Device for Wi-Fi Security Testing

Ing. Petr Heřmánek
academia@hermanek.org

Department of Computer Systems
Faculty of Information Technology
Czech Technical University in Prague

Introduction

- The globally widespread protocols have a well established attack surface often based on unsafe design and critical programming errors.

- Availability of efficient tools and IoT advancements makes wireless network compromise a serious threat to both personal and enterprise modes.

- Consequences of such attacks include the loss of traffic confidentiality, integrity, and authenticity.

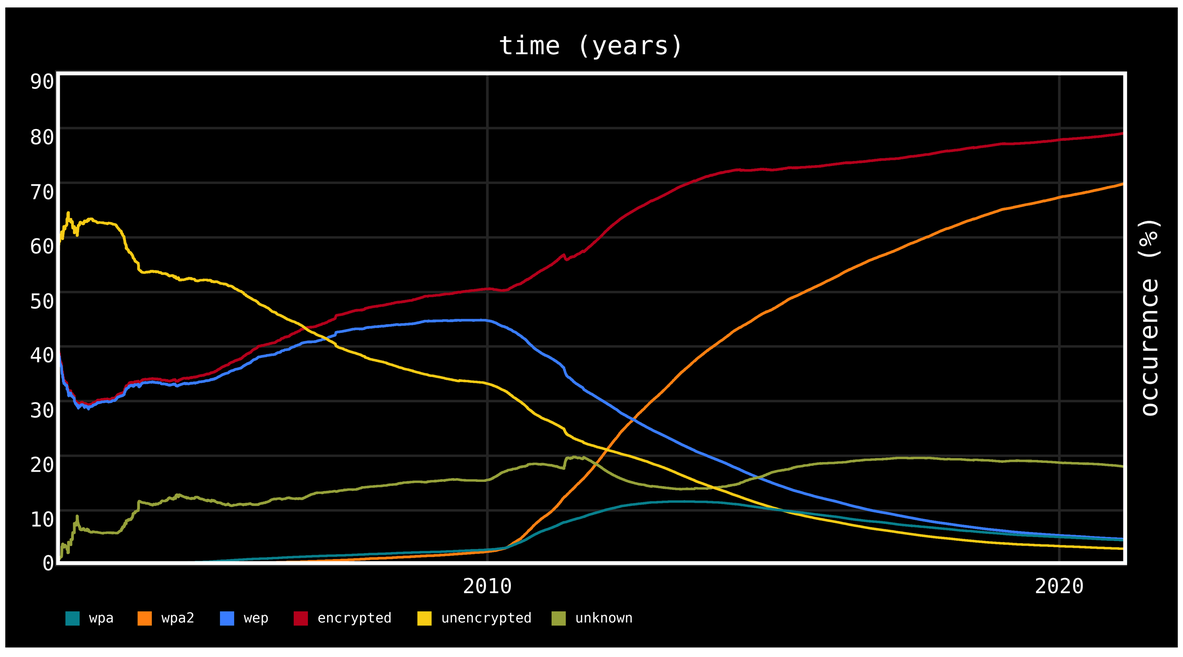
- Adversaries may leverage enterprise variants to gain an initial foothold in target network and move laterally to obtain sensitive resources.

- WPA2 still remains the most used protocol globally for Wi-Fi security and it may take years for the WPA3 to take over.

- Therefore, the risks of leveraging known techniques such as eavesdropping, packet forgery, Denial-of-Service, device infection, or credential theft require special attention.

- To better protect also means to periodically monitor evolving trends in wireless security and update/patch the networking equipment.

Wi-Fi security protocol adoption



Attack Surface

- The focus was on researching the recurring threats to provide a modern taxonomy overview and general protection guidelines.

- Vulnerable design and implementation of authentication/encryption protocols allows adversaries to recover access keys or decrypt traffic.

- Man-in-the-Middle is focused on rerouting traffic through the adversary or leveraging a rogue access point (RAP) to eavesdrop/manipulate traffic.

4.1. Taxonomy Overview

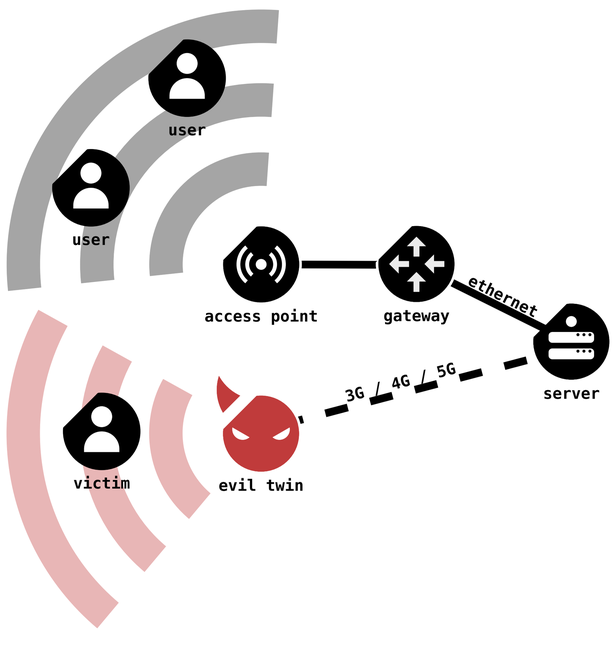
Taxonomy Overview		
Type	Protocol	Name
Man-in-the-Middle	*-*	Evil Twin
	-	KARMA Attack
	-	MANA Attack
	WPA*-Open	Known Beacon Attack
Key-recovery	WPA2-PSK	Dictionary Attack
	WPA2-PSK	WPS Brute-force Attack
	WPA2-PSK	WPS Pixie Dust Attack
	WPA2-PSK	PMKID Hash Dictionary Attack
	WPA3-PSK	Dragonblood
Traffic Decryption	WPA2-*	KRACK Attacks
	WPA2-*	KR00K vulnerability
Denial of Service	*-*	Resource Exhaustion Attack
	WPA2-*	Deauthentication Flooding Attack
	WPA3-*	Dragonfly Resource Exhaustion

Table 4.1: Proposed taxonomy

- Evil Twin Attack impersionates a legitimate AP. Its variants are based on changes in the management frame behaviour and protection development.

- Attacks differ for corporate and personal networks, restricted probing, PNL maintenance and evasion from different detection techniques.

- Defense against RAP also greatly varies and some protections are not fully capable of detecting advanced forms of exploitation alone.



Evil TwinBerries

- Device actively used for the development and research of Wi-Fi security in partnership with Avast software s.r.o..

- Project prototype utilizes commonly available hardware while preserving portability and monitor mode functionality.

- RAP solution capable of a parallel handshake collection and a fully automated Evil Twin kill chain.

- Pipeline modifiable via module inclusion mechanism (Bash/Python).

- Service configuration templates, multi-layer logging and subprocess management.

- Fully automated Wardriving capabalities via Bluetooth target intercommunication.

- CI/CD support and staging environment.

- Contemporary Wi-Fi auditing toolkit options, for example Kismet, Bettercap, Aircrack-ng, EAPHammer or KR00K are available.

- Additional modules for KR00K, ARP injection and a simple DNS amplification had their proof of concepts deployed in a controlled staging environment.

- **Wireless toolbox:** Raspberry Pi 3 (Raspberry Pi OS)
- **WNIC:** Alfa AWUS036NHA (Atheros AR9271, 2.4GHz 5dBi dipole)
- **Handshake collection:** Raspberry Pi Zero WH (custom Pwnagotchi)
- **Power management:** ATX style PCB by Pi Supply
- **LCD touchscreen:** Waveshare 13.3" HDMI IPS
- **PSU:** Dual 10000mAh, QC3.0: 4.6V-12V 3A-1.5A (Auto-Detection) 18W