Wi-Fi Security Threats - an Integrative Review

Students

Alice Glaus

Mario Burger

Advisor

Urs Baumann

Subject Area

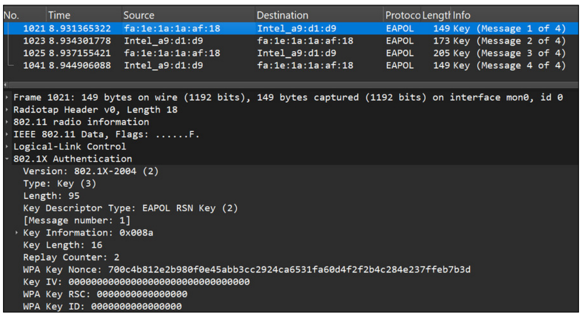
Security, Networks, Security & Cloud Infrastructure

Objective: "What are possible threats against Wi-Fi infrastructure?" is the main research question we wanted to answer in an integrative literature-review. Whether those threats are adequately dealt with, and how impactful the real-world implications appeared to be, are additional research goals.

Approach: The attack tree shows possible attack vectors and paths. With this information we collected papers published in the last seven years (2017-2024) to create an integrative literature-review. In a first part each selected source was summarized, highlighting their individual focus on the discussed threats or attacks and the resulting findings. The second part, the literature-review, consists of interwove comparisons of the sources' topics and findings, categorized by threats or attack types.
Additionally, we conducted an experiment in which a 4-way handshake between an access point and a client was recorded by a third party. This experiment laid the foundation for further tests and implementations, which will be carried out in the Bachelor's thesis in the next semester.

Conclusion: The literature-review concludes that many of the presented threats and attacks are enabled by inherent vulnerabilities in Wi-Fi protocols or implementation flaws. Some vulnerabilities may have been partially addressed in amendments to Wi-Fi standards, while others persist due to backward compatibility requirements.
Regarding improvements and future fields of study, the literature-review recognized the need for more rigorously defined standards in Wi-Fi technology. Implementations should be formally verified in a way to eliminate lacking adherence to standards and to reduce risks of bugs. Testing of Wi-Fi implementations must be expanded to include a broader range of devices, real-world environments, and configurations. This includes vendor-specific features and implementations, which often rely on Wi-Fi standards but due to ambiguous specifications lack security.

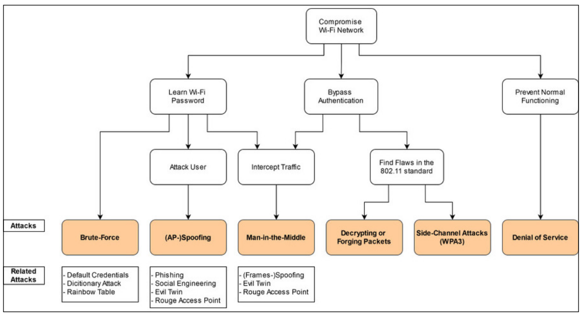
Wireshark Capture of a 4-way Handshake
Own presentment



```
No.   Time         Source               Destination          Protoco Lengtl Info
 1021 8.931365322  fa:1e:1a:1a:af:18    Intel_a9:d1:d9       EAPOL    149 Key (Message 1 of 4)
 1023 8.934301778  Intel_a9:d1:d9       fa:1e:1a:1a:af:18    EAPOL    173 Key (Message 2 of 4)
 1025 8.937155421  fa:1e:1a:1a:af:18    Intel_a9:d1:d9       EAPOL    205 Key (Message 3 of 4)
 1041 8.944906088  Intel_a9:d1:d9       fa:1e:1a:1a:af:18    EAPOL    149 Key (Message 4 of 4)

› Frame 1021: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface mon0, id 0
› Radiotap Header v0, Length 18
› 802.11 radio information
› IEEE 802.11 Data, Flags: ......F.
› Logical-Link Control
⌄ 802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: Key (3)
    Length: 95
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 1]
  › Key Information: 0x008a
    Key Length: 16
    Replay Counter: 2
    WPA Key Nonce: 700c4b812e2b980f0e45abb3cc2924ca6531fa60d4f2f2b4c284e237ffeb7b3d
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
```

Attack Tree: Possible Threats against a Wi-Fi Network
Own presentment



List of Sources Included in the Review
Own presentment

Attack Type	Source Title	Pub. Year	Authors
Brute-Force	Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd	2020	Mathy Vanhoef, Eyal Ronen
	WLAN Security Protocols and WPA3 Security Approach Measurement through Aircrack-ng Technique	2021	Elyas Baray, Nitish Kumar Ojha
	From Dragondoom to Dragonstar: Side-channel Attacks and Formally Verified Implementation of WPA3 Dragonfly Handshake	2023	Daniel De Almeida Braga, Natalia Kulatova, Mohamed Sabt, Pierre-Alain Fouque, Karthikeyan Bhargavan
	A Security Analysis of WPA3-PK: Implementation and Precomputation Attacks	2024	Mathy Vanhoef, Jeroen Robben
Spoofing and Evil Twin	WiFi vulnerability caused by SSID forgery in the IEEE 802.11 protocol	2019	Krisztián Juhász, Valéria Póser, Miklós Kozlovszky, Anna Bánáti
	Deciphering WEP, WPA, and WPA2 Pre-shared Keys Using Fluxion	2021	Sidharth Atluri, Revanth Rallabandi
	Fragment and forge: Breaking Wi-Fi through frame aggregation and fragmentation	2021	Mathy Vanhoef
	Preamble Injection and Spoofing Attacks in Wi-Fi Networks	2021	Zhengguang Zhang, Marwan Krunz
	Cut It: Deauthentication Attacks on Protected Management Frames in WPA2 and WPA3	2022	Karim Lounis, Steven H.H. Ding, Mohammad Zulkernine
Man in the Middle	Systematically Analyzing Vulnerabilities in the Connection Establishment Phase of Wi-Fi Systems	2022	Naureen Hoque, Hanif Rahbari, Cullen Rezendes
	Framing Frames: Bypassing Wi-Fi Encryption by Manipulating Transmit Queues	2023	Domien Schepers, Aanjhan Ranganathan, Mathy Vanhoef
	Man-in-the-Middle Attacks without Rogue AP: When WPAs Meet ICMP Redirects	2023	Xuewei Feng, Qi Li, Kun Sun, Yuxiang Yang, Ke Xu
	Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2	2017	Mathy Vanhoef, Frank Piessens
	Release the Kraken: New KRACKs in the 802.11 Standard	2018	Mathy Vanhoef, Frank Piessens
Decrypting or Forging Packets	Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2	2017	Mathy Vanhoef, Frank Piessens
	Release the Kraken: New KRACKs in the 802.11 Standard	2018	Mathy Vanhoef, Frank Piessens
	Fragment and forge: Breaking Wi-Fi through frame aggregation and fragmentation	2021	Mathy Vanhoef
Side-Channel Attacks (WPA3)	Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd	2020	Mathy Vanhoef, Eyal Ronen
	From Dragondoom to Dragonstar: Side-channel Attacks and Formally Verified Implementation of WPA3 Dragonfly Handshake	2023	Daniel De Almeida Braga, Natalia Kulatova, Mohamed Sabt, Pierre-Alain Fouque, Karthikeyan Bhargavan
Denial of Service	Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd	2020	Mathy Vanhoef, Eyal Ronen
	Fragment and forge: Breaking Wi-Fi through frame aggregation and fragmentation	2021	Mathy Vanhoef
	Preamble Injection and Spoofing Attacks in Wi-Fi Networks	2021	Zhengguang Zhang, Marwan Krunz
	Cut It: Deauthentication Attacks on Protected Management Frames in WPA2 and WPA3	2022	Karim Lounis, Steven H.H. Ding, Mohammad Zulkernine
	Systematically Analyzing Vulnerabilities in the Connection Establishment Phase of Wi-Fi Systems	2022	Naureen Hoque, Hanif Rahbari, Cullen Rezendes
	Framing Frames: Bypassing Wi-Fi Encryption by Manipulating Transmit Queues	2023	Domien Schepers, Aanjhan Ranganathan, Mathy Vanhoef

OST