

Bezpieczeństwo sieci WiFi

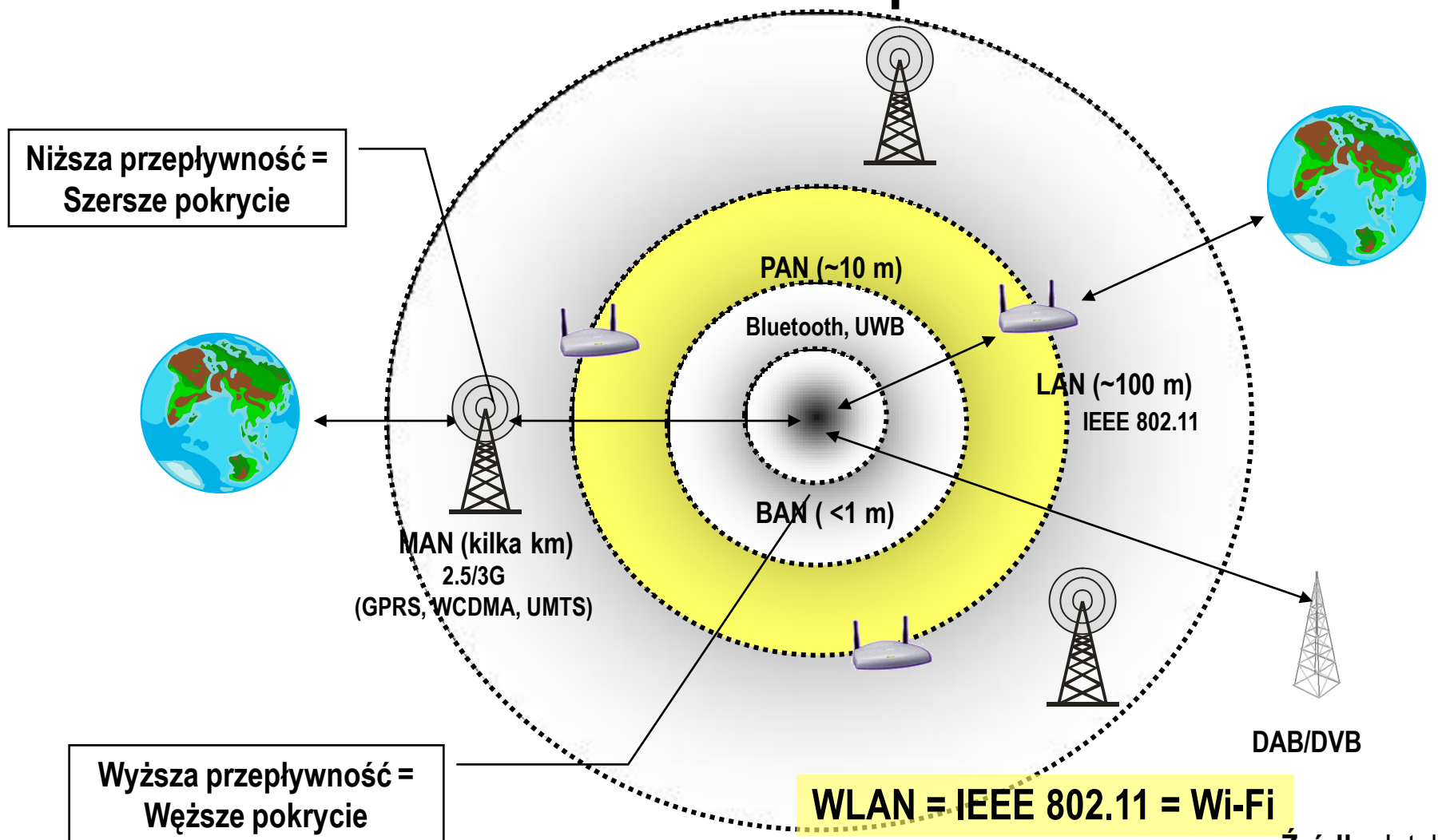
Krzysztof Cabaj II PW

Krzysztof Szczypiorski IT PW

Plan wykładu

- Wprowadzenie
 - WiFi a inne sieci radiowe
 - Podstawy działania sieci WiFi
- Zagrożenia
- Sposoby zabezpieczania
- Przykładowe narzędzia

WLAN a inne sieci bezprzewodowe

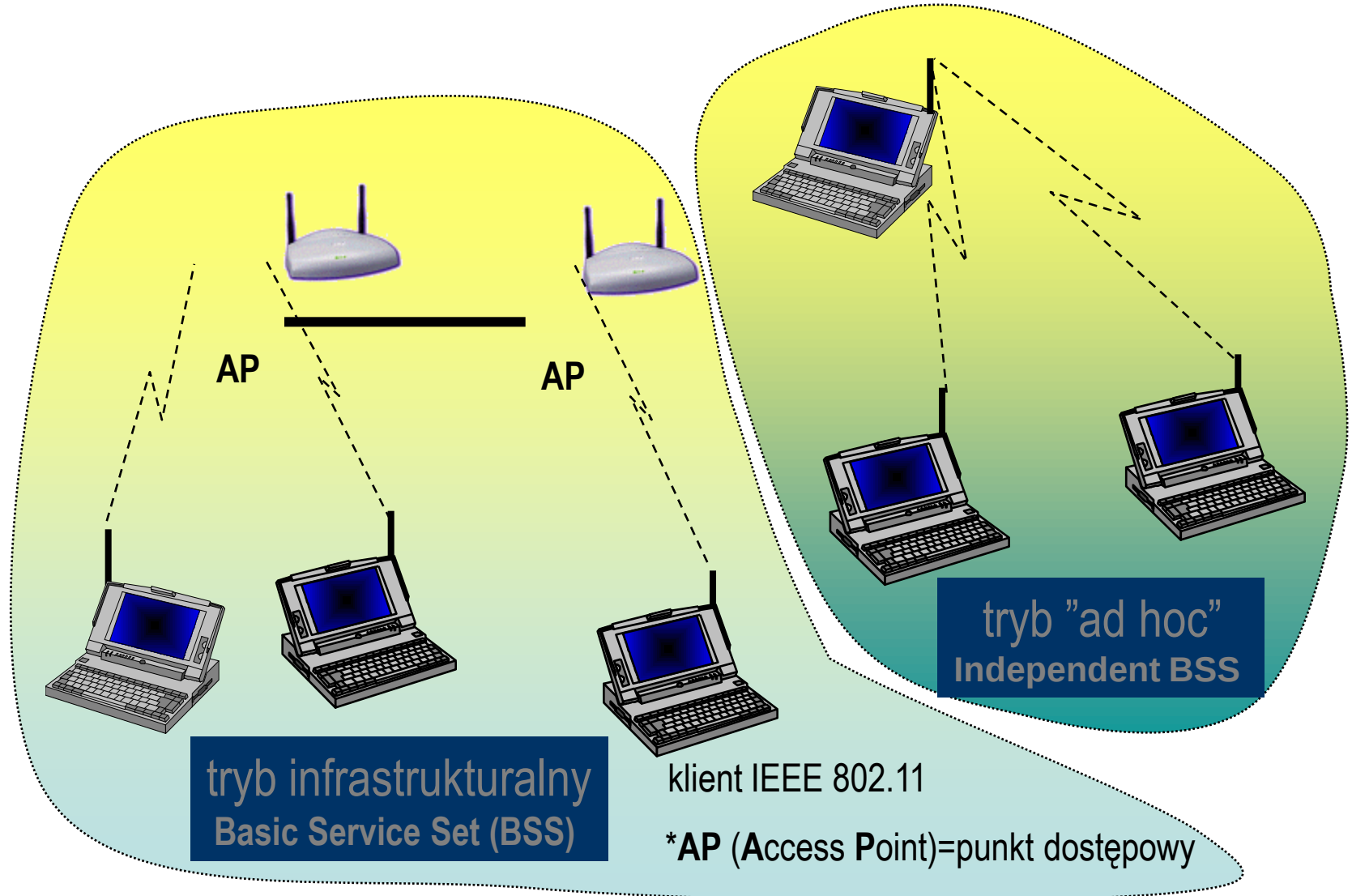


Źródło: Intel

Podstawy działania

- Radiowa sieć lokalna – rodzina standardów 802.11
 - Dwie częstotliwości
 - 802.11a 5GHz
 - 802.11b/g 2,4GHz
 - 802.11n 2,4GHz i 5GHz (na razie Draft 2.0, standard planowany na 2009)
 - Dostępne prędkości 1, 2, 5.5, 11, 54, 108, 248*, 300* Mbps
- (* standard n)

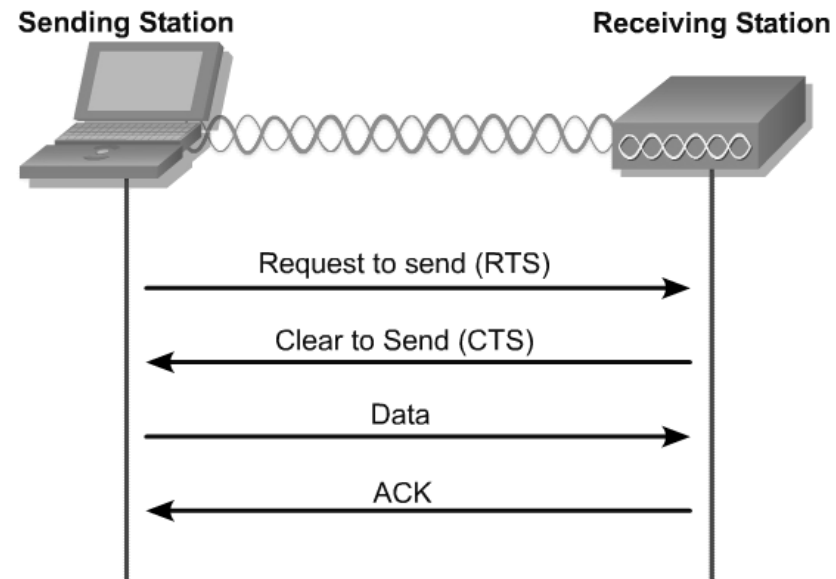
Podstawy działania - architektury



Unikanie kolizji w WLAN

- **DCF z RTS/CTS**

- Załóżmy, że A chce wysłać ramkę do B
 - A wysyła RTS (request to send)
 - Jeśli B nie nasłuchuje innej transmisji (tj. B odbiera RTS) wtedy wysyła do A CTS (clear to send)
 - Kiedy ramka jest poprawnie odebrana wysyłany jest ACK przez B do A
 - Teraz jeśli inna stacja chce wysłać coś do B, musi usłyszeć CTS... A więc czeka



Źródło: Cisco

Różnice w stosunku do 802.3 (Ethernet)

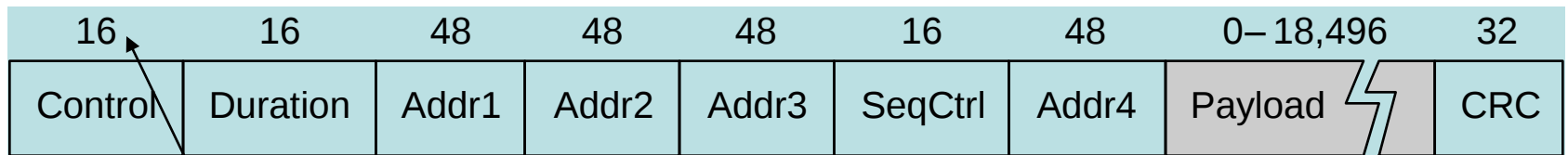
- W sieciach standardów 802.11 mamy 3 rodzaje ramek
 - Zarządzające (management)
 - Kontrolne (control)
 - Danych (data)
- Proces uwierzytelnienia (stacji!!!) i nawiązania asocjacji
- Inny sposób rozwiązywania problemu kolizji

Ramki w sieciach 802.11

- Management Frames
 - Association request frame
 - Association response frame
 - Probe request frame
 - Probe response frame
 - Beacon frame
 - Authentication Frame
- Control Frames
 - Request to send (RTS)
 - Clear to send (CTS)
 - Acknowledgment (ACK)
- Data frames

Format ramki MAC

- Max. 2312 bajtów danych



Długości w bitach

Format ramek RTS/CTS/ACK

RTS

frame control 16 00011011X...X	duration 16	receiver address 48	transmitter address 48	CRC 32
--------------------------------------	----------------	------------------------	---------------------------	-----------

CTS

frame control 16 00011100X...X	duration 16	receiver address 48	CRC 32
--------------------------------------	----------------	------------------------	-----------

ACK

frame control 16 00011101X...X	duration 16	receiver address 48	CRC 32
--------------------------------------	----------------	------------------------	-----------

Plan wykładu

- Wprowadzenie
- Zagrożenia
 - Wprowadzenie
 - Atak parkingowy
 - WarDriving
 - Nieautoryzowane punkty dostępowe
- Sposoby zabezpieczania
- Przykładowe narzędzia

Zagrożenia - wprowadzenie

- Największym zagrożeniem jest wykorzystywane medium – każdy może podsłuchać ruch (a także wygenerować własny ruch)
- Związane z tym ataki/pojęcia
 - Atak parkingowy
 - Wardriving

Atak parkingowy

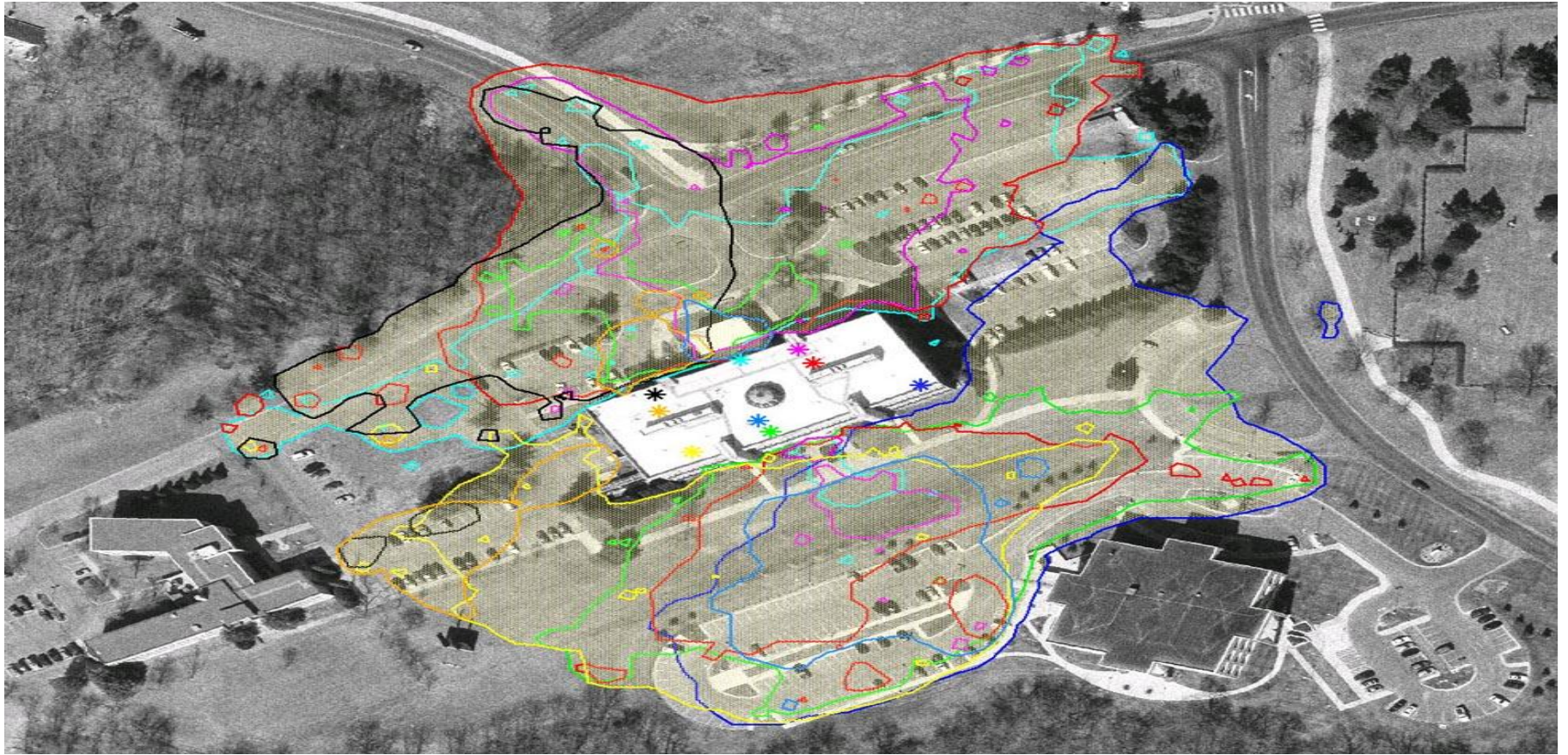
- Aby zaatakować sieć kablową trzeba albo obejść zabezpieczenia od strony Internetu ... albo wpiąć się fizycznie do sieci
- Aby zaatakować sieć WiFi wystarczy być z laptopem w okolicy punktu dostępowego, Np. siedzieć z laptopem w samochodzie na parkingu – stąd popularna nazwa tego typu ataków
- Ale dzisiaj może to być także atak za pomocą urządzeń mniejszych – palmtopy, komórki

Propagacja sygnału radiowego



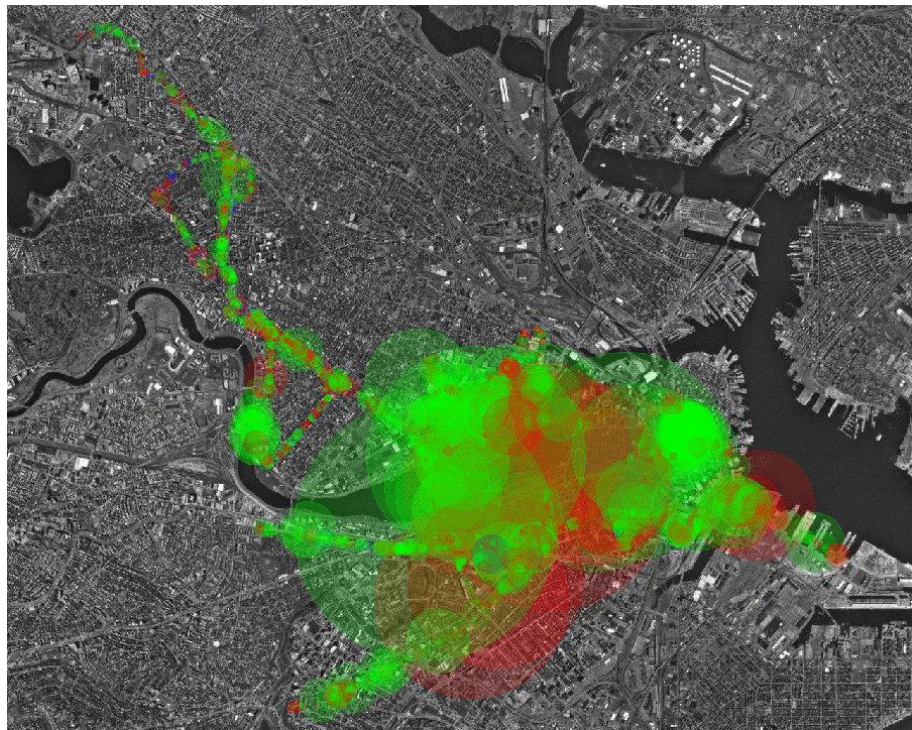
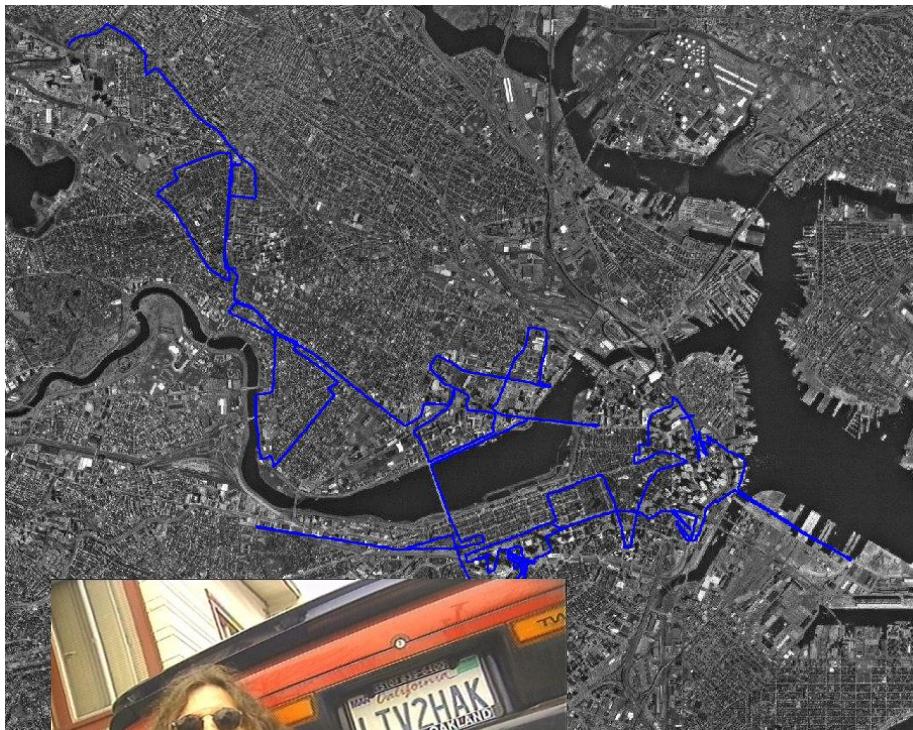
Źródło: David Wagner - Why Swiss-Cheese Security Isn't Enough

Ryzyko ataku z dużej odległości



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

Wardriving, warflying...



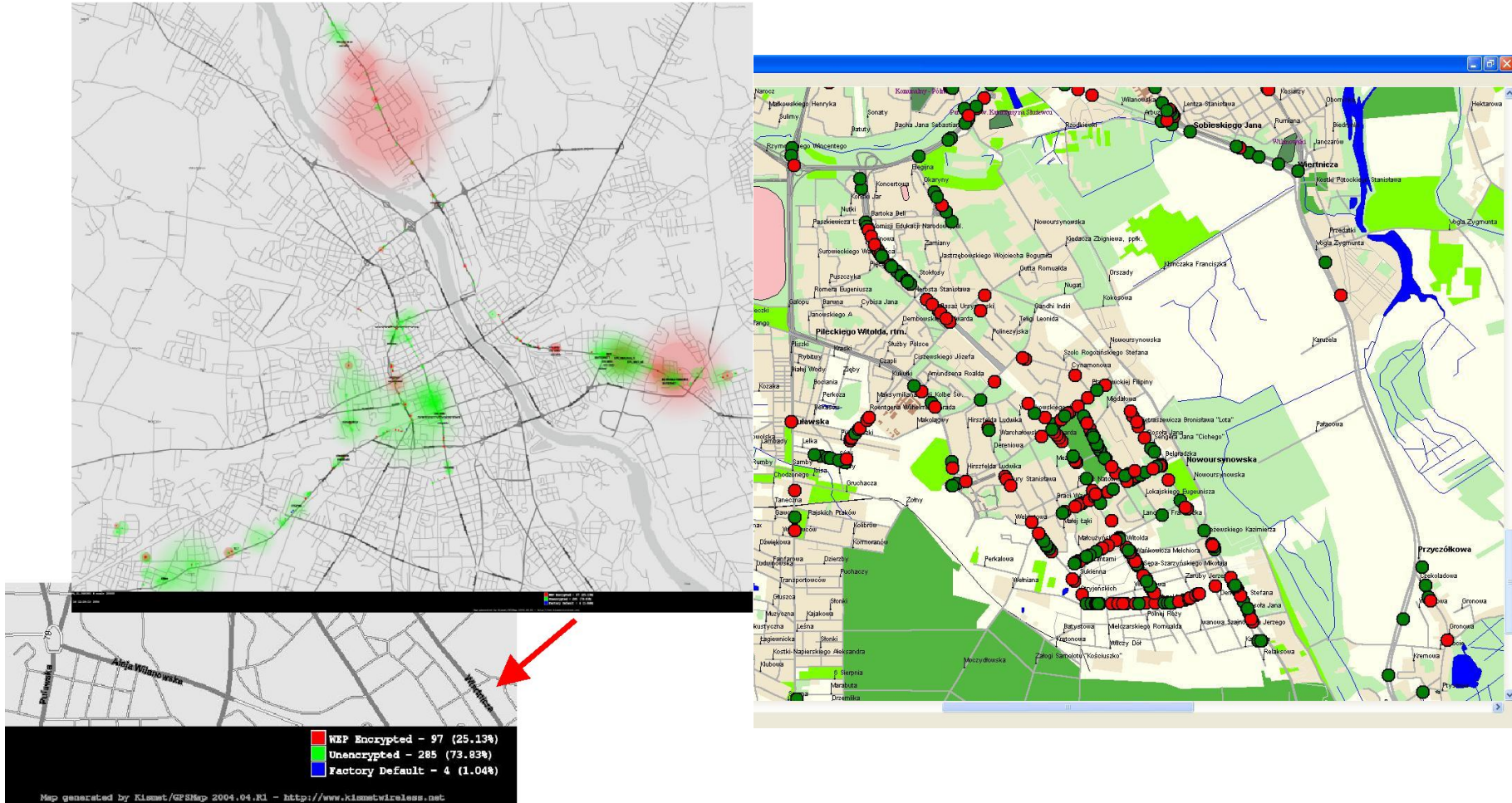
Źródło map: <http://www.wardriving.com/boston>

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



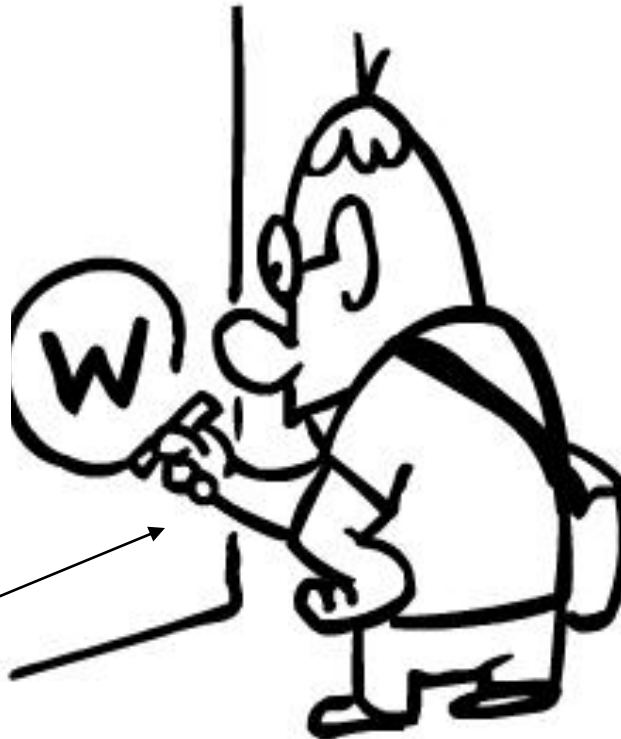
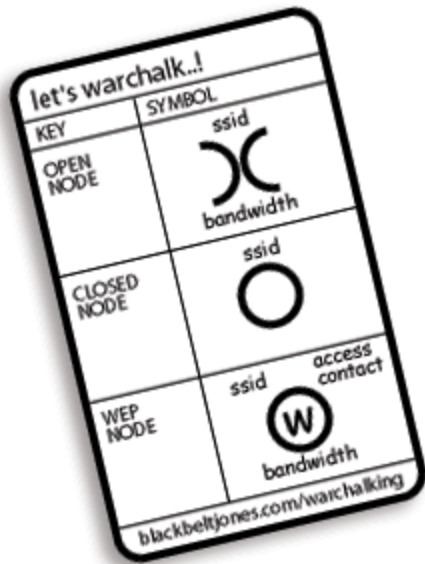
Peter Shipley - prekursor

„Polacy nie gęsi ... „



<http://wardriving.legionowo.eu.org/mapy/wawka-20040914-range.jpg>

Warchalking cz. 1/2



chalk (kreda)

www.warchalking.org

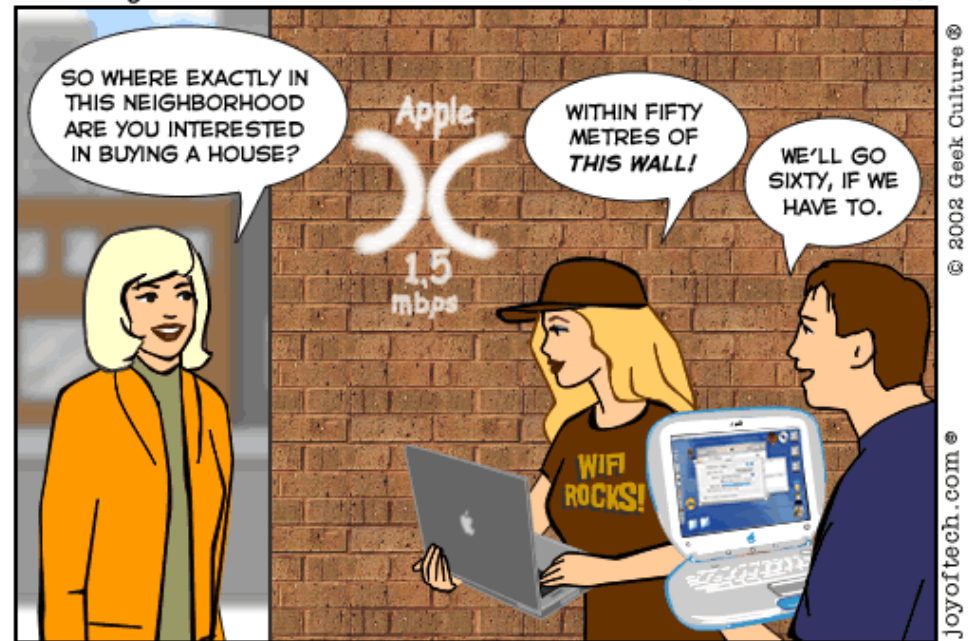


Warchalking cz. 2/2



The Joy of Tech

by Nitrozac & Snaggy



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>

Inne podatności sieci Wi-Fi...

- Słabość WEP (Wired Equivalent Privacy) ze statycznym kluczem – ataki pasywne i aktywne
- Kiepskie uwierzytelnienie
- Rozgłaszanie SSID (Service Set Identifier)
- Podszywanie się – na poziomie adresów MAC i IP
- Niewłaściwa konfiguracja punktów dostępowych
- DoS – odmowa usługi

Uruchamianie nieautoryzowanych punktów dostępowych

- Nagminnie pracownicy firmy, bez zgody i wiedzy osób odpowiedzialnych za bezpieczeństwo uruchamiają sieci dostępowe
- Niska cena tego typu urządzeń na rynku oraz prostota instalacji
- Standardowa niebezpieczna konfiguracja
- Sieć korporacyjna staje się dostępna dla każdego posiadacza komputera przenośnego z kartą Wi-Fi



Pani Ania
z działu marketingowego.

Plan wykładu

- Wprowadzenie
- Zagrożenia
- Sposoby zabezpieczania
 - Usługi ochrony informacji w WiFi
 - Bezpieczna architektura
- Przykładowe narzędzia

Usługi ochrony informacji w WiFi

- Początki słabe
 - WEP
- 802.11i, (WPA, WPA2)
 - TKIP
 - CCMP (AES)
 - 802.1x+EAP (uwierzytelnianie, zarządzanie kluczami)

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

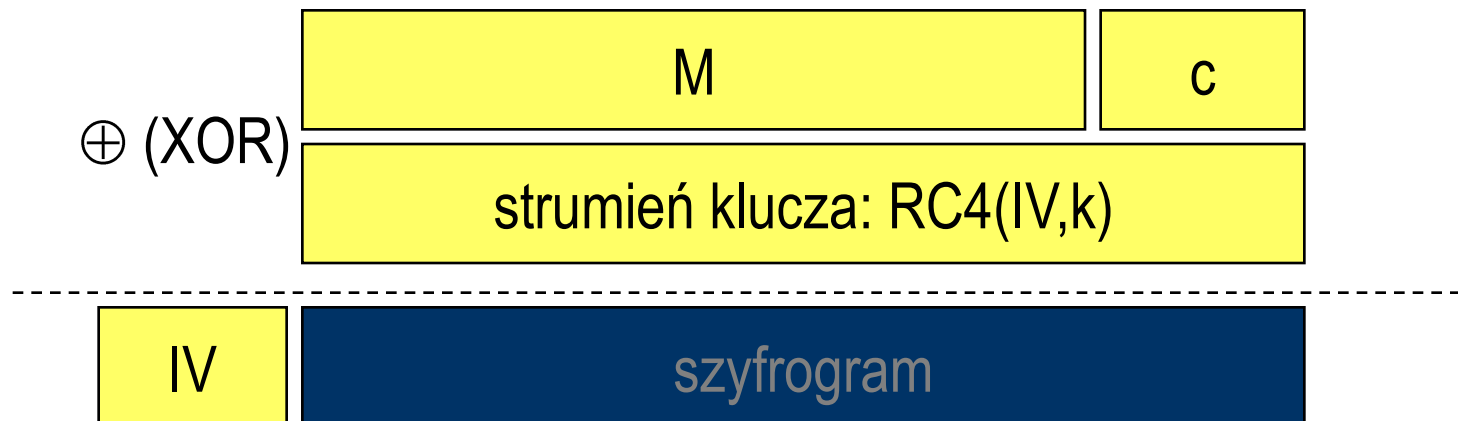
Założenia projektowe IEEE 802.11:1997 i 1999

- **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 $\sim 10^{-5}$)
 - **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 - problemy

- Brak mechanizmu zarządzania kluczami – klucze trzeba ustawiać manualnie
- Kompromitacja klucza przez jedną osobę kompromituje całą sieć
- Prostota złamania kluczą po nasłuchu odpowiedniej liczby ramek
- Rozwiązanie: zastosowanie 802.11i

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-odpowieź
- **SKA** przeważnie nie implementowany

IEEE 802.11i

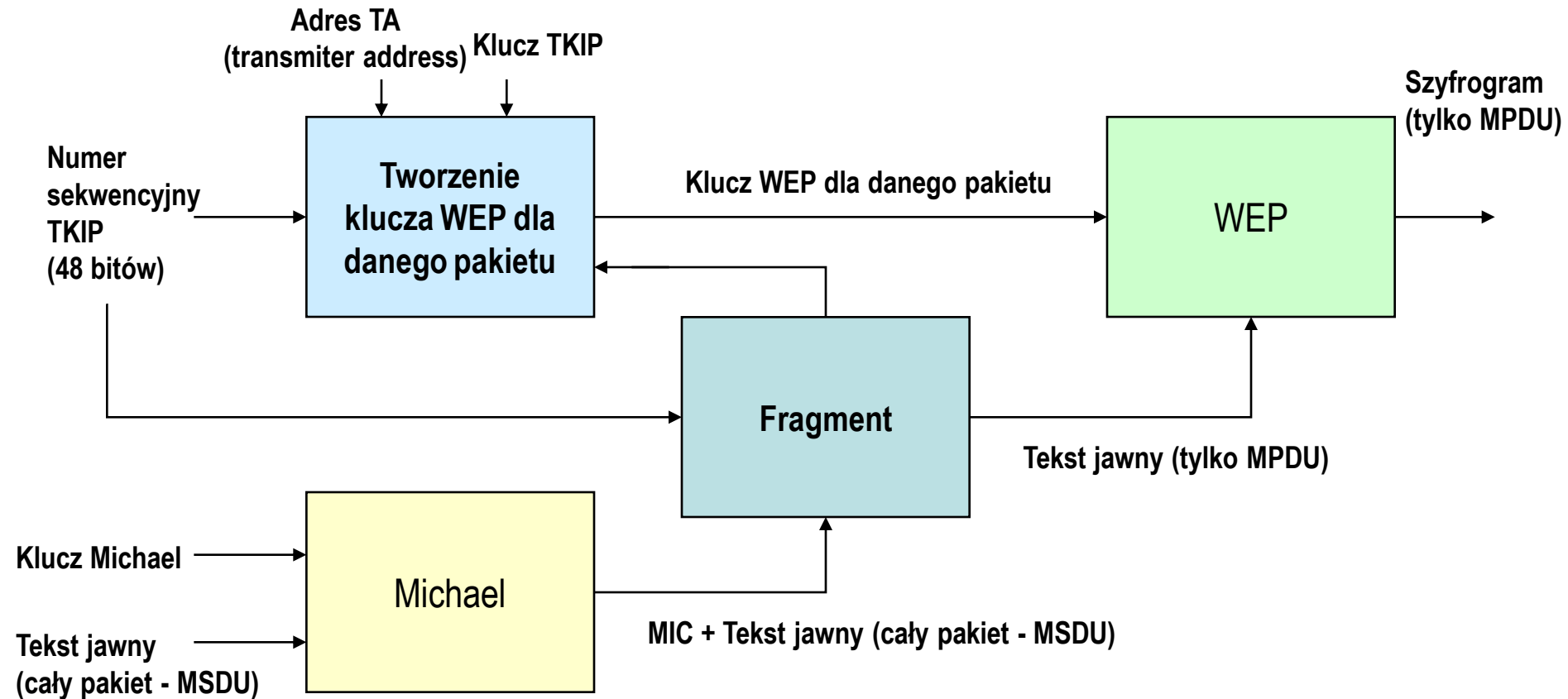
- TGi powołana w ramach 802.11 w maju 2001
 - IEEE P802.11i/D7 Unapproved Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems – LAN/MAN Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification 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)
- Standard zatwierdzony w 2004 (IEEE 802.11i-2004)

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

Przetwarzanie danych w TKIP

(uproszczona enkapsulacja)



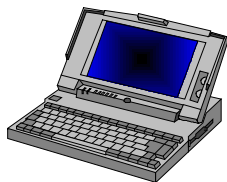
CCMP - cechy

- 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:
 - pojawią się nowe AP
 - pojawią się nowe urządzenia klienckie klasy hand-held
 - ale pozostaną PC
- Brak związku z WEP

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)

Poszczególne komponenty



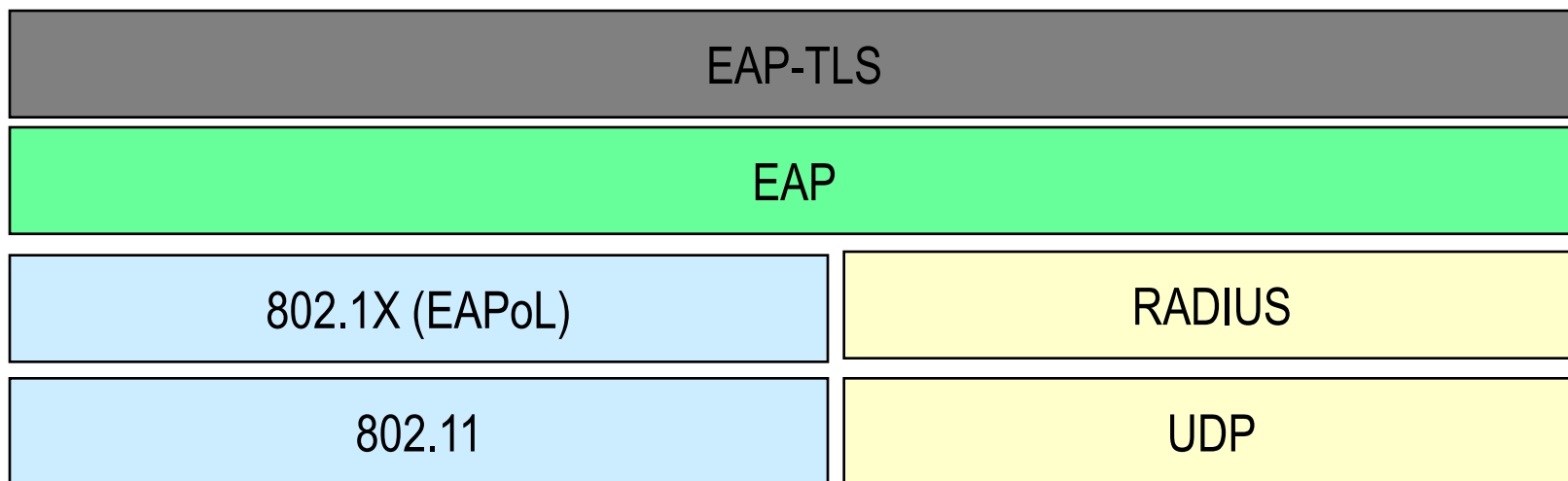
Stacja



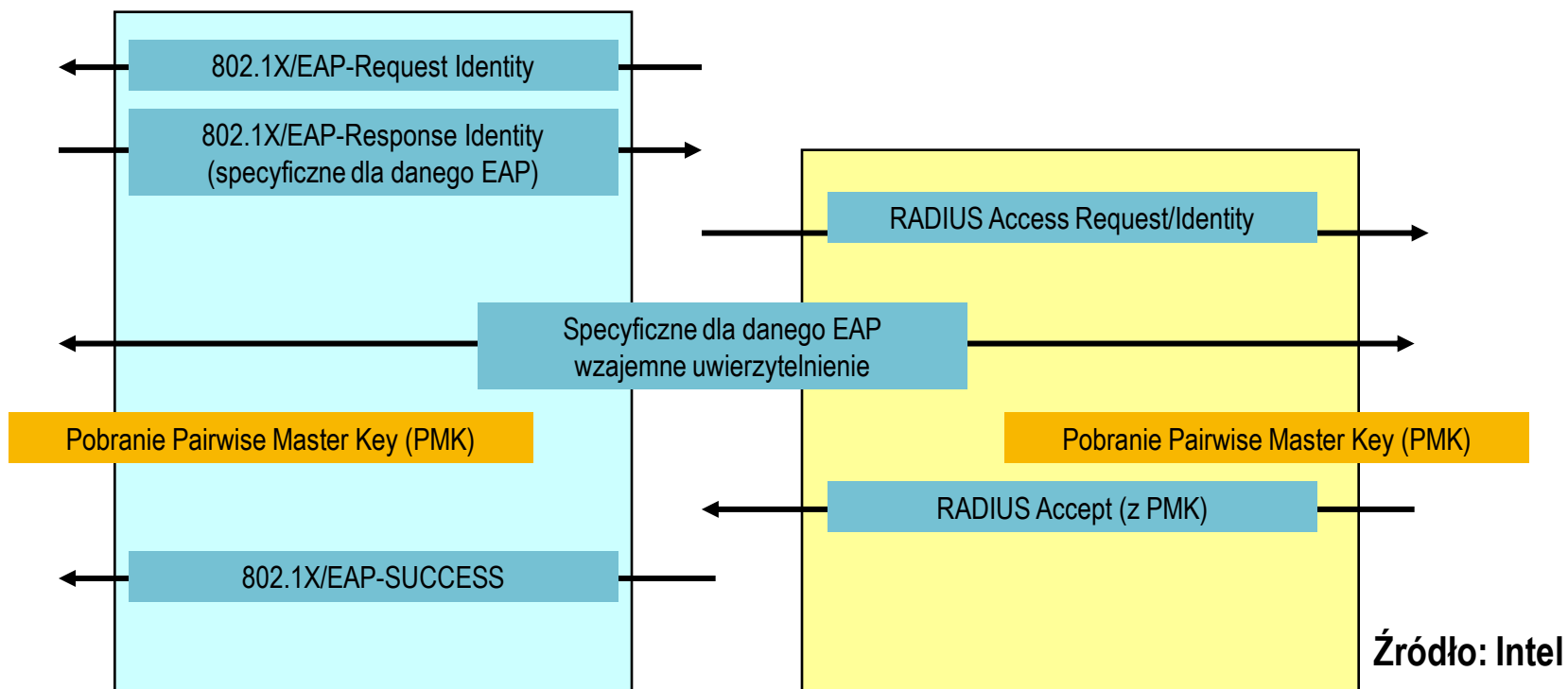
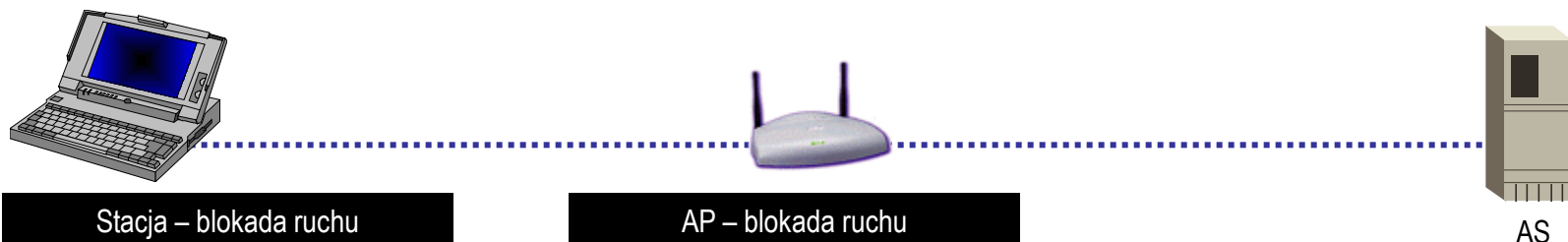
AP



AS



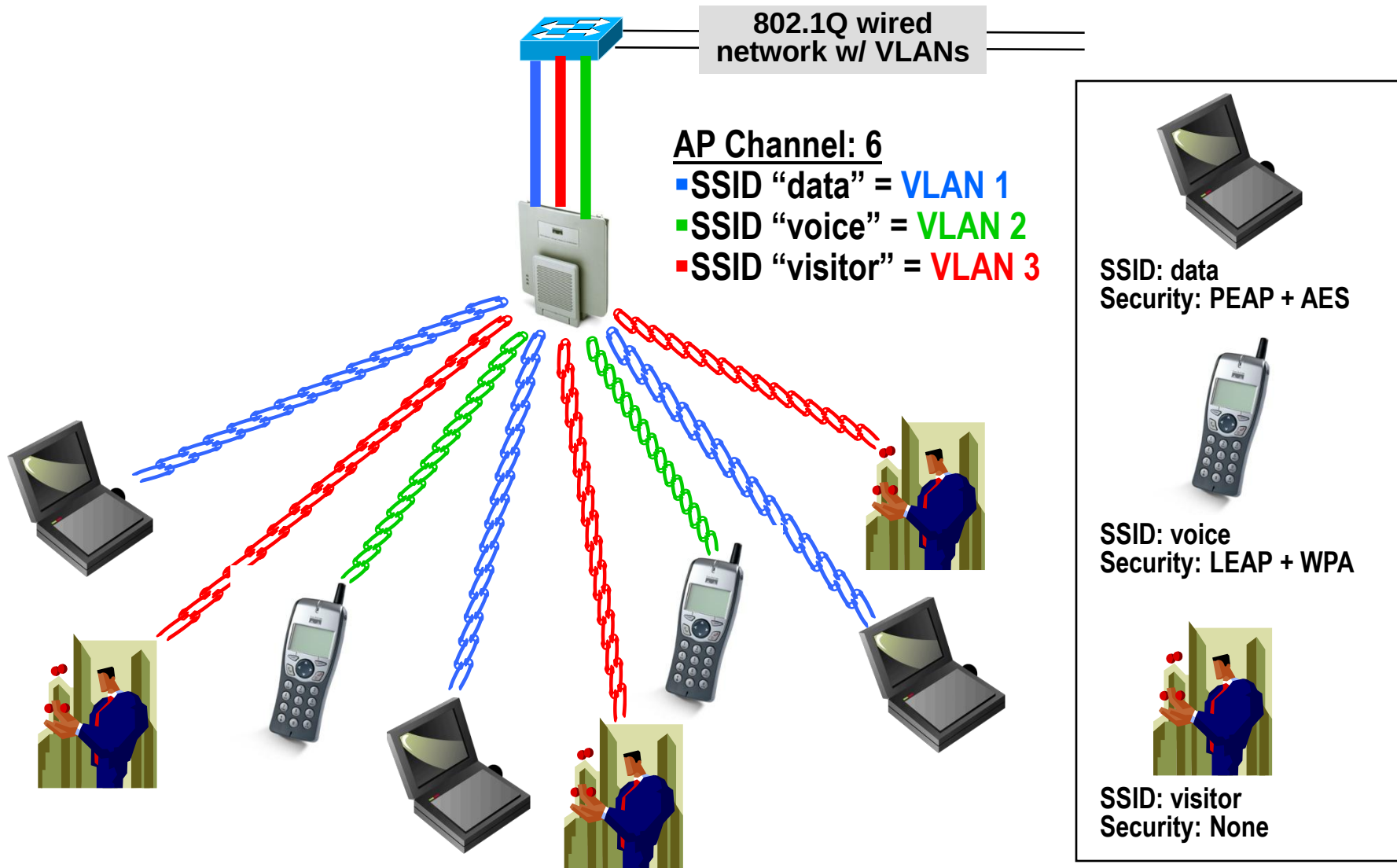
802.1X/EAP – idea działania



Bezpieczna architektura

- Zrezygnować z WEP !!!
- Używać co najmniej TKIP'a, jeśli możliwe to CCMP
- Wdrożyć w sieci uwierzytelnianie 802.1x
- Jeśli przez sieć WiFi przesyłane są ważne dane skorzystać z szyfrowania w warstwie 3 np. IPsec.

Bezpieczna architektura -użycie VLAN



Plan wykładu

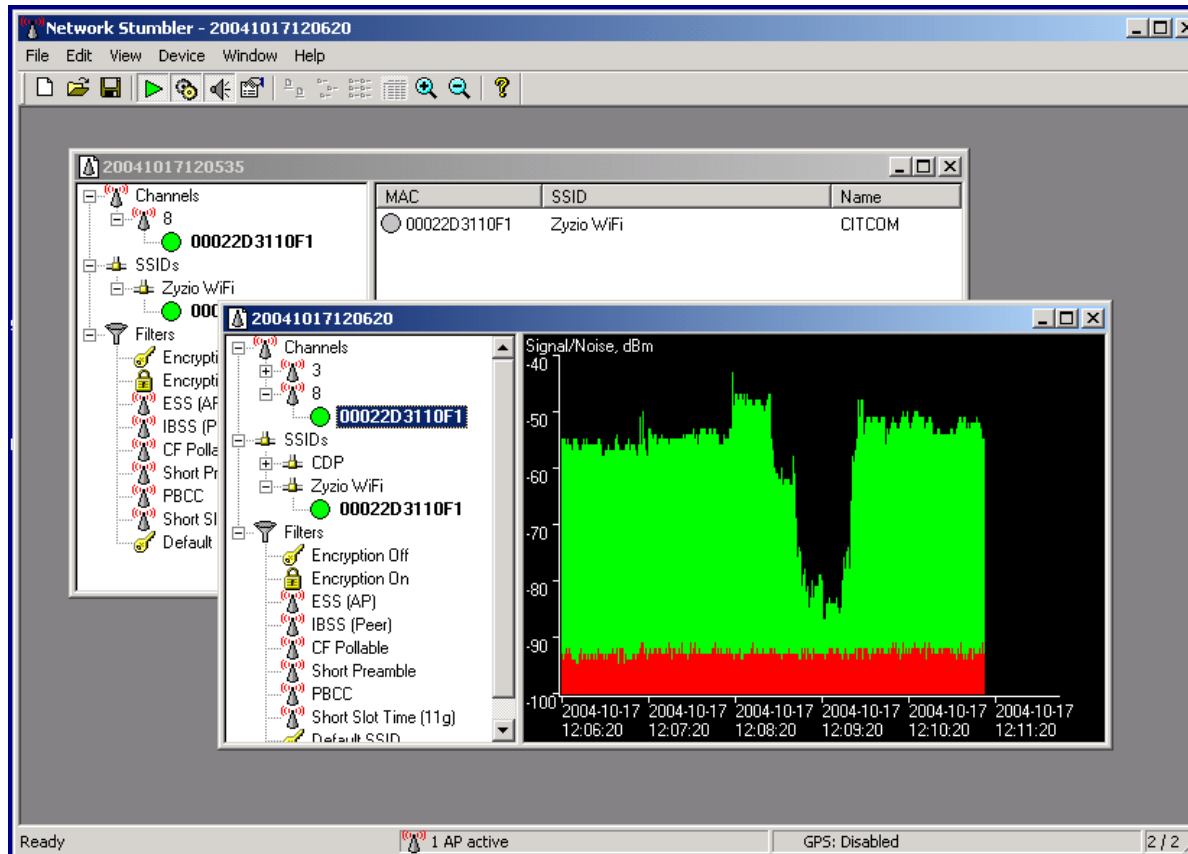
- Wprowadzenie
- Zagrożenia
- Sposoby zabezpieczania
- Przykładowe narzędzia
 - Skanery sieci
 - Programy umożliwiające „łamanie” kluczy
 - Systemy WIDS (Wireless IDS)

Skannery

- Programy umożliwiające wykrywanie i zdobywanie szczegółowych informacji na temat widocznych sieci
- Podział skanerów
 - aktywne
 - pasywne

Skanery - Netstumbler

- Skaner aktywny

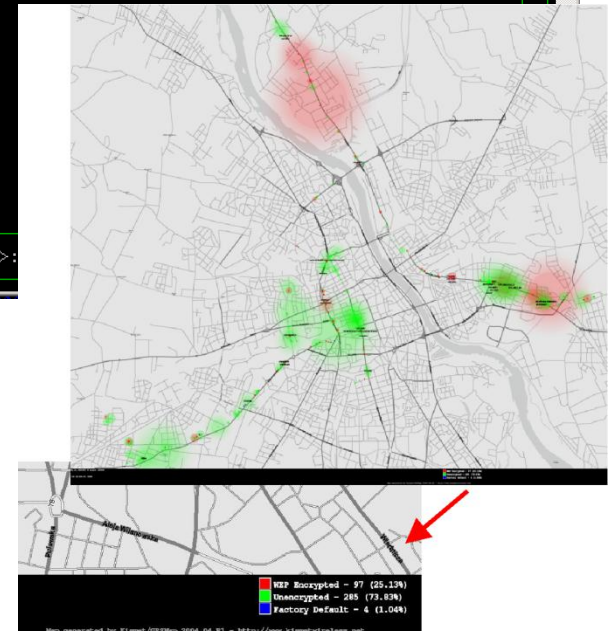


Skanery – Kismet 1/2

- Bardzo zaawansowany skaner pasywny
- Funkcje prostego systemu IDS dedykowanego sieciom WiFi
- Możliwość podłączenie odbiornika GPS. Nanoszenie na dostarczone mapy wykrytych informacji

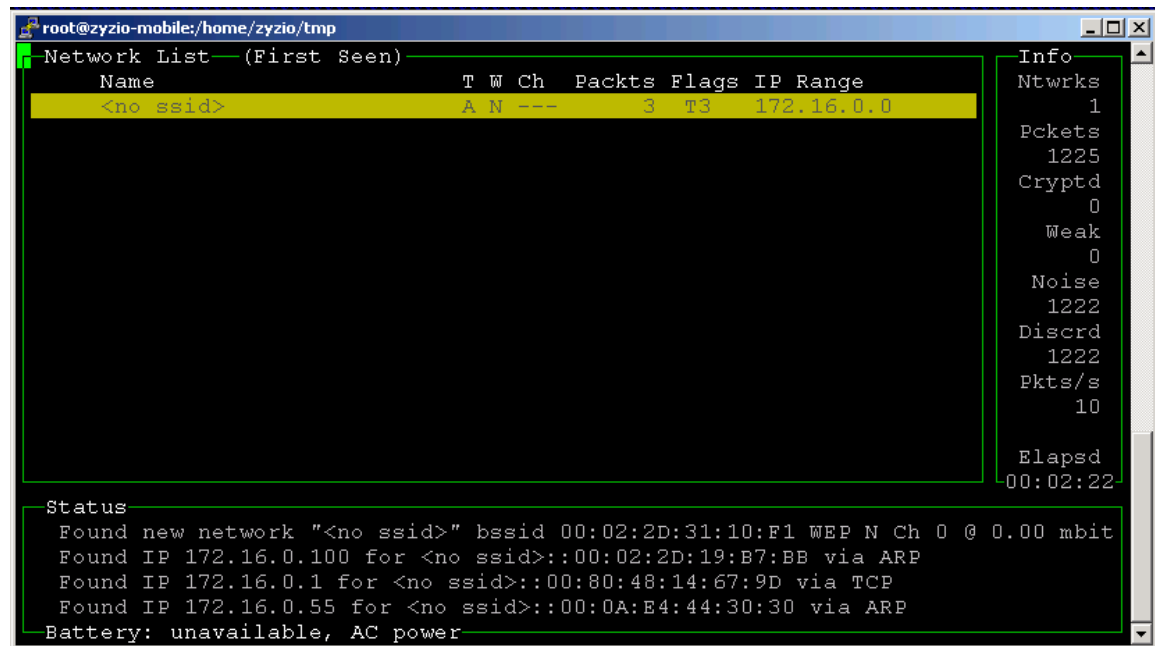
```
root@zyzio-mobile:/home/zyzio/tmp
Network List (First Seen) Info
Network Details (-) Up
SSID : <no ssid>
Server : localhost:2501
BSSID : 00:02:2D:31:10:F1
Carrier : IEEE 802.11b
Manuf : Lucent
Model : Unknown
Matched : 00:02:2D:00:00:00/FF:FF:FF:00:00:00
Max Rate: 0.0
First : Sun Oct 17 12:57:37 2004
Latest : Sun Oct 17 12:59:34 2004
Clients : 2
Type : Access Point (infrastructure)
Info :
Channel : 0
WEP : No
Beacon : 0 (0.000000 sec)
Packets : 3
  Data : 3
  LLC : 0
  Crypt : 0
  Weak : 0
  Dupe IV : 0
Data : 423B
Signal :

Found IP 172.16.0.55 for <no ssid>:
Battery: unavailable, AC power
```



Skannery – Kismet 2/2

- Wykrywania sieci WiFi które nie rozgłaszają swojego SSID
- Wykrywanie zakresów sieci IP jedynie poprzez nasłuch transmitowanych pakietów protokołów ARP, UDP, TCP
- pracy w modelu klient-serwer
(możliwość analizy w centralnym punkcie danych z wielu sensorów)



```
root@zyzio-mobile:/home/zyzio/tmp
Network List (First Seen)
Name          T W Ch  Packts Flags IP Range
<no ssid>    A N ---    3   T3  172.16.0.0

Info
Ntwrks      1
Pckets     1225
Cryptd       0
Weak        0
Noise      1222
Discrd     1222
Pkts/s      10
Elapsd     00:02:22

Status
Found new network "<no ssid>" bssid 00:02:2D:31:10:F1 WEP N Ch 0 @ 0.00 mbit
Found IP 172.16.0.100 for <no ssid>::00:02:2D:19:B7:BB via ARP
Found IP 172.16.0.1 for <no ssid>::00:80:48:14:67:9D via TCP
Found IP 172.16.0.55 for <no ssid>::00:0A:E4:44:30:30 via ARP
Battery: unavailable, AC power
```

Programy umożliwiające „łamanie” kluczy 1/2

- Z powodu podatności WEP’a złamanie kluczy jest dość proste
- Wystarczy nasłuch sieci ... i odpowiednie oprogramowanie
- Po zdobyciu odpowiedniej liczby ramek, klucz WEP można złamać

Programy umożliwiające „łamanie” kluczy 2/2

- Ataki na klucz
 - przeszukanie wszystkich możliwych haseł (możliwych do podania)
 - próba wykorzystania podatności w RC4 (atak FMS)
- Przykładowe narzędzia
 - AirSnort
 - WepCrack

Systemy WIDS 1/3

- Wykorzystywane w sieciach WiFi mechanizmy powodują występowanie specyficznych ataków.
- Przykładowo
 - Pojawianie się nieautoryzowanych AP (Rogue AP)
 - Próby deasocjacji stacji
 - Użycie skanerów aktywnych
- Do wykrycia tego typu ataków potrzebne są specjalizowane systemy IDS – WIDS (Wireless IDS)

Systemy WIDS 2/3

- Systemy WIDS analizują wszystkie ramki (także kontrolne i zarządzania)
- Do ich działania trzeba mieć kartę radiową i sterowniki umożliwiające dostęp do ramek kontrolnych i zarządzających

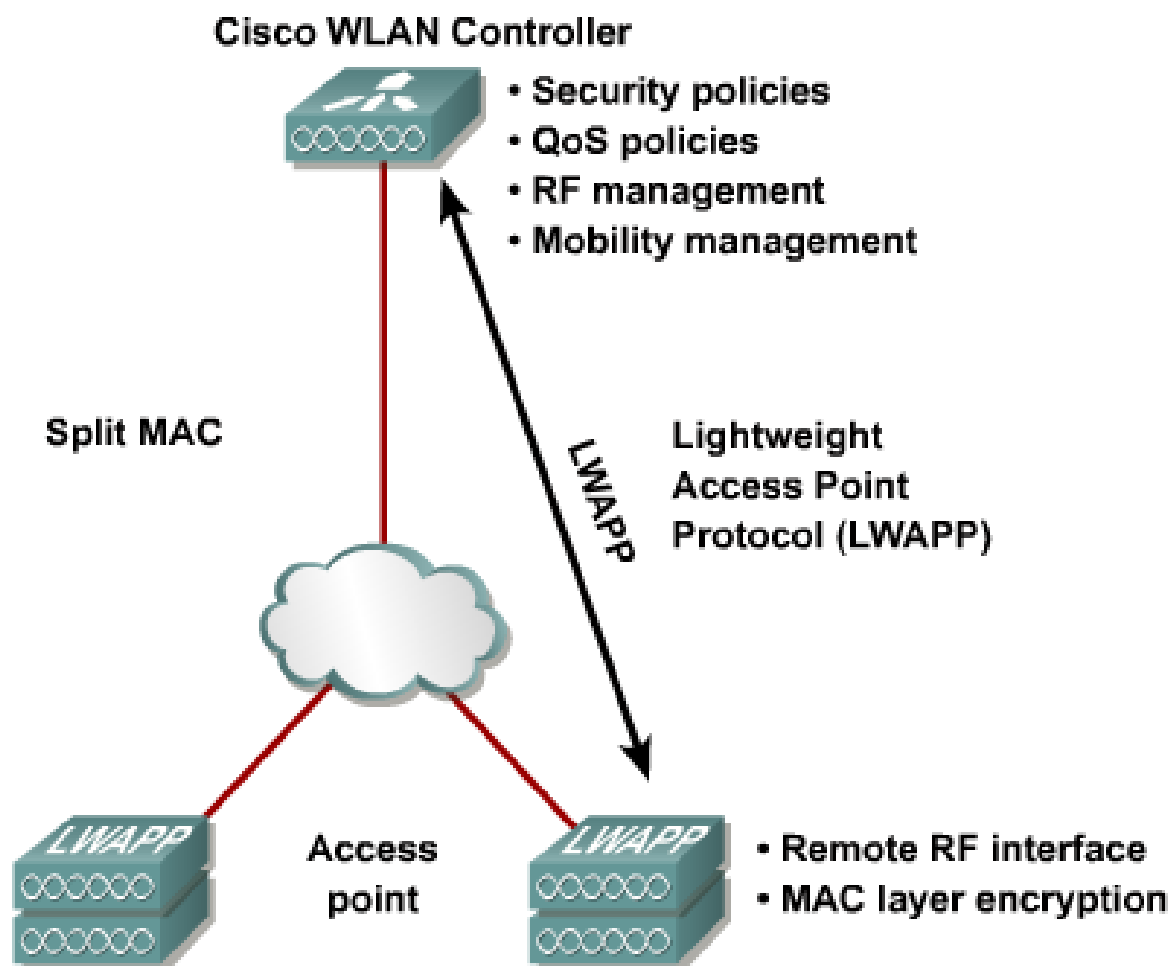
Systemy WIDS 3/3

- Przykładowe systemy
 - Widz_apmon – wykrywa pojawienie się AP o tym samym SSID a innym kanale, adresie MAC itp.
 - SnortWireless – patch do systemu Snort, dodający nowy protokół - wifi (reguły, które mogą analizować ramki zarządzania w sieciach 802.11)

Komercyjne

- CiscoWorks WLSE
- Elementy IDS w rozwiązaniu Cisco opartym na LWAPP
- NetworkChemistry

WiFi w oparciu o LWAPP



IDS na kontrolerze 1/3



Save Configuration | Ping | Logout | Refresh

MONITORWLANsCONTROLLERWIRELESSSECURITYMANAGEMENTCOMMANDSHELP

Monitor

- Summary
- Access Points
- Statistics
- CDP
- Rogues
- Clients
- Multicast

Summary

Controller Summary

Management IP Address	172.16.100.101
Software Version	4.2.112.0
System Name	WiFiController
Up Time	0 days, 1 hours, 15 minutes
System Time	Mon Apr 21 15:23:03 2008
802.11a Network State	Disabled
802.11b/g Network State	Enabled
Default Mobility Group	Mobil

Access Point Summary

	Total	Up	Down	
802.11a/n Radios	2	0	2	Detail
802.11b/g/n Radios	2	2	0	Detail
All APs	2	2	0	Detail

Client Summary

Current Clients	1	Detail
Excluded Clients	0	Detail

Rogue Summary

Active Rogue APs	10	Detail
Active Rogue Clients	1	Detail
Adhoc Rogues	0	Detail
Rogues on Wired Network	0	

Top WLANs

Profile Name	# of Clients	
CCNP	0	Detail

Most Recent Traps

Load Profile Updated to Pass for Base Radio MAC: 00:1c:
Load Profile Failed for Base Radio MAC: 00:1c:58:f1:52:1
RF Manager updated TxPower for Base Radio MAC: 00:1
AP's Interface:0(802.11b) Operation State Up: Base Rad
AP's Interface:0(802.11b) Operation State Down: Base F
[View All](#)

This page refreshes every 30 seconds.

IDS na kontrolerze 2/3



Save Configuration | Ping | Logout | Refresh

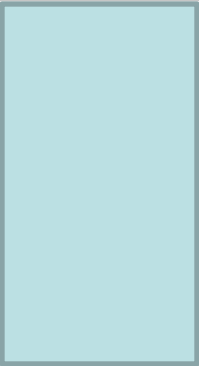
MONITORWLANsCONTROLLERWIRELESSSECURITYMANAGEMENTCOMMANDSHELP

Monitor

- Summary
- Access Points
- Statistics
- CDP
- Rogues
- Clients
- Multicast

Rogue APs

Entries 1 - 10 of 10

MAC Address	SSID	# Detecting Radios	Number of Clients	Status
	549	2	0	Alert
	elka_test	2	0	Alert
	wut1	2	0	Alert
	sala331b	2	1	Alert
	KTP	2	0	Alert
	SPOML	2	0	Alert
	WIL	2	0	Alert
	IR_540	1	0	Alert
	w-codmuca	2	0	Alert
	ztv	2	0	Alert

IDS na kontrolerze 3/3



Save Configuration | Ping | Logout | Refresh

MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP

Monitor

- Summary
- ▶ Access Points
- ▶ Statistics
- ▶ CDP
- ▶ Rogues
 - Clients
 - Multicast

Rogue AP Detail

< Back | Apply

MAC Address

Type

AP

Is Rogue On Wired Network?

No

First Time Reported On

Mon Apr 21 14:21:39 2008

Last Time Reported On

Mon Apr 21 15:24:13 2008

Current Status

Alert

Update Status

-- Choose New Status --

Maximum number of APs to contain the rogue

-- Choose Number of APs --

APs that detected this Rogue

Base Radio MAC	AP Name	SSID	Channel	Type	WEP	WPA	Pre-Ambble	RSS
	CCNP_AP3	sala331b	11	802.11g	Enabled	Enabled	Long	-58
	CCNP_AP1	sala331b	11	802.11g	Enabled	Enabled	Long	-67

Clients associated to this Rogue AP