

# Wybrane aspekty bezpieczeństwa komputerowego z wykorzystaniem komputerów SBC

Gabriel Wechta

Promotorem pracy dyplomowej jest dr Maciej Gębala.

# Single-Board-Computers

Single-Board-Computer (SBC) – komputer, którego wszystkie podzespoły (mikroprocesor, RAM, piny I/O, HDMI, itd.) znajdują się na jednej zintegrowanej płycie drukowanej.

## Przykłady

- NanoPi NEO4
- ASUS Tinker Board S
- **Raspberry Pi 3B**

## Wybór urządzenia

- Wbudowany moduł Wi-Fi
- Dedykowane wersje systemu operacyjnego (Kali Linux ARM)
- Wsparcie społeczności
- Power over Ethernet
- Cena

## Zalety

- Serwer Command&Control
- Zasilanie akumulatorem/bateriami
- Niska cena
- Mały rozmiar

## Niezbędny hardware

- Karta sieciowa USB, z monitor mode (TP-Link TL-WN722N)
- Szybka karta pamięci MicroSD
- Radiatory ciepła
- Wentylator zasilany GPIO

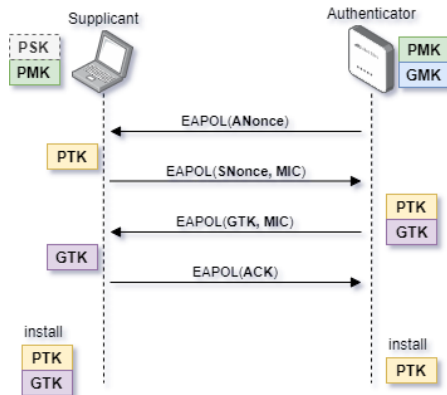
## Cel pracy

Wykorzystanie SBC do:

- **Automatyzacji ataku na WPA2-PSK.**
  - Przedstawienie i analiza technik maksymalizujących skuteczność ataku.
- **Implementacji detektora Evil Twin Access Point.**
  - Modyfikacja algorytmu Legal Access Point Finder (LAF) opracowana przez Hsu et al. [1].

# TCP 4-Way Handshake

W standardzie WPA2-Personal, klient uzyskuje dostęp do Access Pointa (AP) po podaniu Pre-Shared Key (PSK). Jako, że medium radiowe może być podsłuchane, stosuje się 4-Way Handshake uzgadniający klucz szyfrujący znany tylko klientowi i AP.



$$PTK = \text{PRF}(\text{PMK}, \text{ANonce}, \text{SNonce}, \text{MAC}_{\text{AP}}, \text{MAC}_{\text{SUPP}}),$$

$$\text{PMK} = \text{PBKDF2}(\text{PSK}, \text{SSID}, 4096, \text{HMAC-SHA1})[0 : 32],$$

# Atak na WPA2-PSK

## Etapy ataku na WPA2-PSK

- Przechwycenie pól 4-Way Handshake podczas komunikacji klienta z AP.
- Generowanie kandydatów do ataku słownikowego.
- Odzyskiwanie PSK offline.

Implementacja obejmuje automatyzację trzech rodzajów przechwyty:

- EAPOL dla aircrack-ng
- EAPOL dla hashcat
- PMKID

Zarówno z GUI jak i w trybie headless dla łączenia z SBC za pomocą SSH.

# Przechwyt za pomocą narzędzia aircrack-ng

```
Type the interface: wlan1

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    811 NetworkManager
    1024 wpa_supplicant

PHY      Interface      Driver      Chipset
phy0     wlan0               iwlwifi     Intel Corporation Dual Band Wireless-AC 3168NGW [Stone Peak] (rev 10)
phy2     wlan1               ath9k_htc   Qualcomm Atheros Communications AR9271 802.11n
          (mac80211 monitor mode vif enabled for [phy2]wlan1 on [phy2]wlan1mon)
          (mac80211 station mode vif disabled for [phy2]wlan1)

Starting airodump-ng on wlan1mon.
Type BSSID: 6C:60:EB:87:88:99
Type channel: 4
In order to keep level of network jamming at minimum you will send deauth signal by hand. Look on the second termina
l if you see :WPA handshake: (right top corner) you are golden.
To send deauth package press [Enter], to exit press [q]
```

Rysunek: Wynik `capture_aircrack_4WH.sh`, przypadek dla części parametrów wywołania.

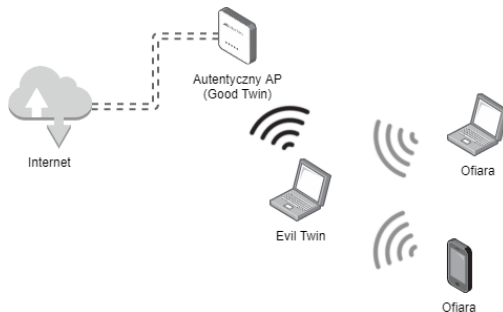
```
CH 4 ][ Elapsed: 1 min ][ 2021-11-19 08:44 ][ WPA handshake: 6C:60:EB:87:88:99

BSSID          PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID
6C:60:EB:87:88:99 -54 100    1126      419  0  4 130  WPA2 CCMP  PSK  Korbank-internet-72a0_2,4GHz

BSSID          STATION          PWR   Rate Lost  Frames  Notes  Probes
6C:60:EB:87:88:99 40:A3:CC:F9:93:A9 -33   1e- 2e    0    16  EAPOL
6C:60:EB:87:88:99 94:17:00:26:93:C0 -47   24e- 1    0   468
```

Rysunek: Okno pomocnicze nasłuchujące komunikacji klienta z AP.

# Evil Twin



Rysunek: Schemat Rogue Access Point typu Evil Twin.

Większość OS, mając do wyboru Access Pointy o takim samym SSID wybiera ten z najsilniejszym RSSI (Received Signal Strength Indication).

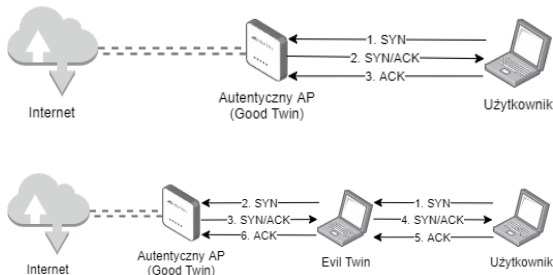


# TCP 3-Way Handshake i packet forwarding

## TCP 3-Way Handshake

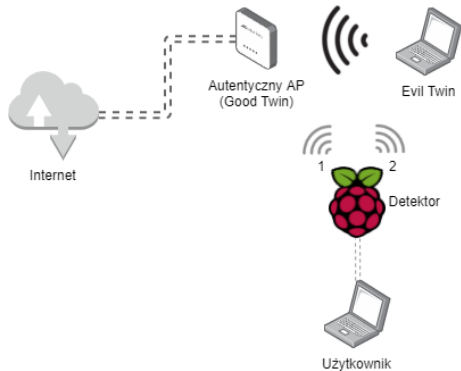
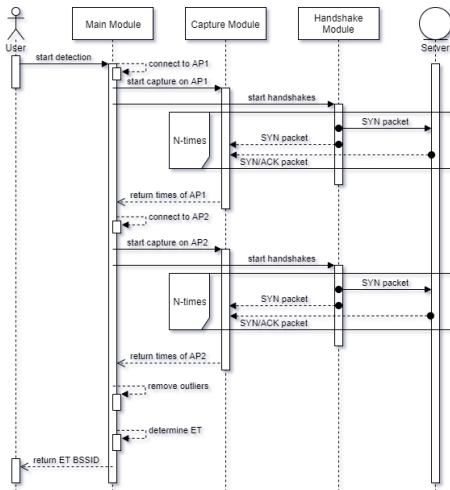
- $\Rightarrow$  SYN
- $\Leftarrow$  SYN/ACK
- $\Rightarrow$  ACK

## Packet Forwarding



$$t_{\text{total}} = t_{\text{SYN/ACK}} - t_{\text{SYN}}$$

# Detektor ET



Rysunek: Użycie SBC jako detektora ET.

Rysunek: Diagram sekwencyjny detektora Evil Twin Access Point.

[1] O. C.-W. H. Y.-L. Hsu F-H, Wang C-S.

A passive user-side solution for evil twin access point detection at public hotspots.  
*International Journal of Communication Systems*, 2018.

Dziękuję za uwagę.

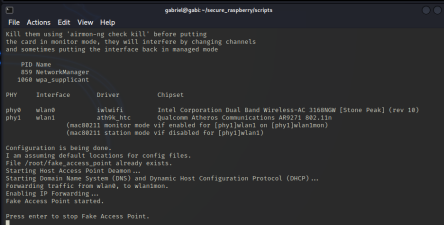
## Evil Twin - implementacja

[illegible]

```

hostapd
Configuration File: /root/.fake_access_point/hostapd.conf
Using interface wlan0 with hwaddr 04:16:0b:1e:20:0f and ssid 'YorkWare-Interne
5-7-2017 12:40:46
wlan0mon: interface state UNINITIALIZED->ENABLED
wlan0mon: #0-ENABLED
wlan0mon: STA 02:04:0f:04:0c:b4 IEEE 802.11: authenticated
wlan0mon: STA 02:04:0f:04:0c:b4 IEEE 802.11: associated (aid 1)
wlan0mon: #10-CONNECTED: 02:04:0f:04:0c:b4
wlan0mon: STA 02:04:0f:04:0c:b4 REAUTH: starting accounting session 85461c70200956

```



```

gabriel@gabi-secure-raspberry:scripts
File Actions Edit View Help
I'll then using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

PID Name
630 NetworkManager
1800 wpa_supplicant

PHY Interface Driver Chipset
phy0 wlan0 iwlwifi Intel Corporation Dual Band Wireless-AC 3168WGN [Stone Peak] (rev 18)
phy1 wlan1 rtl8821au Qualcomm Atheros Communications AR9271 802.11a
(mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0mon)
(mac80211 station mode vif disabled for [phy1]wlan1)

Configuration is being done.
I am assuming default locations for config files.
File /root/.fake_access_point already exists.
Starting Host Access Point Daemon ...
Starting Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) ...
Forwarding traffic from wlan0, to wlan0mon.
Enabling IP Forwarding...
Fake Access Point started.

Press enter to stop Fake Access Point.

```

**Rysunek:** Lewa – AP daemon (hostapd), prawa-góra – serwer DNS i DHCP (dnsmasq), prawa-dół główne okno konfiguracyjne ET.