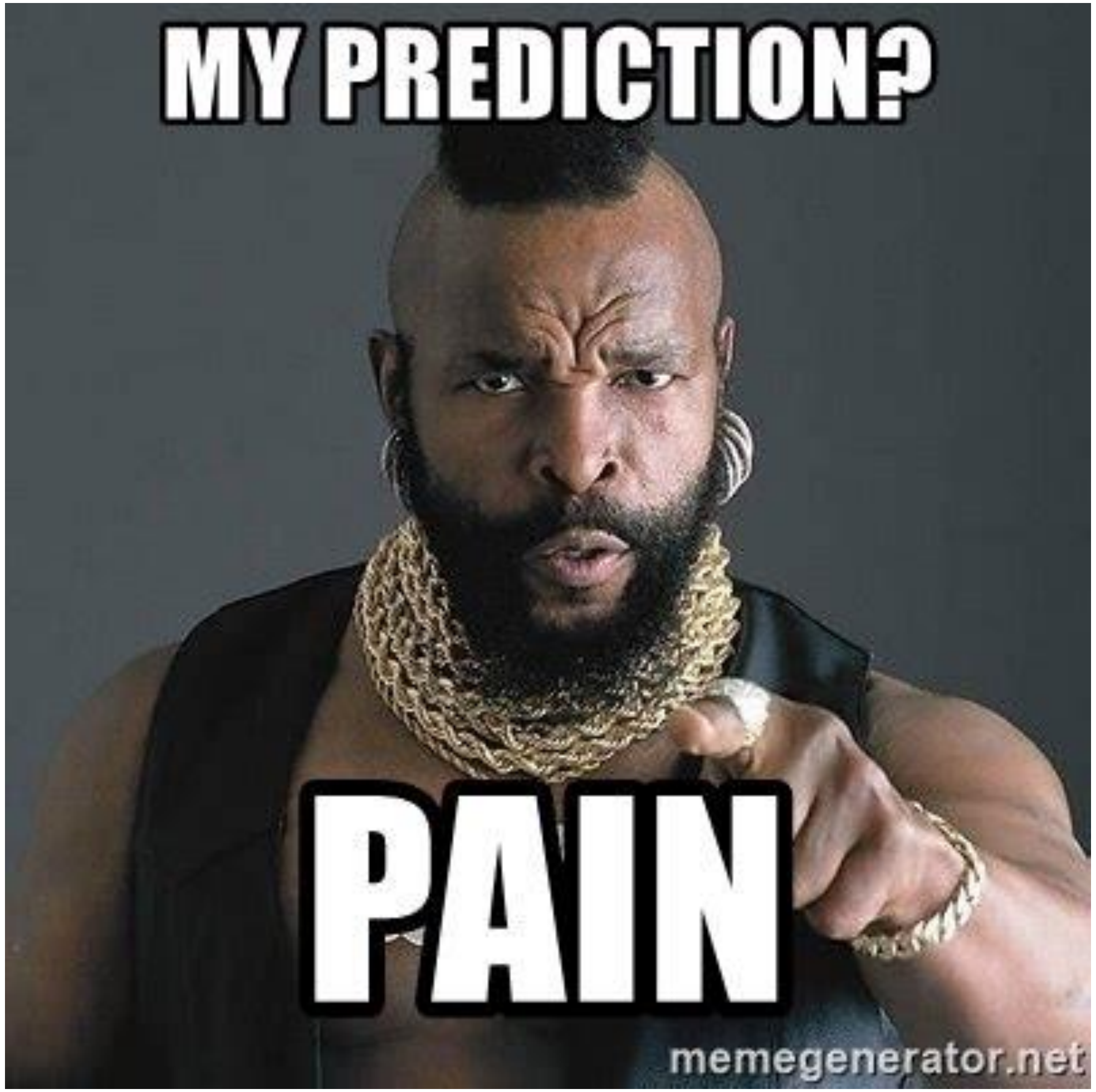
2016 Olympic Games: Brazil
2017 Kuala Lumpur: Malaysia
MH17 Investigation
2017 Lausanne: Switzerland
WADA
2018 The Hague: Netherlands
OPCW
2018 Spiez: Switzerland
OPCW



Attacks against WiFi

Do the new standards resolve all weaknesses?

Attacks against OWE



Attacks against OWE

https://tools.ietf.org/html/rfc8110 7. Security Considerations

> “OWE is susceptible to an active attack in which an adversary impersonates an access point and induces a client to connect to it via OWE while it makes a connection to the legitimate access point. In this particular attack, the adversary is able to inspect, modify, and forge any data between the client and legitimate access point.”

EvilTwin

Requirements:

- WiFi Interface with AP capabillities
- The victim AP SSID
- The victim AP authentication scheme

- More power than the victim AP

or

- Be closer to the victims client
- or
- DoS the Specific SSID

Demo – EvilTwin for OWE

Hooking the Browser

Attacks against WPA2

Attack	WPA2-PSK-TKIP	WPA2-PSK-CCMP
Clientless Password Cracking	🟥	🟥
Cracking four-way handshake	🟥	🟥
KRACK Attack	🟨	🟨
Evil Twin (with PSK)	🟥	🟥
Rogue Access Point	🟨	🟨
Decrypting sniffed Traffic (with PSK)	🟥	🟥
Injecting Traffic	🟥	🟩
Deauthentication	🟨	🟨

Attacks against WPA3

Attack	WPA3-PSK-CCMP
Clientless Password Cracking	🟩
Cracking four-way handshake	🟩
KRACK Attack	🟩
Evil Twin (with PSK)	🟥
Rogue Access Point	🟨
Decrypting sniffed Traffic (with PSK)	🟩
Injecting Traffic	🟩
Deauthentication	🟩

Demo – EvilTwin for WPA3

Stripping the „S“ from HTTPS

Attacks against WPA2-Enterprise and WPA3-Enterprise

- EvilTwin
- Rogue Access Points
- Capture Challenge Response
- Online Brute Force Attacks
- EAP-Spray
- Decryption with knowledge of the key
- Indirect Wireless Pivots (Bypass for 802.1x)

Demo WPA3-Enterprise

Getting Windows Credentials

Defenses

Protection against the known bad!

Security for Enterprise Networks

Implement Security from the Client to the Authentication Server!

- ✓ Enforce Certificate Validation on clients and Radius Servers
- ✓ Validate all participating parties
- ✓ Only use encrypted authentication Protocols
- ✓ EAP-TLS with X.509 is the most secure protocol
- ✓ EAP-PWD for employee access
- ✓ Use an internal PKI
- ✓ Enforce VPN for non-corporate Networks

Hardenings:

- ✓ Enable KRACK mitigations
- ✓ Enable Client isolation
- ✓ Use 802.1X based NAC
- ✓ Enable Management Frame Protection (802.11w)

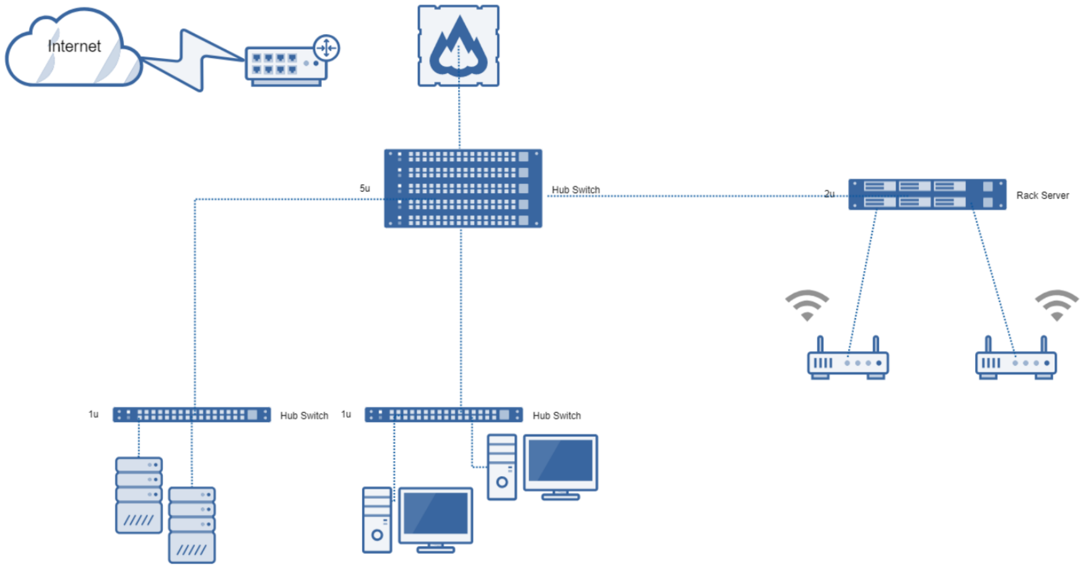
Monitoring and Logging

Detect:

- Rogue Access Points
- Brute Force Attacks
- Changes of channels/frequencies
- Evil Twins

Implement a WIPS:

Kismet



Log events into your favorite Log Analyzer.

Security for End Users

Clients:

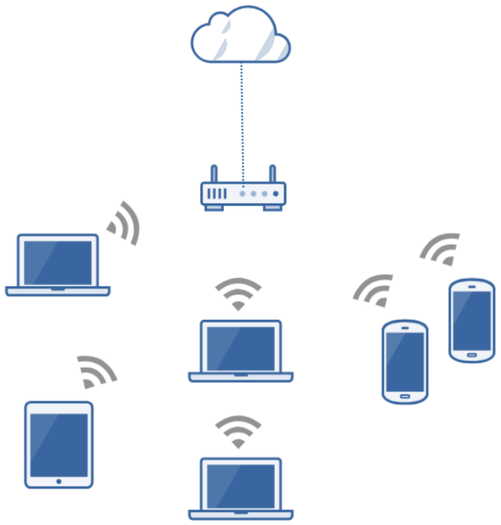
- ✓ Disable auto-connect!
- ✓ Turn off WiFi if not needed
- ✓ MAC-Randomization

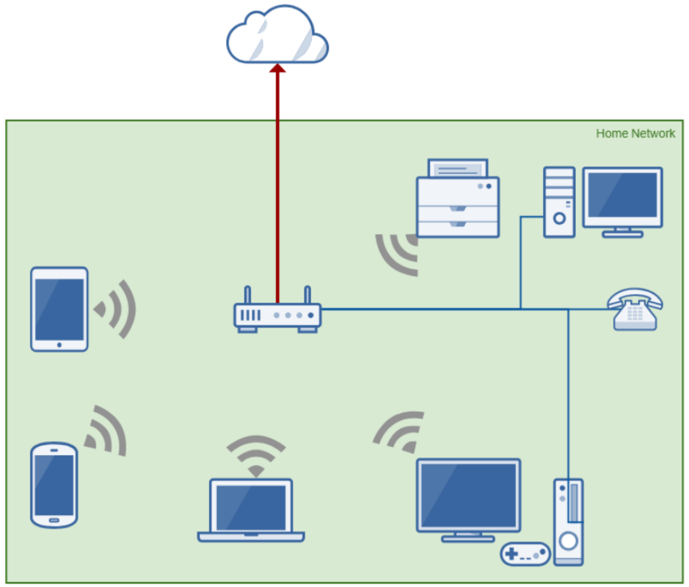
Hotspots:

- ✓ Hotspots might not be legitimate.
- ✓ If you need to use a Hotspot use a VPN

Your Home Network:

- ✓ WPA2-PSK-CCMP or WPA3-PSK-CCMP
- ✓ Management Frame Protection (802.11w)
- ✓ KRACK Mitigations
- ✓ Strong and Secure PSK
- ✓ Disable WPA and Open Networks
- ✓ Disable WPA2-TKIP





Really disable auto-connect for every WiFi network!
It does not mean you have to re-type credentials ;)

COMPASS
SECURITY

Images Credits

- Pixabay
- https://svgsilh.com/image/1985537.html
- www.jisc.ac.uk
- https://commons.wikimedia.org/wiki/File:1905_home_network_-_multi_devices_graphic.jpg

Sources

A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3 Christopher P. Kohlios and Thaier Hayajneh
https://papers.mathyvanhoef.com/ccs2017.pdf
Python Scapy Dot11: Python Programming for Wi-Fi pentesters by Yago Hansen
ISBN: 1722351496
https://papers.mathyvanhoef.com/ccs2017.pdf
https://wlan1nde.wordpress.com/2014/10/27/4-way-handshake/
https://tools.ietf.org/html/rfc7664
https://tools.ietf.org/html/rfc8110
https://github.com/s0lst1c3/evil_twin
https://github.com/s0lst1c3/eaphammer
https://github.com/bettercap/bettercap