Trendy zabezpieczeń w bezprzewodowych sieciach lokalnych

Krzysztof Szczypiorki, Igor Margasiński
Instytut Telekomunikacji PW
e-mail: krzysztof@szczypiorski.com, igor@margasinski.com

Streszczenie

W referacie przedstawiono trendy zabezpieczeń związane z bezprzewodowymi sieciami lokalnymi (WLAN – Wireless LAN). W ewolucji zabezpieczeń WLAN można wyróżnić cztery etapy:

1. etap: brak mechanizmów bezpieczeństwa - 1997-2001
2. etap: WEP (Wired Equivalent Privacy) - 1997-2003
3. etap: WPA (Wi-Fi Protected Access WPA) - 2003-2004
4. etap: WPA2/ IEEE 802.11i - 2004-???

Dla każdego etapu, w szczególności dla 3. i 4., zostaną krytycznie przedstawione najważniejsze protokoły, w tym TKIP (Temporal Key Integrity Protocol), Michael, CCMP (Counter-Mode-CBC-MAC Protocol) oraz IEEE 802.1X/EAP – składające się na nowy niepublikowany jeszcze standard IEEE 802.11i.

Trendy zabezpieczeń w bezprzewodowych sieciach lokalnych

Krzysztof Szczypiorski, Igor Margasiński
Instytut Telekomunikacji PW
E-mail: krzysztof@szczypiorski.com, igor@margasinski.com

VIII Krajowa Konferencja Zastosowań Kryptografii Enigma 2004
Warszawa, 10-13 maja 2004

THE WALL STREET JOURNAL.

© 2001 Dow Jones & Company, Inc. All Rights Reserved.

VOL. CCXXXVII NO. 23 WEDA ★★★ MONDAY, FEBRUARY 5, 2001 WSJ.com ★★★★

Hackers Can Penetrate Wireless Network

By JARED SANDBERG
Staff Reporter of THE WALL STREET JOURNAL

A group of respected security research- ple, brought to light by network-security specialists around the globe. Mr. Goldberg himself found a significant flaw in the rel." He adds that the IEEE is working on future versions that won't be vulnerable. But Mr. Ennis says this type of attack

The weakness is another reminder of the difficulty in implementing effective network security.

connect to networks using simple radio antennas in their laptop or desktop PCs. The technology, also called Wi-Fi, is sold by many vendors but was popularized by Apple Computer Inc. under the name AirPort and is quickly being deployed in networks at a growing number of businesses, college campuses, hotels and airports. By the end of 2001, an estimated 10 million Wi-Fi radios will be deployed, according to research firm Cahners In-Stat. Starbucks Corp., for instance, plans to use the technology to allow latte quaffers to noodle

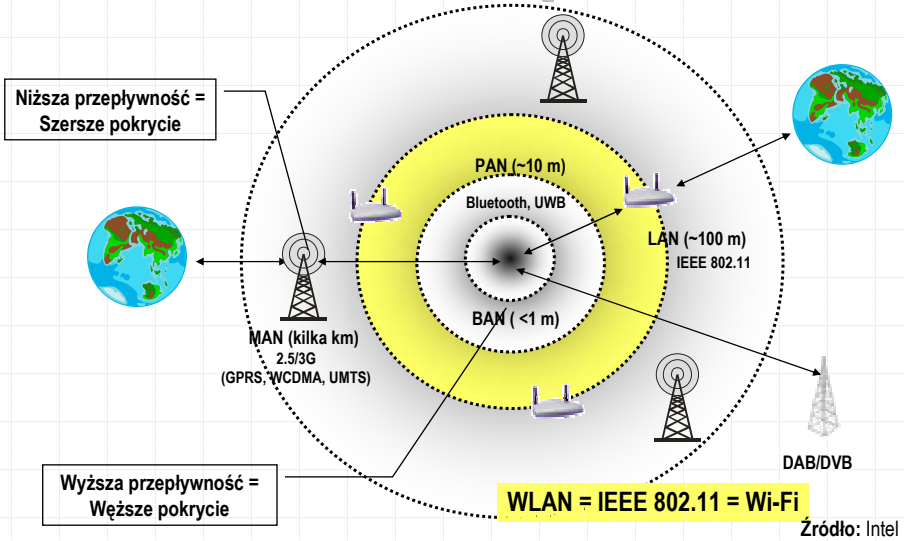
chief scientist at Zero Knowledge Systems Inc., a privacy-software firm in Montreal.

...esses deploy wireless networks, connected to their internal conventional networks, without activating security measures such as WEP. One computer-security consultant in New York, who asked not to be identified, said he was able to access the computer network of his client, a major financial-services firm on Wall Street, while sitting on a bench across the street. Though he didn't have free range of the network, it was as if he walked through the building lobby, past a receptionist and sat down at one of the firm's computers.

Główne punkty prezentacji

- WLAN a inne sieci bezprzewodowe
- Propagacja sygnału radiowego i związane z nim ryzyko podsłuchu
- Historia WLAN w kontekście bezpieczeństwa
- „Ochrona łącza” (poufność, integralność):
  - WEP, TKIP, CCMP
- Zarządzania kluczami i uwierzytelnienie:
  - od zera do IEEE 802.1X + EAP
- Tajemny krąg standardów: IEEE 802.11i, WPA, WPA2…
- Jaka będzie przyszłość?

WLAN a inne sieci bezprzewodowe

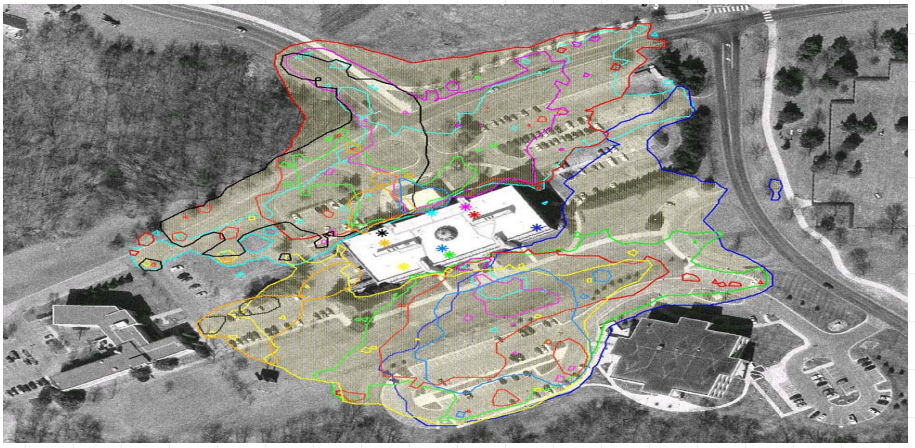


Źródło: Intel

Propagacja sygnału radiowego

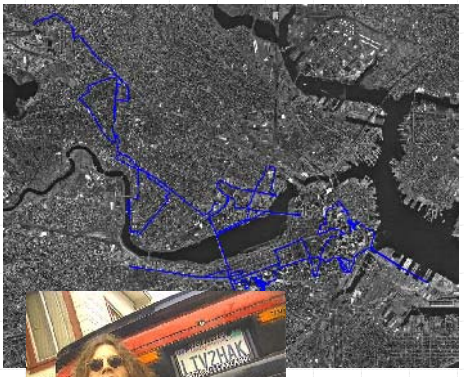
Źródło: David Wagner - Why Swiss-Cheese Security Isn't Enough

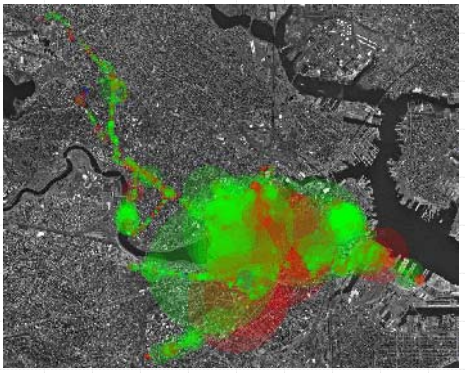
Ryzyko ataku z dużej odległości



Źródło: David Wagner - Why Swiss-Cheese Security Isn't Enough

Wardriving, warflying...



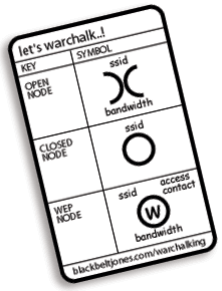


Peter Shipley - prekursor

Źródło map: http://www.wardriving.com/**boston**

Wi-Fi + car = Wardriving
Wi-Fi + plane = Warflying

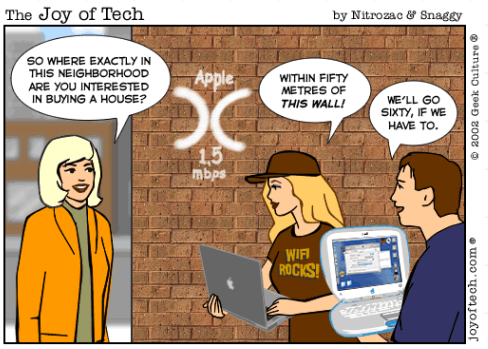
Warchalking cz. 1/2



www.warchalking.org

chalk (kreda)

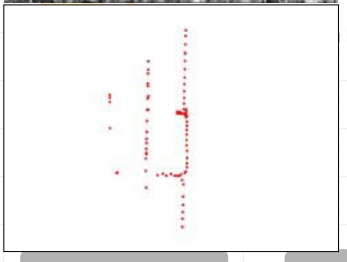
Warchalking cz. 2/2



They always dreamed of having a home *in* the range.

Źródło: http://www.doc-x.de/cgi-bin/wiki.pl?action=browse&diff=1&id=WarChalking

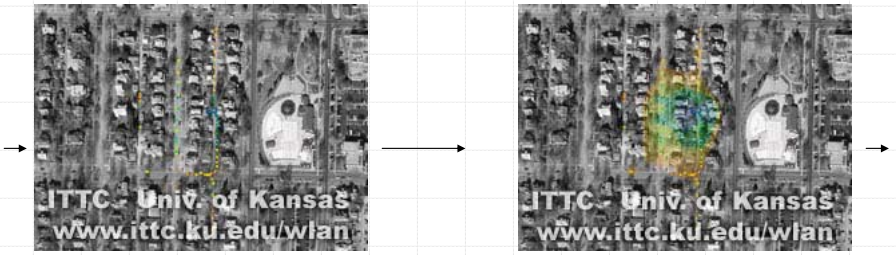
Tworzenie map sieci cz. 1/3



Project

http://www.ittc.ku.edu/wlan/

Tworzenie map sieci cz. 2/3



Inverse Distance Weighted (IDW)

Tworzenie map sieci cz. 3/3

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

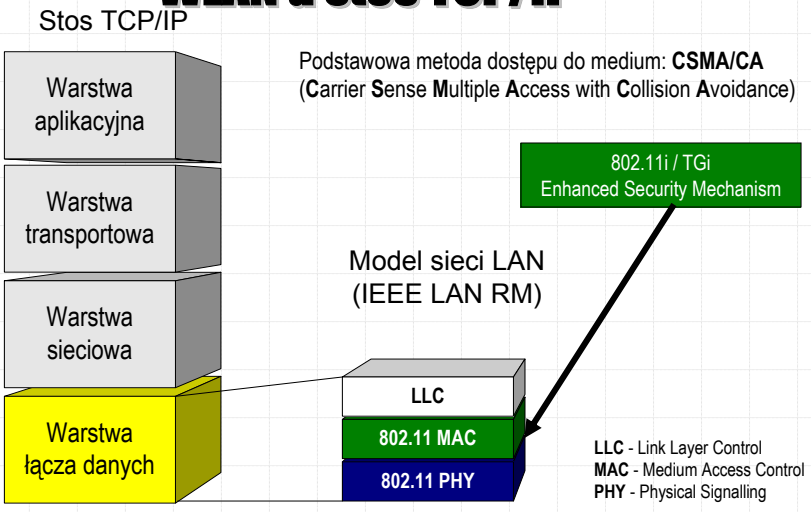
– wiosna – IEEE wydziela w ramach 802.11 grupę (TGi) poświęconą bezpieczeństwu

– 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

2004 – standaryzacja IEEE 802.11i (???)

WLAN a stos TCP/IP

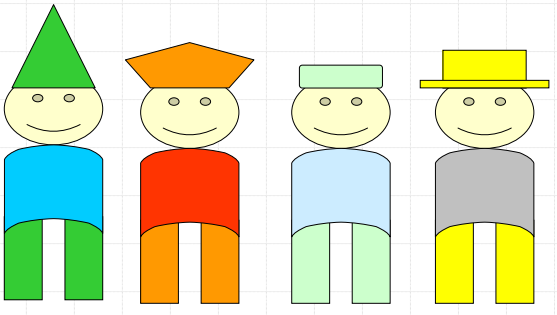


Mit bezpieczeństwa warstwy fizycznej

„I can't keep my eyes open - wish I had my radio."
Kate Bush

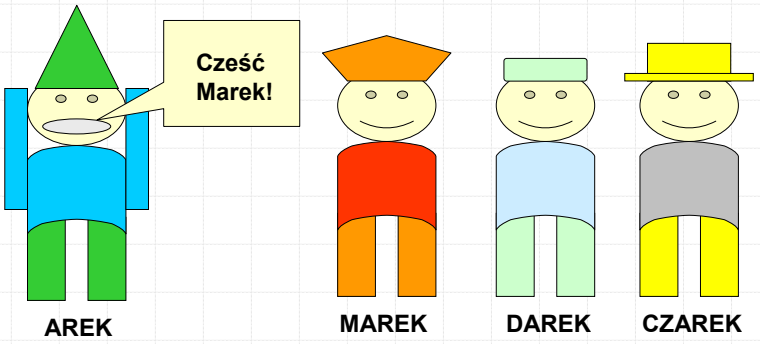
- Wyrafinowane metody modulacji i kodowania sygnałów radiowych
- Jeśli chcę posłuchać Radia X FM – kupuję radioodbiornik z UKF
- Jeśli chcę oglądać TVP X – kupuję telewizor
- Jeśli chcę podsłuchiwać WLAN – kupuję kartę sieciową WLAN
- Historyczne podejście do ochrony danych przez stosowanie tajnych metod komunikacji – np. frequency hopping wynalezione przez **Hedy Lammar**

CSMA/CA cz. 1/8



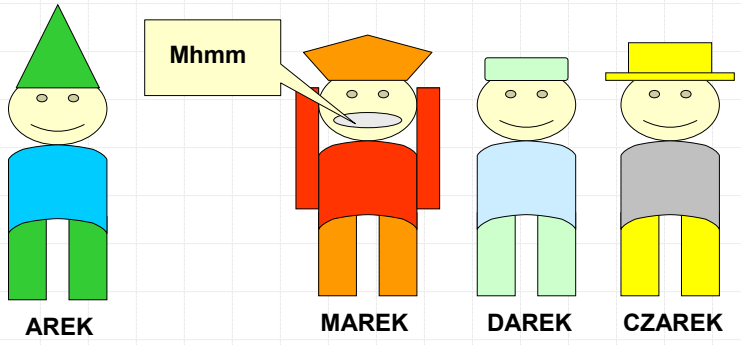
W kanale radiowym wszystkie stacje znajdujące się w zasięgu mogą słyszeć się nawzajem.

CSMA/CA cz. 2/8



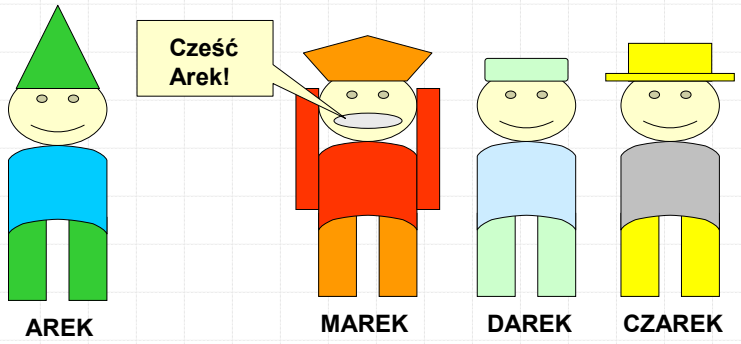
Arek sprawdza, czy nikt nie mówi, zatyka uszy (dlaczego?) i wita się z Markiem.

CSMA/CA cz. 3/8



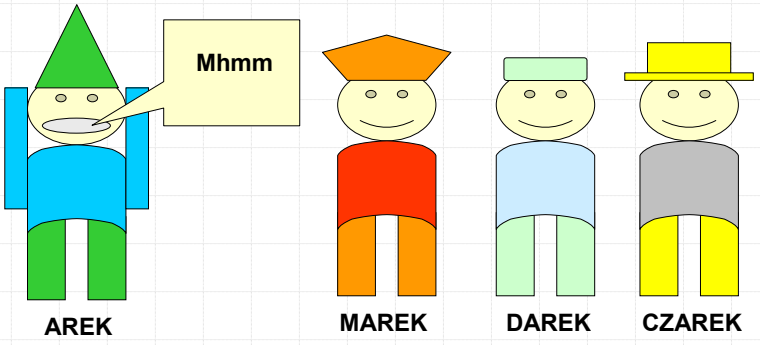
Marek sprawdza, czy nikt nie mówi, zatyka uszy i potwierdza, że usłyszał Arka.

CSMA/CA cz. 4/8



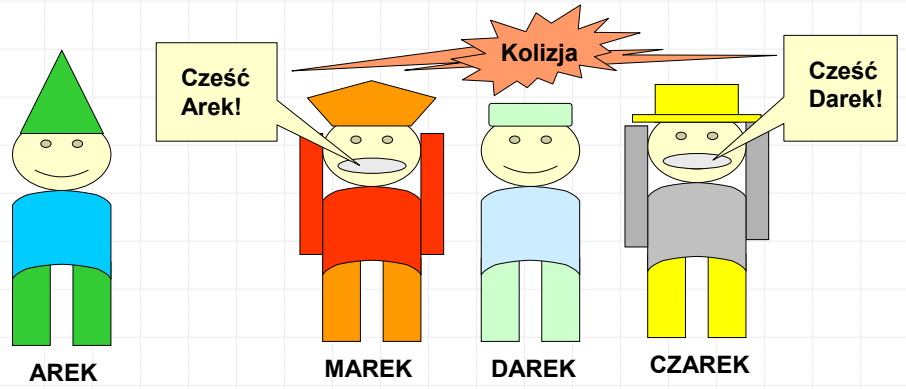
Sytuacja 1: Marek sprawdza, czy nikt nie mówi, zatyka uszy i kontynuuje rozmowę z Arkiem.

CSMA/CA cz. 5/8



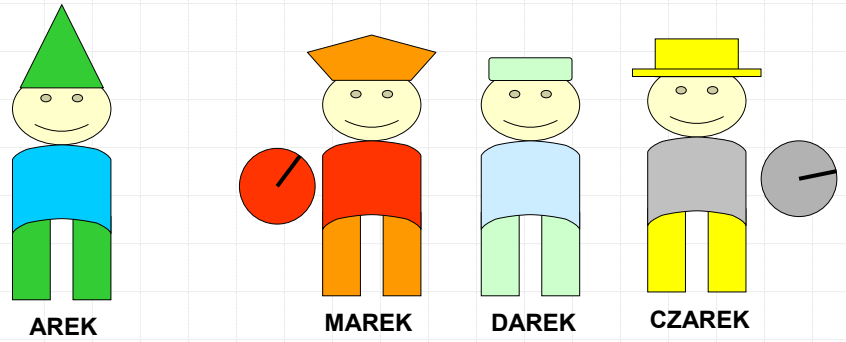
Sytuacja 1: Arek sprawdza, czy nikt nie mówi, zatyka uszy i potwierdza, że usłyszał Marka.

CSMA/CA cz. 6/8



Sytuacja 2: Marek sprawdza, czy nikt nie mówi, zatyka uszy i kontynuuje rozmowę z Arkiem. W tym samym momencie co Marek Czarek sprawdził, że nikt nie mówi, zatkał uszy i wita się z Darkiem. Następuje kolizja.

CSMA/CA cz. 7/8



Sytuacja 2: Nikt nic nie potwierdza. Panowie, którzy mówili coś, a nie dostali potwierdzenia, milczą przez chwilę.

CSMA/CA cz. 8/8

- Ponieważ każdy ma „swoją chwilę” – jest spora szansa, że następnym razem nie będzie kolizji
- Dodatkowo, aby polepszyć wykorzystanie pasma radiowego – Panowie przed powiedzeniem czegoś mogą zarezerwować sobie pasmo – np. Marek: „Arek, masz chwilę?” Arek odpowiada „Tak” – bądź milczy
- **W tej warstwie realizuje się usługi ochrony informacji – TGi: poufność i uwierzytelnienie**

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

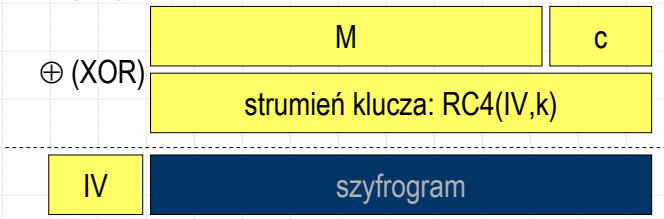
- **siła** w tajności klucza
- **samosynchronizacja** algorytmu ze względu na charakter warstwy łącza danych (“best effort” i duża bitowa stopa błędów w kanale radiowym ~10^{-5})
- **efektywność** w sprzęcie i oprogramowaniu
- **eksportowalność** algorytmu poza USA
- **opcjonalność** – implementacja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

Przeszukiwanie przestrzeni klucza

- autor: Tim Newsham
- **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)

Atak na słabe klucze RC4 (FMS)

- autorzy: Fluhrer, Mantin, Shamir (FMS)
- **najczęściej implementowany atak (m.in. 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”

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 nowe protokoły
  - TKIP – kosmetyczna poprawka dla obecnych urządzeń
  - CCMP – lepsze bezpieczeństwo w nowych urządzeniach
- Świadoma polityka zapewniająca zgodność wstecz
- Zarządzanie kluczami i uwierzytelnienie: 802.1X + 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

Algorytm Michael

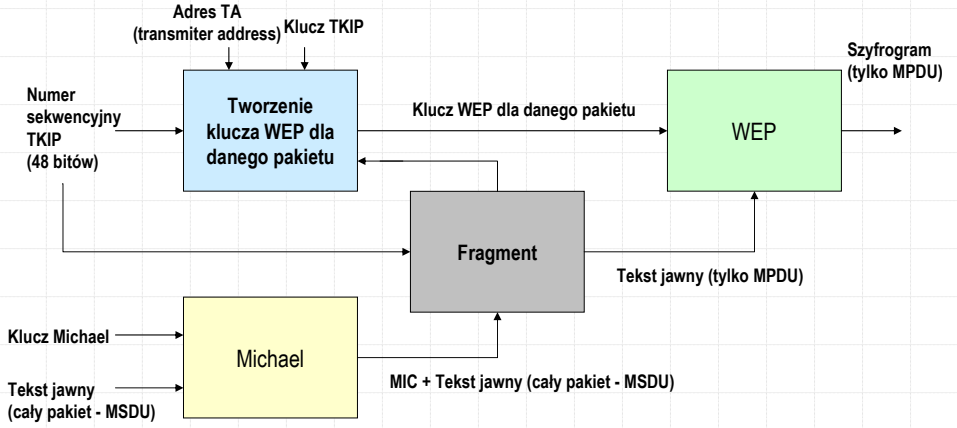
Algorytm 1: Przetwarzanie wiadomości
Wejście: Klucz (K_0, K_1) i wiadomość $M_0,...,M_N$
Wyjście: wartość MIC (V_0, V_1)
MICHAEL((K_0, K_1) , (M_0,...,M_N))
(L,R) ← (K_0, K_1)
for i=0 to N-1
L ← L ⊕ M_i
(L, R) ← ***b*(L, R)**
return (L,R)

Klucz: 64 bity (K0, K1 po 32 bity)
Wiadomość: 32 bitowe bloki

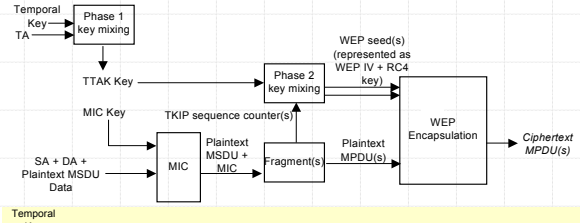
Algorytm 2: Michael – funkcja blokowa b()
Wejście: (L,R)
Wyjście: (L,R)
***b*(L, R)**
R ← R ⊕ (L <<< 17)
L ← (L + R) mod 2^{32}
R ←R ⊕ XSWAP(L)
L ← (L + R) mod 2^{32}
R ←R ⊕ (L <<< 3)
L ← (L + R) mod 2^{32}
R ←R ⊕ (L >>> 2)
L ← (L + R) mod 2^{32}
return (L,R)

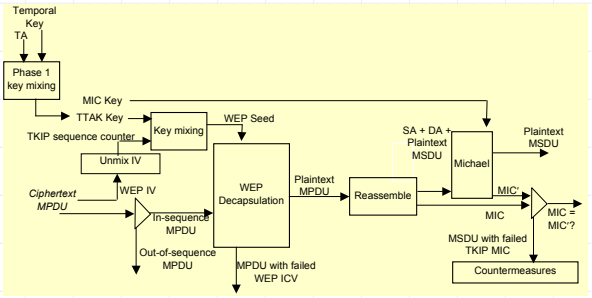
<<< obrót w lewo
>>> obrót w prawo
XSWAP – zamiana pozycji dwóch najmłodszych bajtów z dwoma najstarszymi

Przetwarzanie danych w TKIP
(uproszczona enkapsulacja)

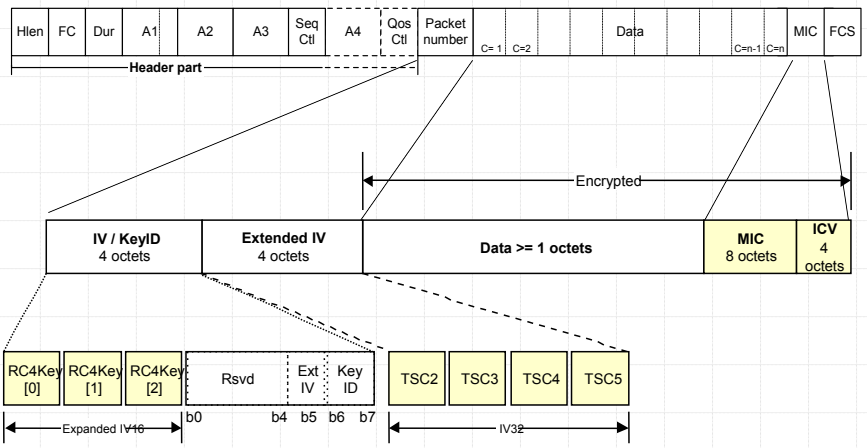


TKIP - szczegóły



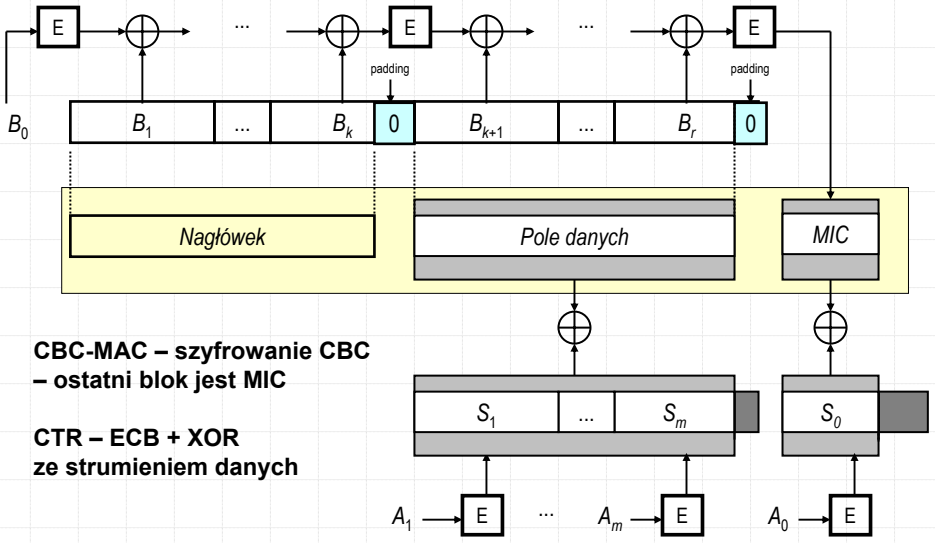


Format ramki zabezpieczonej TKIP



CCMP - cechy

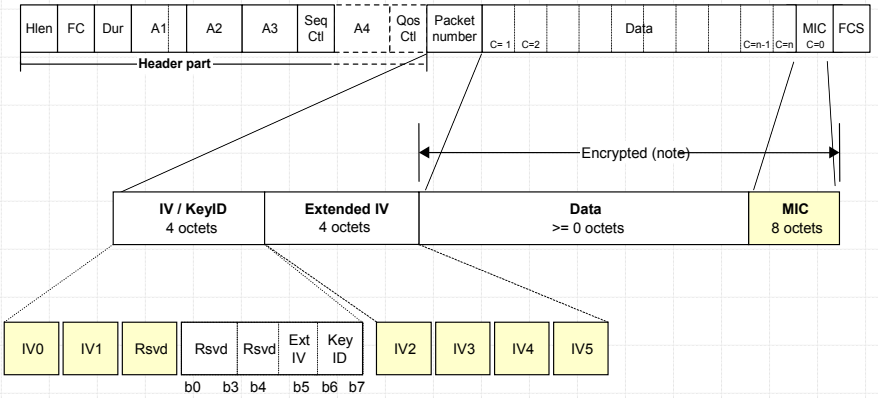
- Opcjonalne rozwiązanie długo-terminowe
- CCMP = **C**ounter-Mode-**C**BC-**M**AC **P**rotocol
- Bazuje na AES (Advanced Encryption Standard) w trybie pracy CCM
- AES wymaga wydajnego sprzętu zatem:
  - pojawią się nowe AP
  - pojawią się nowe urządzenia klienckie klasy hand-held
  - ale pozostaną PC
- Niewielki związek z WEP



CBC-MAC – szyfrowanie CBC – ostatni blok jest MIC

CTR – ECB + XOR ze strumieniem danych

Format ramki zabezpieczonej CCMP



802.1X/EAP

- Użycie zmodyfikowanego na potrzeby IEEE 802.11 szkieletu zarządzania kluczami 802.1X
- Nowy model:
  - **Pairwise Master Key (PMK)**
  - AP i stacja używają PMK aby ustanowić **Pairwise Transient Key (PTK)**
  - PTK jest używany do ochrony łącza
- Extensible Authentication Protocol (EAP)
  - Rodzina 50 prawie protokołów – część bardzo podobnych do siebie
  - EAPoL – EAP over LANs
  - Najistotniejsze z punktu widzenia WLAN:
    - EAP-TLS (Transport Layer Security)
    - EAP-TTLS (Tunneled TLS)
    - PEAP (Protected EAP)
    - EAP-FAST (Flexible Authentication via Secure Tunneling)
    - Cisco LEAP (Lightweight Extensible Authentication Protocol)

COMPUTERWORLD

Home | News | Browse Topics | Departments | Services | Subscribe | Events | Store | Jobs

Cisco warns its WLAN security can be cracked

The company has urged customers to implement strong password policies

News Story by Bob Evwin

Szczypiorski, Margasiński | Trendy w WLAN | 39

Poszczególne komponenty

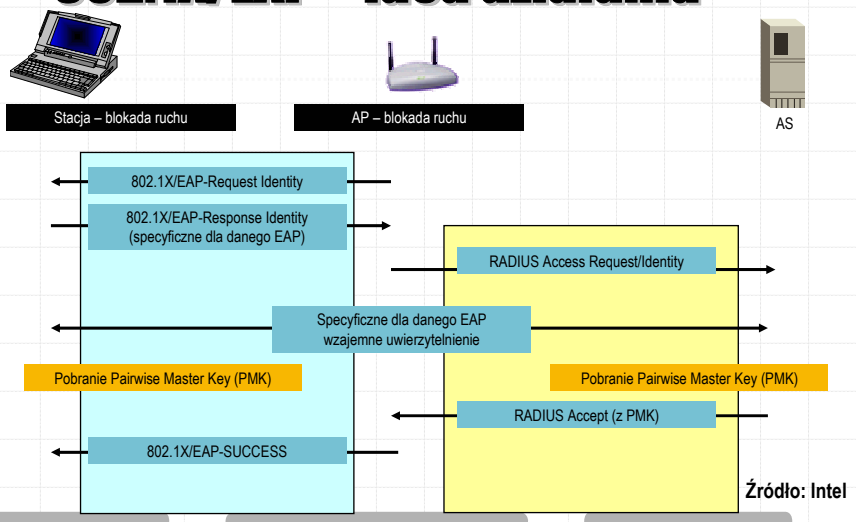
Stacja

AP

AS

EAP-TLS	
EAP	
802.1X (EAPoL)	RADIUS
802.11	UDP

802.1X/EAP – idea działania



Źródło: Intel

Wi-Fi Protected Access (WPA)

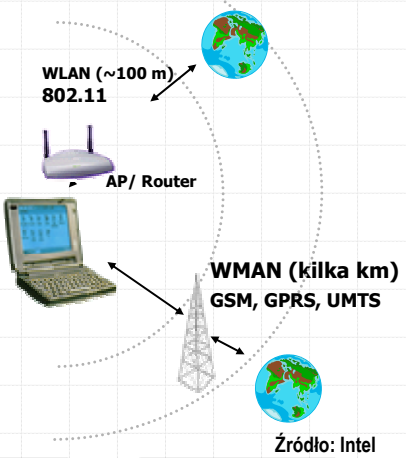
- **WPA:** 2003-2004
  - Od 2003 obowiązkowy przy certyfikacji Wi-Fi
  - Podzbiór standardu 802.11i
    - 802.1X/EAP, TKIP
- **WPA2:** 2004-???
  - 2004 (cezura: testy współpracy 802.11i) – opcjonalny
  - Od 2005 (???) - obowiązkowy
  - W pełni zgodny z 802.11i
    - WPA + (Fast) Roaming + CCMP

WLAN a ...

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

EAP-SIM - Extensible Authentication Protocol - Subscriber Identity Module

- **WLAN a UMTS**



Źródło: Intel

Wnioski

- Bezpieczeństwo WLAN wciąż nie jest stabilne
- Opóźnienie we wprowadzaniu IEEE 802.11i
- Przestroga: bezpieczeństwo korzystania z hot spotów = bezpieczeństwo korzystania z kawiarenek internetowych
- Bezpieczeństwo WLAN w sieciach korporacyjnych = wybór „bezpiecznego” dostawcy (?), odpowiednie traktowanie ruchu bezprzewodowego
- Technika IEEE 802.11 nie powinna być stosowana w podsieciach instytucji/firm, w których są przetwarzane „czułe” informacje

Pytania?