DINOSEC CYBERSECURITY
www.dinosec.com
@dinosec

GUARDEDBOX
www.guardedbox.es
@guardedbox

Raúl Siles
Founder & Senior Security Analyst
raul@dinosec.com
Enero, 2026

¡Póngame 3 **más**!
Whisky, **P**acharán y **A**nís… y una Zurra

1

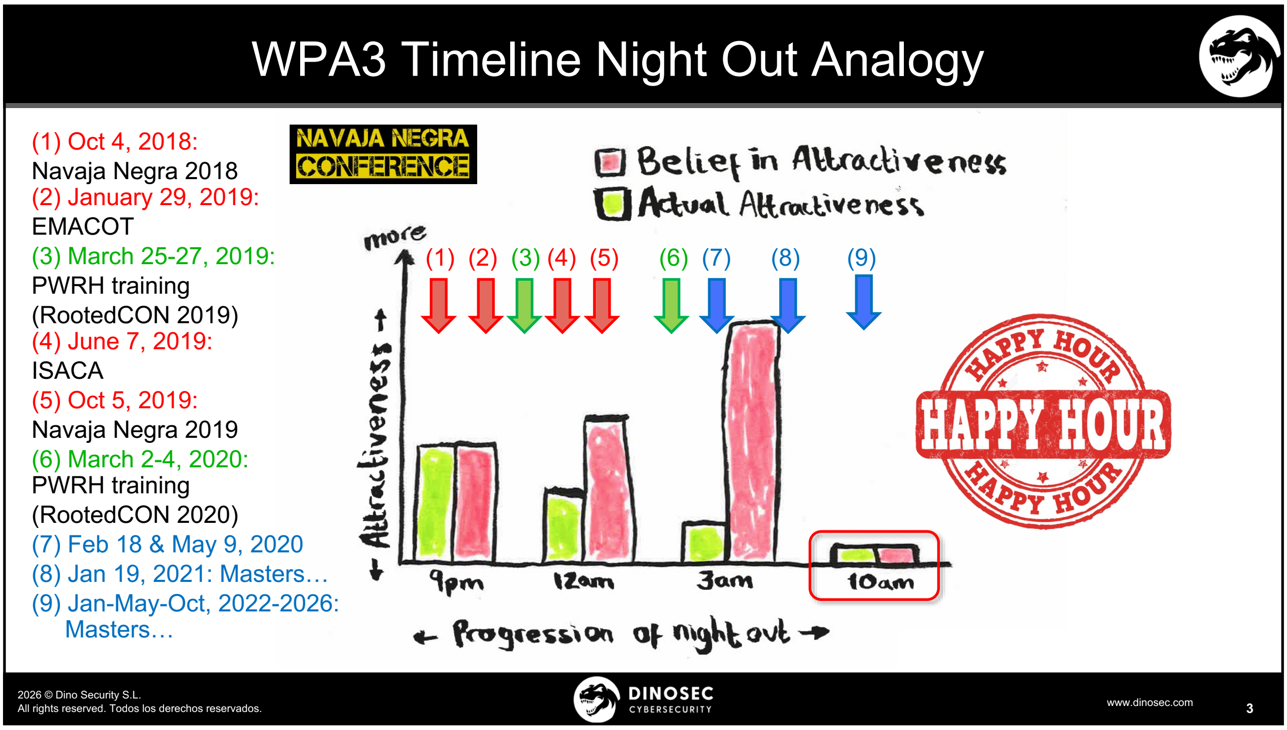
Speaker

Raúl Siles

DINOSEC CYBERSECURITY
www.dinosec.com
@dinosec

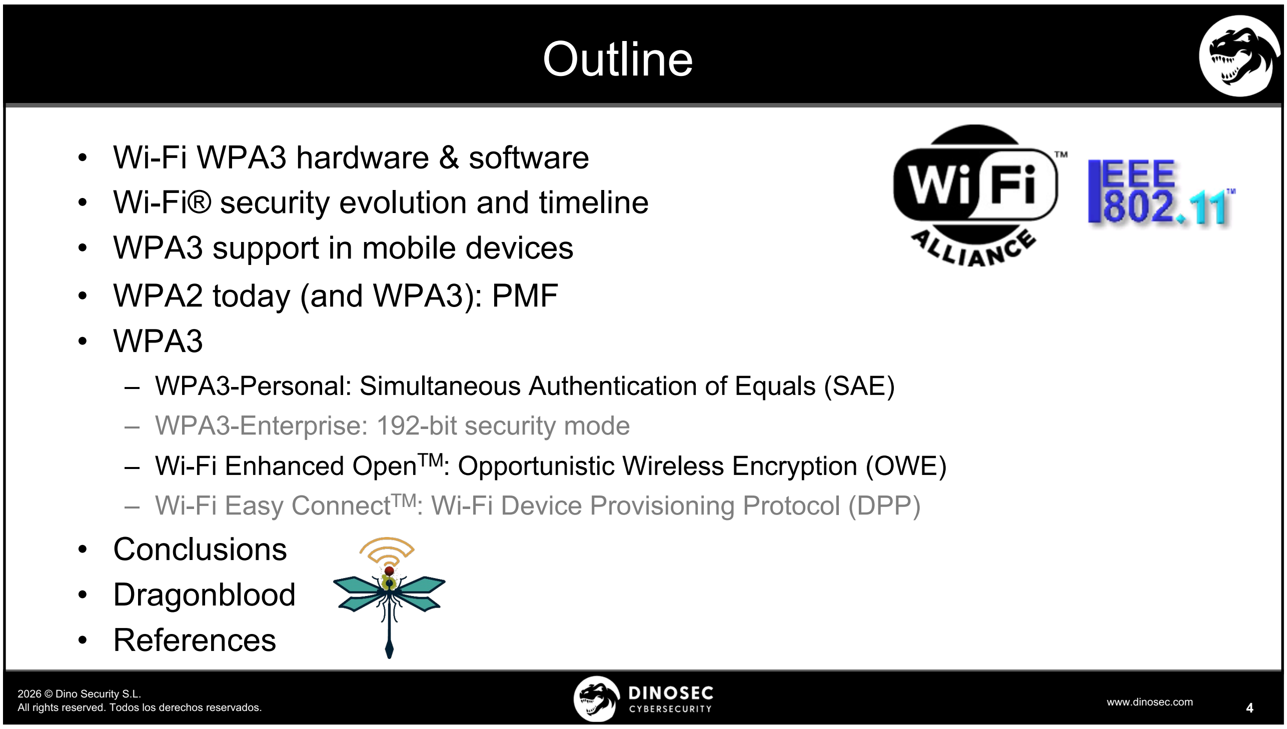
GUARDEDBOX
www.guardedbox.es
@guardedbox

2



WPA3 Timeline Night Out Analogy

(1) Oct 4, 2018:
Navaja Negra 2018
(2) January 29, 2019:
EMACOT
(3) March 25-27, 2019:
PWRH training
(RootedCON 2019)
(4) June 7, 2019:
ISACA
(5) Oct 5, 2019:
Navaja Negra 2019
(6) March 2-4, 2020:
PWRH training
(RootedCON 2020)
(7) Feb 18 & May 9, 2020
(8) Jan 19, 2021: Masters…
(9) Jan-May-Oct, 2022-2026:
Masters…



Outline

- Wi-Fi WPA3 hardware & software
- Wi-Fi® security evolution and timeline
- WPA3 support in mobile devices
- WPA2 today (and WPA3): PMF
- WPA3
  - WPA3-Personal: Simultaneous Authentication of Equals (SAE)
  - WPA3-Enterprise: 192-bit security mode
  - Wi-Fi Enhanced Open^{TM}: Opportunistic Wireless Encryption (OWE)
  - Wi-Fi Easy Connect^{TM}: Wi-Fi Device Provisioning Protocol (DPP)
- Conclusions
- Dragonblood
- References

Recommended Wi-Fi Card: Alfa AWUS036ACM

- 802.11a/b/g/n/ac (AC1200) - https://alfa-network.eu/awus036acm
  - 867 Mbps (11ac – 5 GHz) – 80 MHz channels +
  - 300 Mbps (11n – 2.4 GHz) – 40 MHz channels
- Dual band: 2.4 & 5 GHz (2.412GHz-2.472GHz + 5.15GHz-5.825GHz)
- Chipset MT7612U (MediaTek) – PMF – <-- Atheros
- MIMO (2x2): 2 transmitter & 2 receivers
- 11b/g: 200 mW (23 dBms) & high (-97/-90 dBm) sensitivity
- 11n: 125 mW (21 dBms) & high (-90 dBm) sensitivity
- 11ac: 100 mW (20 dBms) & 'high' (-86 dBm) sensitivity
- External RP-SMA female antenna connector x 2
  - 2 x 5 dBi dual band dipole antenna (omni-directional)
- USB 3.0 (Super speed) – Male A
- Windows, Linux, OS X
- EAN: 4718050307371

Wi-Fi Cards with "WPA3" Support

- Wi-Fi drivers/chipsets with support for 802.11w / PMF / MFP (required for WPA3)
  - Atheros, Prism54, Mediatek…
- https://wireless.wiki.kernel.org/welcome?do=search&id=**11w**
  - ath9k: https://wireless.wiki.kernel.org/en/users/drivers/ath9k?s[]=11w
  - p54: https://wireless.wiki.kernel.org/en/users/drivers/p54?s[]=11w
  - carl9170: https://wireless.wiki.kernel.org/en/users/drivers/carl9170?s[]=11w
- https://wireless.wiki.kernel.org/welcome?do=search&id=**mfp**
  - ath10k: https://wireless.wiki.kernel.org/en/users/drivers/ath10k/mesh?s[]=mfp
- mt7601u: https://www.spinics.net/lists/linux-wireless/msg175188.html
- Linux drivers that are MFP_CAPABLE in the latest stable Linux kernel version:
  - https://elixir.bootlin.com/linux/latest/ident/**MFP_CAPABLE**
  - For mac80211-based drivers, but there are cfg80211-based, *aka fullmac*, drivers
  - E.g. brcmfmac (Broadcom) does support MFP when the device/firmware supports it
  - Check if their cipher list mentions WLAN_CIPHER_SUITE_AES_CMAC
  - https://elixir.bootlin.com/linux/latest/ident/**WLAN_CIPHER_SUITE_AES_CMAC**

hostap & WPA3

- hostapd.conf (https://w1.fi/cgit/hostap/plain/hostapd/hostapd.conf)

```
# 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)
```

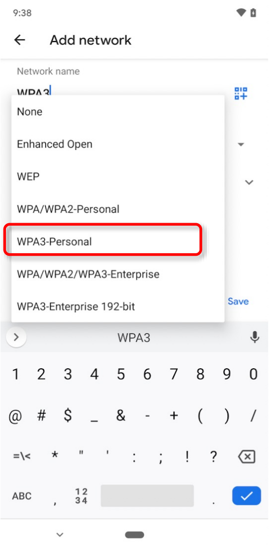
- wpa_supplicant.conf (https://w1.fi/cgit/hostap/plain/wpa_supplicant/wpa_supplicant.conf)

```
# 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)
```

WPA3-Personal Support

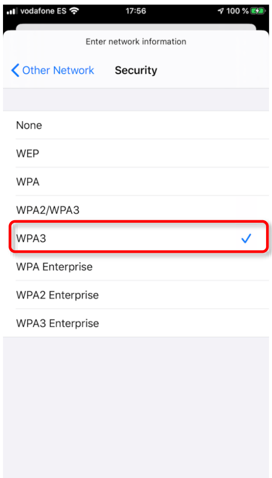
- January - June 2018
- Mandatory PMF or MFP
- iOS 13+
  - Personal hotspot: iOS 15+
- Android 10+
  - Including OWE
- Wi-Fi hacking tools…



Add network

Network name: WPA3

Security: WPA3-Personal



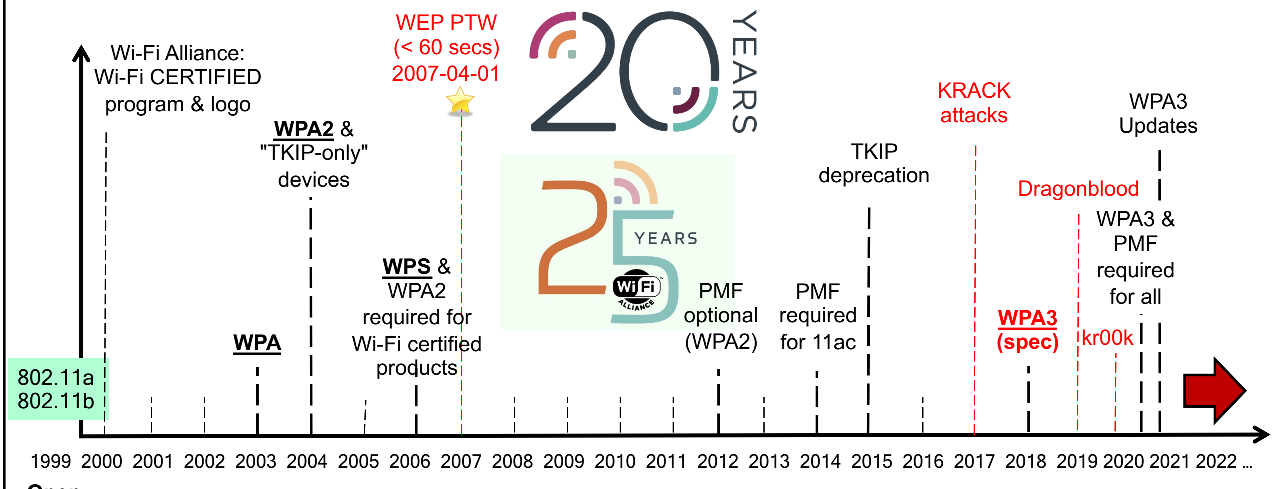
Enter network information

Security: WPA3 ✓

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 (SAE) & Enterprise

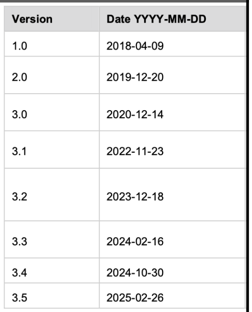
Wi-Fi® Security Timeline



https://www.wi-fi.org/sites/default/files/public/Infographic_20_years_of_Wi-Fi.pdf

WPA3

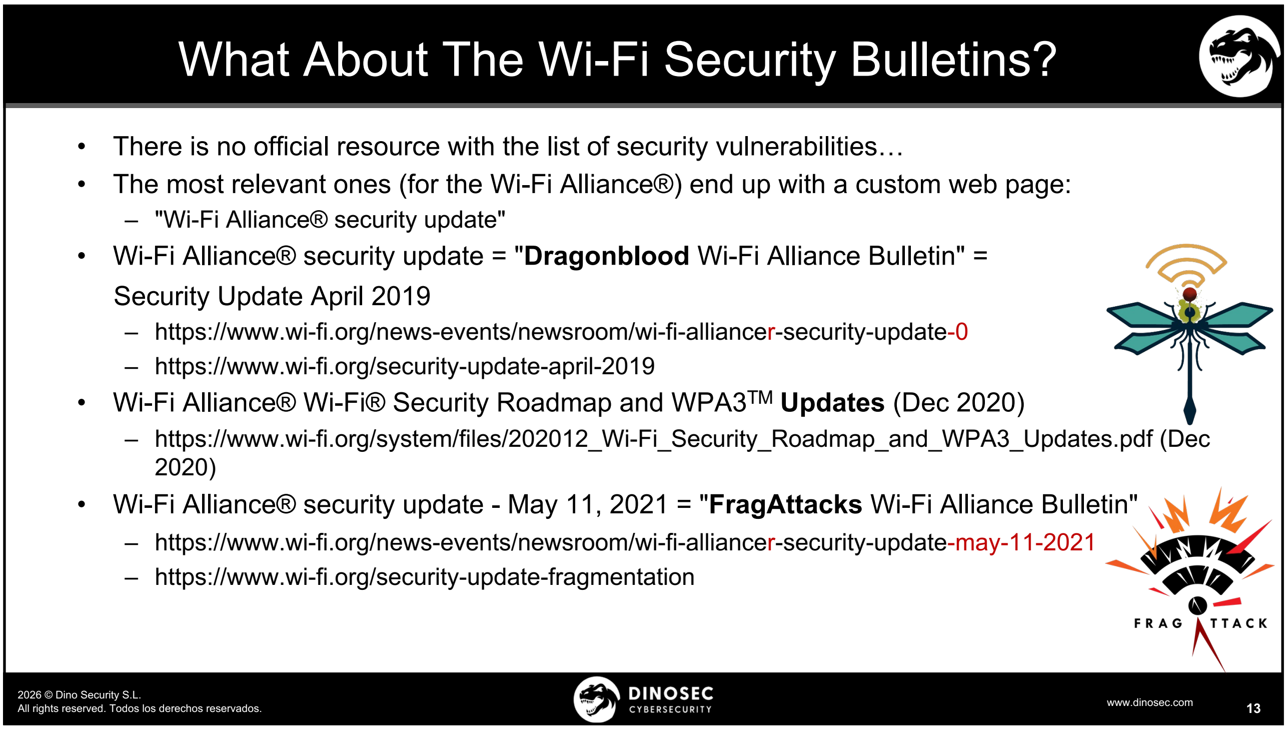
Wi-Fi Security: WPA3



Version	Date YYYY-MM-DD
1.0	2018-04-09
2.0	2019-12-20
3.0	2020-12-14
3.1	2022-11-23
3.2	2023-12-18
3.3	2024-02-16
3.4	2024-10-30
3.5	2025-02-26

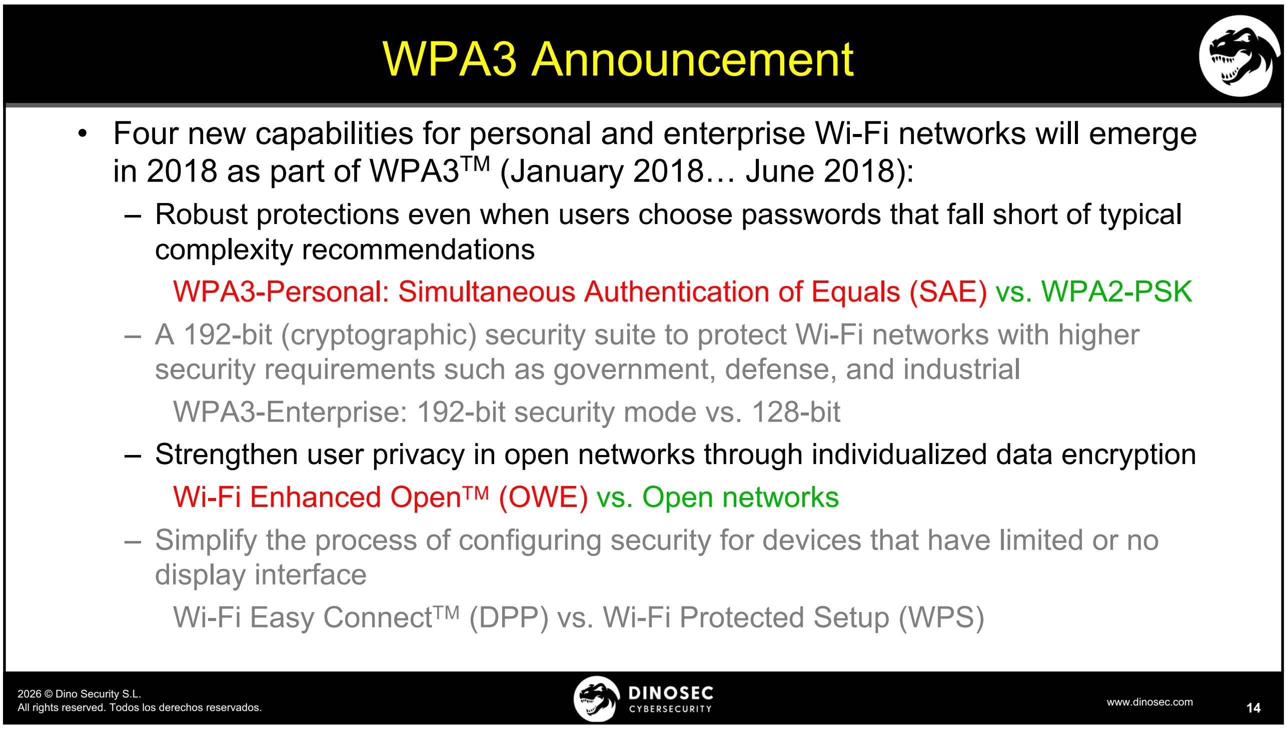
- Wi-Fi security overview… + interesting resources…
  - WPA3™ Specification (v3.5) – Feb 2025
    - https://www.wi-fi.org/system/files/WPA3%20Specification%20v3.5.pdf
  - Wi-Fi … WPA3™ Technology Overview (2021)
    - https://www.wi-fi.org/file/wi-fi-certified-wpa3tm-technology-overview-2021 (Web form: January 2021)
  - Wi-Fi Protected Access® Security Considerations
    - https://www.wi-fi.org/system/files/Security_Considerations_20210511.pdf (May 2021)
  - Security Development (IEEE standards & RFCs)
    - https://www.wi-fi.org/security-development
  - IEEE 802.11-2020: https://standards.ieee.org/ieee/802.11/7028/ (4,379 pg)

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



What About The Wi-Fi Security Bulletins?

- There is no official resource with the list of security vulnerabilities…
- The most relevant ones (for the Wi-Fi Alliance®) end up with a custom web page:
  - "Wi-Fi Alliance® security update"
- Wi-Fi Alliance® security update = "**Dragonblood** Wi-Fi Alliance Bulletin" = Security Update April 2019
  - https://www.wi-fi.org/news-events/newsroom/wi-fi-alliancer-security-update-0
  - https://www.wi-fi.org/security-update-april-2019
- Wi-Fi Alliance® Wi-Fi® Security Roadmap and WPA3™ **Updates** (Dec 2020)
  - https://www.wi-fi.org/system/files/202012_Wi-Fi_Security_Roadmap_and_WPA3_Updates.pdf (Dec 2020)
- Wi-Fi Alliance® security update - May 11, 2021 = "**FragAttacks** Wi-Fi Alliance Bulletin"
  - https://www.wi-fi.org/news-events/newsroom/wi-fi-alliancer-security-update-may-11-2021
  - https://www.wi-fi.org/security-update-fragmentation



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)

Dragonblood

DRAGONBLOOD

Analysing WPA3's Dragonfly Handshake

By Mathy Vanhoef (NYUAD) and Eyal Ronen (Tel Aviv University & KU Leuven)

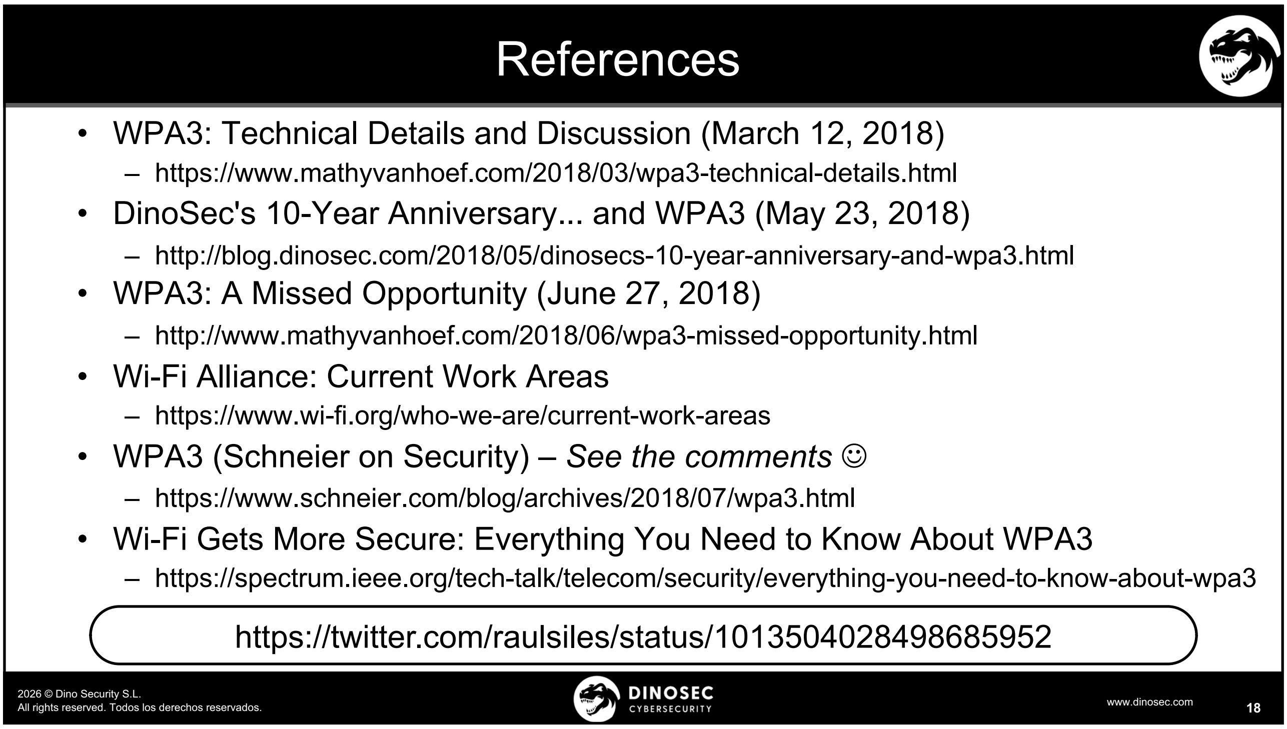
Dragonblood

- Analysing WPA3's (and EAP-PWD) Dragonfly Handshake
  - Mathy Vanhoef & Eyal Ronen (April 2019 & August 2019)
- Downgrade attacks against WPA3-capable devices
  - WPA3-Transtition mode: dictionary attacks
  - Security group downgrade
- Weaknesses in the Dragonfly handshake of WPA3 (SAE) / EAP-PWD
  - WPA3 Personal
  - Timing-based & Cache-based side-channel attacks (MODP & Brainpool)
    - Brute-force all 8-character lowercase passwords (~~125$~~ $67 with Amazon EC2 instances)
  - Resource consumption attack (DoS)

https://wpa3.mathyvanhoef.com

References

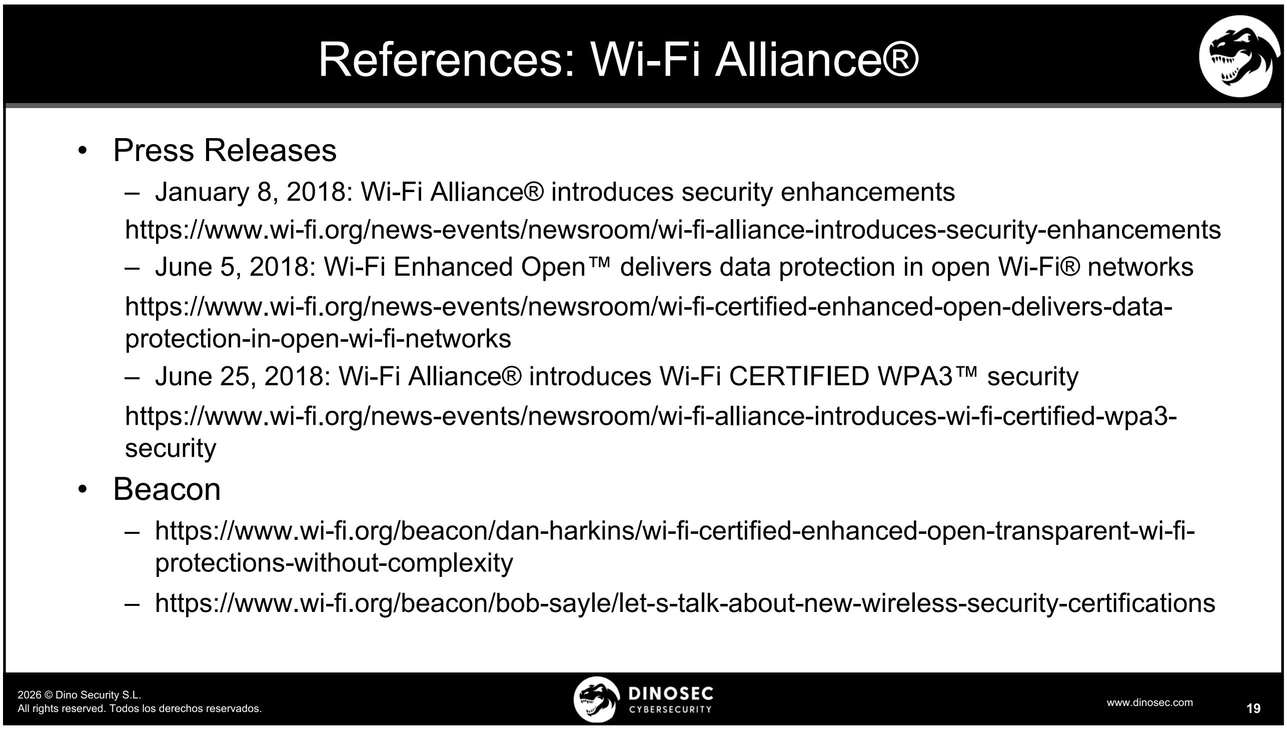
http://bit.ly/wpa3-references-2026



References

- WPA3: Technical Details and Discussion (March 12, 2018)
  - https://www.mathyvanhoef.com/2018/03/wpa3-technical-details.html
- DinoSec's 10-Year Anniversary... and WPA3 (May 23, 2018)
  - http://blog.dinosec.com/2018/05/dinosecs-10-year-anniversary-and-wpa3.html
- WPA3: A Missed Opportunity (June 27, 2018)
  - http://www.mathyvanhoef.com/2018/06/wpa3-missed-opportunity.html
- Wi-Fi Alliance: Current Work Areas
  - https://www.wi-fi.org/who-we-are/current-work-areas
- WPA3 (Schneier on Security) – *See the comments* ☺
  - https://www.schneier.com/blog/archives/2018/07/wpa3.html
- Wi-Fi Gets More Secure: Everything You Need to Know About WPA3
  - https://spectrum.ieee.org/tech-talk/telecom/security/everything-you-need-to-know-about-wpa3

https://twitter.com/raulsiles/status/1013504028498685952



References: Wi-Fi Alliance®

- Press Releases
  - January 8, 2018: Wi-Fi Alliance® introduces security enhancements

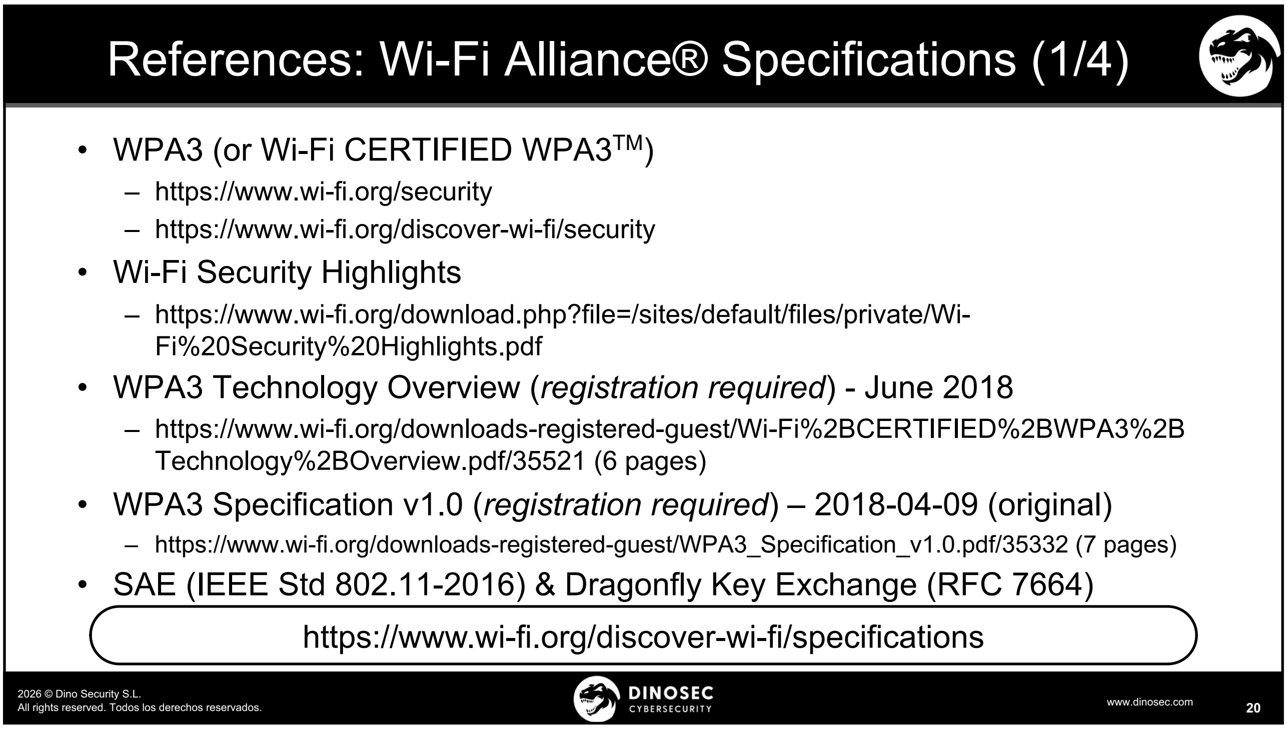
  https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-security-enhancements
  - June 5, 2018: Wi-Fi Enhanced Open™ delivers data protection in open Wi-Fi® networks

  https://www.wi-fi.org/news-events/newsroom/wi-fi-certified-enhanced-open-delivers-data-protection-in-open-wi-fi-networks
  - June 25, 2018: Wi-Fi Alliance® introduces Wi-Fi CERTIFIED WPA3™ security

  https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security
- Beacon
  - https://www.wi-fi.org/beacon/dan-harkins/wi-fi-certified-enhanced-open-transparent-wi-fi-protections-without-complexity
  - https://www.wi-fi.org/beacon/bob-sayle/let-s-talk-about-new-wireless-security-certifications

DINOSEC CYBERSECURITY

www.dinosec.com



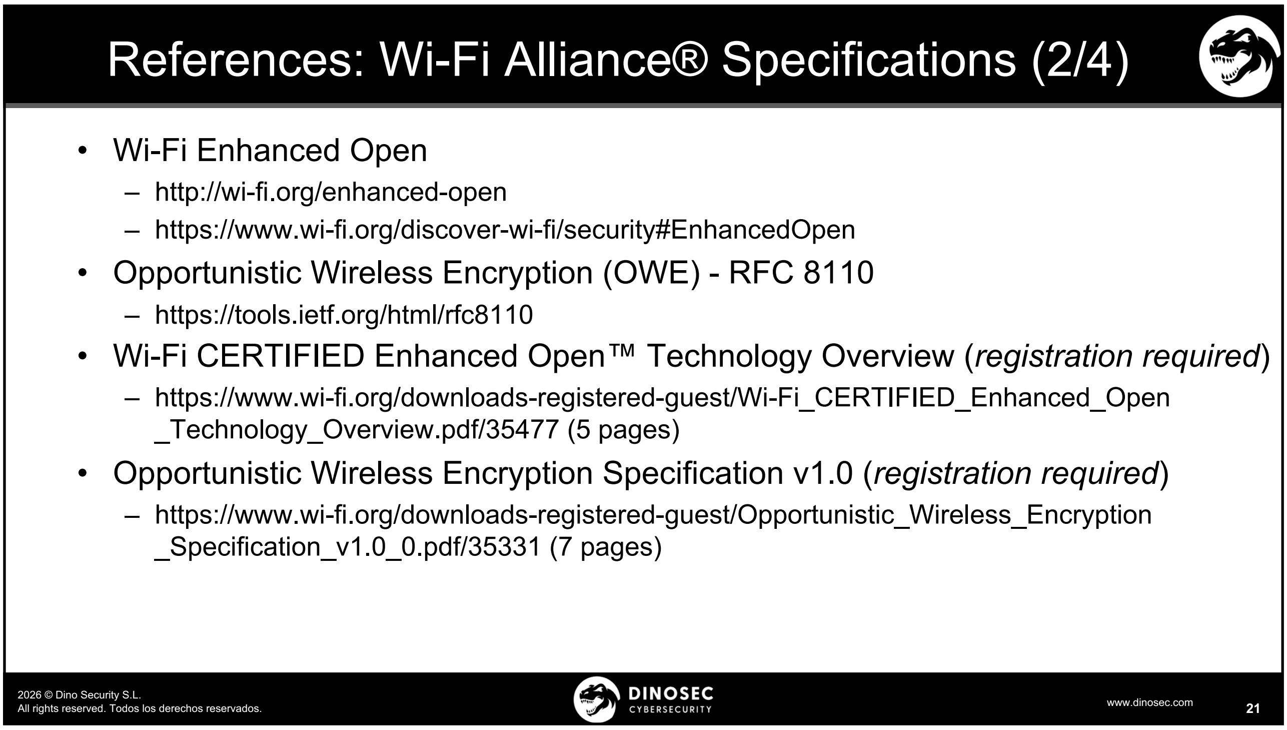
References: Wi-Fi Alliance® Specifications (1/4)

- WPA3 (or Wi-Fi CERTIFIED WPA3^{TM})
  - https://www.wi-fi.org/security
  - https://www.wi-fi.org/discover-wi-fi/security
- Wi-Fi Security Highlights
  - https://www.wi-fi.org/download.php?file=/sites/default/files/private/Wi-Fi%20Security%20Highlights.pdf
- 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 (original)
  - https://www.wi-fi.org/downloads-registered-guest/WPA3_Specification_v1.0.pdf/35332 (7 pages)
- SAE (IEEE Std 802.11-2016) & Dragonfly Key Exchange (RFC 7664)

https://www.wi-fi.org/discover-wi-fi/specifications

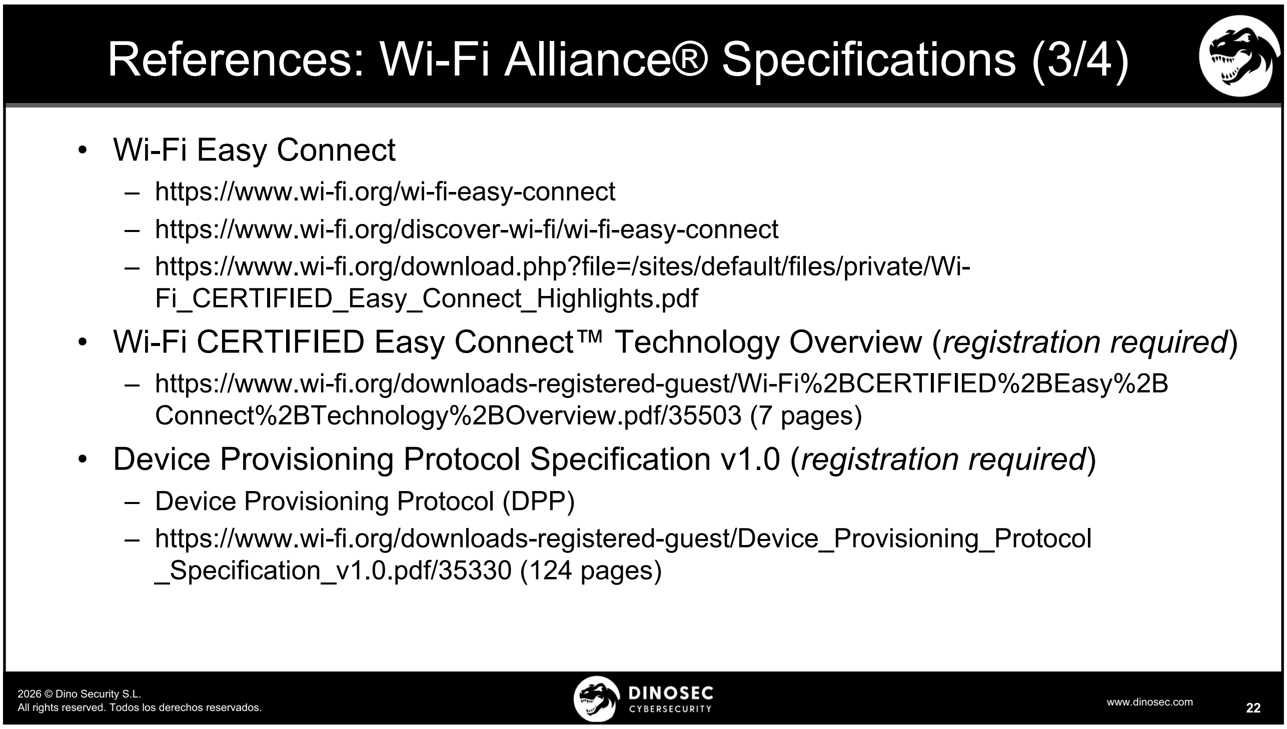
DINOSEC CYBERSECURITY

www.dinosec.com



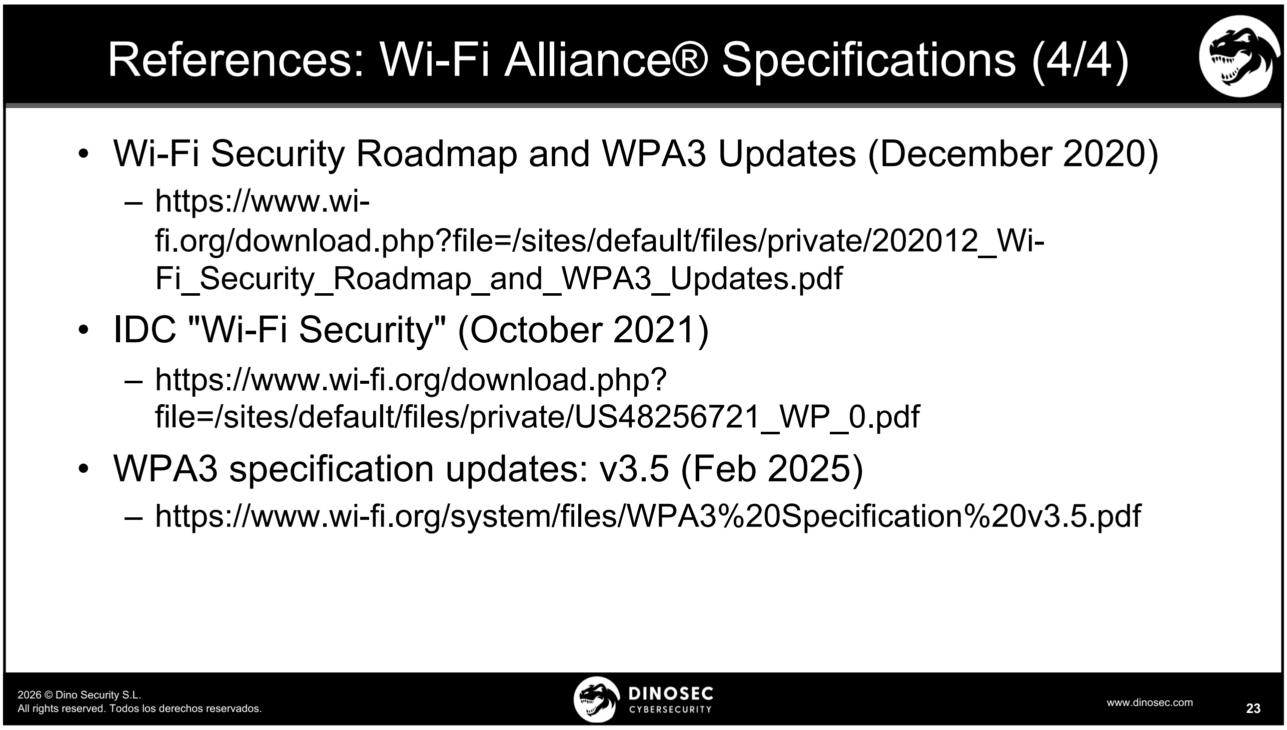
References: Wi-Fi Alliance® Specifications (2/4)

- Wi-Fi Enhanced Open
  - http://wi-fi.org/enhanced-open
  - https://www.wi-fi.org/discover-wi-fi/security#EnhancedOpen
- Opportunistic Wireless Encryption (OWE) - RFC 8110
  - https://tools.ietf.org/html/rfc8110
- Wi-Fi CERTIFIED Enhanced Open™ Technology Overview (*registration required*)
  - https://www.wi-fi.org/downloads-registered-guest/Wi-Fi_CERTIFIED_Enhanced_Open_Technology_Overview.pdf/35477 (5 pages)
- 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)



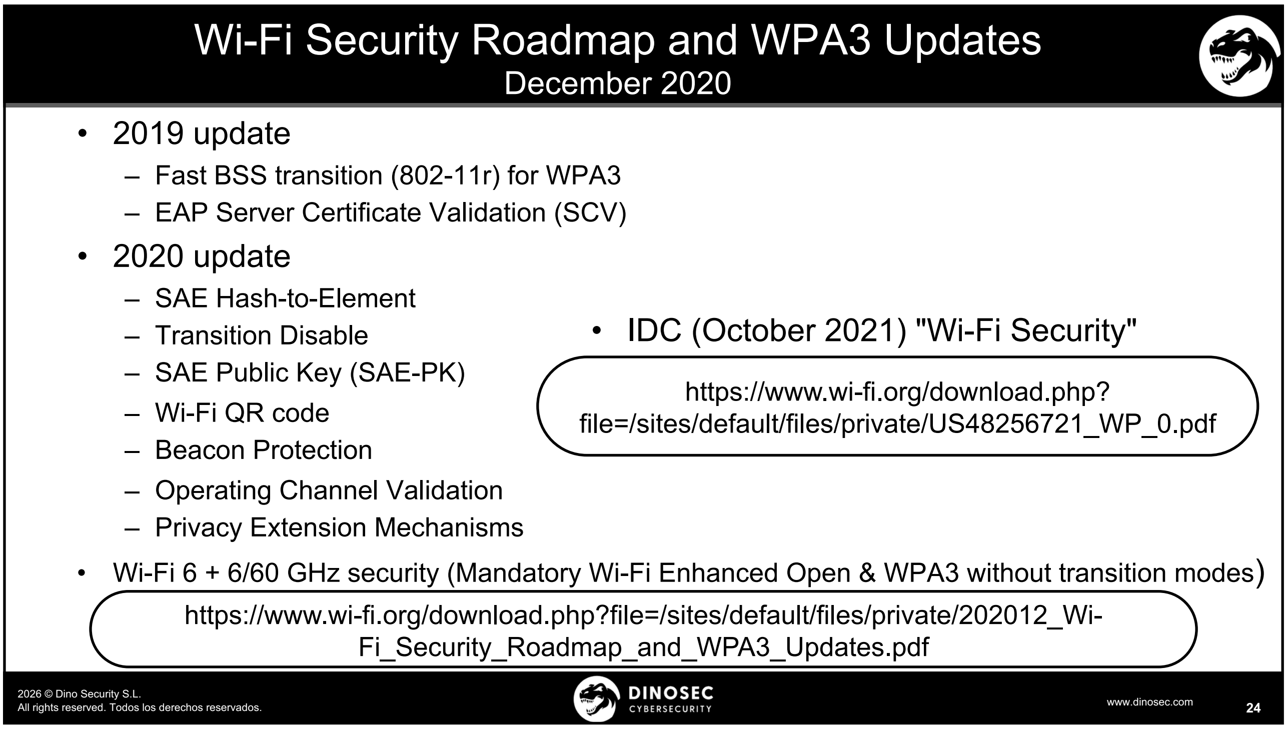
References: Wi-Fi Alliance® Specifications (3/4)

- Wi-Fi Easy Connect
  - https://www.wi-fi.org/wi-fi-easy-connect
  - https://www.wi-fi.org/discover-wi-fi/wi-fi-easy-connect
  - https://www.wi-fi.org/download.php?file=/sites/default/files/private/Wi-Fi_CERTIFIED_Easy_Connect_Highlights.pdf
- 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)
  - https://www.wi-fi.org/downloads-registered-guest/Device_Provisioning_Protocol_Specification_v1.0.pdf/35330 (124 pages)



References: Wi-Fi Alliance® Specifications (4/4)

- Wi-Fi Security Roadmap and WPA3 Updates (December 2020)
  - https://www.wi-fi.org/download.php?file=/sites/default/files/private/202012_Wi-Fi_Security_Roadmap_and_WPA3_Updates.pdf
- IDC "Wi-Fi Security" (October 2021)
  - https://www.wi-fi.org/download.php?file=/sites/default/files/private/US48256721_WP_0.pdf
- WPA3 specification updates: v3.5 (Feb 2025)
  - https://www.wi-fi.org/system/files/WPA3%20Specification%20v3.5.pdf



Wi-Fi Security Roadmap and WPA3 Updates
December 2020

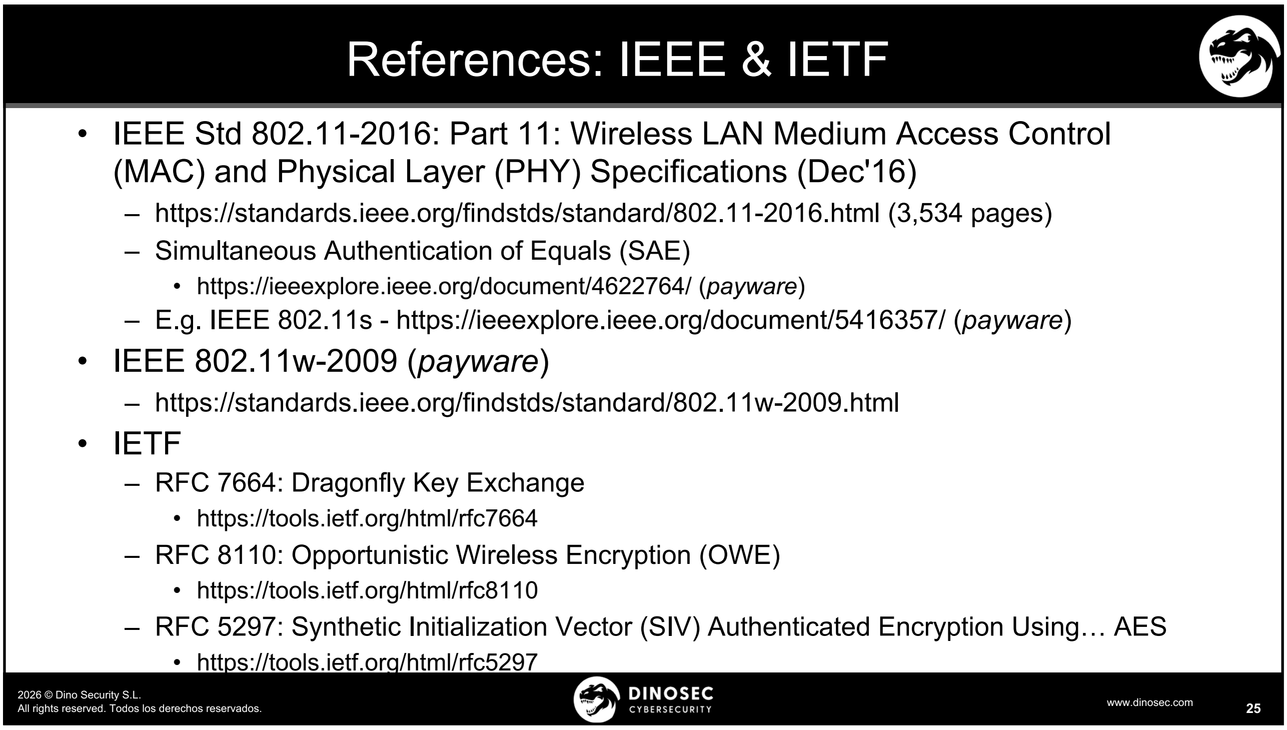
- 2019 update
  - Fast BSS transition (802-11r) for WPA3
  - EAP Server Certificate Validation (SCV)
- 2020 update
  - SAE Hash-to-Element
  - Transition Disable
  - SAE Public Key (SAE-PK)
  - Wi-Fi QR code
  - Beacon Protection
  - Operating Channel Validation
  - Privacy Extension Mechanisms

- IDC (October 2021) "Wi-Fi Security"

https://www.wi-fi.org/download.php?file=/sites/default/files/private/US48256721_WP_0.pdf

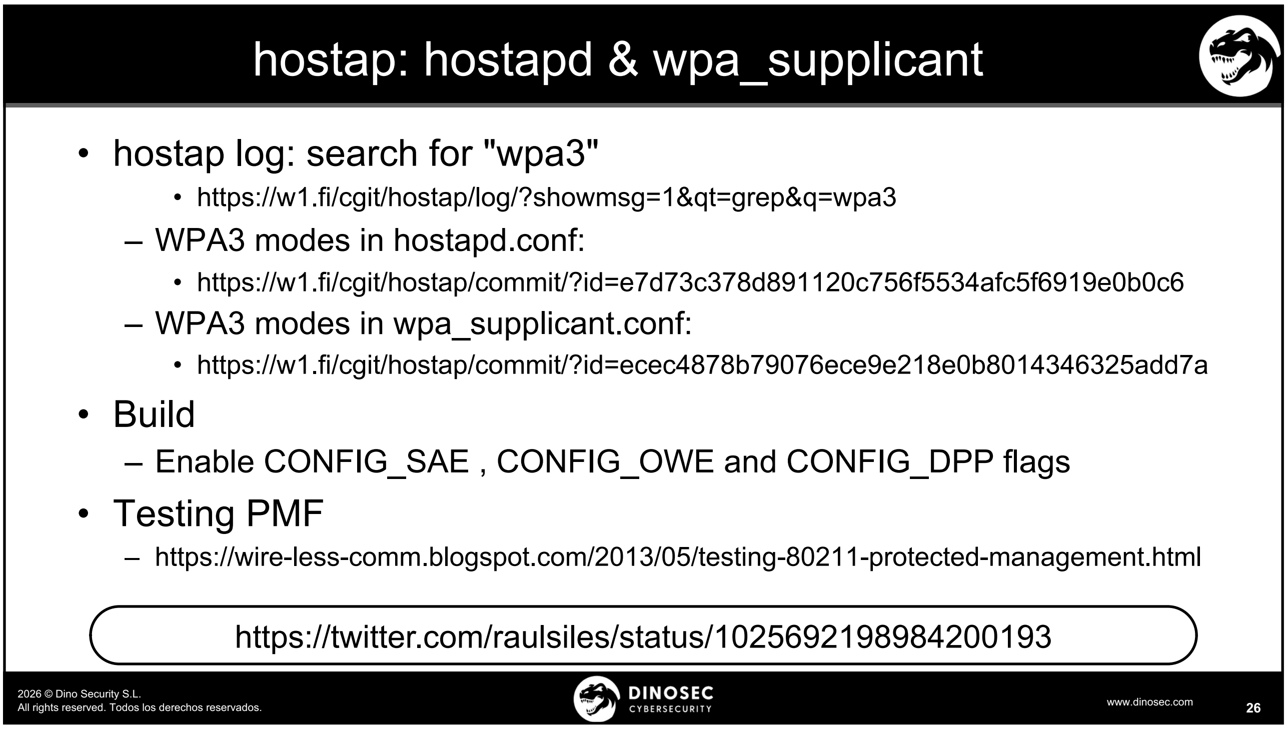
- Wi-Fi 6 + 6/60 GHz security (Mandatory Wi-Fi Enhanced Open & WPA3 without transition modes)

https://www.wi-fi.org/download.php?file=/sites/default/files/private/202012_Wi-Fi_Security_Roadmap_and_WPA3_Updates.pdf



References: IEEE & IETF

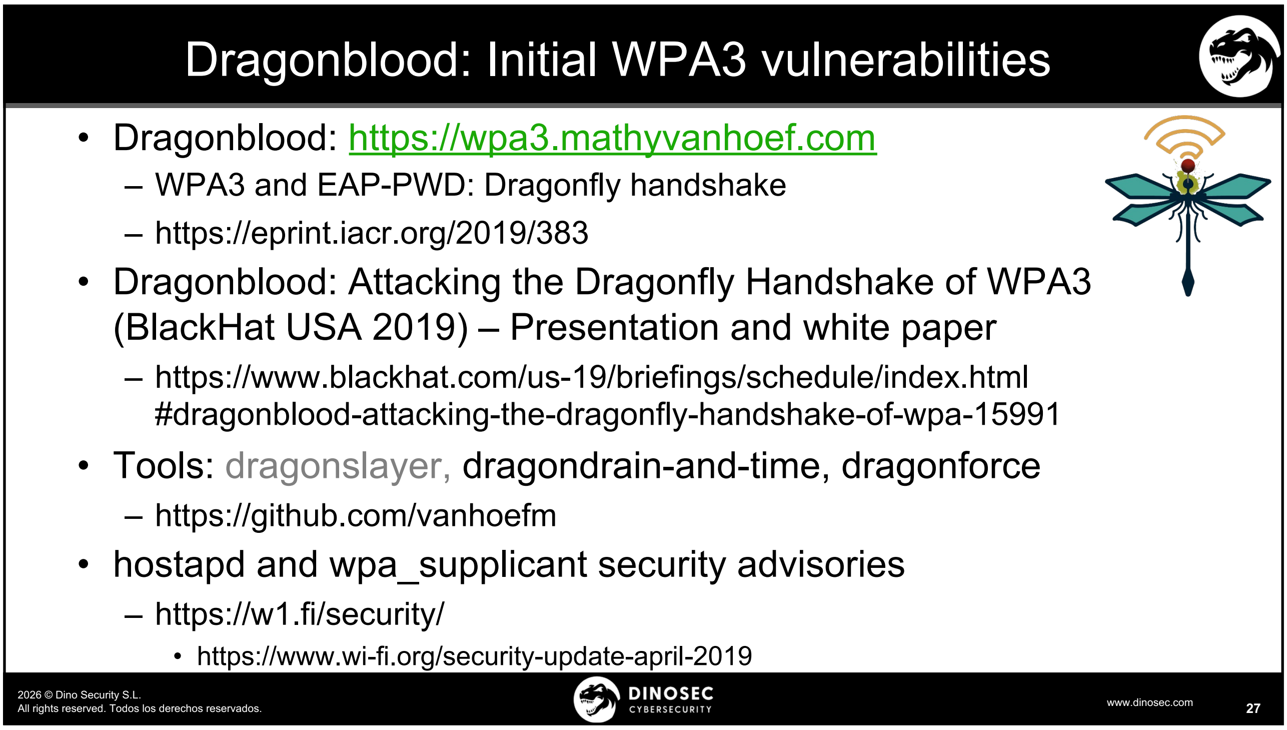
- IEEE Std 802.11-2016: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (Dec'16)
  - https://standards.ieee.org/findstds/standard/802.11-2016.html (3,534 pages)
  - Simultaneous Authentication of Equals (SAE)
    - https://ieeexplore.ieee.org/document/4622764/ (*payware*)
  - E.g. IEEE 802.11s - https://ieeexplore.ieee.org/document/5416357/ (*payware*)
- IEEE 802.11w-2009 (*payware*)
  - https://standards.ieee.org/findstds/standard/802.11w-2009.html
- IETF
  - RFC 7664: Dragonfly Key Exchange
    - https://tools.ietf.org/html/rfc7664
  - RFC 8110: Opportunistic Wireless Encryption (OWE)
    - https://tools.ietf.org/html/rfc8110
  - RFC 5297: Synthetic Initialization Vector (SIV) Authenticated Encryption Using… AES
    - https://tools.ietf.org/html/rfc5297



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=ecec4878b79076ece9e218e0b8014346325add7a
- 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



Dragonblood: Initial WPA3 vulnerabilities

- Dragonblood: https://wpa3.mathyvanhoef.com
  - WPA3 and EAP-PWD: Dragonfly handshake
  - https://eprint.iacr.org/2019/383
- Dragonblood: Attacking the Dragonfly Handshake of WPA3 (BlackHat USA 2019) – Presentation and white paper
  - https://www.blackhat.com/us-19/briefings/schedule/index.html #dragonblood-attacking-the-dragonfly-handshake-of-wpa-15991
- Tools: dragonslayer, dragondrain-and-time, dragonforce
  - https://github.com/vanhoefm
- hostapd and wpa_supplicant security advisories
  - https://w1.fi/security/
    - https://www.wi-fi.org/security-update-april-2019

Questions?

DINOSEC
CYBERSECURITY

www.dinosec.com
@dinosec

DINOSEC CYBERSECURITY

www.dinosec.com
@dinosec

GUARDEDBOX

www.guardedbox.com
@guardedbox

Raúl Siles
raul@dinosec.com

DINOSEC CYBERSECURITY

www.dinosec.com