¡Póngame 3! 
Whisky, Pacharán y Anís
WPA3
(v. "Happy Hour")
WPA3 Timeline Night Out Analogy
Outline

• Wi-Fi® security evolution and timeline
• WPA2 today: TKIP & PMF
• WPA3
  – WPA3-Personal: Simultaneous Authentication of Equals (SAE)
  – WPA3-Enterprise: 192-bit security mode
  – Wi-Fi Enhanced Open™: Opportunistic Wireless Encryption (OWE)
  – Wi-Fi Easy Connect™: Wi-Fi Device Provisioning Protocol (DPP)
• Conclusions
• References
Wi-Fi® Security Evolution

- Open
- WEP (Wired Equivalent Privacy)
- WPA (Wi-Fi Protected Access®)
- WPA2 (Wi-Fi Protected Access® 2)
  - Personal (PSK – Pre-Shared Key)
  - Enterprise (802.1x/EAP – Extensible Authentication Protocol)
  - WPA / WPA2 mixed mode
    - TKIP, AES, TKIP/AES
- WPA3 (Wi-Fi Protected Access® 3)
  - Personal & Enterprise
WPA2
WPA2 Today

• Enhance the WPA2 certification program
  – It has continually evolved to meet security needs as the security environment changes (e.g. **TKIP**, or **WEP**, removal)

• 2018
  – Standardize 128-bit cryptographic suites
  – Mandatory use of **PMF** (Protected Management Frames)
  – Enhanced validation of vendor security implementations
    • E.g. KRACK attacks

https://www.wi-fi.org/discover-wi-fi/security
WPA3
WPA3 Announcement

- Four new capabilities for personal and enterprise Wi-Fi networks will emerge in 2018 as part of WPA3™ (January 2018… June 2018):
  - Robust protections even when users choose passwords that fall short of typical complexity recommendations
    - WPA3-Personal: Simultaneous Authentication of Equals (SAE) vs. WPA2-PSK
  - A 192-bit (cryptographic) security suite to protect Wi-Fi networks with higher security requirements such as government, defense, and industrial
    - WPA3-Enterprise: 192-bit security mode vs. 128-bit
  - Strengthen user privacy in open networks through individualized data encryption
    - Wi-Fi Enhanced Open™ (OWE) vs. Open networks
  - Simplify the process of configuring security for devices that have limited or no display interface
    - Wi-Fi Easy Connect™ (DPP) vs. Wi-Fi Protected Setup (WPS)
WPA3

• WPA3 (or Wi-Fi CERTIFIED WPA3™)
  – Home networks (Personal) & Corporate environments (Enterprise)
• Backward "compatibility"
  – All devices supporting WPA3 will continue to work with WPA2 devices (WPA2 is still mandatory)
• Network resiliency
  – Protected Management Frames (PMF) required
• Cryptographic consistency
  – Use of Advanced Encryption Standard (AES)
  – No legacy protocols: Temporal Key Integrity Protocol (TKIP) / WEP
Thanks!

Fecha: "finales de marzo 2019"
(4ª Edición)

Practical Wireless & Radio Hacking (PWRH)
- Bootcamp -

/RootedCON 2018 2019
References
References

• WPA3: Technical Details and Discussion (March 12, 2018)

• DinoSec's 10-Year Anniversary... and WPA3 (May 23, 2018)

• WPA3: A Missed Opportunity (June 27, 2018)

• Wi-Fi Alliance: Current Work Areas
  – https://www.wi-fi.org/who-we-are/current-work-areas

• WPA3 (Schneier on Security) – See the comments 😊

• Wi-Fi Gets More Secure: Everything You Need to Know About WPA3
References: Wi-Fi Alliance®

• Press Releases
  – January 8, 2018: Wi-Fi Alliance® introduces security enhancements
  – June 5, 2018: Wi-Fi Enhanced Open™ delivers data protection in open Wi-Fi® networks
  – June 25, 2018: Wi-Fi Alliance® introduces Wi-Fi CERTIFIED WPA3™ security

• Beacon
References: Wi-Fi Alliance® Specifications (1/3)

• WPA3 (or Wi-Fi CERTIFIED WPA3™)
  – https://www.wi-fi.org/security

• Wi-Fi Security Highlights

• WPA3 Technology Overview (registration required) - June 2018
  – https://www.wi-fi.org/downloads-registered-guest/Wi-Fi%2BCERTIFIED%2BWPA3%2BTechnology%2BOverview.pdf/35521 (6 pages)

• WPA3 Specification v1.0 (registration required) – 2018-04-09

• SAE (IEEE Std 802.11-2016) & Dragonfly Key Exchange (RFC 7664)
References: Wi-Fi Alliance® Specifications (2/3)

• Wi-Fi Enhanced Open
  – http://wi-fi.org/enhanced-open
• Opportunistic Wireless Encryption (OWE) - RFC 8110
• Wi-Fi CERTIFIED Enhanced Open™ Technology Overview (registration required)
• Opportunistic Wireless Encryption Specification v1.0 (registration required)
  – https://www.wi-fi.org/downloads-registered-guest/Opportunistic_Wireless_Encryption _Specification_v1.0_0.pdf/35331 (7 pages)
References: Wi-Fi Alliance® Specifications (3/3)

• Wi-Fi Easy Connect
  – https://www.wi-fi.org/wi-fi-easy-connect

• Wi-Fi CERTIFIED Easy Connect™ Technology Overview (registration required)
  – https://www.wi-fi.org/downloads-registered-guest/Wi-Fi%2BCERTIFIED%2BEasy%2BConnect%2BTechnology%2BOverview.pdf/35503 (7 pages)

• Device Provisioning Protocol Specification v1.0 (registration required)
  – Device Provisioning Protocol (DPP)
References: IEEE & IETF

- IEEE Std 802.11-2016: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (Dec'16)
  - https://standards.ieee.org/findstds/standard/802.11-2016.html (3,534 pages)
  - Simultaneous Authentication of Equals (SAE)

- IEEE 802.11w-2009 (payware)

- IETF
  - RFC 7664: Dragonfly Key Exchange
  - RFC 8110: Opportunistic Wireless Encryption (OWE)
  - RFC 5297: Synthetic Initialization Vector (SIV) Authenticated Encryption Using… AES
hostap: hostapd & wpa_supplicant

- hostap log: search for "wpa3"
  - https://w1.fi/cgit/hostap/log/?showmsg=1&qt=grep&q=wpa3
  - WPA3 modes in hostapd.conf:
    - https://w1.fi/cgit/hostap/commit/?id=e7d73c378d891120c756f5534afc5f6919e0b0c6
  - WPA3 modes in wpa_supplicant.conf:
    - https://w1.fi/cgit/hostap/commit/?id=eclec4878b79076ece9e218e0b8014346325add7a

- Build
  - Enable CONFIG_SAE, CONFIG_OWE and CONFIG_DPP flags

- Testing PMF
  - https://wire-less-comm.blogspot.com/2013/05/testing-80211-protected-management.html

https://twitter.com/raulsiles/status/1025692198984200193
hostap & WPA3

• **hostapd.conf** ([https://w1.fi/cgit/hostap/plain/hostapd/hostapd.conf](https://w1.fi/cgit/hostap/plain/hostapd/hostapd.conf))

```plaintext
# WPA3 is also configured with bit1 since it uses RSN just like WPA2.
wpa=2

# Key Management:
# wpa_key_mgmt=WPA-PSK    # WPA-Personal / WPA2-Personal
# wpa_key_mgmt=SAE        # SAE (WPA3-Personal, instead of WPA-PSK (WPA2))
# wpa_key_mgmt=OWE        # Opportunistic Wireless Encryption (Enhanced Open)
# wpa_key_mgmt=DPP        # Device Provisioning Protocol (DPP)
```

• **wpa_supplicant.conf** ([https://w1.fi/cgit/hostap/plain/wpa_supplicant/wpa_supplicant.conf](https://w1.fi/cgit/hostap/plain/wpa_supplicant/wpa_supplicant.conf))

```plaintext
# WPA3 and WPA2/IEEE 802.11i (also WPA2 can be used as an alias for RSN).
proto=RSN

# Key Management:
# key_mgmt=WPA-PSK      # WPA-Personal / WPA2-Personal (WPA2 Pre-Shared Key)
# key_mgmt=SAE          # SAE (WPA3-Personal), Simultaneous Authentication of Equals
# key_mgmt=OWE          # Opportunistic Wireless Encryption (Enhanced Open)
# key_mgmt=DPP          # Device Provisioning Protocol (DPP)
```
www.dinosec.com
@dinosec

Raúl Siles
raul@dinosec.com
Questions?

NAVAJA NEGRA
CONFERENCE

www.dinosec.com
@dinoSec