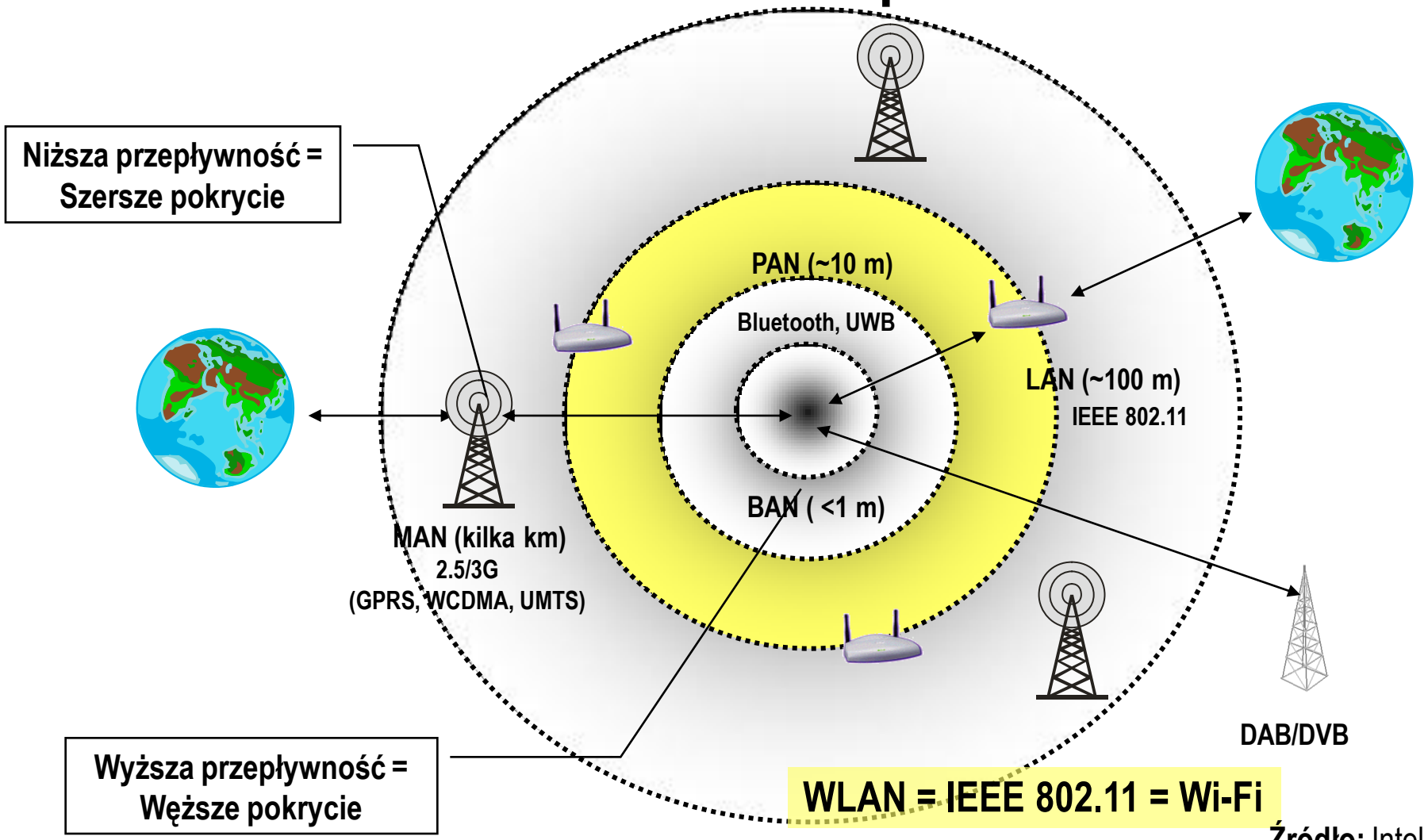
Bezpieczeństwo sieci WiFi

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



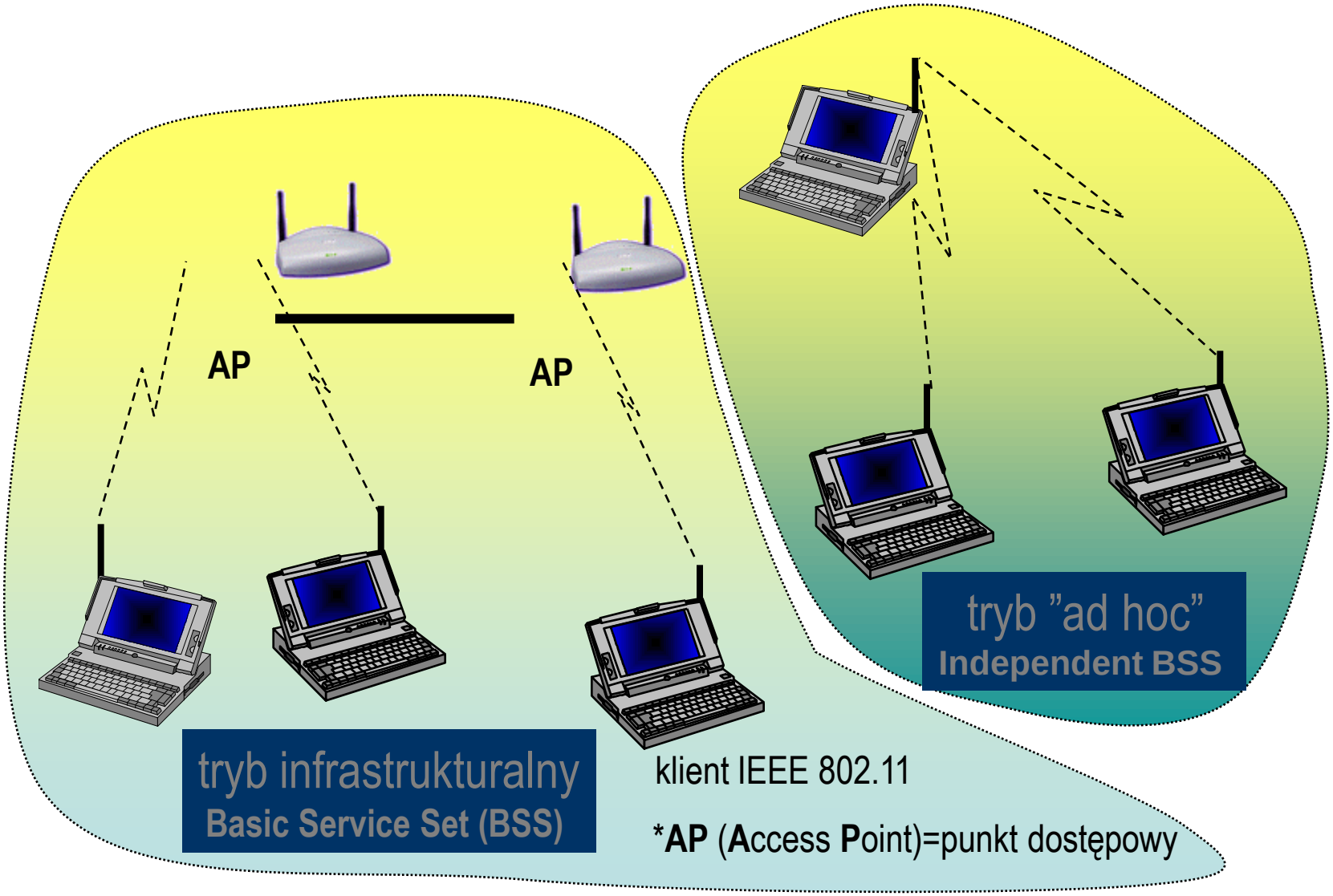
Źródło: Intel

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

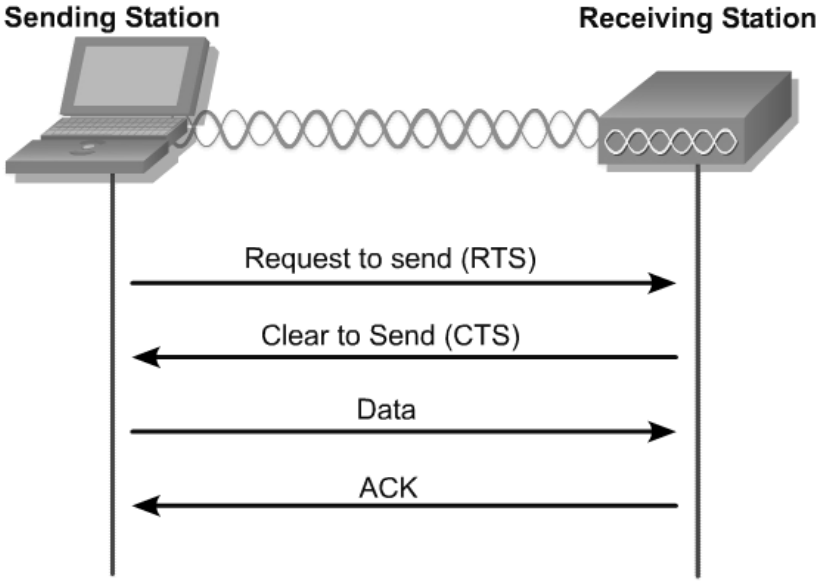
(* standard n)

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)

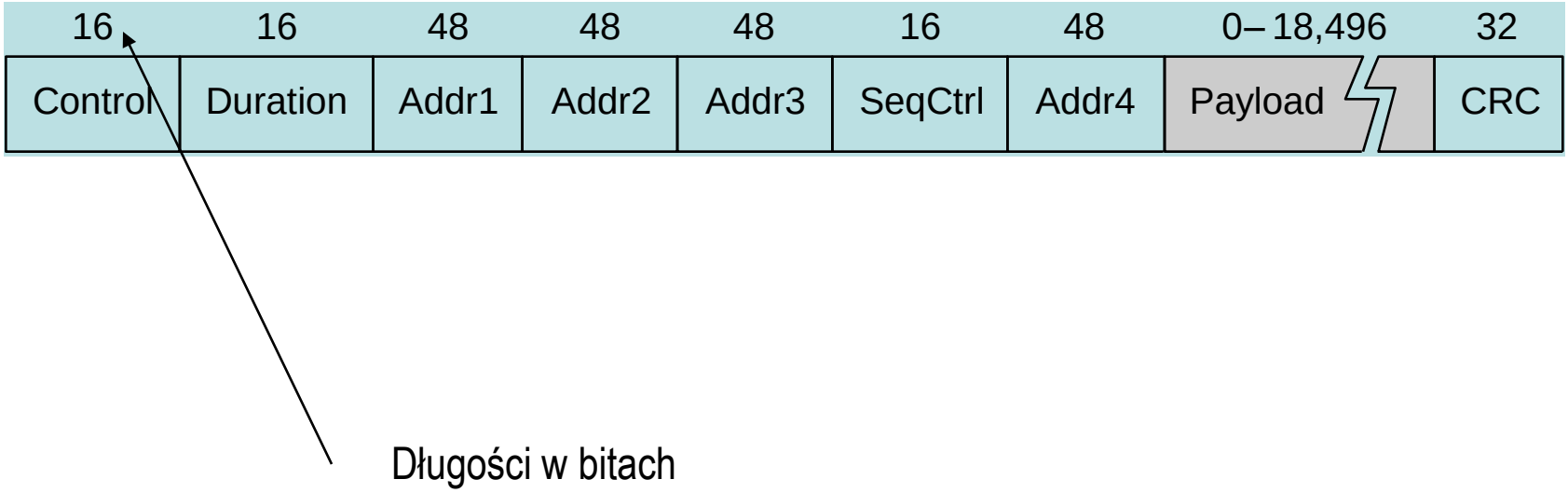
- W sieciach standardów 802.11 mamy 3 rodzaje ramek
  - Zarządzające (managment)
  - Kontrolne (control)
  - Danych (data)
- Proces uwierzytelnienia (stacji!!!) i nawiązania asocjacji
- Inny sposób rozwiązania problemu kolizji

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



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

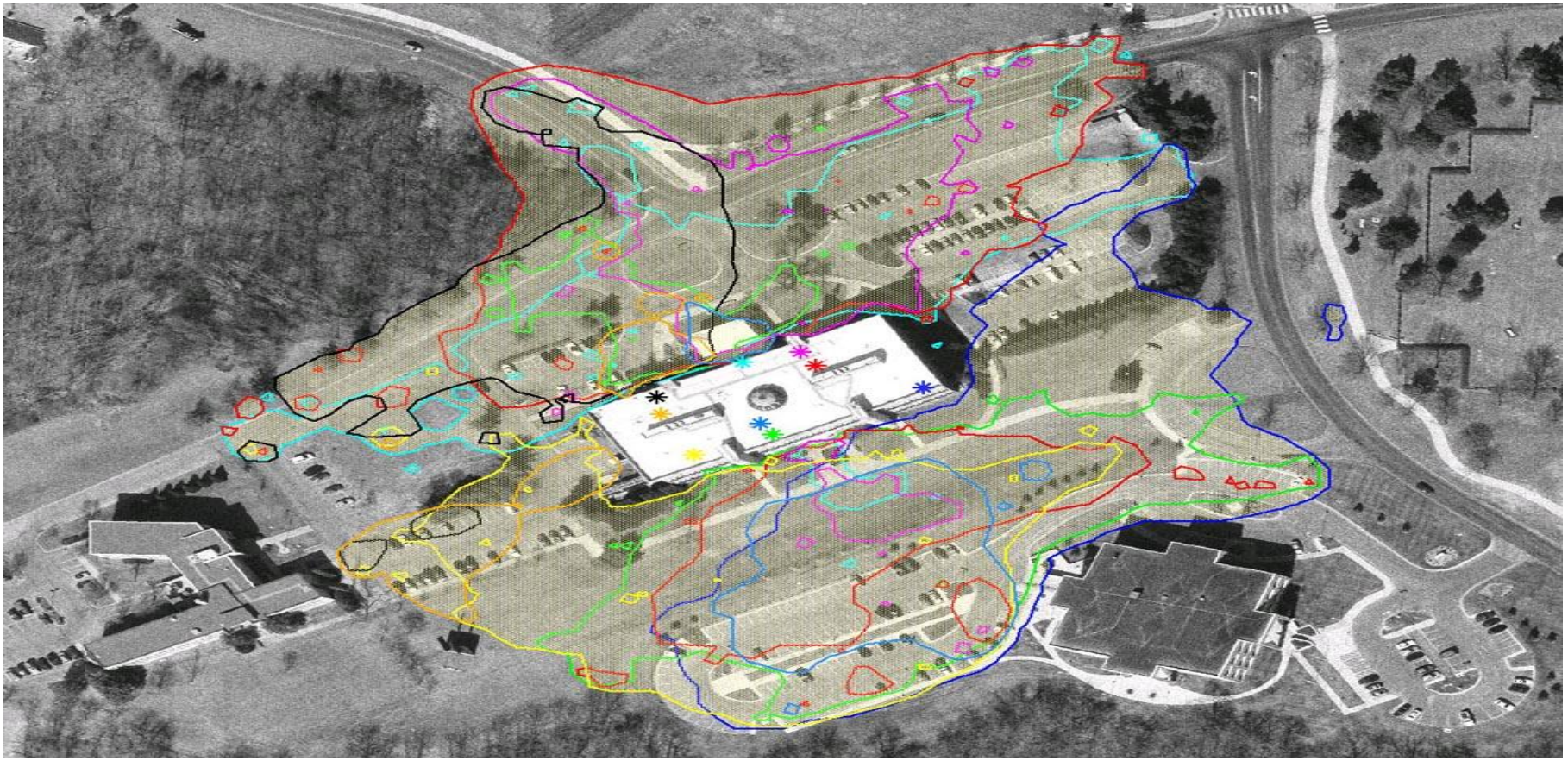
- Aby zaatakować sieć kablową trzeba albo obejść zabezpieczenia od strony Internetu … albo wpiąć się fizycznie do sieci
- Aby zaatakować sieć WiFi wystarczy być z laptopem w okolicy punktu dostępowego, Np. siedzieć z laptopem w samochodzie na parkingu – stąd popularna nazwa tego typu ataków

- Ale dzisiaj może to być także atak za pomocą urządzeń mniejszych – palmtopy, komórki

Propagacja sygnału radiowego

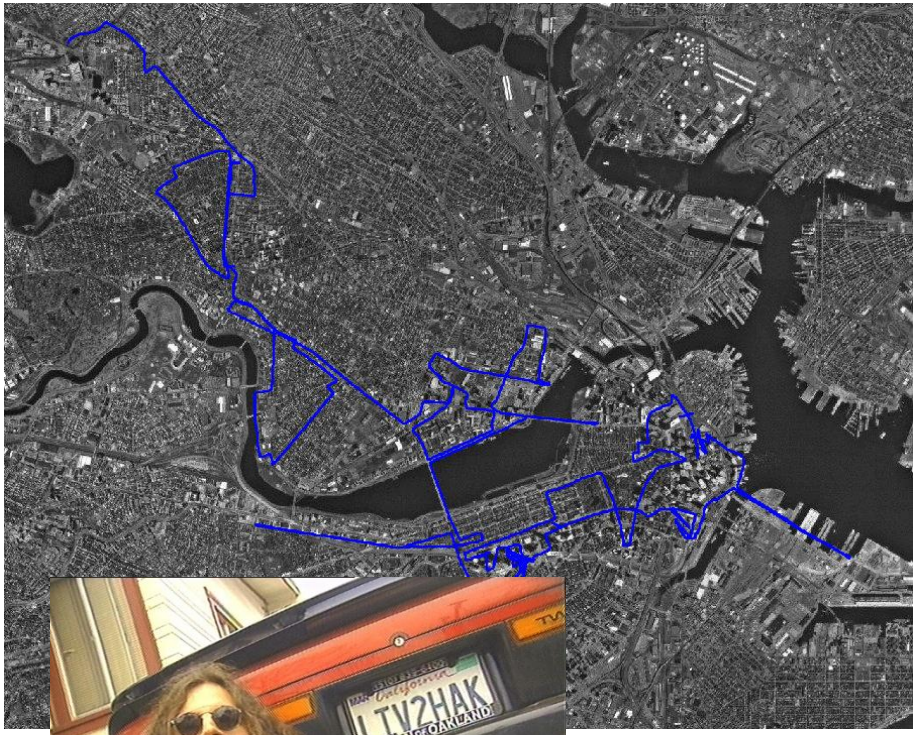
Źródło: David Wagner - Why Swiss-Cheese Security Isn't Enough

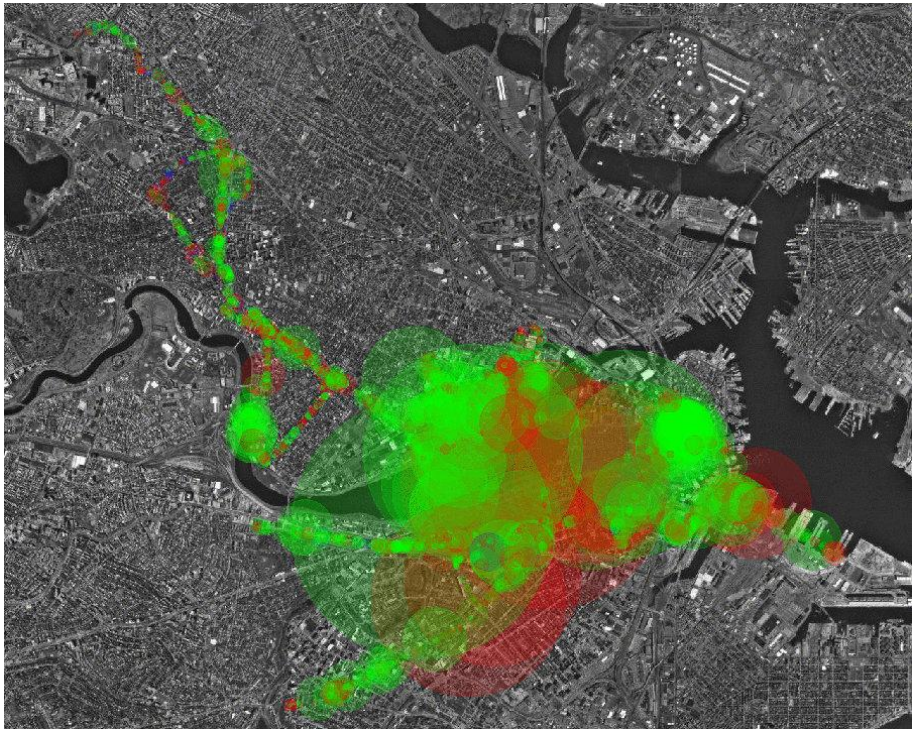
Ryzyko ataku z dużej odległości



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

Wardriving, warflying…



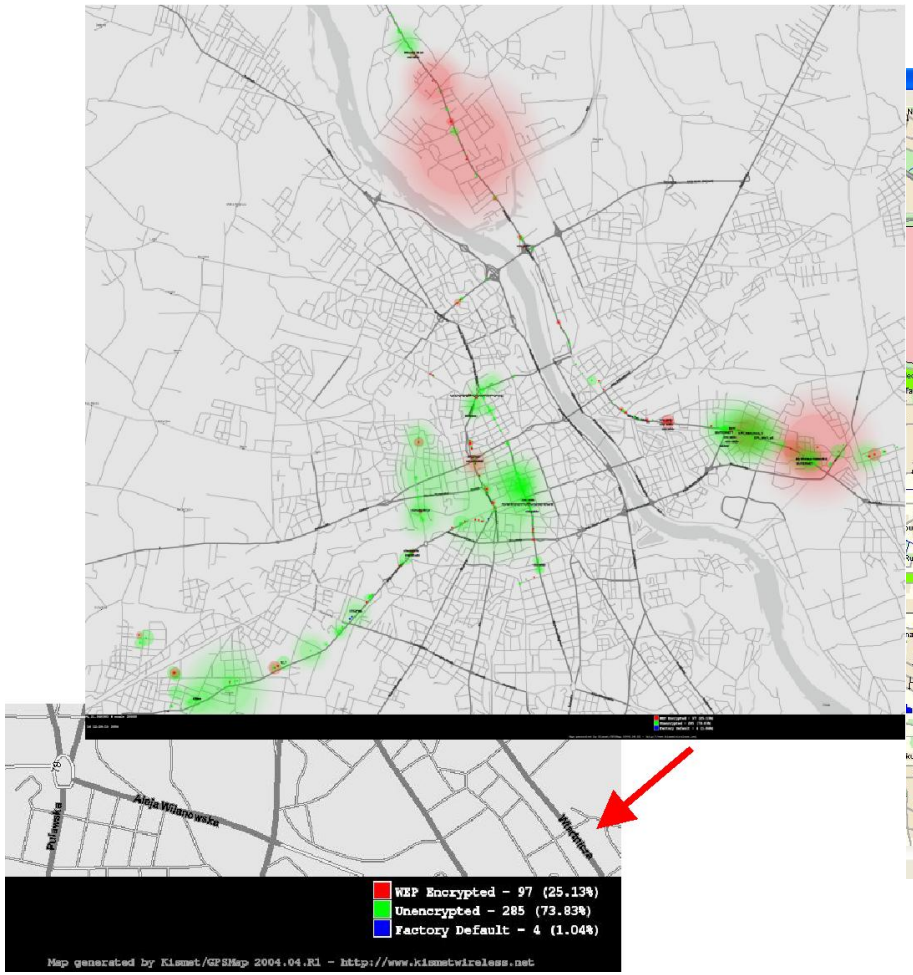


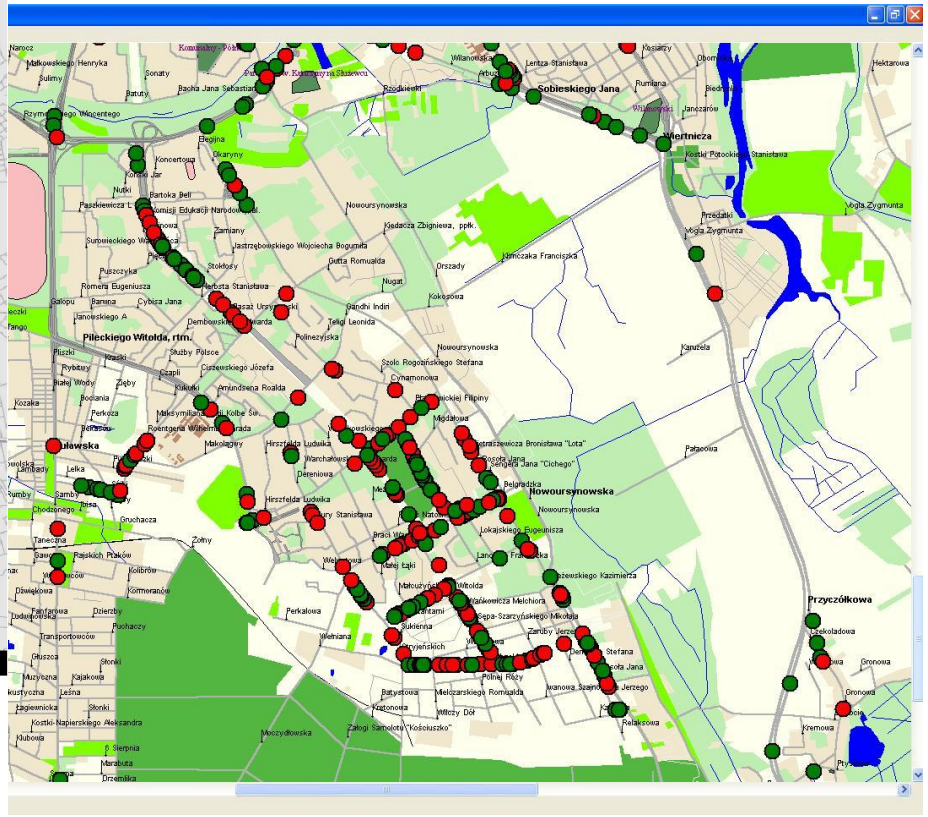
Peter Shipley - prekursor

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

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

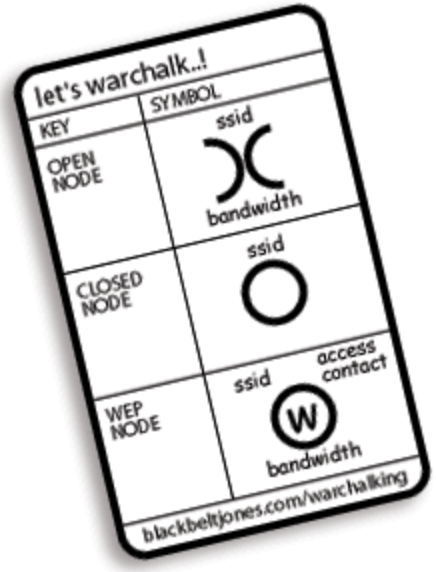
„Polacy nie gęsi … „

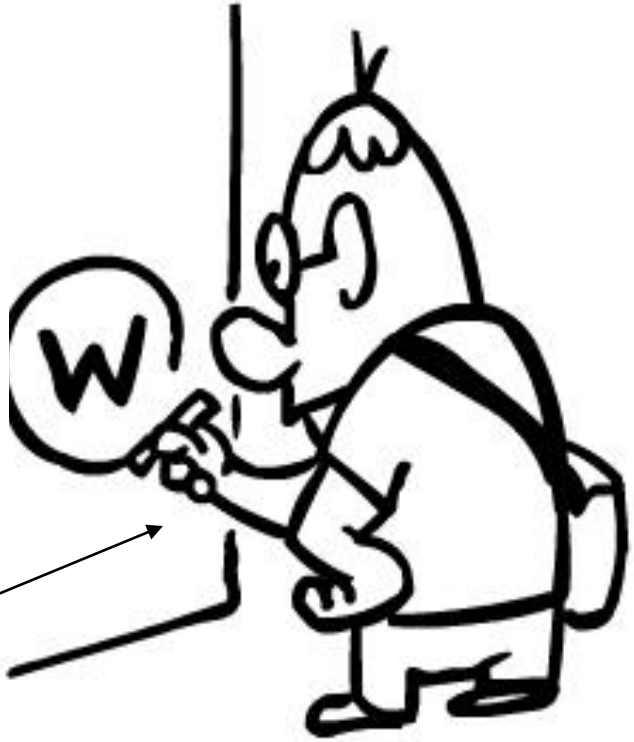




http://wardriving.legionowo.eu.org/mapy/wawka-20040914-range.jpg

Warchalking cz. 1/2

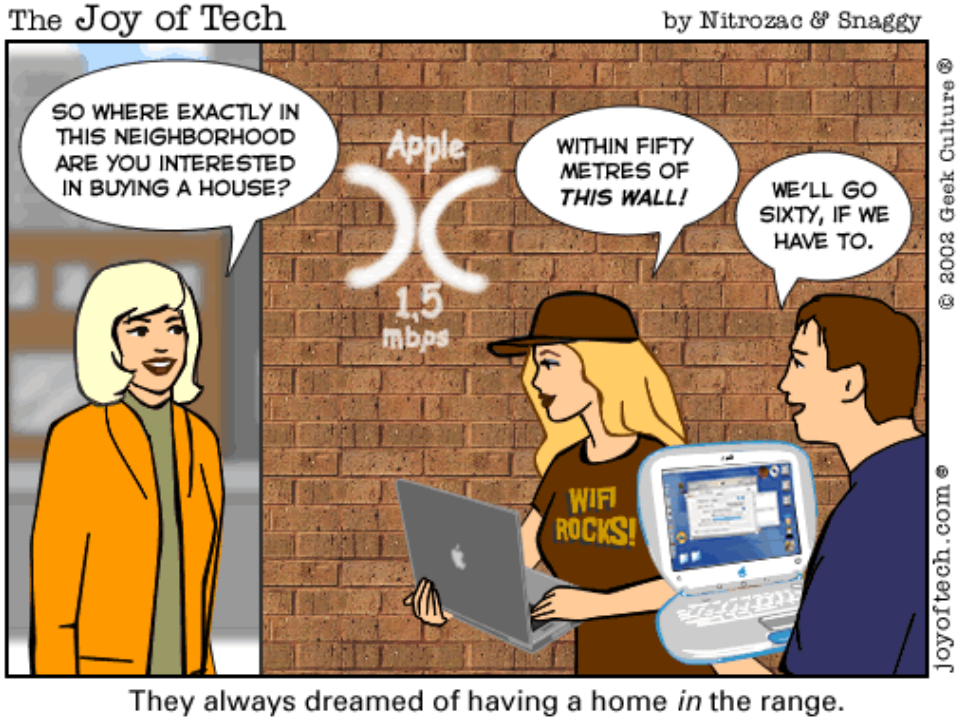




www.warchalking.org

chalk (kreda)

Warchalking cz. 2/2



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

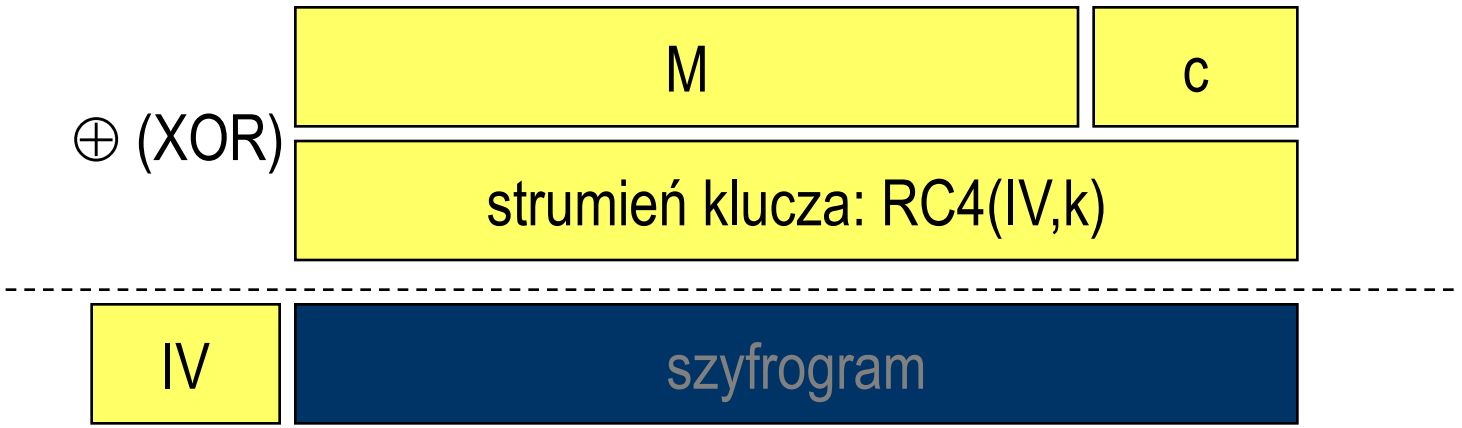
- **Cel:**

  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 ~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 jedna osobę kompromituje całą sieć
- Prostota złamania kluczą po nasłuchu odpowiedniej liczby ramek

- Rozwiązanie: zastosowanie 802.11i

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

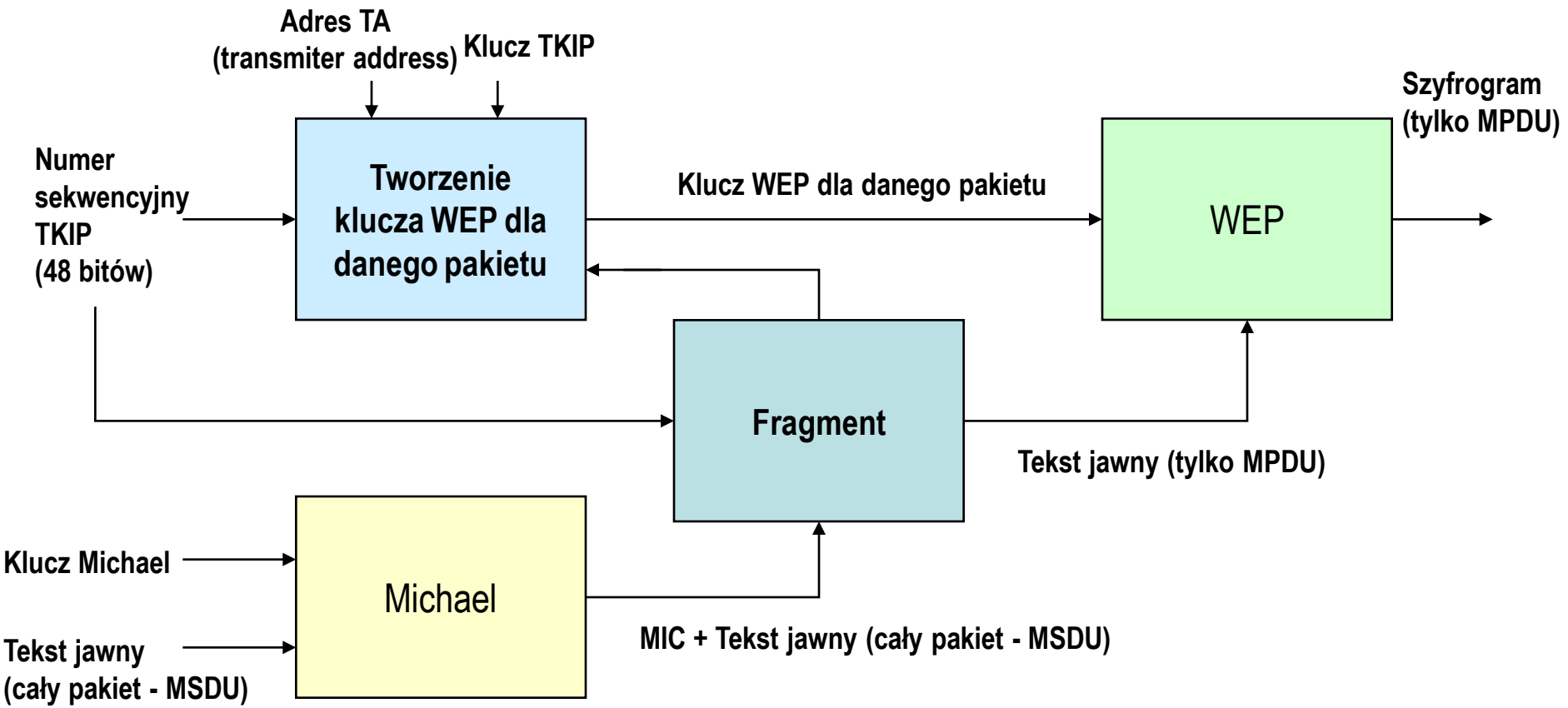
IEEE 802.11i

- 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)



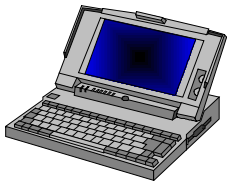
CCMP - cechy

- Opcjonalne rozwiązanie długo-terminowe
- CCMP = **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
- 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)

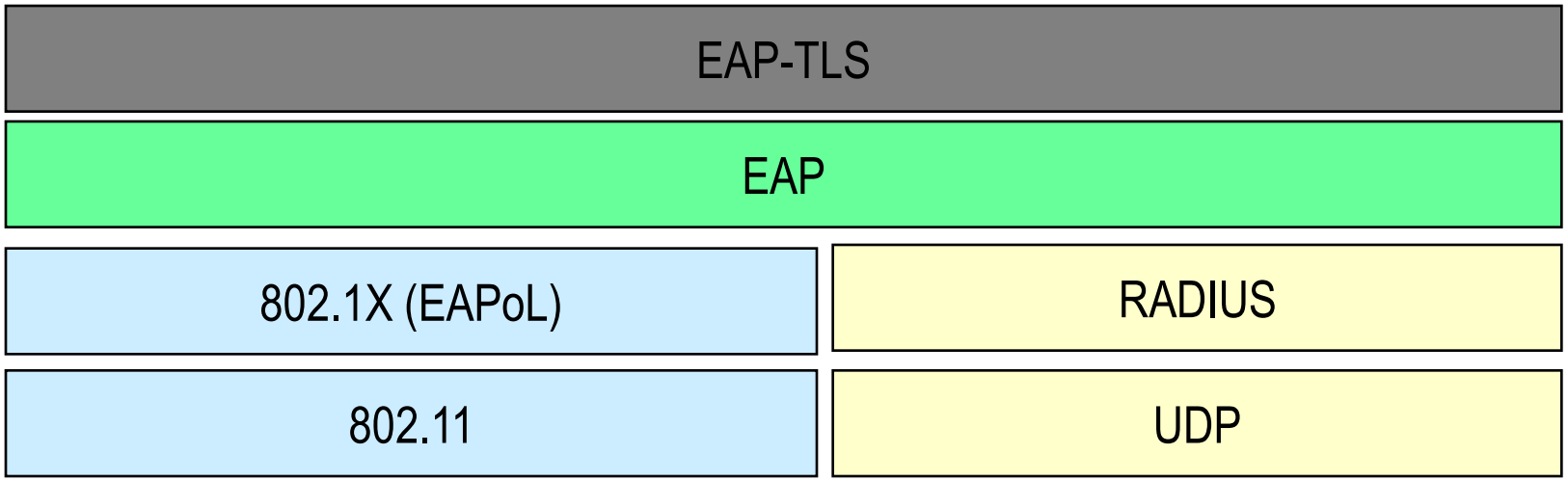
Poszczególne komponenty



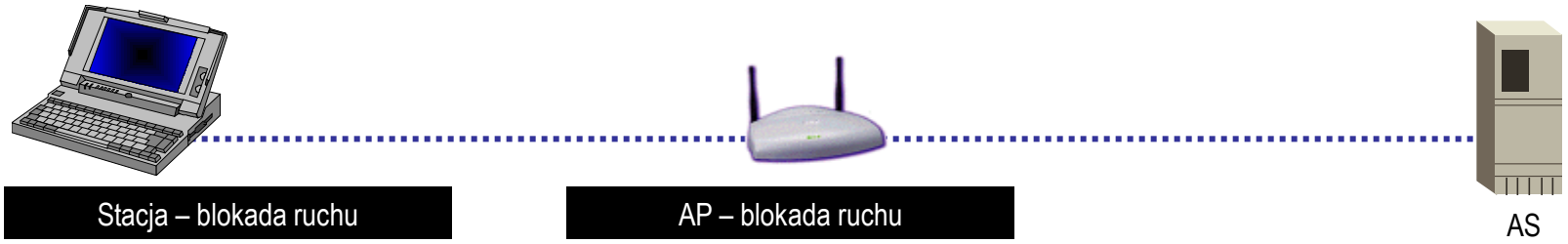
Stacja

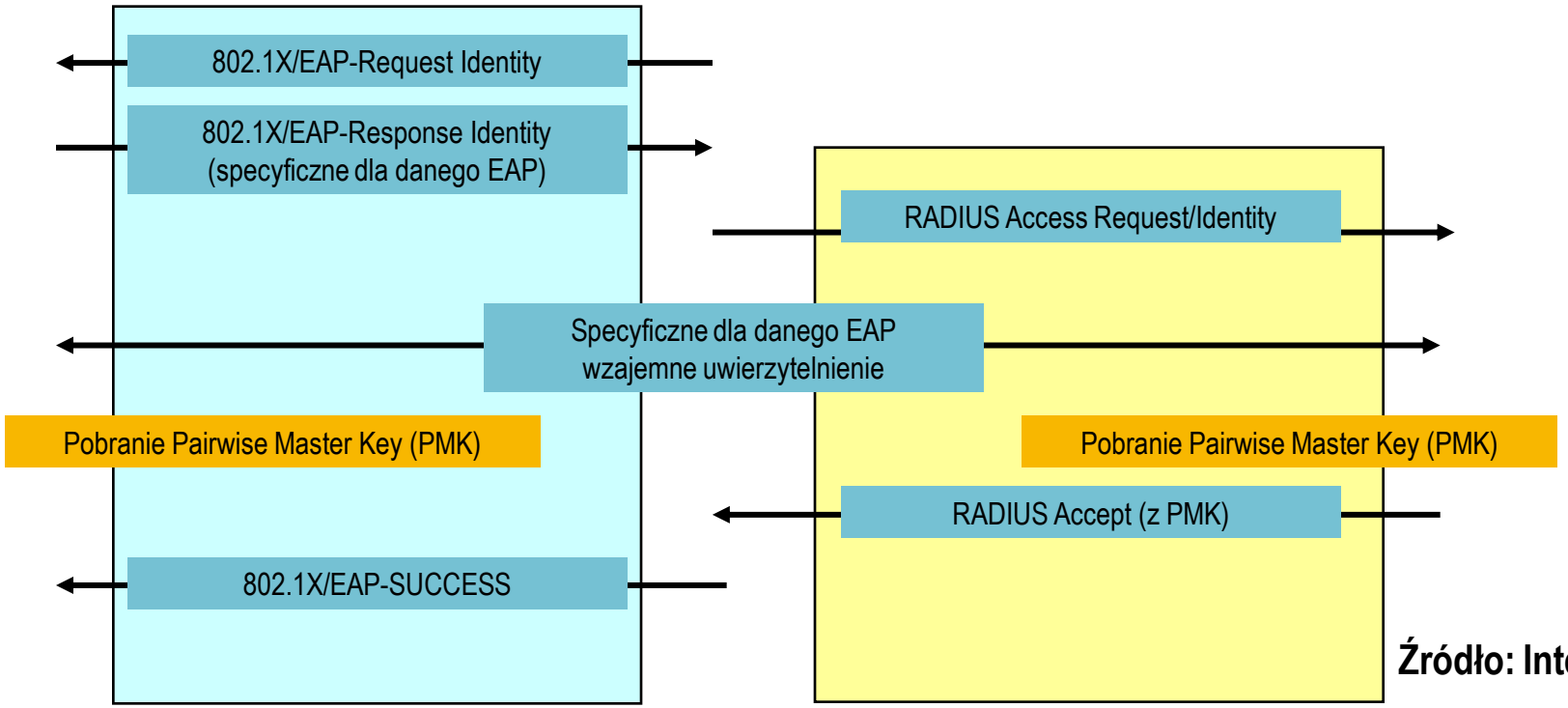
AP

AS



802.1X/EAP – idea działania





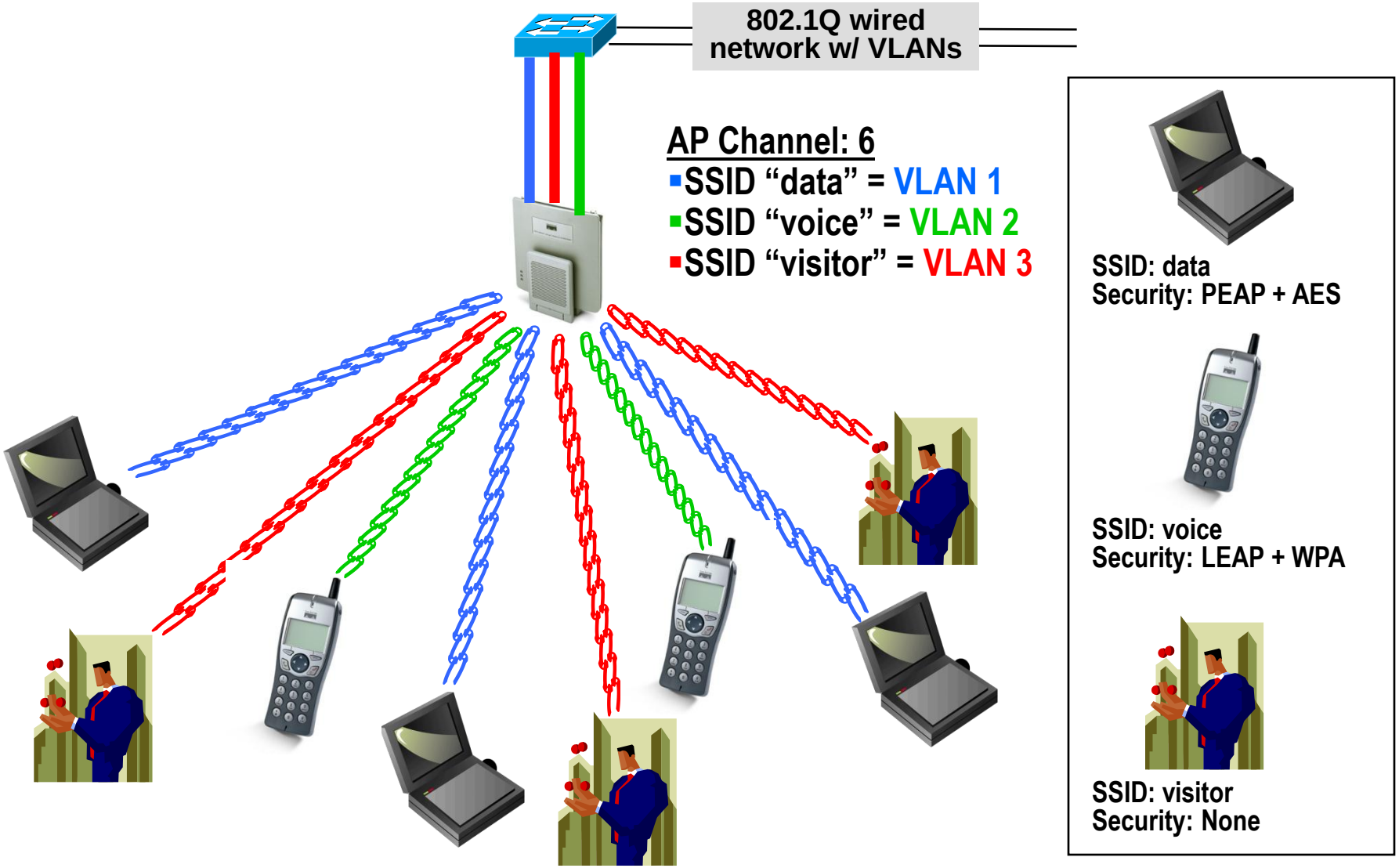
Źródło: Intel

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

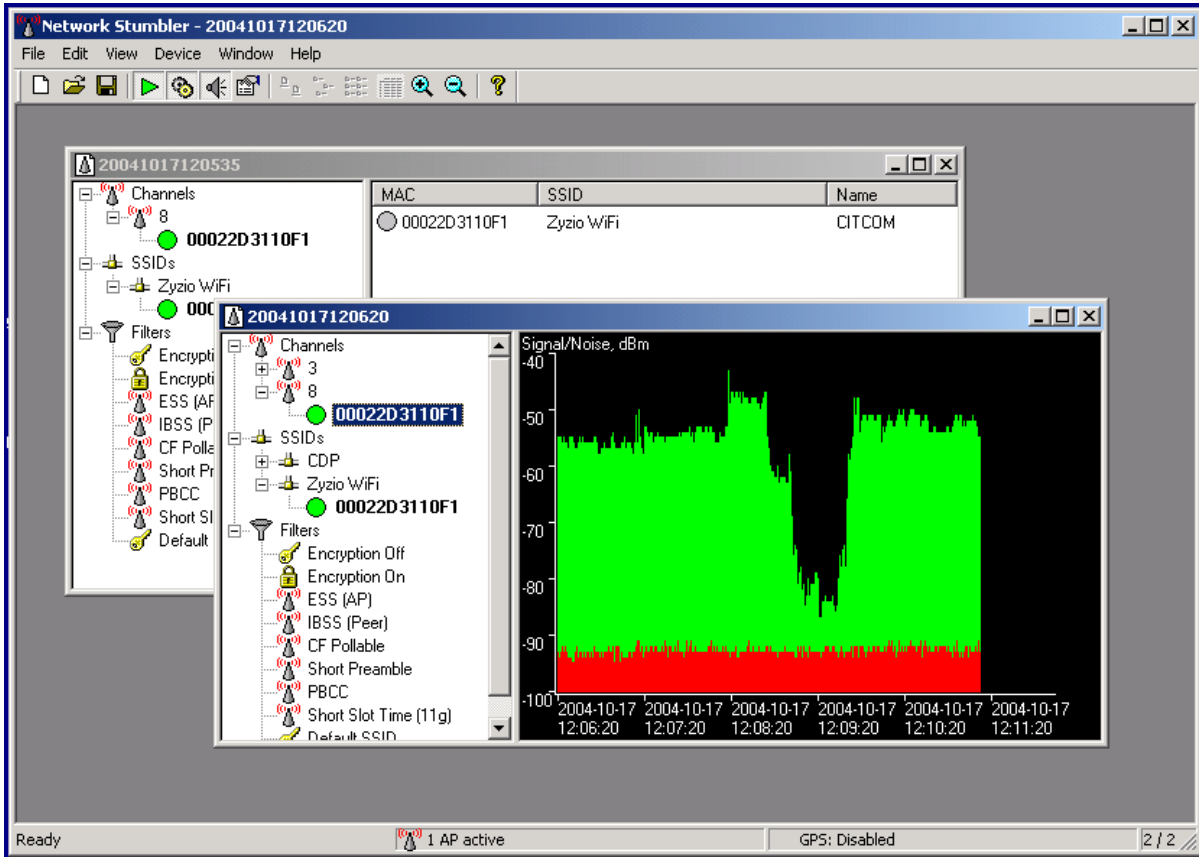
- Wprowadzenie
- Zagrożenia
- Sposoby zabezpieczania
- Przykładowe narzędzia
  - Skanery sieci
  - Programy umożliwiające „łamanie” kluczy
  - Systemy WIDS (Wireless IDS)

Skanery

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

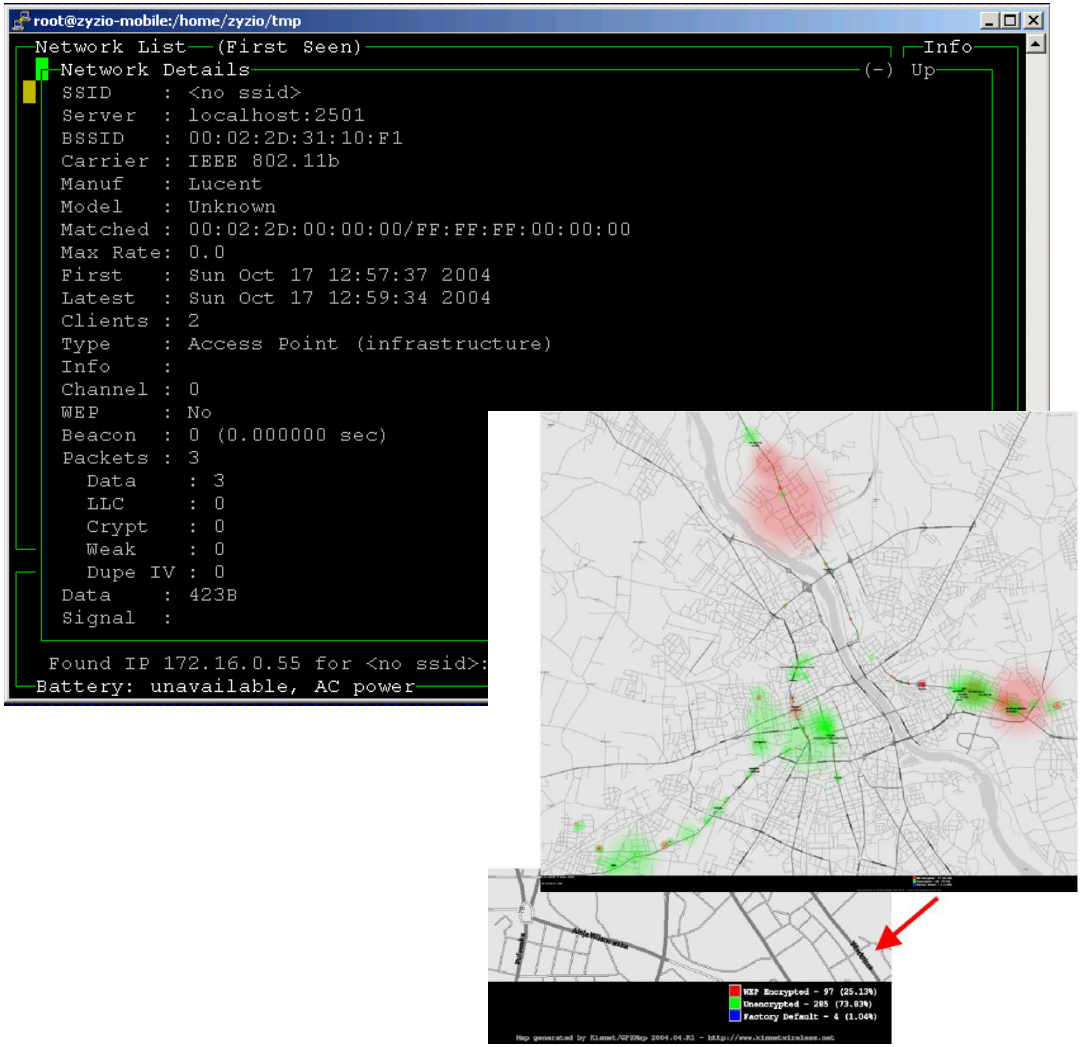
Skanery - Netstumbler

- Skaner aktywny



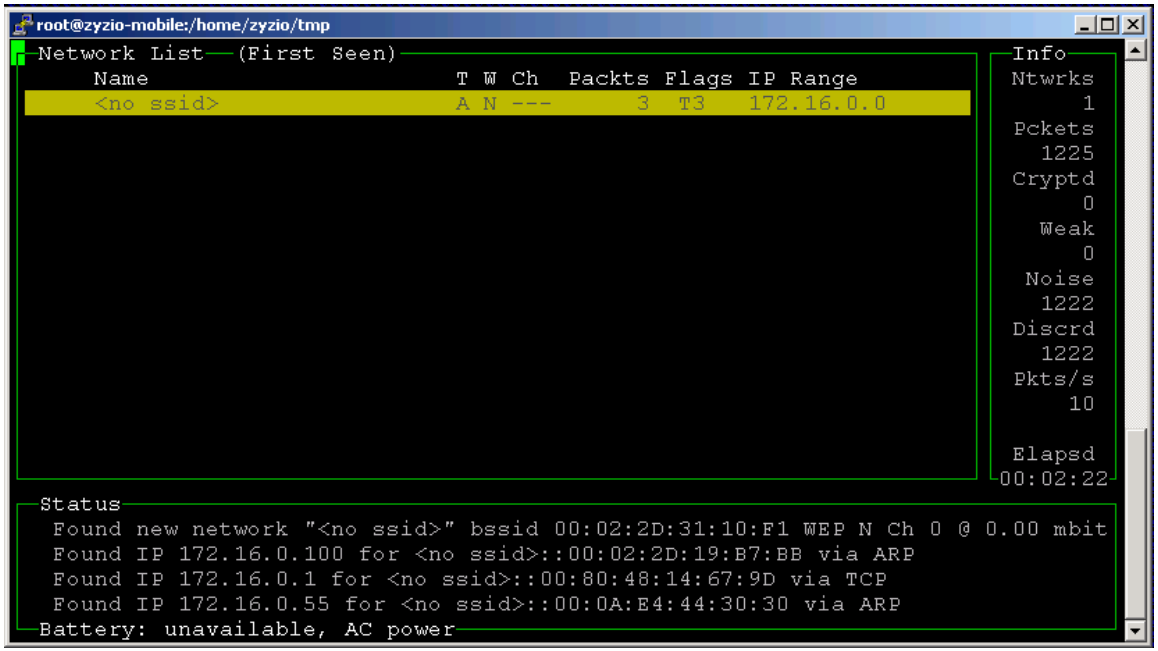
Skanery – Kismet 1/2

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



Skanery – 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)



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 mięć kartę radiową i sterowniki umożliwiające dostęp do ramek kontrolnych i zarządzających

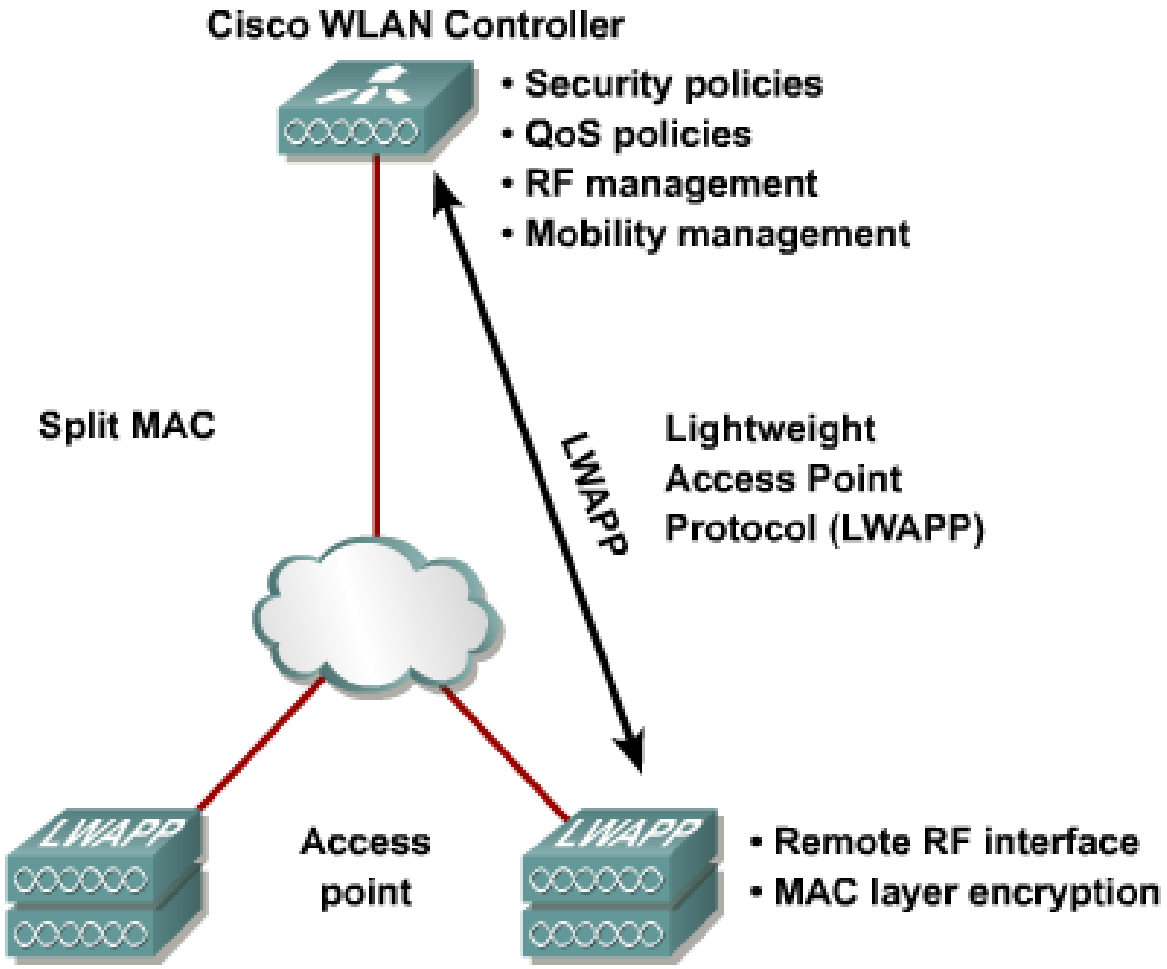
Systemy WIDS 3/3

- 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)

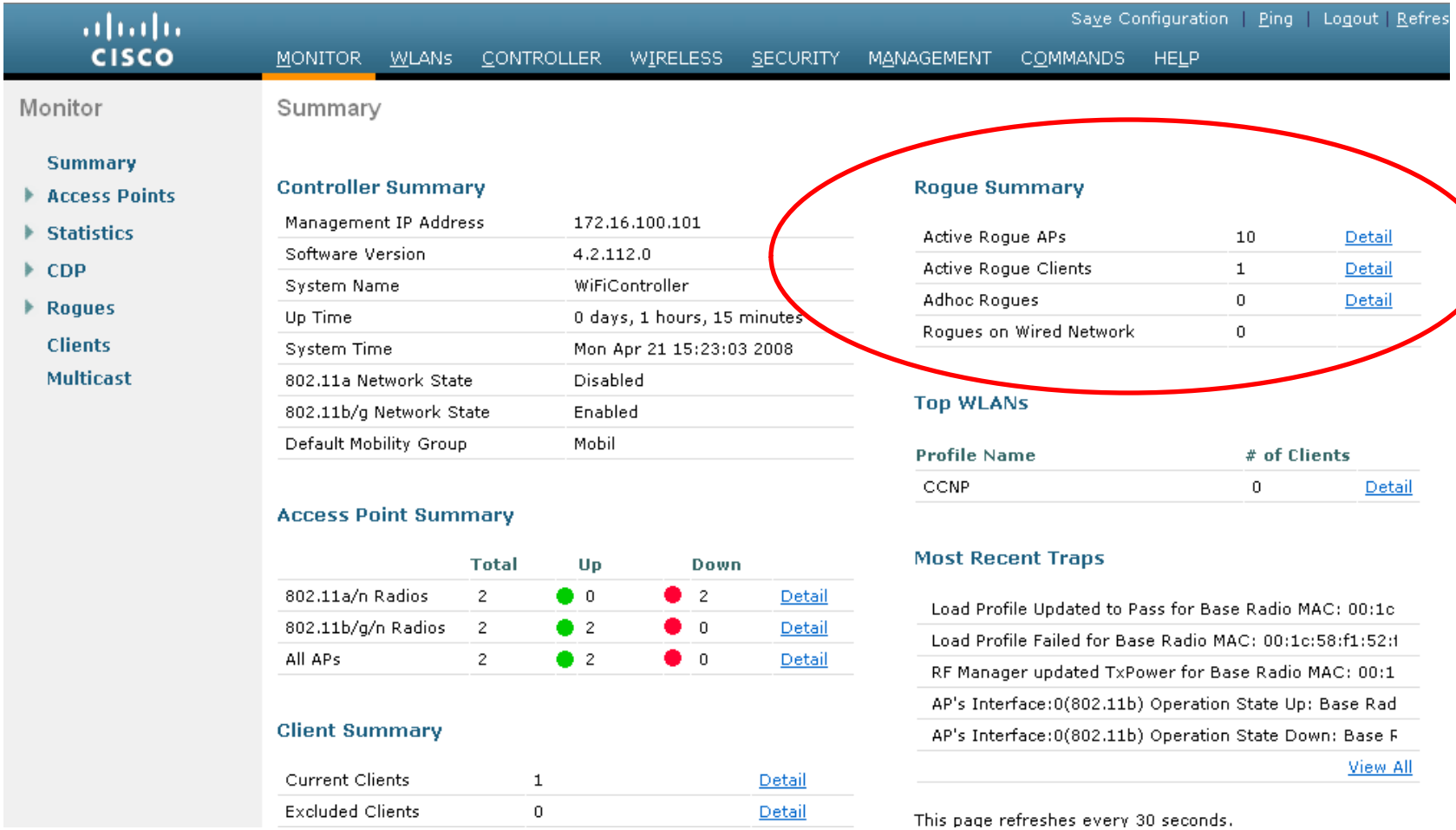
Komercyjne

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

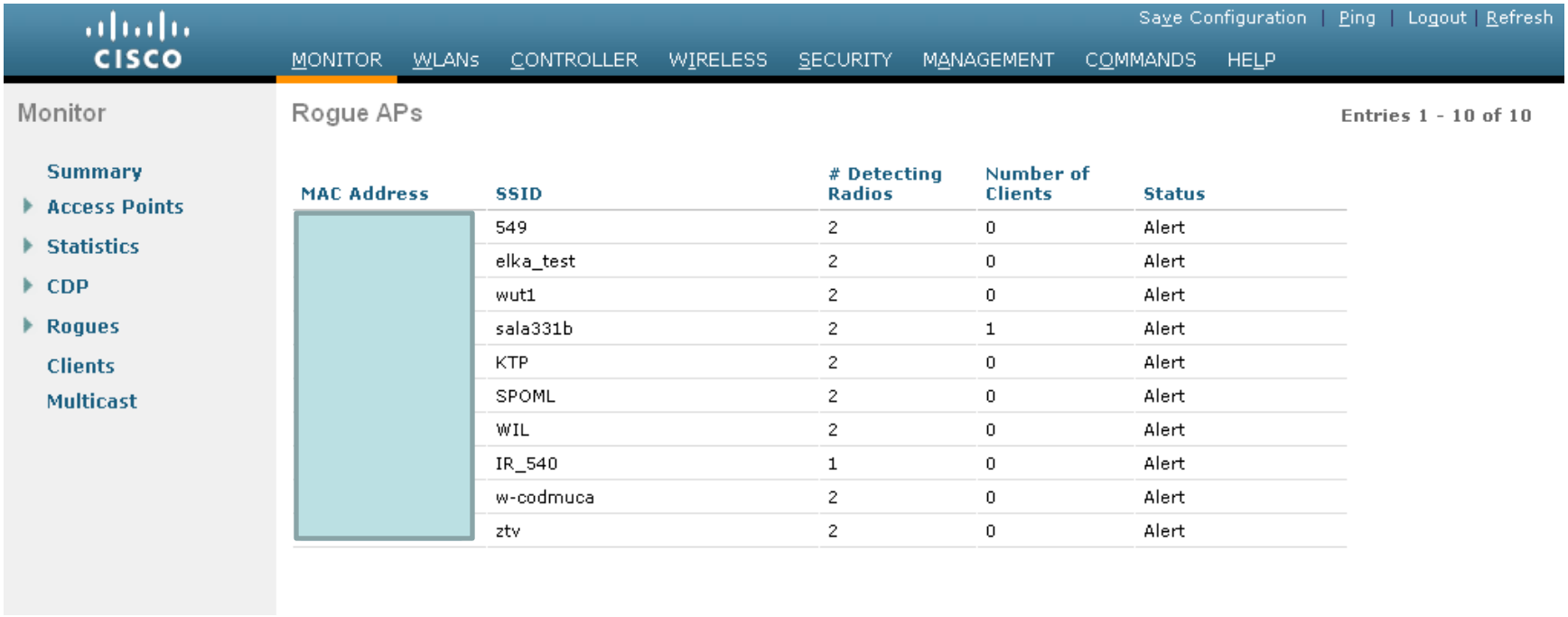
WiFi w oparciu o LWAPP



IDS na kontrolerze 1/3



IDS na kontrolerze 2/3



IDS na kontrolerze 3/3