



Bezpieczeństwo komunikacji bezprzewodowej i transakcji sieciowych

Jan Luch
218150

Pytanie kierunkowe
nr 6

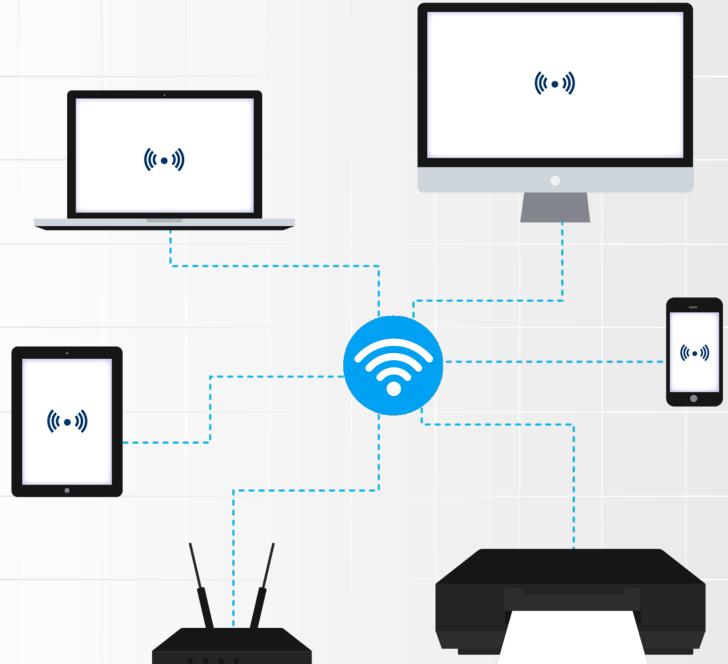
Wrocław 2019



Plan prezentacji

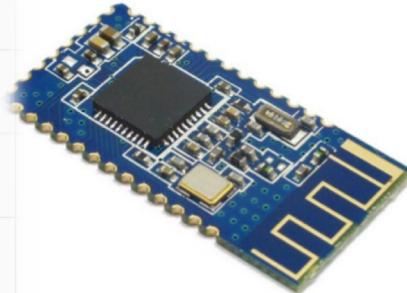
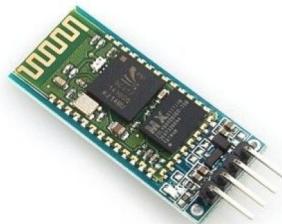
1. Komunikacja bezprzewodowa
2. Zagrożenia komunikacji bezprzewodowej
3. Bezpieczeństwo komunikacji bezprzewodowej
4. Transakcje sieciowe
5. Zagrożenia transakcji sieciowych
6. Bezpieczeństwo transakcji sieciowych
7. Źródła

Komunikacja bezprzewodowa





Przykłady komunikacji bezprzewodowej



Zagrożenia komunikacji bezprzewodowej

1. Rouge Access Point
2. MITM
3. Packet Injection
4. Sieci Ad-Hoc
5. Bluetooth
6. Listy MAC
7. DoS
8. Caffe-Latte



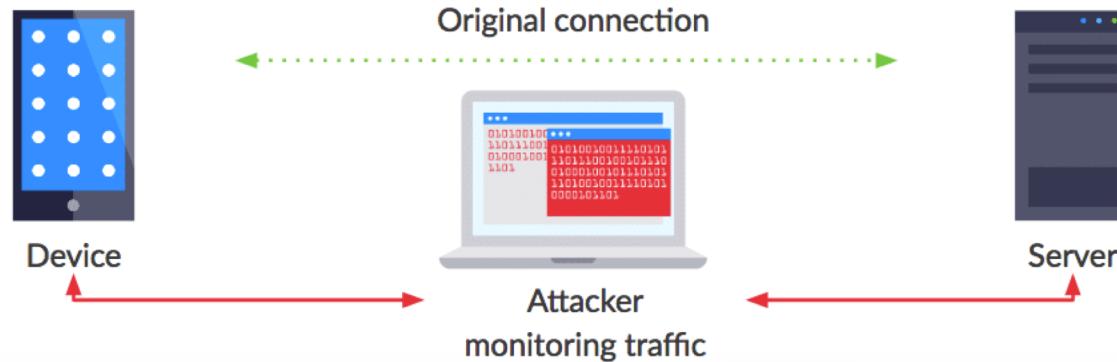


Rouge Access Point

1. Dodatkowy punkt dostępowy
2. Podłączony do sieci lokalnej współpracującej z siecią bezprzewodową będącą celem ataku
3. Pozwala na gromadzenie informacji przekazywanych w ramach sieci lokalnej
4. Trudny do wykrycia w przypadku wyłączonego rozsyłania SSID

Man in the middle

1. Dodatkowy punkt pomiędzy klientem i punktem dostępowym
2. Przechwytuje dane
3. Przekazuje dalej aby nie wzbudzić podejrzeń
4. Może wpływać na wymieniane informacje





Packet Injection

1. Wstrzykiwanie pakietów
2. Sztuczne generowanie ruchu
3. Wstrzykiwanie pakietów ARP przyspiesza łamanie klucza WEP
4. Wykorzystywane również w atakach DoS





Ataki w sieciach Ad-Hoc

1. Pasywne:

- Obserwowanie komunikacji
- Brak ingerencji
- Wymierzone przeciwko poufności danych

2. Aktywne:

- Modyfikacja pakietów
- Zakłócanie usług
- Szkodzenie poufności, uwierzytelnianiu, integralności oraz dostępności



Ataki z wykorzystaniem technologii Bluetooth

1. Wysyłanie niechcianych wiadomości – Bluejacking
2. Nieautoryzowany dostęp do funkcji urządzenia - Bluesnarfing
3. Próby wydobycia poufnych informacji z telefonu

Zabezpieczenia:

1. Wyłączenie modułu BT
2. Wyłączenie trybu wyszukiwania (parowania)
3. Ustawienie zapytania przed odbiorem informacji



Zmiana adresu MAC

1. Ustalenie akceptowanych przez punkt dostępowy adresów MAC
2. Podszycie się poprzez zmianę adresu MAC własnej karty sieciowej





Ataki typu DoS

1. „Blokada usług”
2. Zwykle przeciążenie aplikacji obsługującej klientów
3. Najczęściej poprzez zalewanie danymi (ang. flooding)
4. Zajęcie pasma, którym dysponuje atakowany host



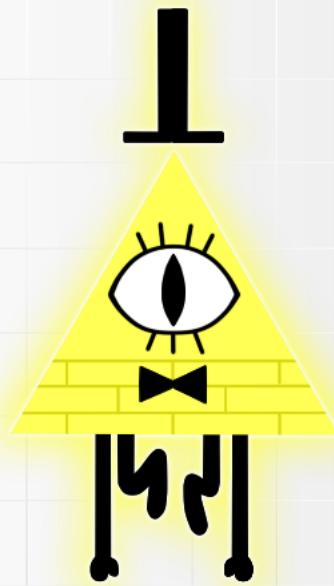


Ataki Caffe-Latte

1. Uzyskanie klucza do sieci nie będąc w zasięgu AP
2. Skierowane na odizolowanego klienta posiadającego klucz
3. Wykorzystanie zapisanych ustawień oraz opcji automatycznego łączenia z siecią
4. Podszycie pod AP i odpowiadanie na żądania połączenia klienta
5. Oczekiwanie na pakiety Gratuitous ARP po pomyślnej asocjacji

Bezpieczeństwo komunikacji bezprzewodowej

1. Standardy bezpieczeństwa – IEEE 802.11i
2. Uwierzytelnianie
3. Szyfrowanie





WEP – Wired Equivalent Privacy

1. Domyślny protokół
2. Wprowadzony w pierwszym standardzie 802.11
3. Bazuje na algorytmie RC4
4. Klucz tajny 40 lub 104 bity
5. 24-bitowy wektor inicjalizacyjny (IV)
6. Możliwy do odzyskania poprzez przechwycenie unikatowych wektorów inicjalizacyjnych



WPA – Wi-Fi Protected Access

1. Standard przejściowy między WEP i WPA2
2. Możliwy do wprowadzenia bez konieczności zmiany sprzętu
3. Wykorzystanie TKIP/RC4 oraz MIC
4. Podatny na ataki siłowe oraz kryptologiczne



WPA 2 – WiFi Protected Access 2

1. Najbardziej rozpowszechniony i bezpieczny
2. Wykorzystuje 128-bitowe klucze kryptograficzne
3. Wykorzystuje dynamiczne klucze
4. Nowe urządzenia używają WPA 2 bez zbędnych konfiguracji
5. Występuje w dwóch wersjach Personal i Enterprise



WPA 2 – Personal

1. PSK (Pre-Shared Key)
2. Zaprojektowany dla małych biur i domów
3. Wszyscy użytkownicy używają jednego klucza
4. Router szyfruje ruch za pomocą klucza
5. Klucz jest obliczany razem z hasłem do Wi-Fi

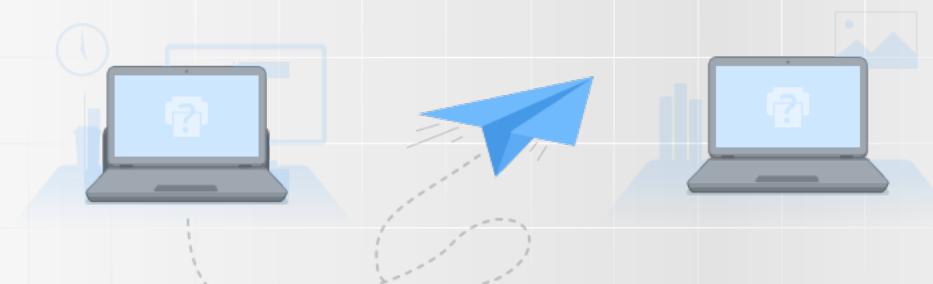


WPA 2 – Enterprise

1. WPA2 – Standard 802.1X
2. Wymaga więcej sprzętu niż PSK
3. Trudniejszy w konfiguracji i utrzymaniu
4. Wymaga serwera uwierzytelniania RADIUS
5. Połączenie z każdym klientem osobno szyfrowane unikalnym kluczem
6. Możliwość blokowania dostępu określonym użytkownikom bez wpływu na pozostałych

Transakcje sieciowe

Realizacja techniczna, sformalizowanej procedury przesłania informacji w sieci.





Zagrożenia transakcji sieciowych

1. Phishing
2. Sniffing
3. Spoofing
4. Pharming



Phishing

1. Próba nakłonienia do ujawnienia informacji osobistych
2. Wysyłanie fałszywych e-maili
3. Przekierowywanie na fałszywe strony



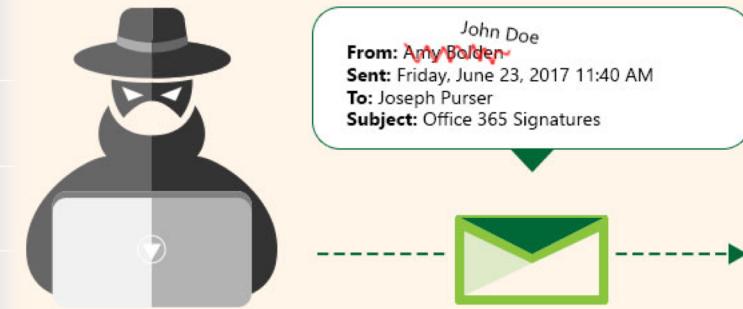
Sniffing

1. Monitorowanie i analizowanie ruchu w sieci
2. Wykradanie danych
3. Szpiegowanie aktywności
4. Gromadzenie informacji o użytkownikach
5. Niezabezpieczone sieci WiFi – miejsca publiczne



Spoofing

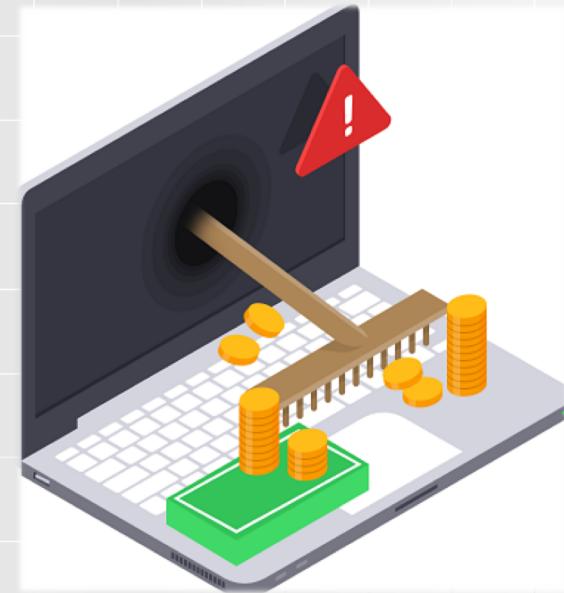
1. Podszywanie się pod kogoś lub coś
2. Uzyskanie informacji lub dostępu
3. Spoofing IP
4. Spoofing e-mail
5. Spoofing DNS





Pharming

1. Przypomina Phishing
2. Przekierowanie na fałszywą stronę
3. Wykorzystanie złośliwego oprogramowania
4. Infekcja serwera DNS





Bezpieczeństwo transakcji sieciowych

1. Korzystanie z unikalnych haseł – menedżer haseł
2. Sprawdzanie źródeł wiadomości
3. Sprawdzanie certyfikatów odwiedzanych stron
4. Ostrożność przy udostępnianiu wrażliwych danych
5. Virtual Private Network

Źródła grafik

<https://www.connexusuk.com/wp-content/uploads/2017/11/WiFi-Diagram.png>

<https://tls-bocasystems.com/foto/header/tls-boca-systems-icon-security-thumb.png>

https://vignette.wikia.nocookie.net/villains/images/9/9b/Bill_cipher.png/revision/latest?cb=20160825064511

<https://www.flexihub.com/images/articles-landing/img-sharePrinter.png>

<https://www.lorextechnology.com/accessories-for-security-cameras/100-foot-cul-certified-uv-treated-cat6-ethernet-cable-4-pack/CBL100C6RXU-4PK-1-p>

<https://hackaday.io/project/11326/gallery#4f6532e32be9a3084afddac5d9f39e57>

https://www.nicepng.com/png/full/97-974133_stock-photo-computer-hacker.png

<https://www.nowsecure.com/wp-content/uploads/2017/04/mobile-man-in-the-middle-attack-diagram.png>

https://s11.flog.pl/media/foto/10530343_man-ng323-lions-city-g-4613.jpg

<https://i.ytimg.com/vi/LQxe-JkSv4o/maxresdefault.jpg>

https://blog-en.webroot.com/wp-content/uploads/2018/09/Cyber-News-Rundown_FirefoxFroze_800x4001.png

https://cdn2.iconfinder.com/data/icons/wedding-hand-drawn-icons/64/wedding_26-512.png

https://blog.malwarebytes.com/wp-content/uploads/2018/09/shutterstock_749866270-900x506.jpg

<https://securebox.comodo.com/theme/images/network-sniffing.png>

<https://www.hs-academypages.com/hubfs/lp/academy/pharming.png>

https://www.codetwo.com/admins-blog/wp-content/uploads/2017/06/2017-06-22-Prevent_Spoofing_Blog_Image.jpg

<http://www.phishing.org/hs-fs/hubfs/Phishing/phishing-macboat.jpg?width=300&name=phishing-macboat.jpg>

<https://i0.wp.com/www.yabaleftonline.ng/wp-content/uploads/2015/10/Thief.png>



Źródła i przydatne materiały

Chris Fry, Martin Nystrom, „Monitoring i bezpieczeństwo sieci” – Helion 2010

<https://www.ietf.org/rfc/rfc4017.txt> [dostęp 26.04.2019]

<https://www.pcworld.pl/news/Bezpieczenstwo-transakcji-internetowych-jak-zabezpieczyc-przepliw-danych-w-sieci,412048.html> [dostęp 26.04.2019]

<https://niebezpiecznik.pl/> [dostęp 26.04.2019]

<https://zaufanatrzciastrona.pl/> [dostęp 26.04.2019]



Bezpieczeństwo komunikacji bezprzewodowej i transakcji sieciowych

Jan Luch
218150

Pytanie kierunkowe
nr 6

Wrocław 2019