Bezpieczeństwo lokalnych sieci bezprzewodowych IEEE 802.11

Krzysztof Szczypiorski
Instytut Telekomunikacji Politechniki Warszawskiej
e-mail: K.Szczypiorski@tele.pw.edu.pl
http://krzysiek.tele.pw.edu.pl

Streszczenie

W referacie zostaną omówione zagadnienia bezpieczeństwa lokalnych sieci bezprzewodowych opartych na standardzie IEEE 802.11. Zaprezentowana zostanie architektura bezpieczeństwa, na którą składa się przede wszystkim algorytm WEP (*Wired Equivalent Privacy*). Algorytm WEP jest przeznaczony do zapewnienia poufności, integralności i opcjonalnie uwierzytelnienia. Wykorzystuje szyfr symetryczny pseudostrumieniowy RC4 o efektywnej długości klucza 40-bitów i kod CRC-32. WEP jest także używany do realizacji uwierzytelnienia opartego na technikach symetrycznych i mechanizmie wyzwanie-odpowiedź. Podczas prezentacji zostanie wykazane, że architektura bezpieczeństwa IEEE 802.11 nie jest odporna na wiele ataków sieciowych w tym: atak ze znanym tekstem jawnym, podszycie się, odmowa usługi (*denial of service*), atak słownikowy i podsłuch w czasie rzeczywistym. Liczne ułomności standardu posłużą do zaprezentowania skomasowanego ataku na sieć lokalną (tzw. ataku parkingowego). W dalszej części referatu zostaną omówione metody zabezpieczenia sieci IEEE 802.11 ograniczające ryzyko penetracji sieci lokalnych. Na zakończenie zostaną przedstawione perspektywy rozwoju standardu pod kątem zabezpieczeń (IEEE 802.11i).

Literatura

[1] IEEE 802.11, 1999 Edition (ISO/IEC 8802-11: 1999) IEEE Standards for Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Network - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
[2] IEEE 802.11a-1999 (8802-11:1999/Amd 1:2000(E)), IEEE Standard for Information Technology - Telecommunications and information exchange between Systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Amendment 1: High-speed Physical Layer in the 5 GHz band
[3] IEEE 802.11b-1999 Supplement to 802.11-1999,Wireless LAN MAC and PHY specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band
[4] Jesse R. Walker IEEE P802.11 - Wireless LANs - Unsafe at any key size - An analysis of the WEP encapsulation, Intel - October 2000
[5] Nikita Borisov, Ian Goldberg, David Wagner - Intercepting Mobile Communications: The Insecurity of 802.11 - University of California at Berkely - January 2001
[6] William A. Arbaugh, Narendar Shankar, Y.C. Justin Wan - Your 802.11 Wireless Network has No Clothes - University of Maryland - March 2001
[7] Scott Fluhrer, Itsik Mantin, Adi Shamir - Weaknesses in the Key Scheduling Algorithm of RC4 - The Weizmann Institute - August 2001
[8] Tim Newsham - Cracking WEP Keys - Blackhat 2001
[9] Arunesh Mishra, William A. Arbaugh - An Initial Security Analysis of the IEEE 802.1X Protocol - January 2002
[10] Zbiór stron internetowych o bezprzewodowych sieciach lokalnych (Wireless LANs) w tym IEEE 802.11 http://www.nwfusion.com/research/wifi.html
[11] Opis anteny wykonanej z puszki po chipsach: http://www.oreillynet.com/cs/weblog/view/wlg/448
[12] Opis anteny wykonanej z puszki po kawie: http://www.oreillynet.com/cs/weblog/view/wlg/1124

Bezpieczenstwo lokalnych sieci bezprzewodowych IEEE 802.11

Krzysztof Szczypiorski
Instytut Telekomunikacji Politechniki Warszawskiej
e-mail: K.Szczypiorski@tele.pw.edu.pl
http://krzysiek.tele.pw.edu.pl

VI Krajowa Konferencja Zastosowań Kryptografii ENIGMA 2002
Warszawa, 14-17 maja 2002 r.

Plan referatu

- Ogólne cechy standardu IEEE 802.11
- Architektura bezpieczeństwa
- Przykład kompletnego ataku
- Znane metody ochrony
- Przyszłość standardu IEEE 802.11

Najważniejsze daty w historii IEEE 802.11

„- Boże, jakież te nowe szaty cesarza są piękne! Jaki wspaniały tren, jaki świetny krój. Nikt nie chciał po sobie pokazać, że nic nie widzi, bo wtedy okazałoby się, że nie nadaje się do swego urzędu albo że jest głupi. Żadne szaty cesarza nie cieszyły się takim powodzeniem jak te właśnie.
- Patrzcie, przecież on jest nagi! - zawołało jakieś małe dziecko."

Hans Christian Andersen „Nowe szaty cesarza"

1997 – pierwsza wersja standardu IEEE 802.11:1997

1999 – druga wersja standardu IEEE 802.11:1999 (ISO/IEC 8802-11: 1999)

2000 – czołowe amerykańskie uniwersytety (w tym Berkeley) wprowadzają sieć IEEE 802.11

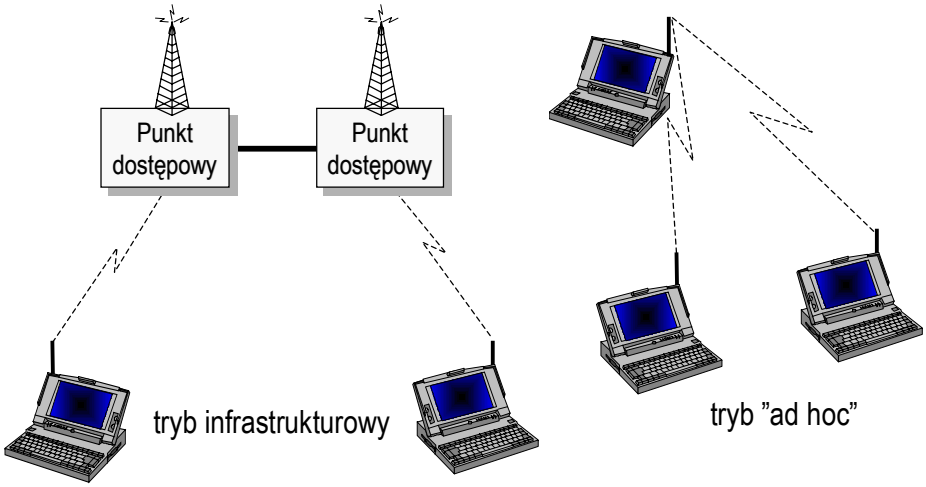
2000 (październik) – pierwszy dokument w ramach IEEE podważający bezpieczeństwo 802.11 (autor: Jesse Walker - Intel)

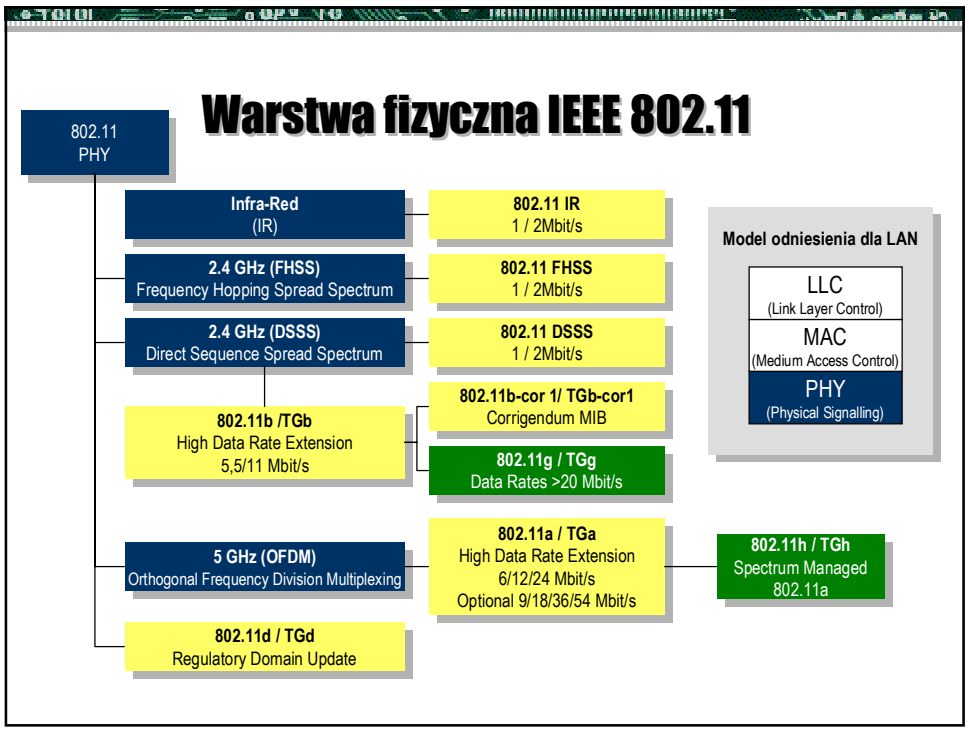
2001 (styczeń) – pierwszy spoza IEEE dokument (z Berkeley) opisujący zagrożenia w IEEE 802.11

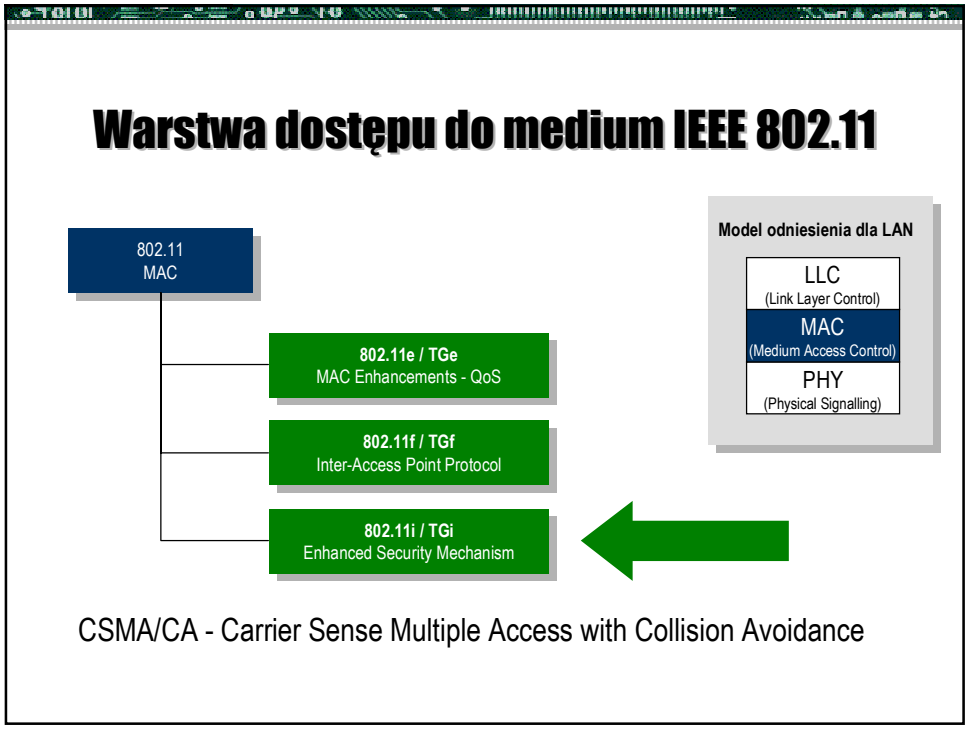
2001 (maj) – IEEE wydziela w ramach 802.11 grupę (TGi) do problemów bezpieczeństwa

2001 (maj) – IEEE udostępnia bezpłatnie standardy 802 po 6 miesiącach od ich publikacji

Podstawowe tryby działania IEEE 802.11




Warstwa fizyczna IEEE 802.11
802.11 PHY
Infra-Red (IR)
802.11 IR 1 / 2Mbit/s
2.4 GHz (FHSS) Frequency Hopping Spread Spectrum
802.11 FHSS 1 / 2Mbit/s
2.4 GHz (DSSS) Direct Sequence Spread Spectrum
802.11 DSSS 1 / 2Mbit/s
802.11b /TGb High Data Rate Extension 5,5/11 Mbit/s
802.11b-cor 1/ TGb-cor1 Corrigendum MIB
802.11g / TGg Data Rates >20 Mbit/s
5 GHz (OFDM) Orthogonal Frequency Division Multiplexing
802.11a / TGa High Data Rate Extension 6/12/24 Mbit/s Optional 9/18/36/54 Mbit/s
802.11h / TGh Spectrum Managed 802.11a
802.11d / TGd Regulatory Domain Update
Model odniesienia dla LAN
LLC (Link Layer Control)
MAC (Medium Access Control)
PHY (Physical Signalling)


Warstwa dostępu do medium IEEE 802.11
802.11 MAC
802.11e / TGe MAC Enhancements - QoS
802.11f / TGf Inter-Access Point Protocol
802.11i / TGi Enhanced Security Mechanism
Model odniesienia dla LAN
LLC (Link Layer Control)
MAC (Medium Access Control)
PHY (Physical Signalling)
CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance

Usługi ochrony informacji w IEEE 802.11

Zrealizowane w warstwie MAC

- Kiepska **poufność**
- Niekryptograficzna **integralność**
- Marne **uwierzytelnienie**

Brak kontroli dostępu
Brak zarządzania kluczami

wszystkie zrealizowane usługi powiązane z
WEP - Wired Equivalent Privacy

WEP - Wired Equivalent Privacy
Założenia projektowe - IEEE 802.11:1997 i 1999

Cel: Osiągnąć za pomocą kryptografii poziom bezpieczeństwa sieci przewodowych (np. IEEE 802.3 – Ethernet)

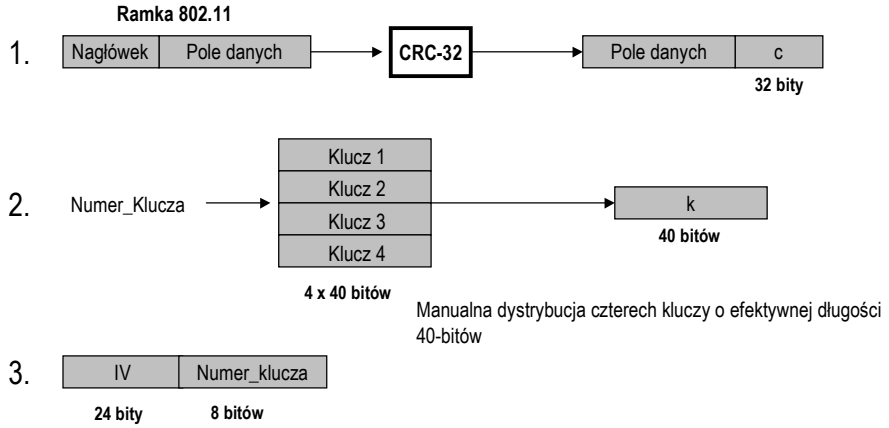
Jak to zrobić? Algorytm WEP o następujących cechach

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

WEP - Wired Equivalent Privacy
Idea działania

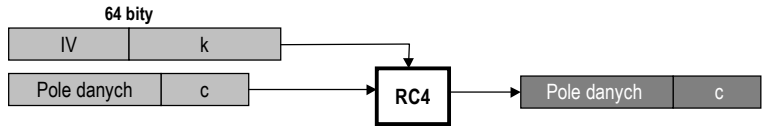
- bazuje na **RC4** z kluczem 64-bitowym (efektywnie 40-bitowym)
- użycie **RC4** z kluczem 128-bitowym jest rozwiązaniem niestandardowym
- nadawca i odbiorca dzielą tajny klucz **k**
- wiadomość - **M**
- wektor inicjalizujący - **IV**
- przekształcenie **RC4(IV,k)**
- suma kontrolna c realizowana za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

WEP - Wired Equivalent Privacy
Szczegóły cz. 1/2



WEP - Wired Equivalent Privacy
Szczegóły cz. 2/2

4.



5.

Ramka 802.11 zabezpieczona WEP

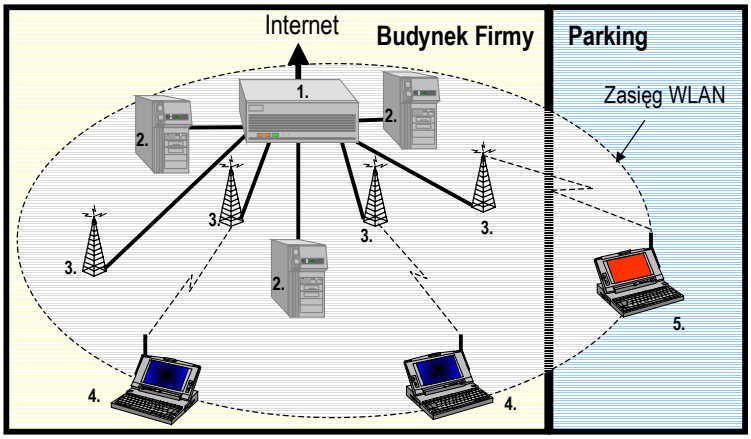
Uwierzytelnienie

- Open System Authentication
  - zgodnie z założeniem projektantów: **zerowe** uwierzytelnienie
- Shared Key Authentication
  - oparte na WEP wykazanie faktu posiadania tajnego klucza
  - mechanizm wymiany uwierzytelniającej: wyzwanie-odpowiedź

Klasy ataków na IEEE 802.11 wykorzystujące słabe punkty WEP

- ♦atak wykorzystujący ponowne użycie IV
- ♦atak ze znanym tekstem jawnym
- ♦atak z częściowo znanym tekstem jawnym
- ♦podszycie się
- ♦odmowa usługi (denial of service)
- ♦atak słownikowy
- ♦deszyfrowanie w czasie rzeczywistym

Przykładowy atak cz. 1/6



- Switch Layer 3/Router+ Firewall
- Serwer
- Punkt dostępowy
- Legalny klient sieci IEEE 802.11
- Atakujący klient IEEE 802.11

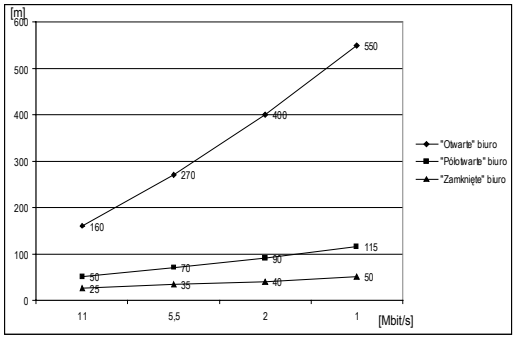
Atak parkingowy

Przykładowy atak cz. 2/6

- Faza I: przygotowania + znalezienie celu ataku
- Faza II: podłączenie się do punktu dostępowego
- Faza III: uruchomienie protokołu warstw wyższych
- Faza IV: praca w sieci

Przykładowy atak cz. 3/6

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



Dane: Instruckcja obsługi Avaya Wireless PC Card

Źródła:
http://www.oreillynet.com/cs/weblog/view/wlg/448 ←
http://www.oreillynet.com/cs/weblog/view/wlg/1124 ↑

Przykładowy atak cz. 5/6

- Faza II: podłączenie się do punktu dostępowego
  - wykrycie sieci
  - wysłanie przez klienta ramki broadcast z prośbą o podłączenie się do punktu dostępowego
  - punkt dostępowy będący w zasięgu wysyła:
    - swoją nazwę
    - numer kanału radiowego
    - ESSID – Extended Service Set ID
    - adres MAC
  - NetStumbler dla Windows

Przykładowy atak cz. 6/6

- Faza III: uruchomienie protokołu warstw wyższych
  - The Dynamic Host Configuration Protocol (DHCP)
  - lub podsłuch pakietów za pomocą sniffera aby określić nieużywany adres IP (Ethereal for Linux)
  - ale jeśli jest uaktywniony WEP:
    - AirSnort lub WEPcrack
- Faza IV: praca w sieci
  - pełnoprawny użytkownik sieci

Zabezpieczenia
czyli jak wdrażać IEEE 802.11 dzisiaj

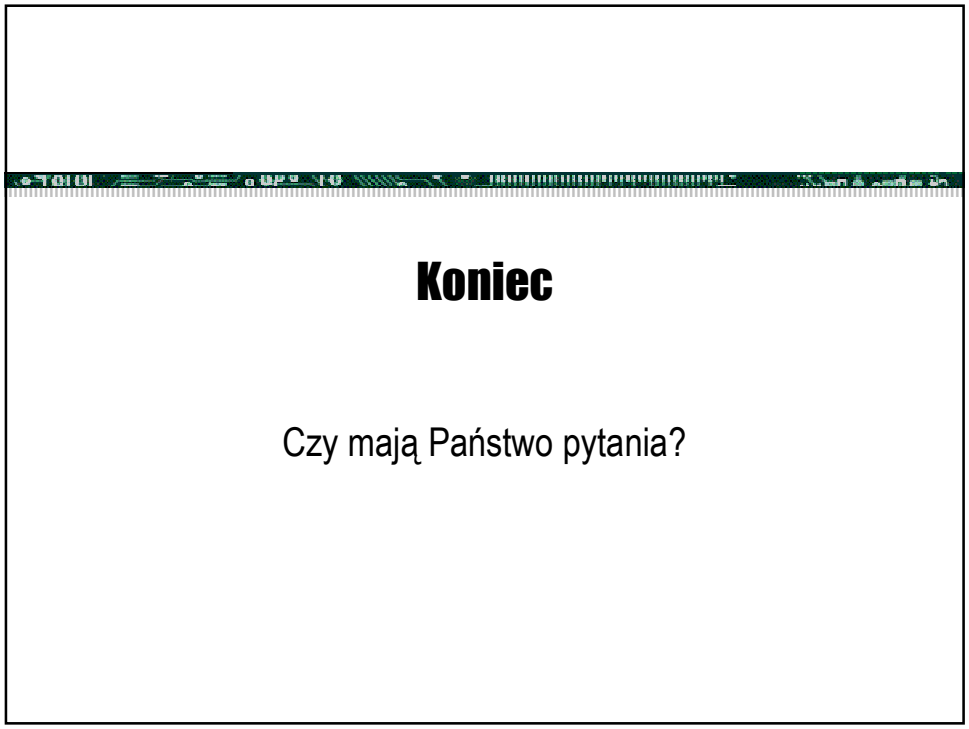
- zbadać zasięg sieci
- uaktywnić WEP – zmienić domyślne hasła - wprowadzić procedury zmiany kluczy (np. codzienne)
- zmienić domyślną nazwę sieci
- używać kluczy sesyjnych, jeśli produkt na to zezwala
- użyć filtrowania na poziomie warstwy MAC (kryteria: adresy, pakiety bez/z WEP)
- wdrożyć wirtualną sieć prywatną - VPN (Virtual Private Network)

Przyszłość

- oczekiwanie na standard 802.11i
  - produkty 2003 ???
- RC4 → AES
- Extensible Authentication Protocol (EAP)
- IEEE 802.1X - Network Port Authentication ???
- IEEE 802.11 roaming

Podsumowanie

- bezpieczeństwo zawarte w IEEE 802.11 jest nikłe i nie jest odpowiednikiem „przewodowej prywatności”
- na dzień dzisiejszy - zwiększenie bezpieczeństwa - wykorzystanie niestandardowych opcji w urządzeniach producentów
- bezpieczne wdrożenia – możliwe – spore nakłady
- stosowanie standardu nie jest zalecane dla instytucji/firm/organizacji przetwarzających dane o dużej wadze


Koniec
Czy mają Państwo pytania?