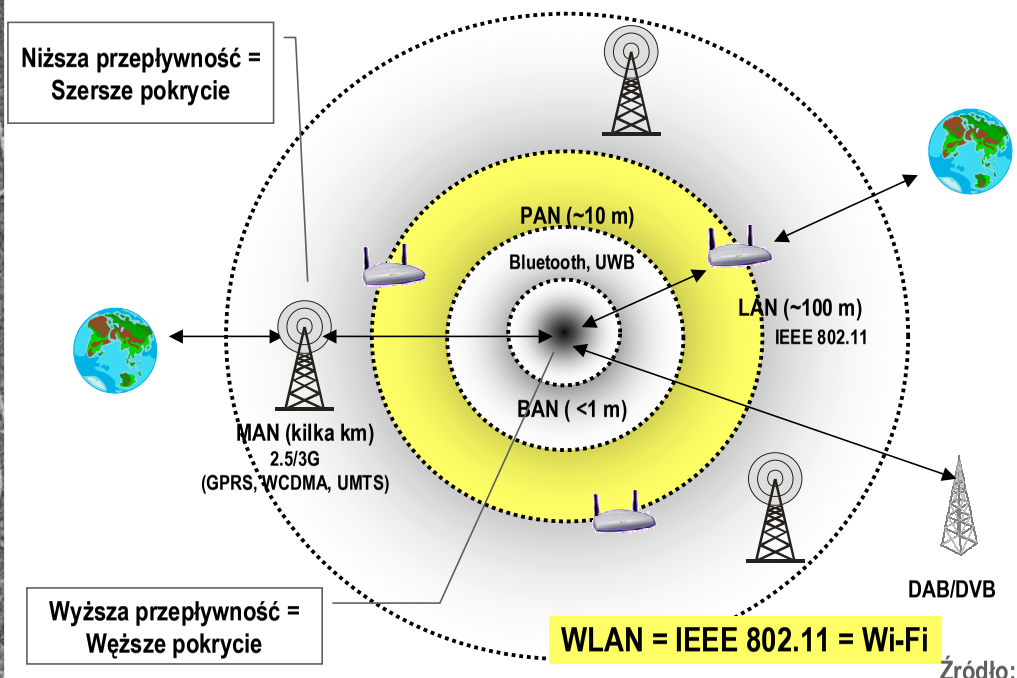
Bezpieczeństwo lokalnych sieci bezprzewodowych: od teorii do praktyki

Krzysztof Szczypiorski
Instytut Telekomunikacji Politechniki Warszawskiej

`Krzysztof@Szczypiorski.com`
`http://Krzysztof.Szczypiorski.com`

"Mobilne biuro – mobilny pracownik"
Warszawa 19.11.2003 r.

WLAN a sieci bezprzewodowe



Źródło: Intel

Plan prezentacji

- Najważniejsze cechy standardu
- 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 – czołowe amerykańskie uniwersytety wprowadzają sieci WLAN w swoich campusach

– 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

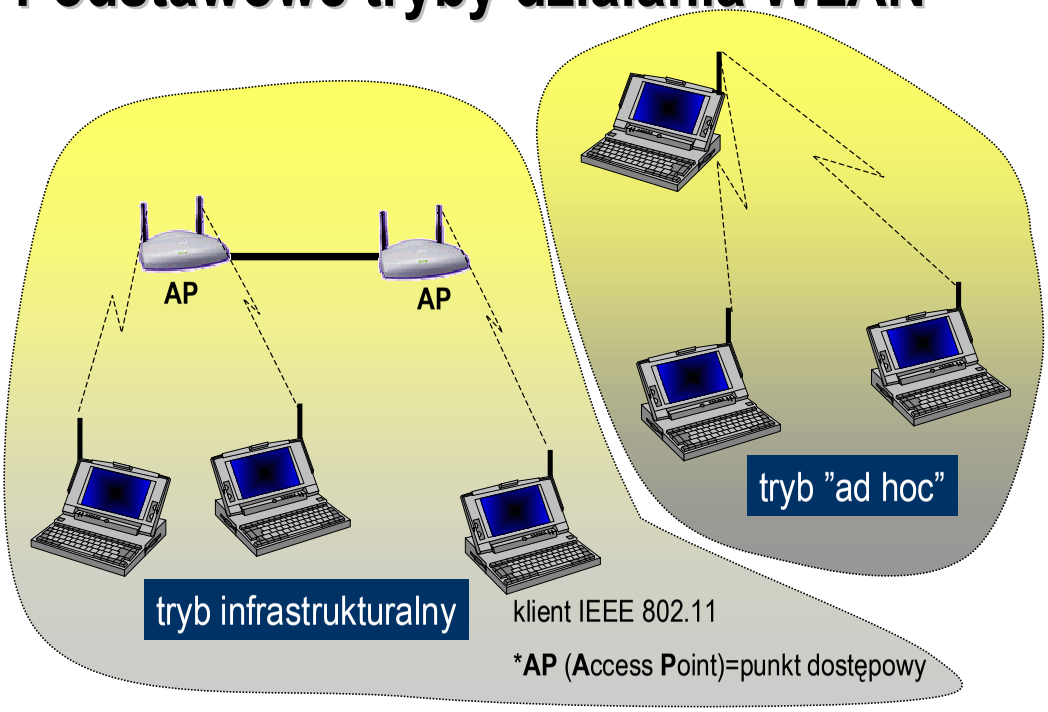
– wiosna – IEEE wydziela w ramach 802.11 grupę (TGi) poświęconą bezpieczeństwu

– wiosna – IEEE udostępnia bezpłatnie standardy 802 po 6 miesiącach od ich publikacji

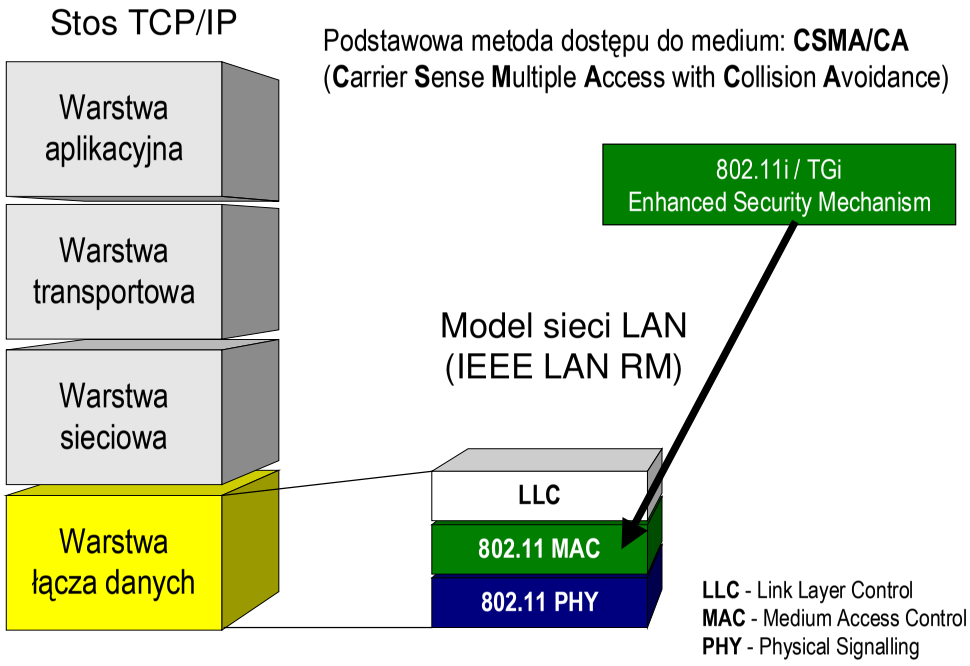
2002 – jesień – Wi-Fi ogłasza Wi-Fi Protected Access (WPA) – jako zbiór przejściowych zasad zwiększających bezpieczeństwo WLAN

2003 – jesień – planowany czas ukończenia prac w grupie TGi

Podstawowe tryby działania WLAN



WLAN a stos TCP/IP



Usługi ochrony informacji w standardzie IEEE 802.11:1999

- Zrealizowane (warstwa MAC):
  - (kiepska) poufność
  - (niekryptograficzna) integralność
  - (marne) uwierzytelnienie
- Niezrealizowane:
  - kontrola dostępu
  - zarządzanie kluczami kryptograficznymi
- Wszystkie zrealizowane usługi powiązane z **WEP** - **W**ired **E**quivalent **P**rivacy (Odpowiednik Przewodowej Prywatności)

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

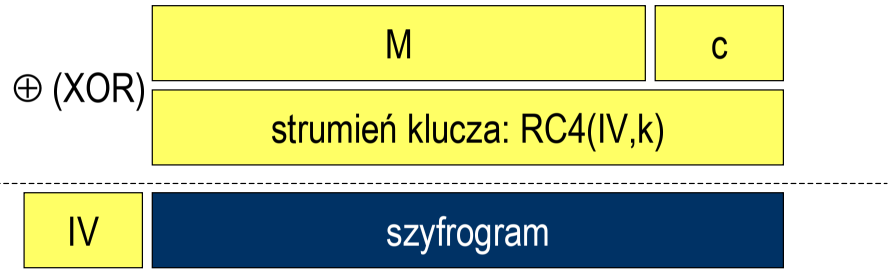
- **siła** w tajności klucza
- **samosynchronizacja** algorytmu ze względu na charakter warstwy łącza danych ("best effort" i duża bitowa stopa błędów w kanale radiowym ~10^{-5})
- **efektywność** w sprzęcie i oprogramowaniu
- **eksportowalność** algorytmu poza USA
- **opcjonalność** – implementacja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

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

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



WEP - Wired Equivalent Privacy

Ramka IEEE 802.11 zabezpieczona WEP

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                            Nagłówek                           |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     IV[0]     |     IV[1]     |     IV[2]     | Numer  klucza |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| . . . . . . SNAP[0] . . . . . | . . . . . SNAP[1] . . . . . . |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| . . . . . . SNAP[2] . . . . . | . . . . ID protokołu  . . . . |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . |
| . . . . . . . . . . . . . Pole danych . . . . . . . . . . . . |
| . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| . . . . . . . . . . . . Suma  kontrolna . . . . . . . . . . . |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

. - oznacza zaszyfrowaną część pakietu

Zawsze SNAP[0] = 0xAA !
```

Uwierzytelnienie w standardzie IEEE 802.11:1999

- **O**pen **S**ystem **A**uthentication (**OSA**)
  - zgodnie z założeniem projektantów: **zerowe** uwierzytelnienie
- **S**hared **K**ey **A**uthentication (**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)

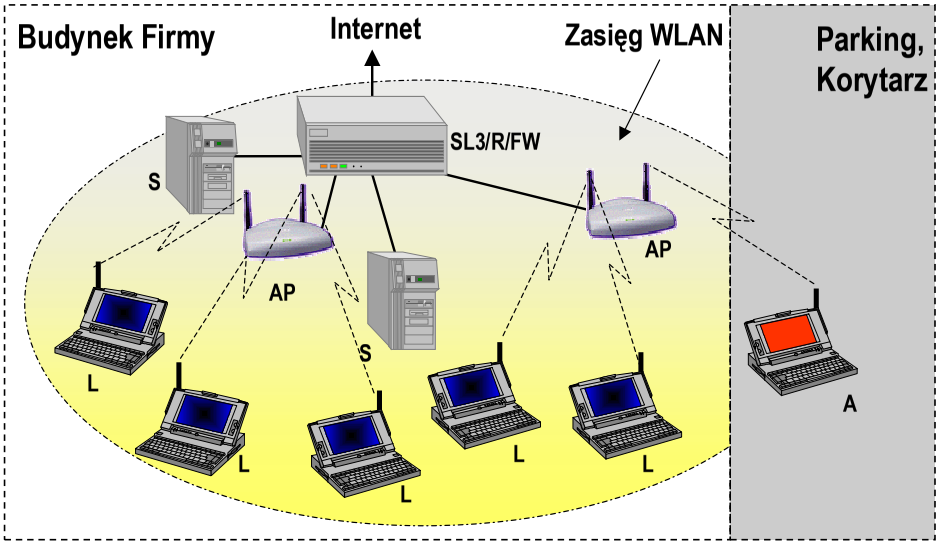
[1] Przeszukiwanie przestrzeni klucza

- 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 klucz!
- 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
- wykrywanie poszczególnych bajtów 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

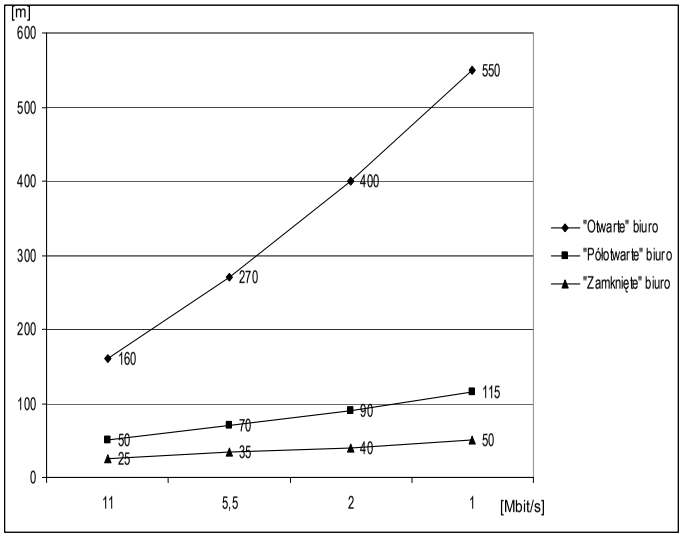
Atak parkingowy cz. 1/4



SL3/R/FW	Switch Layer 3/Router + Firewall	**L**	Legalny klient sieci IEEE 802.11
S	Serwer	**A**	Atakujący klient IEEE 802.11
AP	Punkt dostępowy		

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

Atak parkingowy cz. 3/4

- **Faza II:** podłączenie się do punktu dostępowego
  - wykrycie 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** – **E**xtended **S**ervice **S**et **ID**
    - adres MAC
  - narzędzia np. NetStumbler m.in. dla Windows, iPaq oraz Kismet dla Linuxa

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. Ethereal dla Linuxa)
  - ale jeśli jest uaktywniony WEP:
    - narzędzia: AirSnort, WEPcrack
- **Faza IV:** praca w sieci
    - jeśli wszystko się powiedzie – praca jako pełnoprawny użytkownik sieci

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 zapewniająca zgodność wstecz
- EAP - Extensible Authentication Protocol (IETF)

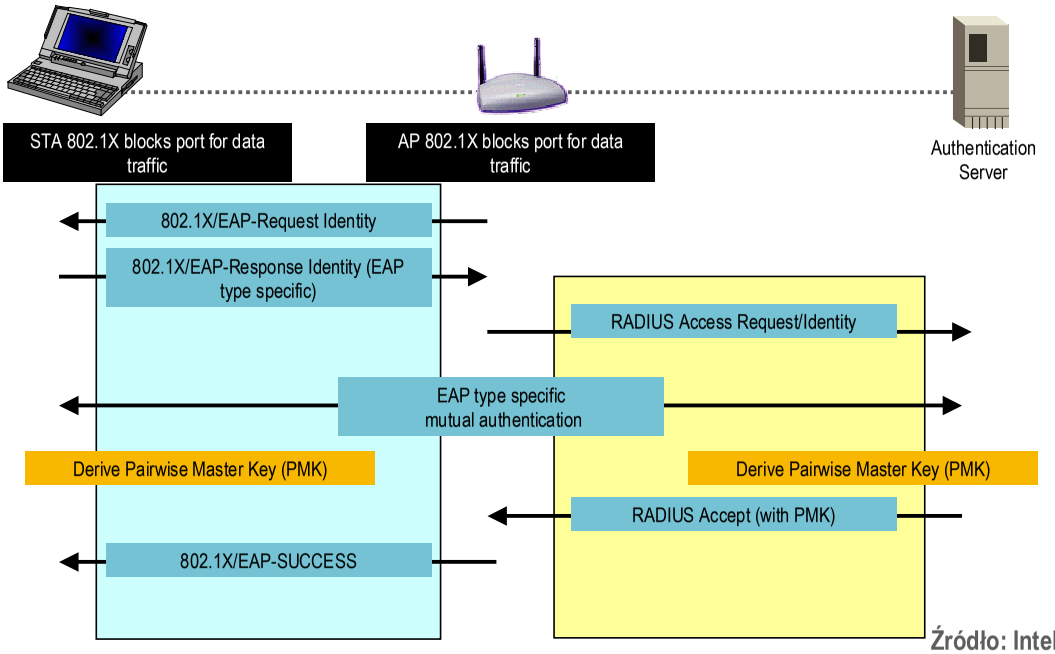
TKIP - cechy

- 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

CCMP - cechy

- Opcjonalne rozwiązanie długo-terminowe
- CCMP = **C**ounter-Mode-**C**BC-**M**AC **P**rotocol
- Bazuje na AES (Advanced Encryption Standard) w trybie pracy CCM
- AES wymaga wydajnego sprzętu zatem:
  - pojawią się nowe AP
  - pojawią 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)

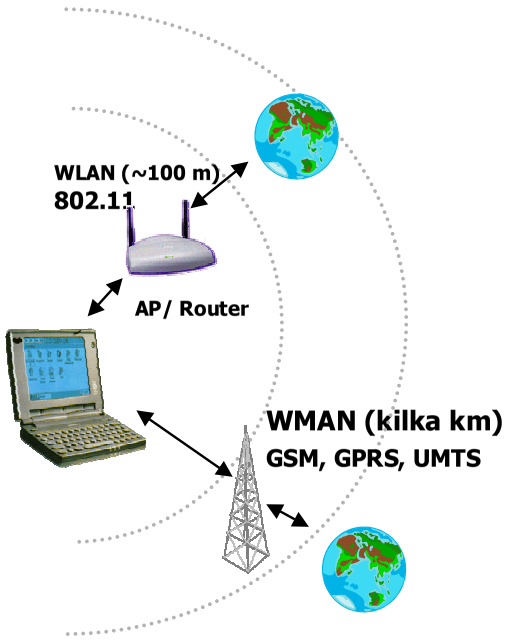
- **WPA:** 2003-2004
  - Od 2003 obowiązkowy przy certyfikacji Wi-Fi
  - Podzbiór standardu 802.11i
    - 802.1X/EAP, TKIP
- **WPA2:** 2004-???
  - 2004 (cezura: testy współpracy 802.11i) – opcjonalny
  - Od 2005 (???) - obowiązkowy
  - W pełni zgodny z 802.11i
    - WPA + Roaming + CCMP

WLAN a …

- **WLAN a PAN**
- **WLAN a GSM/GPRS:**

EAP-SIM - Extensible Authentication Protocol - Subscriber Identity Module

- **WLAN a UMTS**



Źródło: Intel

10 rad jak wdrożyć bezpieczny WLAN

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

Wnioski

- Bezpieczeństwo korzystania z hot spotów = bezpieczeństwo korzystania z kawiarenek internetowych
- Bezpieczeństwo WLAN w sieciach korporacyjnych = wybór „bezpiecznego” dostawcy
- Technika IEEE 802.11 nie powinna być stosowana w podsieciach instytucji/firm, w których są przetwarzane „czułe” informacje

Czy mają Państwo pytania?

Krzysztof Szczypiorski
Instytut Telekomunikacji Politechniki Warszawskiej

Krzysztof@Szczypiorski.com
http://Krzysztof.Szczypiorski.com