



Bezpieczeństwo korzystania z sieci bezprzewodowych WLAN

Krzysztof Szczypiorski

Instytut Telekomunikacji Politechniki Warszawskiej

Krzysztof@Szczypiorski.com

<http://Krzysztof.Szczypiorski.com>

„Wi-Fi. Technologie, regulacje, nowy model biznesu”
Warszawa 19.11.2003 r.

Plan prezentacji

- ◆ Architektura bezpieczeństwa
- ◆ Ataki na WLAN
- ◆ Nowe standardy bezpieczeństwa
- ◆ Metody wdrażania bezpiecznego WLAN



Historia WLAN a bezpieczeństwo

- 1997** – pierwsza wersja standardu WLAN: IEEE 802.11:1997
- 1999** – druga wersja standardu: IEEE 802.11:1999 (ISO/IEC 8802-11: 1999)
 - powstaje Wireless Ethernet Compatibility Alliance (od 2002 Wi-Fi Alliance)
- 2000** – czółowe amerykańskie uniwersytety wprowadzają sieci WLAN w swoich kampusach
 - jesień – pierwszy dokument w ramach IEEE podważający bezpieczeństwo WLAN (autor: Jesse Walker - Intel)
- 2001** – zima – pierwszy spoza IEEE dokument (z Berkeley) opisujący zagrożenia w IEEE 802.11
 - wiosna – IEEE wydziela w ramach 802.11 grupę (TG1) poświęconą bezpieczeństwu
 - wiosna – IEEE udostępnia bezpłatnie standardy 802 po 6 miesiącach od ich publikacji
- 2002** – jesień – Wi-Fi ogłasza Wi-Fi Protected Access (WPA) – jako zbiór przejściowych zasad zwiększających bezpieczeństwo WLAN
- 2003** – jesień – planowany czas ukończenia prac w grupie TG1

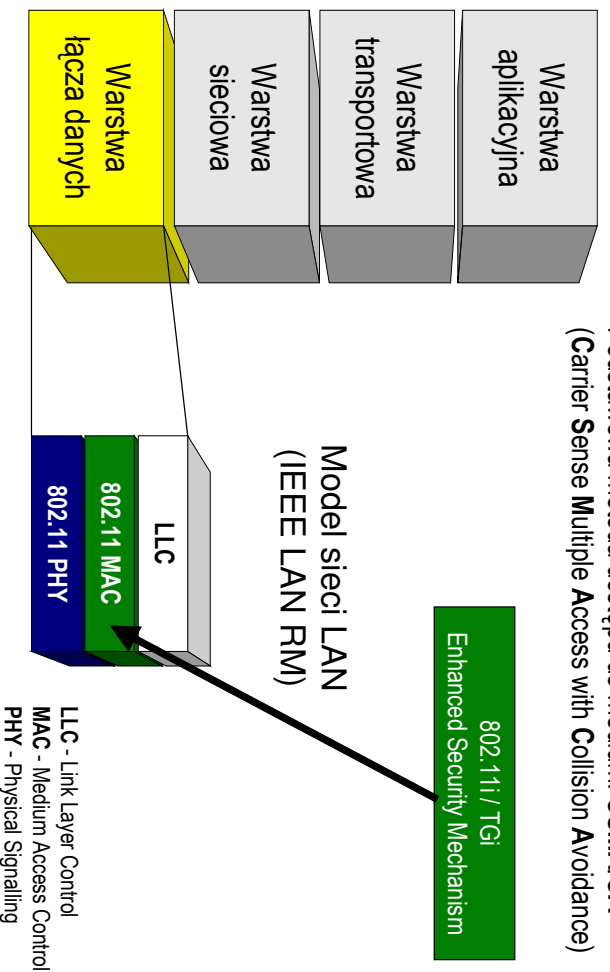
K.Szczypiorski - Bezpieczeństwo korzystania z sieci bezprzewodowych WLAN

3

WLAN a stos TCP/IP

Stos TCP/IP

Podstawowa metoda dostępu do medium: **CSMA/CA**
(Carrier Sense Multiple Access with Collision Avoidance)



K.Szczypiorski - Bezpieczeństwo korzystania z sieci bezprzewodowych WLAN

4



Usługi ochrony informacji w standardzie IEEE 802.11:1999

- Zrealizowane (warstwa MAC):
 - (kieszka) poufność
 - (niekryptograficzna) integralność
 - (marne) uwierzytelnienie
- Niezrealizowane:
 - kontrola dostępu
 - zarządzanie kluczami kryptograficznymi
- Wszystkie zrealizowane usługi powiązane z **WEP - Wired Equivalent Privacy** (Odpowiednik Przewodowej Prywatności)

K.Szczypiorski - Bezpieczeństwo korzystania z sieci bezprzewodowych WLAN

5



WEP - Wired Equivalent Privacy

Założenia projektowe IEEE 802.11:**1997** i 1999

Cel: Osiągnięcie za pomocą kryptografii poziomu bezpieczeństwa przewodowych sieci lokalnych (w tym IEEE 802.3 – Ethernet)

Jak to zrobić? Algorytm WEP o następujących cechach

- **siła** w tajności klucza
- **samosynchronizacja** algorytmu ze względu na charakter warstwy łącza danych ("best effort" i duża bitowa stopa błędów w kanale radiowym $\sim 10^{-5}$)
- **efektywność** w sprężeniu i oprogramowaniu
- **eksportowalność** algorytmu poza USA
- **opcjonalność** – implementacja i użycie WEP jako opcji

Efekt: cel nie zostaje osiągnięty przede wszystkim za sprawą niewłaściwego kontekstu użycia szyfru RC4 i braku zarządzania kluczami

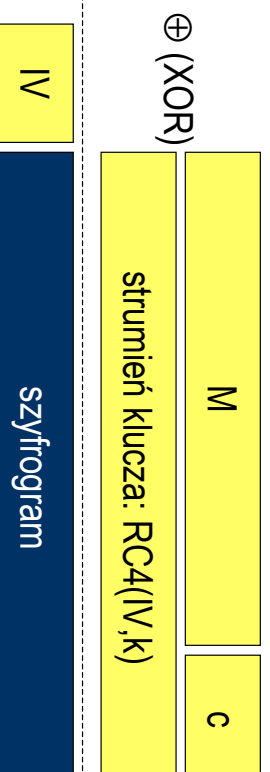
K.Szczypiorski - Bezpieczeństwo korzystania z sieci bezprzewodowych WLAN

6

WEP - Wired Equivalent Privacy

Idea działania

- bazuje na **RC4** z kluczem 64-bitowym (efektywnie 40-bitowym)
- użycie **RC4** z kluczem 128-bitowym (efektywnie 104-bitowym) jest rozwiązaniem niestandardowym
- nadawca i odbiorca dzielą tajny klucz – **k**
- wektor inicjujący – **IV**
- wiadomość – **M**
- przekształcenie **RC4(IV,k)** generujące strumień klucza
- suma kontrolna c realizowana za pomocą **CRC-32**
- manualna dystrybucja klucza

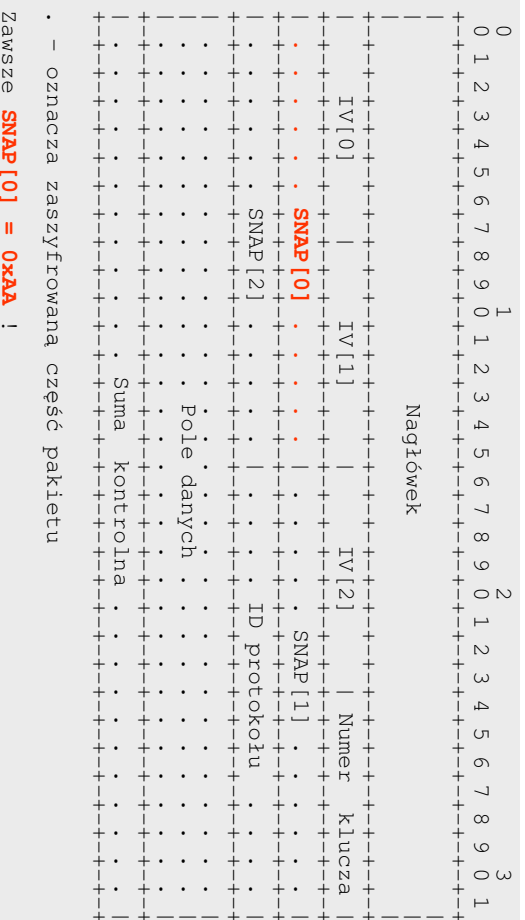


K.Szczypiorski - Bezpieczeństwo korzystania z sieci bezprzewodowych WLAN

7

WEP - Wired Equivalent Privacy

Ramka IEEE 802.11 zabezpieczona WEP



K.Szczypiorski - Bezpieczeństwo korzystania z sieci bezprzewodowych WLAN

8



Uwierzytelnienie w standardzie IEEE 802.11:1999

- **Open System Authentication (OSA)**
 - zgodnie z założeniem projektantów: **zerowe** uwierzytelnienie
- **Shared Key Authentication (SKA)**
 - oparte na **WEP** wykazanie faktu posiadania tajnego klucza
 - mechanizm wymiany uwierzytelniającej: wyzwanie-odpowiedź
- **SKA** przeważnie nie implementowany



Klasy ataków na standard IEEE 802.11:1999

wykorzystujące słabe punkty WEP

- A1. atak wykorzystujący ponowne użycie IV
- A2. atak ze znanym tekstem jawnym
- A3. atak z częściowo znanym tekstem jawnym
- A4. atak słownikowy → [1]
- A5. atak wykorzystujące słabości algorytmu RC4 → [2]

A6. podszycie się

A7. odmowa usługi (denial of service)

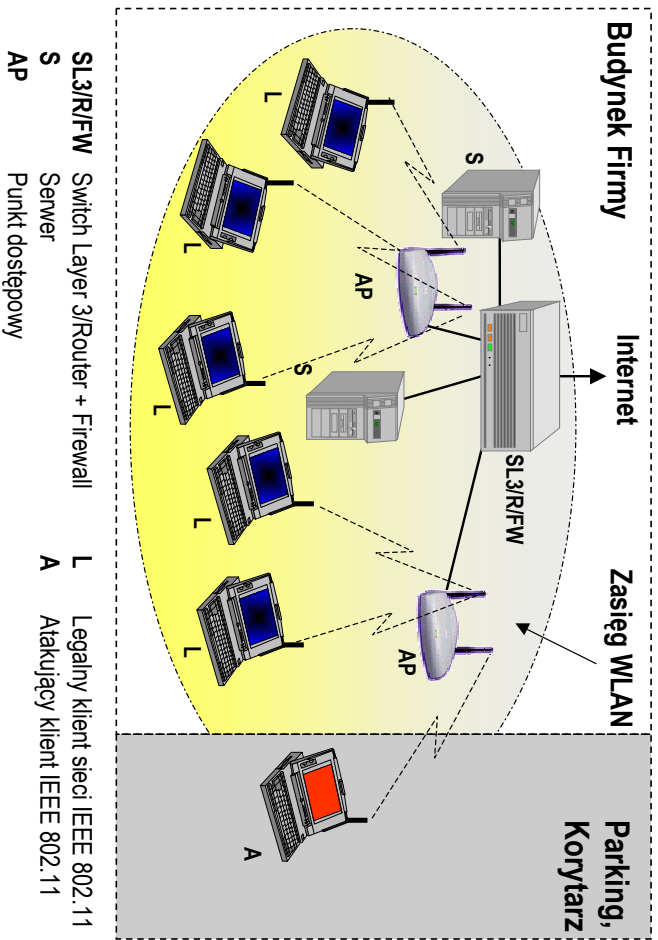
[1] Przeszukiwanie przestrzeni klucza

- autor: Tim Newsham
- przynależność do klasy: A4
- jeden z najefektywniejszych pod względem szybkości ataków atakujący posiada zestaw kluczy:
 - przechwycenie pakietu 802.11
 - deszyfrowanie wybranym kluczem pola użytkowego pakietu
 - zliczenie sumy kontrolnej
 - jeśli suma zgadza się: odszyfrowujemy pole użytkowe następnego pakietu
 - jeśli znowu się zgadza – mamy klucze!
- atak skuteczny na urządzenie IEEE 802.11 mające generatory kluczy bazujące na hasłach: redukcja przestrzeni klucza z 2^{40} do 2^{21}
- w praktyce: zestaw kluczy = słownik (atak słownikowy)
- **wniosek dla użytkowników WLAN:** nie używać kluczy bazujących na hasłach

[2] Atak na słabe klucze RC4

- autorzy: Fluhrer, Mantin, Shamir
- przynależność do klasy: A3 + A5
- najczęściej implementowany atak (AirSnort, WEPCrack)
- atak niezależny od długości klucza RC4
- atak na IV postaci: $(A + 3, N - 1, X)$
- stwierdzenie czy IV jest słabe zaraz po kroku KSA algorytmu RC4: $X = S\{B + 3\}[1] < B + 3, X + S\{B + 3\}[X] = B + 3$
- atak z wykorzystaniem znajomości pierwszego bajtu strumienia klucza – na którym ukazuje się fragment współdzielonego klucza poprzez „probabilistyczne głosowanie”
- **(spóźnione) wnioski dla twórców standardu IEEE 802.11:**
 - 1. pominąć pierwsze bajty strumienia klucza RC4
 - 2. nie używać RC4!
- **wniosek dla wytwórców sprzętu:** nie dopuszczać do użycia słabych IV albo stosować klucze sesyjne

Atak parkingowy cz. 1/4

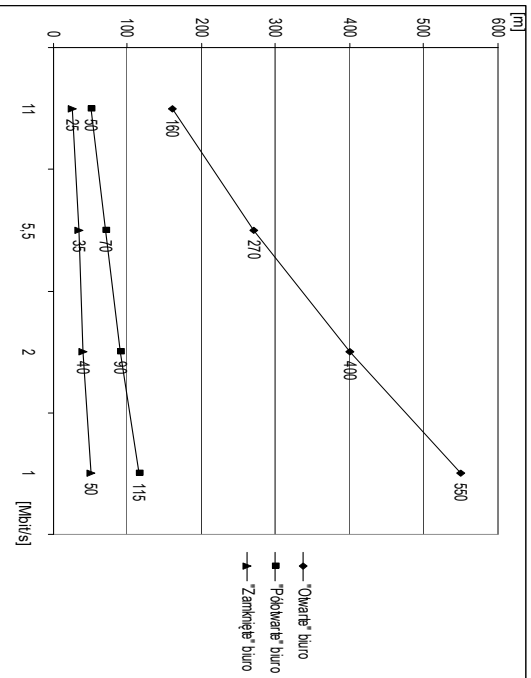


K. Szczypiorski - Bezpieczeństwo korzystania z sieci bezprzewodowych WLAN

13

Atak parkingowy cz. 2/4

- Faza I: przygotowania + znalezienie celu ataku
- 802.11b/g – 2,4 GHz
- tryb infrastrukturalny
- teoretyczny zasięg
- praktyczny zasięg <<100m
- „amatorskie” anteny zewnętrzne
- zwiększające zasięg (puszki, anteny satelitarne)



Dane: Instrukcja obsługi Avaya Wireless PC Card

K. Szczypiorski - Bezpieczeństwo korzystania z sieci bezprzewodowych WLAN

14



Atak parkingowy cz. 3/4

- **Faza II:** podłączenie się do punktu dostępowego
 - wykrucie sieci
 - wysłanie przez klienta ramki broadcast z prośbą o podłączenie się do punktu dostępowego (**wykrywają to dobre IDSy!!!**)
 - punkt dostępowy będący w zasięgu wysyła:
 - swoją nazwę
 - numer kanału radiowego
 - **ESSID** – Extended **S**ervice **S**et ID
 - adres MAC
 - narzędzia np. NetStumbler m.in. dla Windows, iPaq oraz Kismet dla Linuxa

K.Szczypiorski - Bezpieczeństwo korzystania z sieci bezprzewodowych WLAN

15



Atak parkingowy cz. 4/4

- **Faza III:** uruchomienie protokołu warstw wyższych
 - **DHCP** (**D**ynamic **H**ost **C**onfiguration **P**rotocol)
 - lub podsłuch pakietów za pomocą sniffera aby określić nieużywany adres IP (narzędzie: np. Ethernet dla Linuxa)
 - ale jeśli jest uaktywniony WEP:
 - narzędzia: AirSnort, WEPcrack
- **Faza IV:** praca w sieci
 - jeśli wszystko się powiedzie – praca jako pełnoprawny użytkownik sieci

K.Szczypiorski - Bezpieczeństwo korzystania z sieci bezprzewodowych WLAN

16

IEEE 802.11i

- ◆ TGi powołana w ramach 802.11 w maju 2001
 - IEEE P802.11i/D7 Unapproved Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems – LAN/MAN Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security, 2003
- ◆ W drafcie standardu 802.11i zdefiniowano dwa protokoły:
 - TKIP – kosmetyczna poprawka dla obecnych urządzeń
 - CCMP – lepsze bezpieczeństwo w nowych urządzeniach
- ◆ Świadoma polityka zapewnijająca zgodność wstecz
- ◆ EAP - Extensible Authentication Protocol (IETF)

K.Szczypiorski - Bezpieczeństwo korzystania z sieci bezprzewodowych WLAN

17

TKIP - cechy

- ◆ TKIP: Temporal Key Integrity Protocol
 - Może być zaimplementowany programowo
 - Wykorzystuje zaimplementowany sprzętowo WEP
 - Działa jako dodatkowy komponent
- ◆ TKIP klucze
 - 128-bitowy klucz szyfrujący
 - AP i klienci używają tego samego klucza
 - 64-bitowy klucz do zapewnienia integralności
 - AP i klienci nie używają tego samego klucza
- ◆ Algorytm MICHAEL

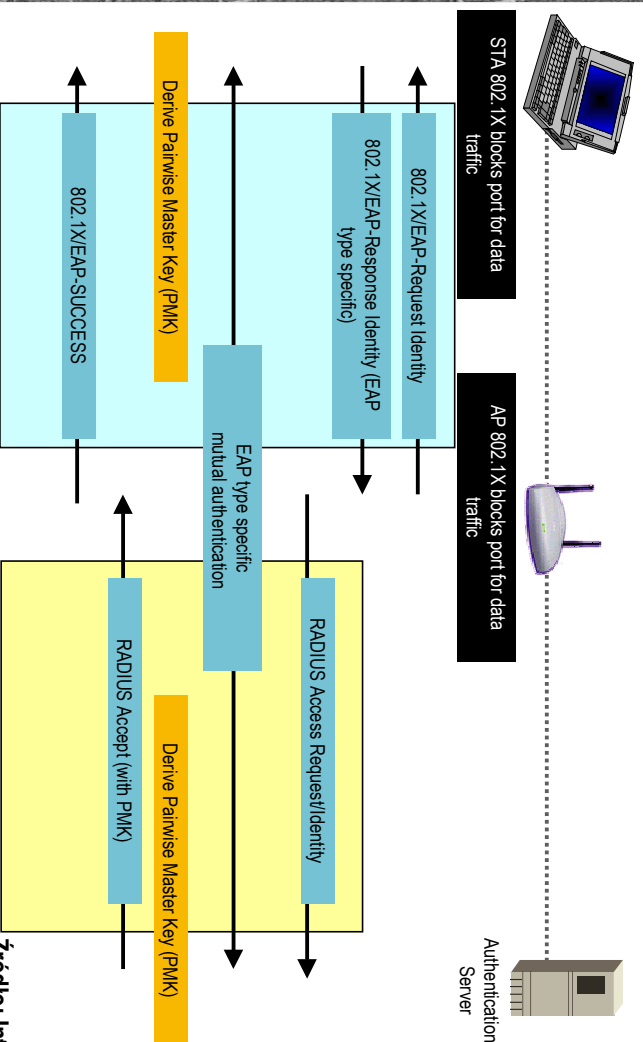
K.Szczypiorski - Bezpieczeństwo korzystania z sieci bezprzewodowych WLAN

18

CCMP - cechy

- ◆ Opcjonalne rozwiązanie długo-terminowe
- ◆ CCMP = Counter-Mode-CBC-MAC Protocol
- ◆ Bazuje na AES (Advanced Encryption Standard) w trybie pracy CCM
- ◆ AES wymaga wydajnego sprzętu zatem:
 - pojawia się nowe AP
 - pojawia się nowe urządzenia klienckie klasy hand-held
 - ale pozostaną PC
- ◆ Niewielki związek z WEP

802.1X/EAP – idea działania



Źródło: Intel



Wi-Fi Protected Access (WPA)

- ◆ **WPA: 2003-2004**
 - Od 2003 obowiązkowy przy certyfikacji Wi-Fi
 - Podzbiór standardu 802.11i
 - 802.1X/EAP, TKIP
- ◆ **WPA2: 2004-???**
 - 2004 (cezura: testy współpracy 802.11i) – opcjonalny
 - Od 2005 (???) - obowiązkowy
 - W pełni zgodny z 802.11i
 - WPA + Roaming + CCMP

K. Szczypiorski - Bezpieczeństwo korzystania z sieci bezprzewodowych WLAN

21



10 rad jak wdrożyć bezpieczny WLAN

1. zmienić domyślną nazwę sieci
2. uaktywnić WEP – zmienić domyślne hasła - wprowadzić procedury zmiany kluczy zbadać zasięg sieci (ogólnodostępne korytarze, „parkingi”...)
3. „zamknąć środowisko”, jeśli produkt na to zezwala
4. używać kluczy sesyjnych, jeśli produkt na to zezwala
5. użyć filtrowania na poziomie warstwy MAC (kryteria: adresy, pakiety bez/z WEP, typy protokołów sieciowych warstw wyższych)
6. wdrożyć system AAA (np. Radius), jeśli produkt na to zezwala
7. wdrożyć wirtualną sieć prywatną - VPN (Virtual Private Network)
8. izolować punkty dostępowe od strony przewodowej sieci lokalnej za pomocą ścian przeciwoogniowych
9. śledzić użycie logi gromadzone w punktach dostępowych

K. Szczypiorski - Bezpieczeństwo korzystania z sieci bezprzewodowych WLAN

22

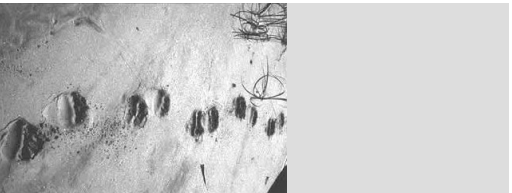
Wnioski

- ◆ Evolucja zabezpieczeń w WLAN (poziom)
 - 1 generacja: brak mech. bezp. 1997-2001 (hot spot)
 - 2 generacja: WEP 1997-2003 (dom)
 - 3 generacja: WPA 2003-2004 (firma)
 - 4 generacja: WPA2/802.11i 2004-
- ◆ Obecnie: niestabilne bezpieczeństwo zamyka drogę dla WLAN w zastosowaniach militarnych, rządowych i niektórych komercyjnych
- ◆ Wystarczający poziom dla użytkowników nie wymagających wyrafinowanych technik zabezpieczeń
- ◆ Atrakcyjne, ale niebezpieczne korzystanie z Hot Spotów



K. Szczypiorski - Bezpieczeństwo korzystania z sieci bezprzewodowych WLAN

23



Czy mają Państwo pytania?

Krzysztof Szczypiorski

Instytut Telekomunikacji Politechniki Warszawskiej

Krzysztof@Szczypiorski.com

<http://Krzysztof.Szczypiorski.com>

