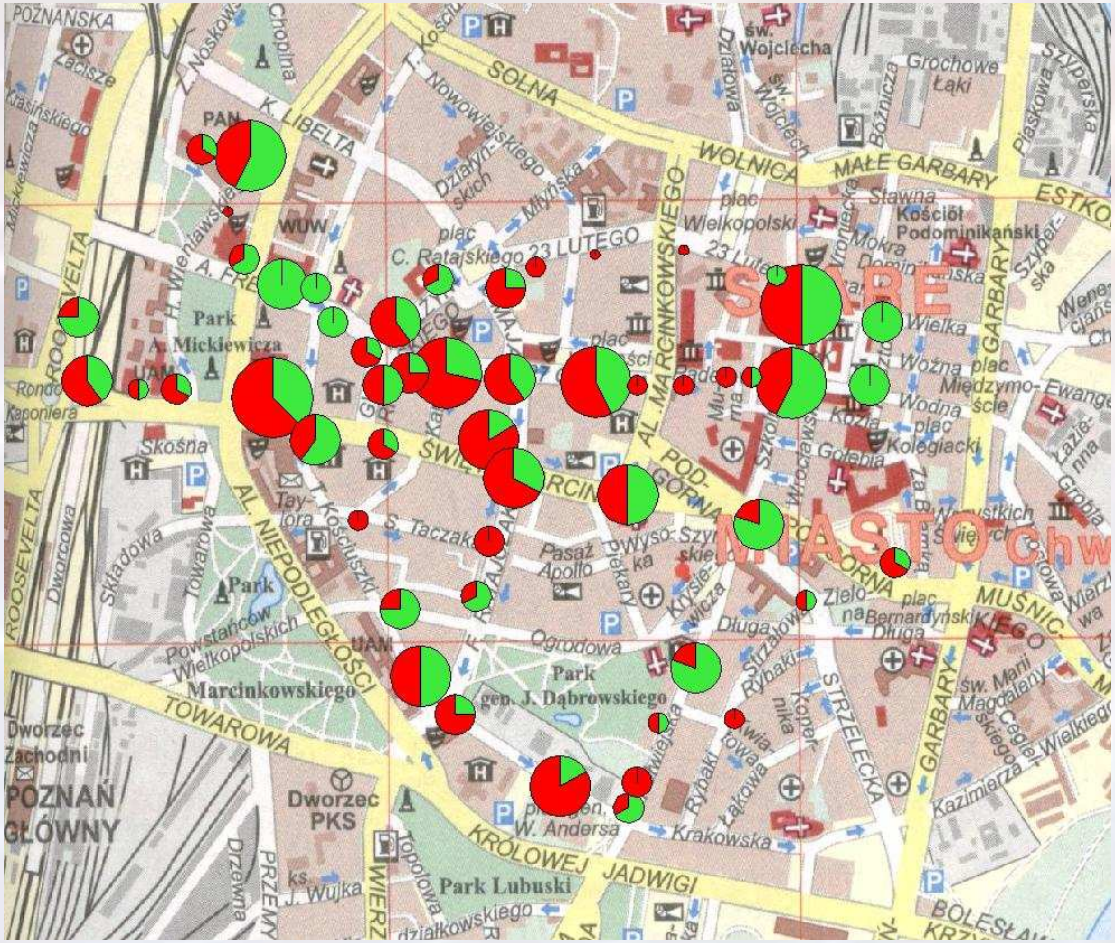
Bezpieczeństwo sieci bezprzewodowych w standardzie 802.11

Szkolenie działu KDM PCSS,
Poznań, 25.04.2006 r.

Jarosław Sajko, Zespół Bezpieczeństwa PCSS

Bezprzewodowy Poznań



Sieci bez zabezpieczeń

Sieci zabezpieczone WEP lub WPA

Data zebrania danych: Marzec 2005

Bezprzewodowy Świat

	2001	2002	2003	2004
Ilość AP	9374	24958	88122	228537
Sieci zaszyfrowane (WEP,WPA…)	2825	6970	28427	87647
Sieci otwarte	6549	17988	25695	140890
Domyślny SSID	2768	8802	24525	71805
Domyślny SSID, brak szyfrowania	2497	7847	21822	62859

Opracowane na podstawie http://www.worldwidewardrive.org/

Plan prezentacji

- Bardzo krótkie wprowadzenie do sieci 802.11
- Dlaczego WEP jest podatny na ataki
- Podstawowy problem dotyczący bezpieczeństwa w sieciach 802.11
- Standard 802.11i
- Bezpieczeństwo fizyczne sieci bezprzewodowych
- Dodatkowe zabezpieczenia
- Sieci bezprzewodowe w polityce bezpieczeństwa informacji

Wprowadzenie (1)

- Standard 802.11
  - 802.11a, 802.11b, 802.11g – warstwa fizyczna oraz MAC
  - 802.11i – bezpieczeństwo
- Sieci 802.11 mają strukturę komórkową
  - IBSS – sieć bez punktu dostępowego
  - BSS – sieć z punktem dostępowym
  - ESS – sieć z wieloma punktami dostępowymi, z roamingiem

Wprowadzenie (2)

Proces dołączenia stacji do komórki (BSS)

Skanowanie

Beacon frame

Skanowanie pasywne

Wprowadzenie (3)

Proces dołączenia stacji do komórki (BSS)

Skanowanie

Beacon frame

Skanowanie pasywne

Probe request

Probe response

Skanowanie aktywne

Wprowadzenie (4)

Proces dołączenia stacji do komórki (BSS)

Uwierzytelnianie

Wprowadzenie (5)

Proces dołączenia stacji do komórki (BSS)

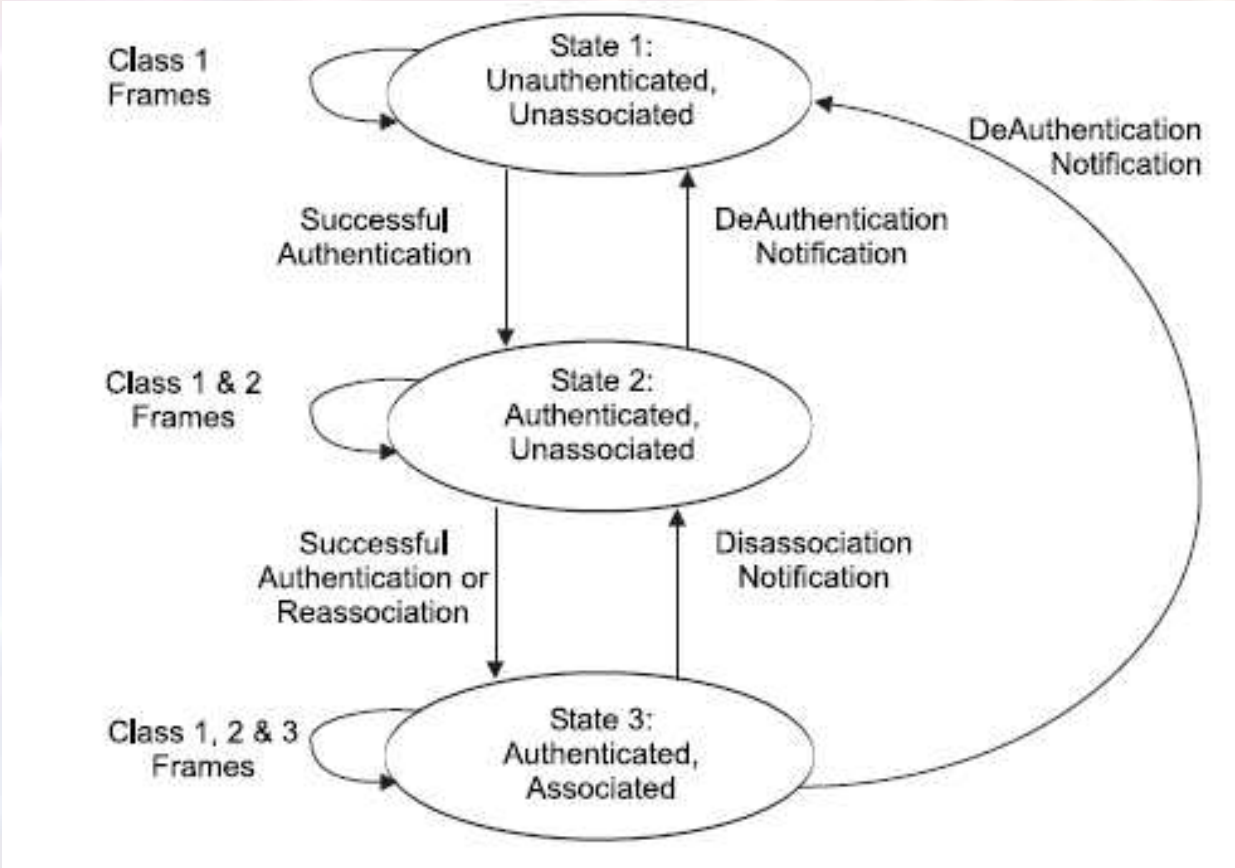
Dołączanie

Assoc Req.

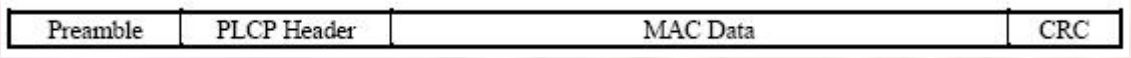
Assoc Res.

Wprowadzenie (6)

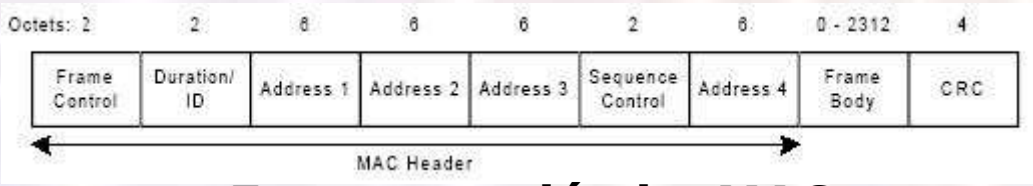
Relacje między poszczególnymi stanami



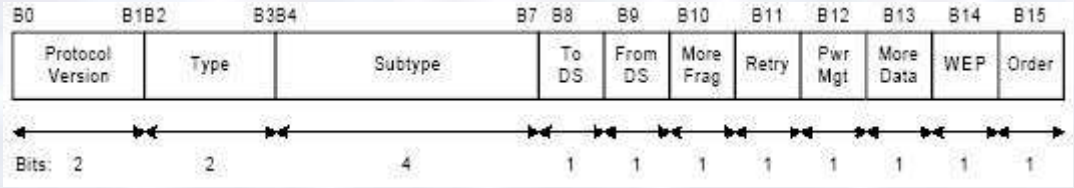
Wprowadzenie (7)



Ogólny format ramki



Format nagłówka MAC



Format pola kontroli ramki

Wprowadzenie (8)

- Ramki typu MGMT
  - assoc req., assoc resp., auth., deauth., beacon, disassoc., probe req., probe resp., reassoc req., reassoc resp., ATIM
- Ramki typu DATA
  - data, cf_ack, cf_poll, cf_ack+poll, null, ...
- Ramki typu CTRL
  - RTS, CTS, ACK, CF-End, ...

WEP (1)

Wired Equivalent Privacy (WEP)

- Samosynchronizujący
- Wydajny, można go zaimplementować łatwo w oparciu o hardware lub software
- Może być eksportowany, nie ma ograniczeń patentowych
- Jest opcjonalny i nie musi być używany podczas transmisji danych

WEP (2)

Transmisja danych z użyciem algorytmu WEP

zaszyfrowane dane

K = IV.SK

K = IV.SK

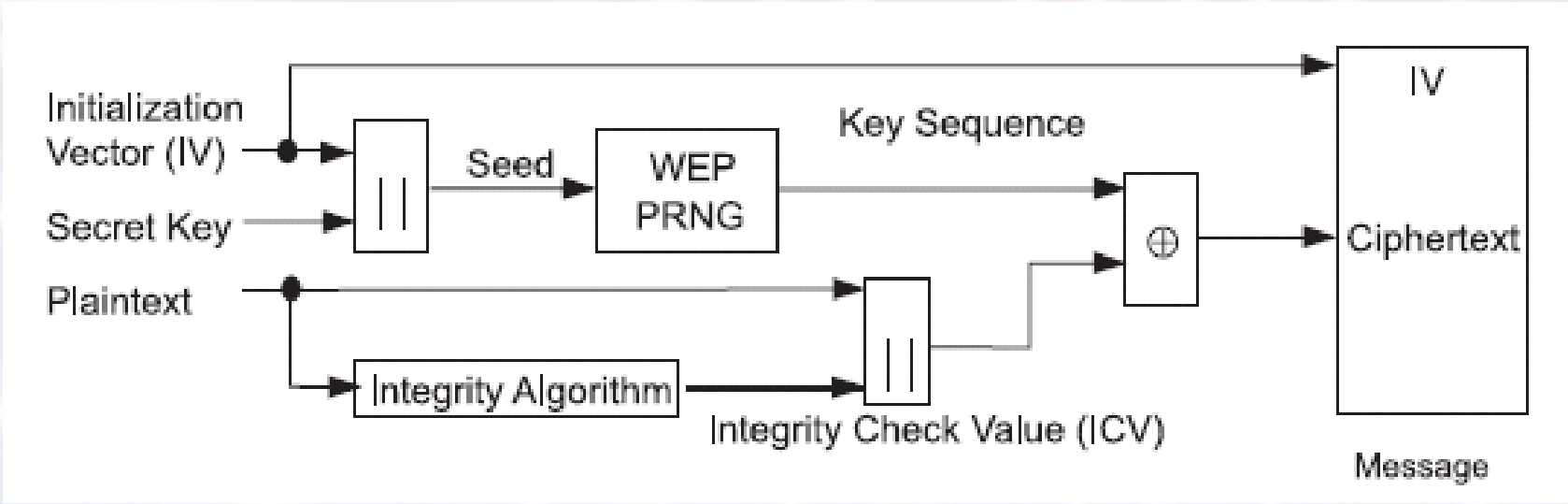
IV – wektor inicjalizujący

SK – tajny klucz

K – klucz szyfrujący

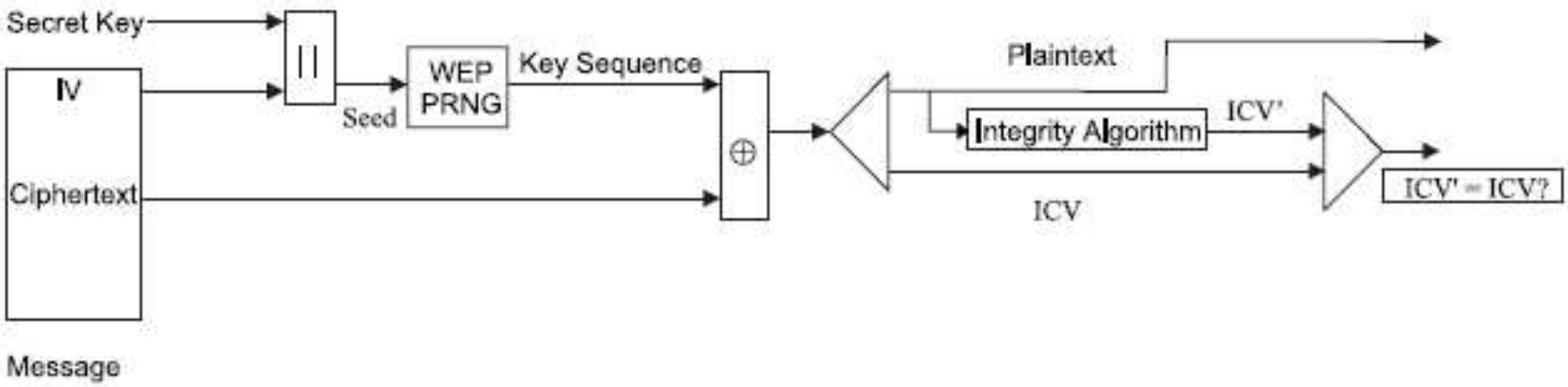
WEP (3)

Schemat szyfrowania pakietów



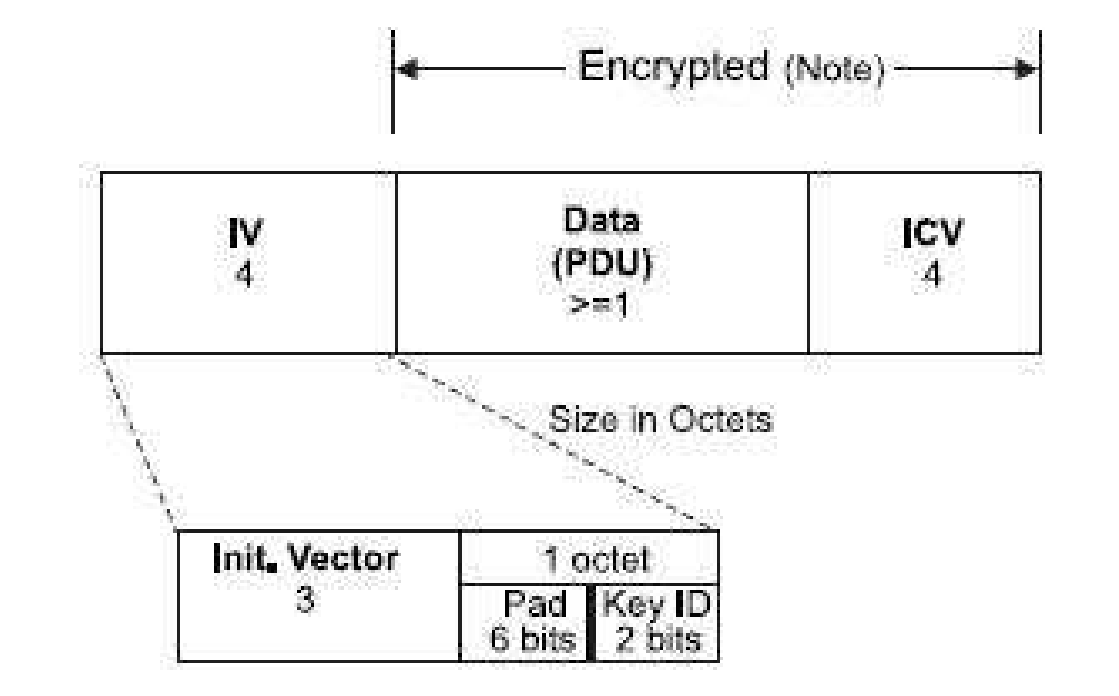
WEP (4)

Schemat deszyfrowania pakietów



WEP (5)

Format danych szyfrowanej ramki



WEP (6)

Algorytm RC4

KSA(K)
Initialization:
    For i = 0 .. N - 1
     S[i] = i
    j = 0
Scrambling:
    For i = 0 .. N - 1
     j = j + S[i] + K[i mod l]
     Swap(S[i], S[j])

PRGA(K)
Initialization:
    i = 0
    j = 0
Generation Loop:
    i = i + 1
    j = j + S[i]
    Swap(S[i], S[j])
    Output z = S[S[i] + S[j]]

WEP (7)

Algorytm WEP możemy zapisać w następującej postaci:

$$P=M||CRC(M)$$

$$C=P \text{ xor } PRNG(IV,KEY)$$

Z równania tego wynika, że:

$$PRNG(IV,KEY)=C \text{ xor } P$$

$$PRNG(IV,KEY) = C \text{ xor } (M \,||\, CRC(M))$$

WEP (8)

Nagłówek komunikatu ma następująca postać:

```
Logical-Link Control:
    DSAP: SNAP (0xaa)
    IG Bit: Individual
    SSAP: SNAP (0xaa)
    CR Bit: Command
    Control field: U, func = UI (0x03)
        000. 00.. = Unnumbered Information
        .... ..11 = Unnumbered frame
    Organization Code: Encapsulated Ethernet (0x000000)
    Type: IP (0x0800)
```

heksadecymalnie:

0xaaaa030000000800

WEP (9)

Oznacza to, że dla wychwyconej zaszyfrowanej ramki WEP, możemy wyznaczyć 8 pierwszych bajtów strumienia PRNG.

```
PRNG(IV,KEY)[0-7]=C[0-7] xor 0xaaaa03000000800
```

Może to posłużyć do:

- ataku *frame injection*
- ataku FMS na KSA algorytmu RC4

WEP (10)

Atak *frame injection*

Korzystając z 8 bajtów odgadniętego klucza PRNG możemy wygenerować dowolny zaszyfrowany pakiet. Aby móc wysyłać pakiety dłuższe niż 8 bajtów korzystamy z fragmentacji jaką oferuje standard 802.11.

```
(8 bajtów x 16 fragmentów ) – 4 bajty ICV  - 8
bajtów nagłówek LLC – 20 bajtów nagłówek IP –
20 bajtów nagłówek TCP =  12 bajtów
```

W każdym wysyłanym pakiecie możemy wysłać 12 bajtów danych. Aby wysłać większą ilość danych możemy skorzystać z fragmentacji IP.

WEP (11)

Atak FMS w dużym skrócie

warunki:

$$S_I[1] + S_I[S_I[1]] = I + B.$$

$$S_I[1] < I$$

Słowo B klucza wtedy można oszacować z 5% prawdopodobieństwem na podstawie następującego wzoru:

$$K[B] = S^{-1}_{I+B-1}[Out] - j_{I+B-1} - S_{I+B-1}[I+B]$$

WEP (12)

Atak FMS w dużym skrócie cd.

- wystarczy zebrać 60 „słabych” wektorów inicjalizujących żeby z prawd. > 0.5 oszacować dany bajt klucza
- przestrzeń „słabych” wektorów jest duża, ale nie wszystkie trzeba obliczać, można zastosować wzór [B + 3, N - 1, X]
- długość klucza ma tutaj niewielkie znaczenie

WEP (13)

Podsumowanie:

Algorytm WEP może być traktowany jedynie w kategoriach czynnika redukującego prawdopodobieństwo wykorzystania naszej sieci bezprzewodowej w nieautoryzowany sposób jeżeli w pobliżu są inne sieci, które tego algorytmu nie stosują. Nie może być traktowany jako zabezpieczenie przed utratą integralności czy też poufności przesyłanych w tej sieci danych.

Podstawowy problem (1)

Authentication attack

Każda stacja bazowa z oczywistych względów ma ograniczenie liczby klientów, których może przyłączyć. Wysyłając ramki *authenticate z* losowym adresem źródłowym możemy zapełnić pamięć stacji bazowej przeznaczoną na przechowywanie informacji o uwierzytelnionych klientach.

Podstawowy problem (2)

Deauthentication attack

Aby odłączyć klienta stacja bazowa wysyła komunikat *deauthenticate*, klient wtedy próbuje ponownie nawiązać sesję ze stacją bazową. Taki komunikat może wysłać dowolny klient „w imieniu” stacji bazowej do pojedynczego lub wszystkich klientów podłączonych do danej stacji bazowej.

Podstawowy problem (3)

Association attack

Atak analogiczny do ataku *authentication attack*, tyle że trzeba się najpierw uwierzytelnić.

Podstawowy problem (4)

Disassociation attack

Atak analogiczny do *deauthentication attack*.

Podstawowy problem (5)

RTS attack

Atak ten polega na nieustannym rezerwowaniu pasma za pomocą pakietów *Request-To-Send*, które można wysyłać niezależnie od tego czy stacja jest uwierzytelniona i podłączona czy też nie.

Podstawowy problem (6)

Beacon attack

Jeżeli stacja kliencka nie ma zdefiniowanego punktu dostępowego w swojej konfiguracji wystarczy jej nieustannie wysyłać komunikaty typu *beacon* z informacjami o nieistniejących punktach dostępowych. Skutecznie zajmie to stację kliencką na tyle, żeby korzystanie z istniejącej sieci stało się niemożliwe.

Podstawowy problem (7)

DIFS attack

Czas DIFS to czas jaki powinien upłynąć pomiędzy końcem transmisji jednej ramki a początkiem transmisji następnej. Zadaniem przerwy między nadawaniem jednej a drugiej ramki jest umożliwienie współdzielenia medium przez wiele węzłów. Modyfikując firmware i skracając czas DIFS możemy skutecznie zmonopolizować pasmo.

Podstawowy problem (8)

Podstawowy problem sieci bezprzewodowych w standardzie 802.11 polega na tym, że nie ma możliwości stwierdzenia wiarygodności odebranego komunikatu typu MGMT co w połączeniu z wolno dostępnym „eterem” sprawia, że sieci te są całkowicie nieodporne na ataki na dostępność.

Warchalking

open node

closed node

WEP node

Standard 802.11i (1)

Cele przyświecające powstawaniu standardu 802.11i:

- otwarty proces ustanawiania
- technologia dostępna dla wszystkich, brak ograniczeń patentowych na stosowane algorytmy
- elastyczna, adaptowalna architektura, nadająca się zarówno dla małych jak i dużych wdrożeń
- zewnętrzne recenzje, aby zminimalizować szanse na kolejny WEP

Standard 802.11i (2)

klient

ap

Serwer AAA

Negocjacja funkcjonalności

Negocjacja parametrów bezp.

Autoryzacja i uwierzytelnianie

Zarządzanie kluczami

Dystrybucja kluczy sesyjnych

Szyfrowanie z użyciem TKIP lub CCMP

TKIP (1)

TKIP założenia

- Możliwość wykorzystania punktów dostępowych pierwszej generacji (4MIPS)
- Możliwość wdrożenia poprzez instalacje nowego oprogramowania
- Naprawić słabości WEP czyli po prostu go zastąpić
- Rozwiązanie tymczasowe

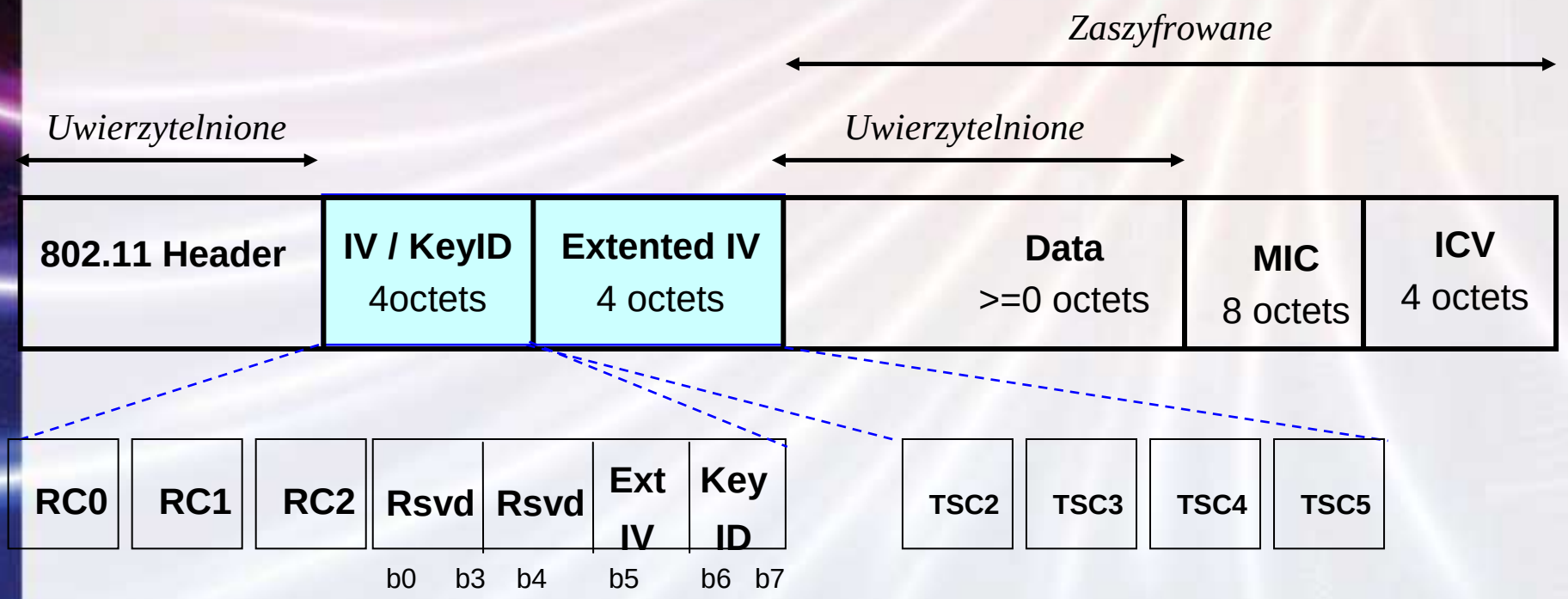
TKIP (2)

TKIP właściwości

- Nowy algorytm zapewniania integralności komunikatów, Michael
- Mechanizm chroniący przed atakami wykorzystującymi powtórzenia nadawanych ramek
- Wykorzystuje ten sam *hardware* co algorytm WEP
- Wprowadza mechanizmy informowania o tym, że sieć jest atakowana (w przeciwieństwie do WEP)

TKIP (3)

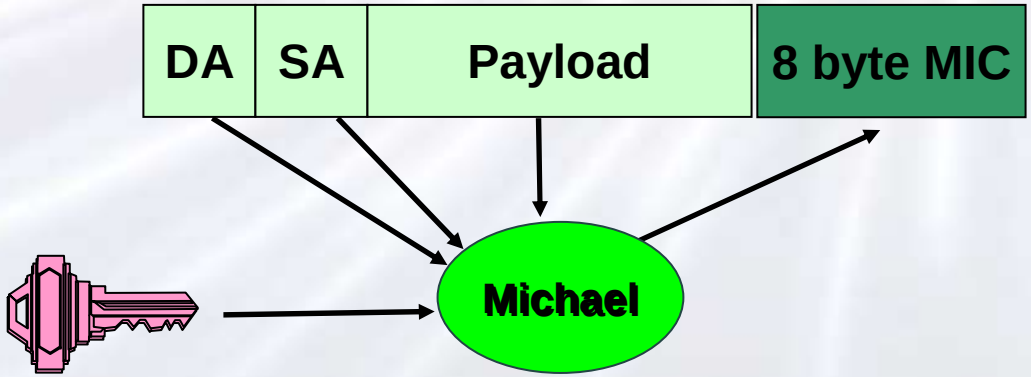
Ramka MPDU TKIP



TKIP (4)

TKIP – Michael

- ochrona integralności komunikatów
- wykorzystuje dwa klucze 64bit, po jednym na kierunek transmisji



TKIP (5)

TKIP – ochrona przed powtórzeniami

- po każdej operacji zmiany klucza licznik jest zerowany
- licznik jest zwiększany o 1 po każdym wysłanym komunikacie
- każdy pakiet, który jest poza sekwencją jest odrzucany
- podczas fragmentacji każdy pakiet poza sekwencją powoduje włączenie ochrony przed atakiem

TKIP (6)

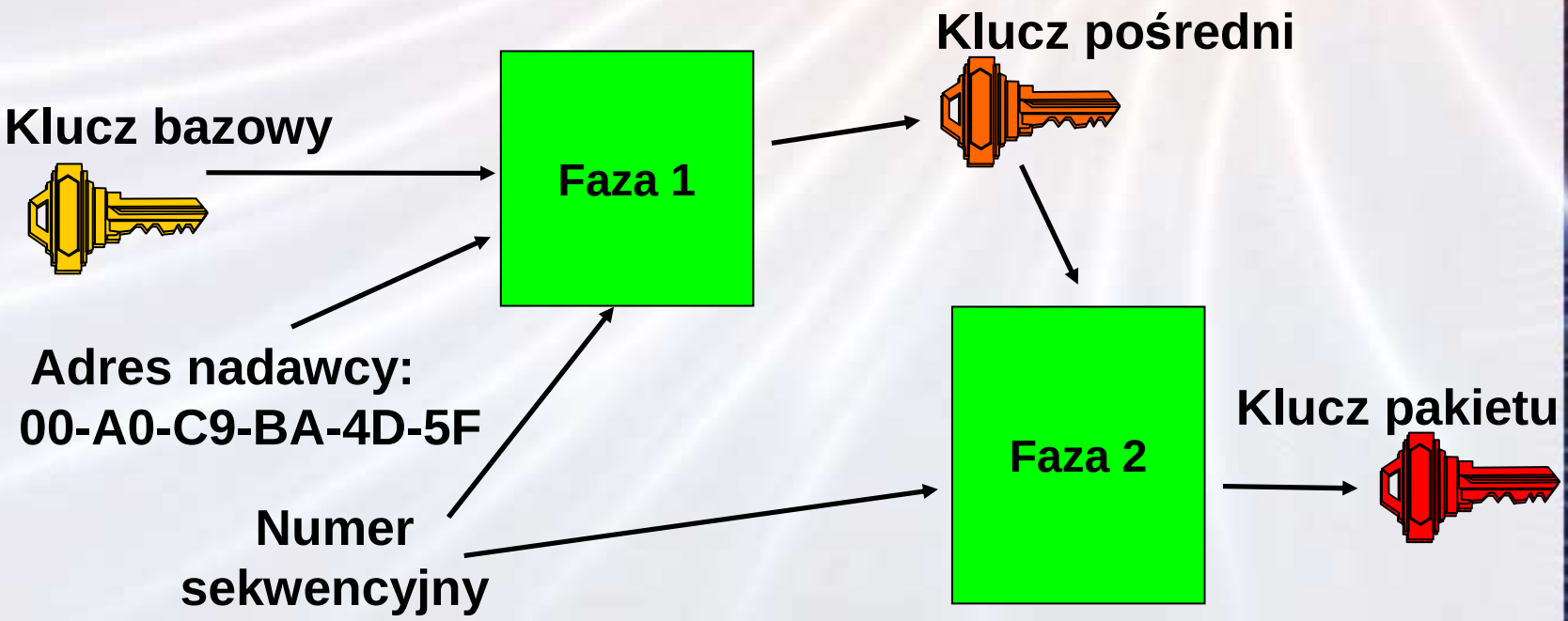
TKIP – ochrona przed atakami

- Sprawdzanie CRC przed MIC minimalizuje fałszywe alarmy
- W przypadku wykrycia ataku:
  - zaprzestaje wykorzystywania kluczy sesyjnych
  - zmniejsza tempo generowania kluczy do 1 na minutę

TKIP (7)

TKIP – mieszanie kluczy

• Zapobiega atakom korelującym IV z pakietem oraz atakom na słabe klucze



TKIP (8)

TKIP – podsumowanie

- Dzięki algorytmowi Michael skuteczne ataki na integralność zostały zamienione na skuteczne ataki DoS
- Mechanizm powtórzeń wykrywa i odrzuca takie komunikaty
- Mechanizm mieszania kluczy eliminuje korelacje pomiędzy kluczem a wektorem inicjalizującym

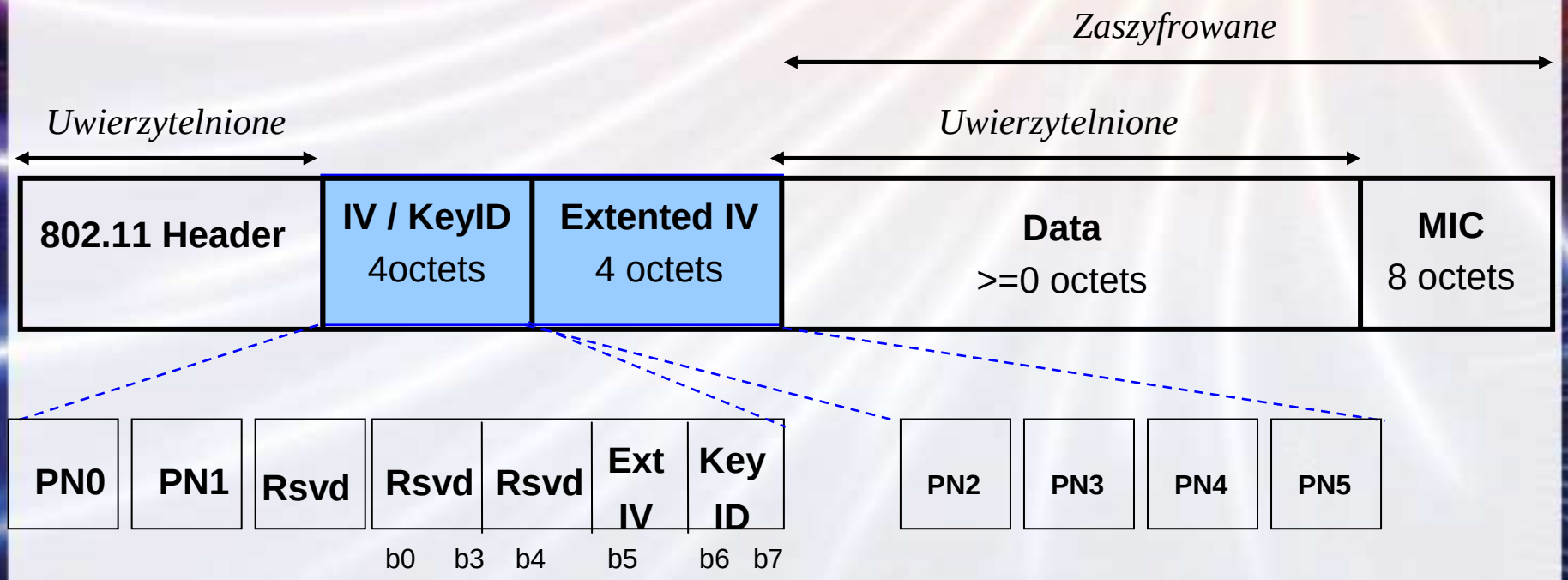
AES-CCMP (1)

AES-CCMP

- Kosztowny obliczeniowo, a więc wymagający nowego sprzętu
- Rozwiązuje problemy związane z bezpieczeństwem WEP
- Rozwiązanie długoterminowe:
  - Kompatybilny z wszystkimi obecnymi i planowanymi standardami 802.11
  - Oparty o sprawdzone rozwiązania kryptograficzne
  - Elastyczny – możliwe stosowanie różnych algorytmów szyfrowania

AES-CCMP (2)

Format ramki MPDU AES-CCMP



AES-CCMP (3)

AES-CCMP Podsumowanie

- Otrzymał pozytywne komentarze oraz zewnętrzne recenzje, wydane m. in. przez: Ron Rivest, David Wagner, Phil Rogaway
- Algorytm AES może zostać zastąpiony poprzez dowolny inny algorytm szyfrujący 128bit
- Realizuje wszystkie cele postawione przed 802.11i
- Kompatybilny w przód z: 802.11e, 802.11k, 802.11n, 802.11r, 802.11s, 802.11t, 802.11v oraz 802.11w

Ochrona danych w 802.11i (1)

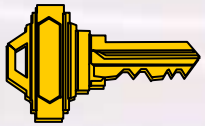
	WEP	TKIP	AES-CCMP
Szyfr	RC4	RC4	AES
Rozmiar klucza	40 lub 104 bity	128bit szyfrowanie, 64bit integralność	128bit
Czas życia klucza	24bit IV, „zawijany”	48bit IV	-
Klucz dla pakietu	Konkatenacja z IV	Funkcja mieszająca	-
Integralność danych	CRC32	Michael	CCM
Integralność nagłówka	brak	Michael	CCM
Powtórzenia	brak	Wykorzystuje IV	Wykorzystuje IV
Zarządzanie kluczami	brak	802.11i 4-Way Handshake	802.11i 4-Way Handshake

Ochrona danych w 802.11i (2)

Nie wszystkie problemy związane z ochroną danych zostały rozwiązane w standardzie 802.11i:

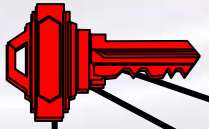
- Komunikaty grupowe zabezpieczane są wspólnym kluczem, a więc poufność ograniczona jest do grupy
- Brak zabezpieczenia dla ramek typu *Management*
- Brak zabezpieczeń w warstwie PHY

Hierarchia kluczy w 802.11i (1)



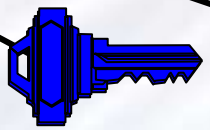
Pirewise Master Key

PTK = 802.11i-PRF(PMK, min(AP Nonce, STA Nonce) || max(AP nonce, STA Nonce) || min(AP MAC, STA MAC) || max(AP MAC, STA MAC))

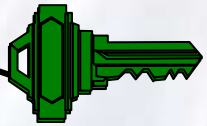


Pirewise Transient Key

Key Confirmation Key (KCK) – PTK bits 0–127



Key Encryption Key (KEK) – PTK bits 128–255



Temporal Key – PTK bits 256–*n*

4-Way Handshake (1)

ANonce

Utwórz PTK

Snonce, MIC

Utwórz PTK

GTK, MIC

MIC

4-Way Handshake i AAA (1)

1. Po podłączeniu stacji klienckiej do punktu dostępowego automat stanowy 802.11i wywołuje funkcje uwierzytelniania (domyślnie 802.1x)
2. 802.11i zakłada, że w tym czasie blokowany jest pozostały ruch dla tej stacji
3. W przypadku procedury uwierzytelniającej zakończonej powodzeniem obie strony połączenia stają się posiadaczami PMK
4. 802.11i wykonuje 4-Way Handshake

4-Way Handshake i AAA (2)

5. Po zakończeniu procedury 4-Way Handshake 802.11i sygnalizuje do funkcji uwierzytelniania zakończenie procedury
6. 802.11i zakłada, że funkcja uwierzytelniania odblokowuje pozostały ruch od danej stacji klienckiej

802.11i i 802.1x (1)

Standard 802.1x nie jest częścią standardu 802.11i, został on wykorzystany w 802.11i jako szkielet autoryzacji i uwierzytelniania. 802.1x jest niezależnym standardem i rozwija się niezależnie. Wykorzystywany jest nie tylko w sieciach WLAN. W 802.11i przyjmuje się że:

- 802.1x dostarcza w odpowiedni sposób klucze sesyjne
- 802.1x potrafi dostarczyć mechanizmów uwierzytelniających strony połączenia

Koncepcje 802.1x (1)

- Supplicant – w przypadku 802.11i stacja kliencka
- Authenticator – w przypadku 802.11i punkt dostępowy
- Authentication Server – logiczny element architektury, centralny węzeł uwierzytelniania
- Controlled Port – umożliwia blokowanie/przepuszczanie „normalnego” ruchu
- Uncontrolled Port – tylko dla ruchu 802.1x

Architektura 802.1x (1)

Supplicant

Authenticator

Authentication Server

Metoda EAP (np. EAP-TLS)	
EAP	
802.1X (EAPOL)	Transport EAP do serwera

EAPOL – EAP transport Over LAN

Schemat komunikacji w 802.1x

Supplicant

Authenticator

Authentication Server

EAP-Request Identity

EAP-Response Identity

EAP-Response Identity

Wzajemne uwierzytelnienie

EAP-Success, PMK

EAP-Success, PMK

802.1x

Transport EAP do serwera

Kontrola portów w 802.1x

Przed uwierzytelnieniem

Ruch 802.1x → **Unontrolled Port**

Ruch pozostały → **Controlled Port**

Po uwierzytelnieniu

Ruch 802.1x → **Unontrolled Port**

Ruch pozostały → **Controlled Port**

802.1x - Podsumowanie

- Poprzez wykorzystanie 802.1x oraz RADIUS IEEE deleguje definicje uwierzytelniania do grupy IETF
- 802.1x nie jest idealnym rozwiązaniem, ale sposób w jaki został użyty przez 802.11i uznawany jest za bezpieczny
- 802.1x spełnia oczekiwania wydajności i skalowalności nawet dla dużych wdrożeń

802.11i PSK (1)

- Małe wdrożenia rzadko kiedy umożliwiają zastosowanie dedykowanego serwera uwierzytelniania
- Odpowiedzią na ten problem jest tryb Pre-Shared Key standardu 802.11i
  - PSK jest konfigurowany na stacji klienckiej jaki i na punkcie dostępowym
  - PSK jest wykorzystywany podczas 4-Way Handshake
- Decyzja o nadaniu dostępu stacji podejmowana jest podczas wdrożenia a nie dynamicznie

802.11i PSK (2)

- Metoda Pre-Shared Key jest tak silna jak wykorzystany w niej *passphrase*
- Aby zabezpieczyć się przed atakiem siłowym uznaje się, że potrzebny jest *passphrase* o długości min. 14 znaków, a najlepiej 22
- W praktyce dużo skutecznych ataków na te sieci przeprowadza się metodą słownikową
- Jeżeli używamy PSK to klucz ten powinien być odpowiednio często zmieniany

WPA

WPA jest stworzonym przez grupę Wi-Fi Alliance standardem rynkowym częściowego wdrożenia 802.11i, tj. wykorzystuje on algorytm TKIP wraz z uwierzytelnianiem Michael. Pozwala na uwierzytelnianie stacji klienckich z użyciem PSK (WPA-Personal) lub z wykorzystaniem 802.1x (WPA-Enterprise). Wprowadzony w 2003 roku.

WPA2

WPA2 to wprowadzony również przez *Wi-Fi Alliance* standard rynkowy, który implementuje obowiązkowe w 802.11i elementy bezpieczeństwa.

- CCMP jako mechanizm zapewniania integralności komunikatów
- AES zamiast RC4
- Niestety standard ten ma kiepskie wsparcie ze strony oprogramowania systemów klienckich

802.11r

- Doświadczenia z wdrożeń pokazują, że zmiana stacji bazowej przez klienta przy włączonym wsparciu dla 802.11i zajmuje > 200msec
- Upowszechnianie się technologii VoIP powoduje, że jest ona wykorzystywana również w sieciach Wi-Fi, taki narzut jest nieakceptowalny
- Standard 802.11r ma za zadanie uporać się z problemami wydajnościowymi związanymi ze zmianą punktów dostępowych

802.11s

Jeżeli chcemy zbudować gęsto połączoną sieć bezprzewodową musimy zmierzyć się z następującymi problemami:

- Jak identyfikować węzły uprawnione do wykonywania routingu?
- Jak ustanowić bezpieczne połączenie między routerami?
- Jak w bezpieczny sposób realizować routing dynamiczny?

Standard 802.11s ma rozwiązywać te problemy.

802.11w

- 802.11i zabezpiecza ramki przesyłające dane
- W sieciach opartych o 802.11 jest bardzo dużo innych ramek typu, które również potrzebują zabezpieczenia, głównie przed ich podrabianiem:
  - 802.11e – QoS
  - 802.11k – pomiary i kontrola warstwy radiowej
  - Ramki disassociation, deauthenticate

Zadanie dla 802.11w

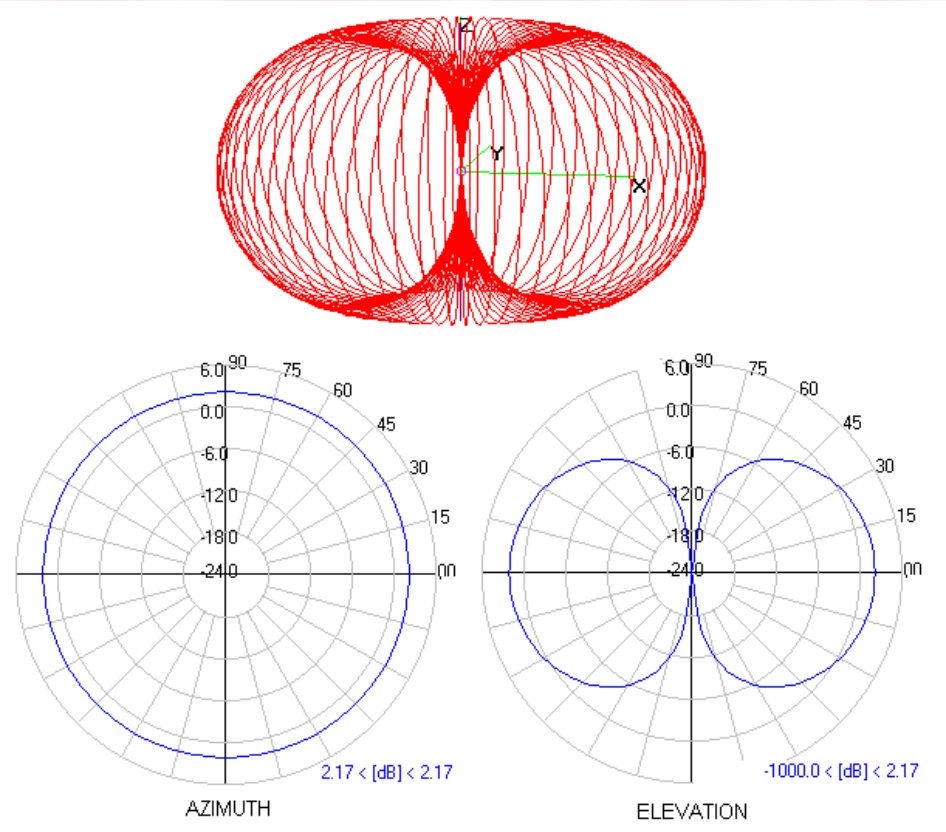
Bezpieczeństwo fizyczne (1)

Promieniowanie anten jest czynnikiem negatywnie wpływającym na bezpieczeństwo sieci bezprzewodowych

grafika: http://hotwireless.co.uk

Bezpieczeństwo fizyczne (2)

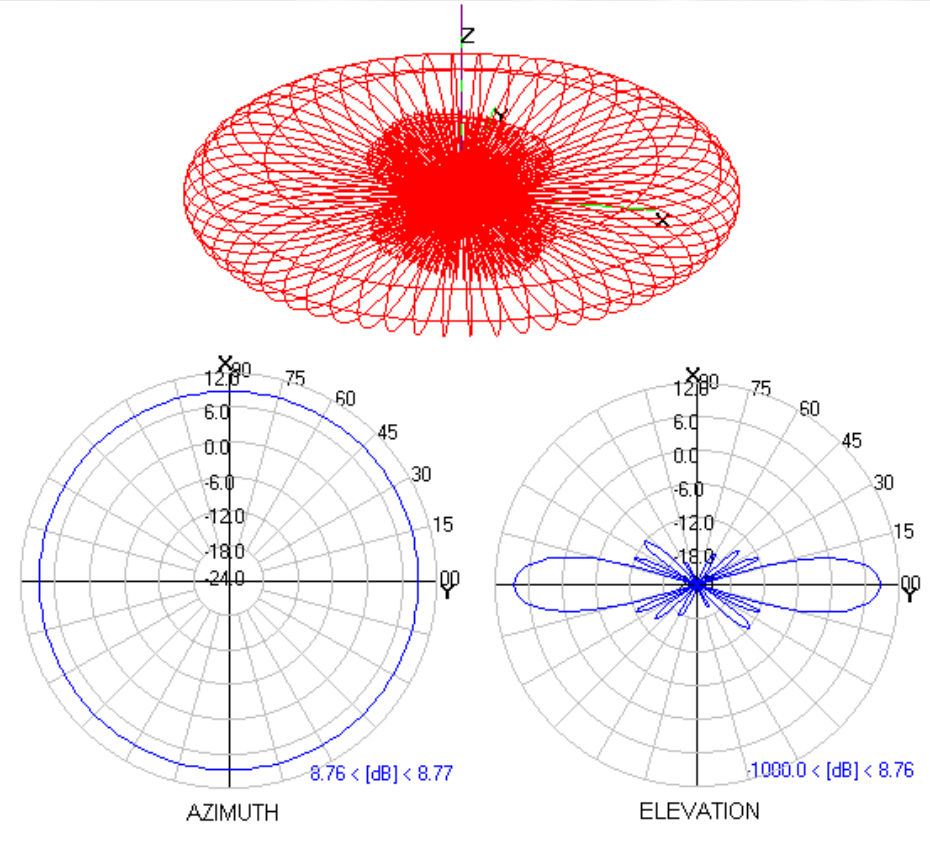
Standardowa antena dipolowa



grafika: http://www.trevormarshall.com

Bezpieczeństwo fizyczne (3)

Zmodyfikowana antena dipolowa



grafika: http://www.trevormarshall.com

Bezpieczeństwo fizyczne (4)

- Polaryzacja
- Współczynnik fali stojącej
- Okablowanie i złącza
- Dobór anteny

grafika:http://www.brain-pro.de/

Bezpieczeństwo fizyczne (5)

Farby oraz tapety ochronne skutecznie uniemożliwiają korzystanie z urządzeń bezprzewodowych w dosyć szerokim zakresie częstotliwości.

grafika: http://www.ritilan.com/

Inne zabezpieczenia (1)

- Wewnętrzne sieci VPN
- Rozwiązanie WAVESEC (http://www.wavesec.org/)
- tinyPEAP
- MAC-Address ACL – to tylko w formie średniej jakości rozrywki dla intruza

Sieci WLAN w polityce bezp. (1)

Stopień ryzyka utraty atrybutów bezpieczeństwa informacji w zależności od stosowanych zabezpieczeń

	Brak zabezpieczeń	WEP	WPA-Personal	WPA-Enterprise lub WPA2 lub VPN
Poufność	**Wysoki**	**Wysoki**	**Średni**	**Niski**
Integralność	**Wysoki**	**Wysoki**	**Niski**	**Niski**
Dostępność	**Wysoki**	**Wysoki**	**Wysoki**	**Wysoki**

Sieci WLAN w polityce bezp. (2)

Ze względu na charakter sieci bezprzewodowych oraz ich obecny stan rozwoju proponujemy następujące podejście:

- Sieci z poziomem zabezpieczeń niższym niż WPA2 traktować jako sieci zewnętrzne lub tzw. sieci dla gości
- Sieci dla gości powinny mieć ponadto ograniczony dostęp „na zewnątrz”
- Nie stosować sieci bezprzewodowych we wdrożeniach wymagających wysokiej dostępności

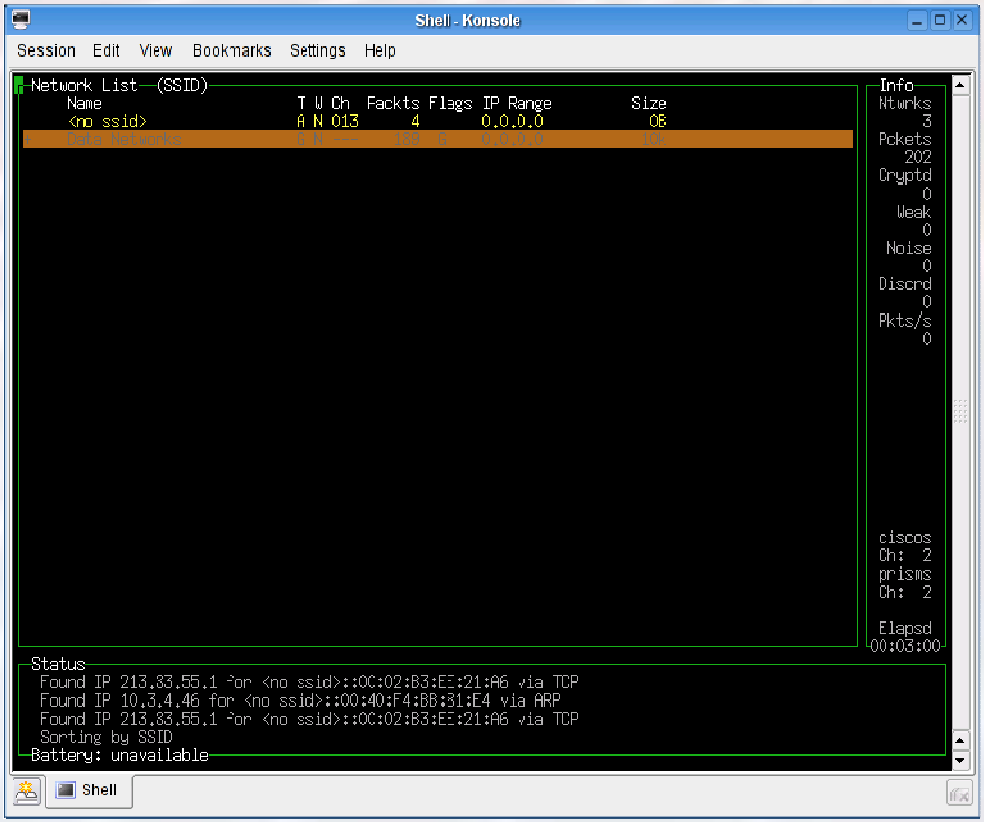
Sieci WLAN w polityce bezp. (3)

- W przypadku stosowania uwierzytelniania 802.1x weryfikacja wiarygodności powinna być obustronna
- Protokołem uwierzytelniania 802.1x powinien być EAP-TLS lub PEAPv2
- Stosować odpowiednio dobrane anteny
- Minimalizować zasięg sieci tam gdzie nie jest on potrzebny

Narzędzia

Kismet

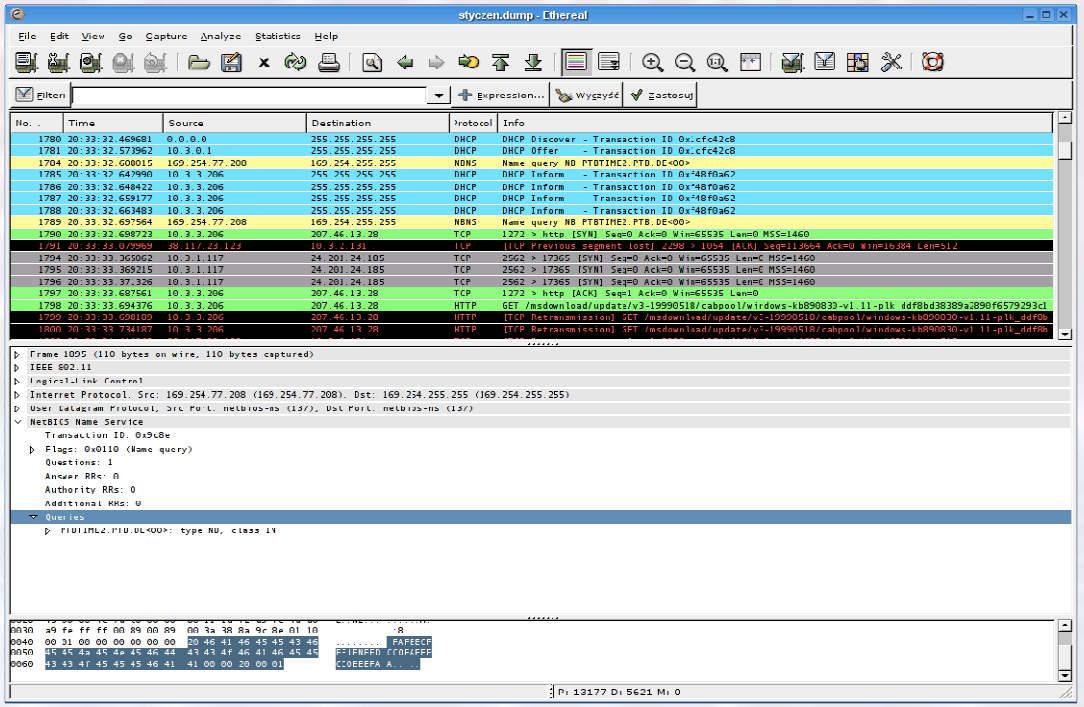
Narzędzie służy do skanowania sieci bezprzewodowych i zbierania przesyłanych w nich danych, uruchamia kartę w trybie monitora. Kismet może również służyć jako IDS.



http://www.kismetwireless.net/

Ethereal

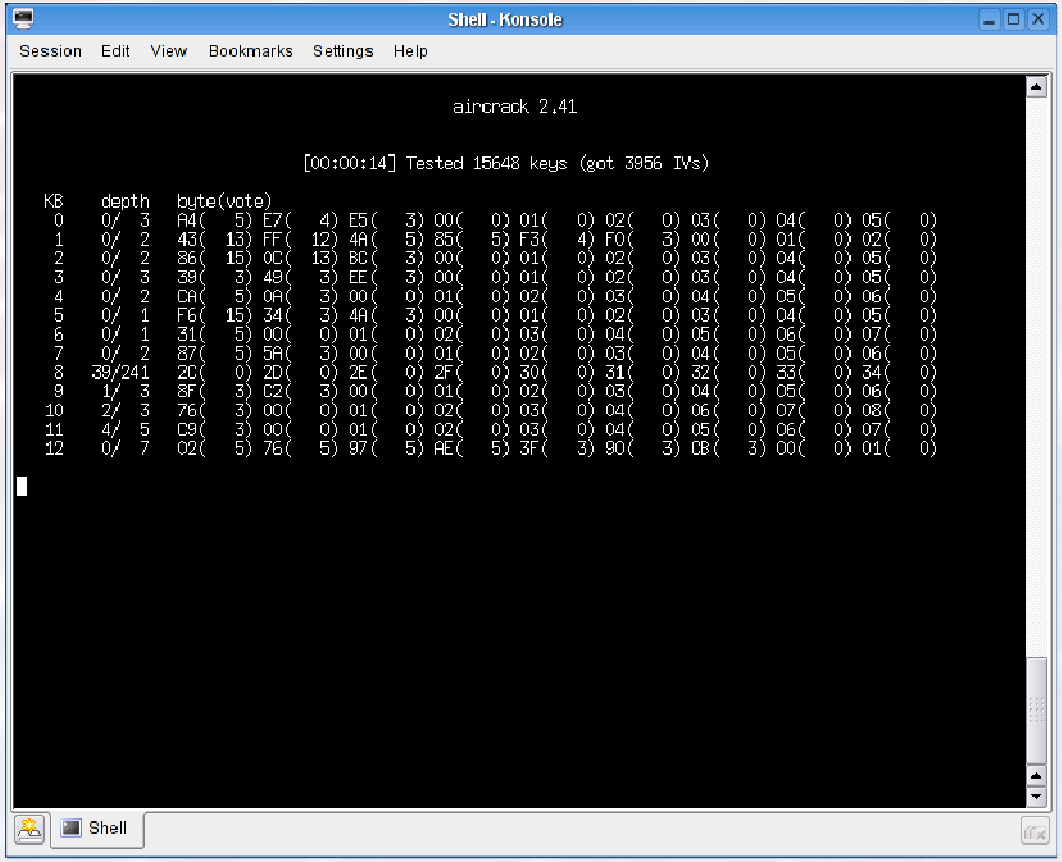
Narzędzie umożliwia analizę zebranych danych, wygodny *interface* znacznie uprzyjemnia to zadanie.



http://www.ethereal.com/

Aircrack

Wygodne narzędzie służące do łamania kluczy WEP oraz WPA-PSK



http://freshmeat.net/projects/aircrack/

Inne przydatne narzędzia

- coWPAtty – łamie klucze PSK
- Netstumbler – inny ciekawy skaner
- Wildpackets Airopeek NX – komercyjny analizator sieci WLAN
- AirMagnet – inny komercyjny analizator sieci WLAN
- 4NEC2 – program do modelowania anten

Podsumowanie

- Sieci bezprzewodowe nieustannie się rozwijają, na etapie na którym są obecnie jest wiele zastosowań, do których się nie nadają
- Można jednak sieć bezprzewodową wdrożyć w sposób wystarczająco bezpieczny dla wielu zastosowań, wszystko jest kwestią wyniku analizy ryzyka i potrzeb użytkownika
- Sieci bezprzewodowe to nie tylko 802.11, ale również Bluetooth, WiMAX, itd...

Dyskusja, pytania

Dziękuję za Uwagę!