Bezprzewodowe sieci lokalne (WLAN) - zagrożenia, standardy bezpieczeństwa

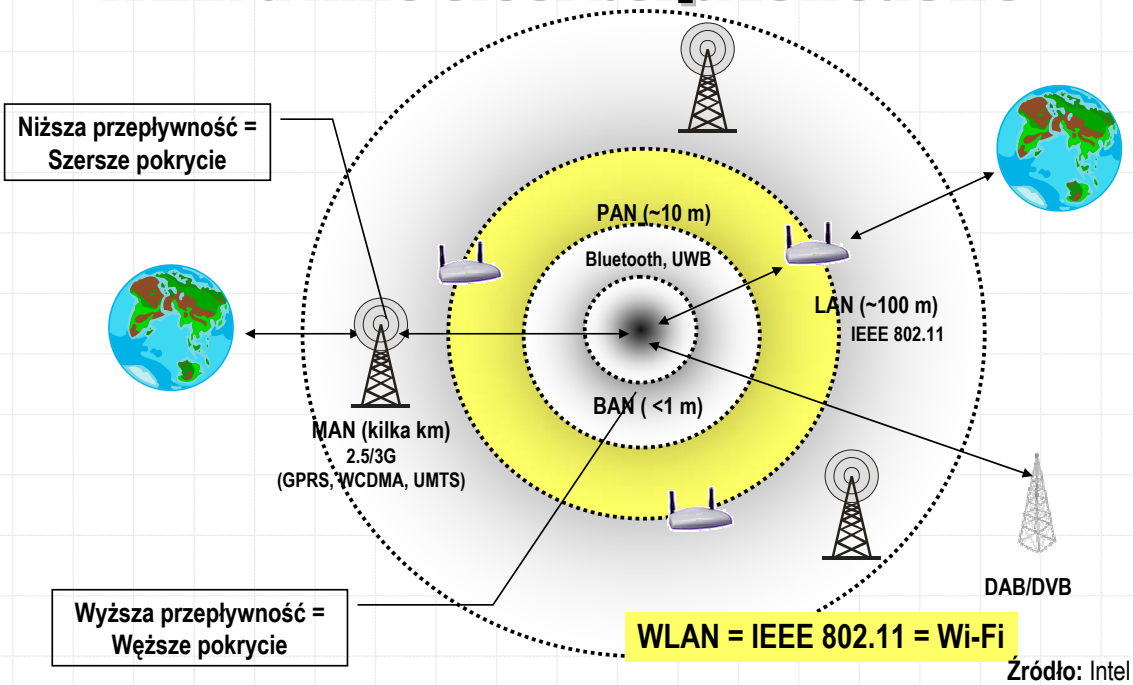
Krzysztof Szczypiorski
Instytut Telekomunikacji PW
E-mail: krzysztof@szczypiorski.com

II Krajowa Konferencja Bezpieczeństwa Biznesu
Warszawa, 10-11 maja 2004

Cele prezentacji

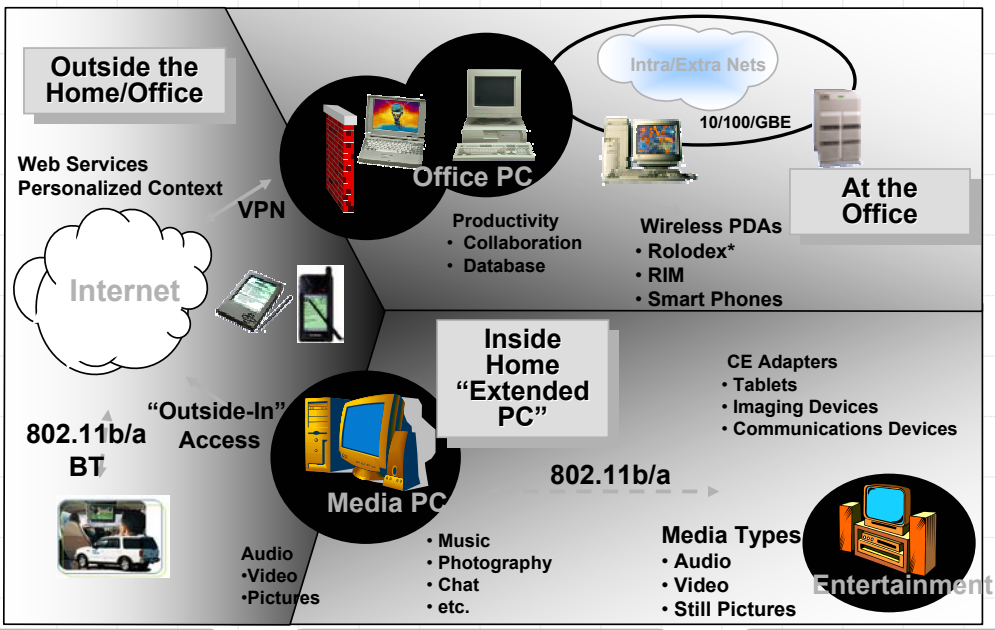
- Przedstawienie zagrożeń związanych z WLAN (Wireless Local Area Networks):
  - Zasięg sieci
  - Mit bezpiecznej warstwy fizycznej
  - Łatwość podsłuchu
  - Ataki parkingowe
  - Kradzieże laptopów
- Stan standaryzacji

WLAN a inne sieci bezprzewodowe

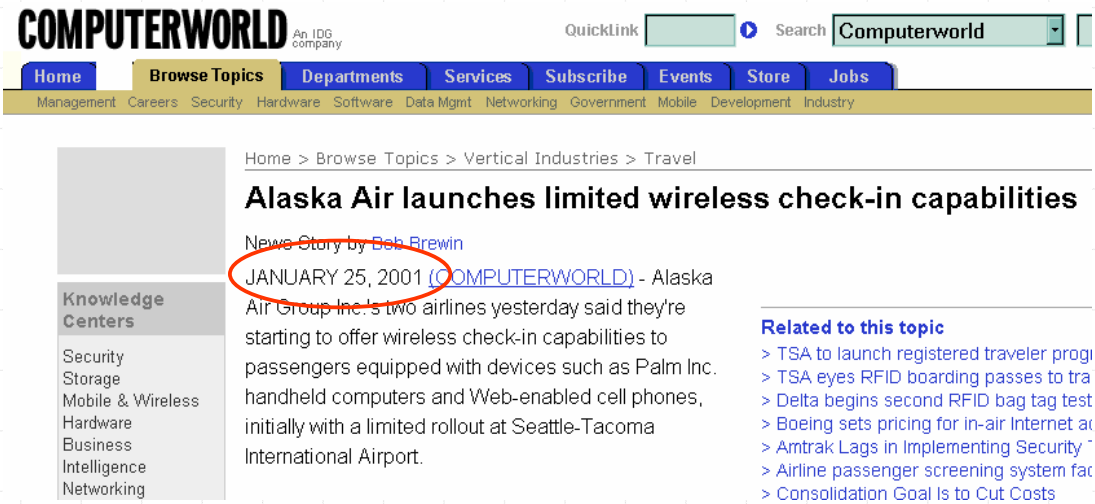


Źródło: Intel

Hasło: „Wireless everywhere”



Źródło: Intel

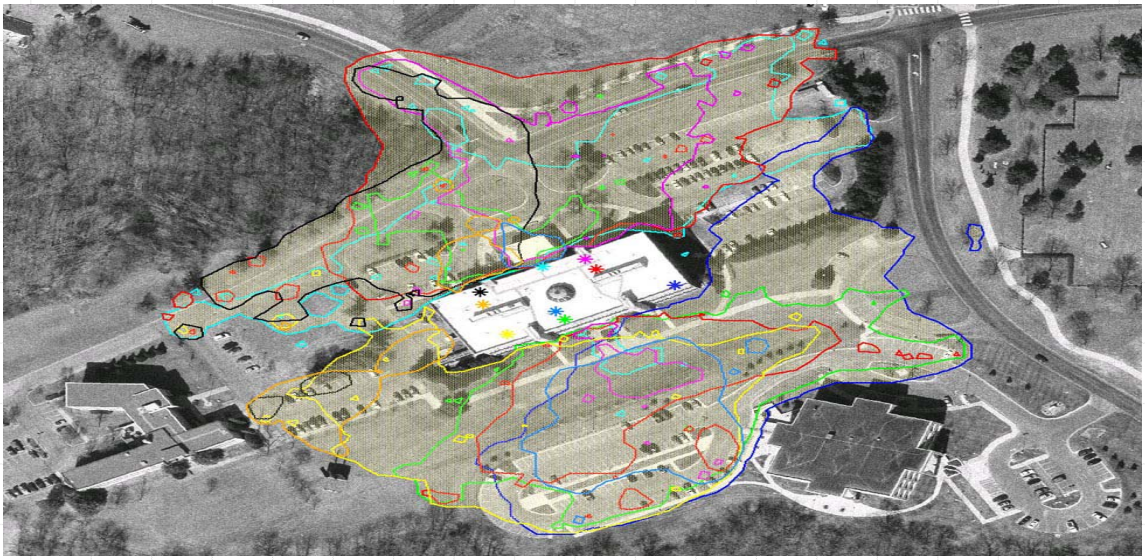

COMPUTERWORLD
An IDG company
QuickLink
Search
Computerworld
Home
Browse Topics
Departments
Services
Subscribe
Events
Store
Jobs
Management Careers Security Hardware Software Data Mgmt Networking Government Mobile Development Industry
Home > Browse Topics > Vertical Industries > Travel
Alaska Air launches limited wireless check-in capabilities
News Story by Bob Brewin
JANUARY 25, 2001 (COMPUTERWORLD) - Alaska Air Group Inc.'s two airlines yesterday said they're starting to offer wireless check-in capabilities to passengers equipped with devices such as Palm Inc. handheld computers and Web-enabled cell phones, initially with a limited rollout at Seattle-Tacoma International Airport.
Knowledge Centers
Security
Storage
Mobile & Wireless
Hardware
Business
Intelligence
Networking
Related to this topic
> TSA to launch registered traveler progr
> TSA eyes RFID boarding passes to tra
> Delta begins second RFID bag tag test
> Boeing sets pricing for in-air Internet a
> Amtrak Lags in Implementing Security
> Airline passenger screening system fa
> Consolidation Goal Is to Cut Costs


U.S. wants Microsoft to widen protoc
ZDNet
Where Technology Means Business
Home
News
Tech Update
White Papers
Downloads
Reviews &
Hardware | Software | Security | Commentary | Headline Archives | Briefs
News Security
Olympics: 802.11 fails to make the cut
By Ben Charny
CNET News.com
February 11, 2002, 9:40 AM PT
Forward in E-MAIL Format for PRINTER
The International Olympic Committee said Monday that equipment based on wireless-networking staple 802.11 won't be used to run operations of any Games until at least 2008 because of security and performance concerns.

Propagacja sygnału radiowego

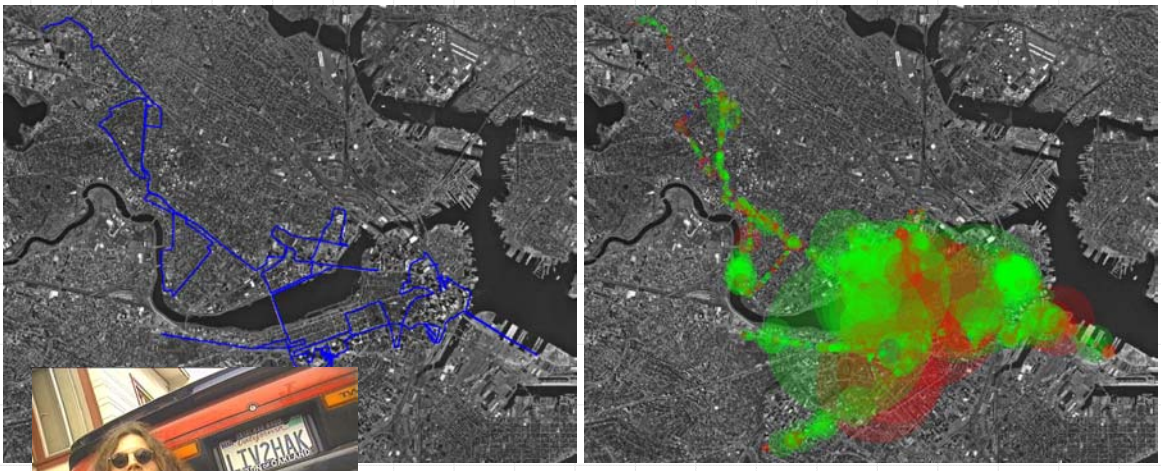
Źródło: David Wagner - Why Swiss-Cheese Security Isn't Enough

Ryzyko ataku z dużej odległości



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

Wardriving, warflying...

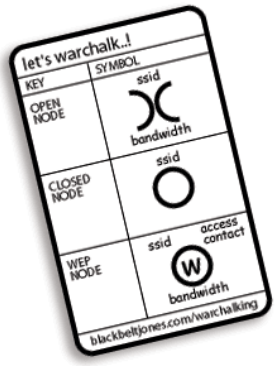


Peter Shipley - prekursor

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

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

Warchalking



www.warchalking.org

chalk (kreda)

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

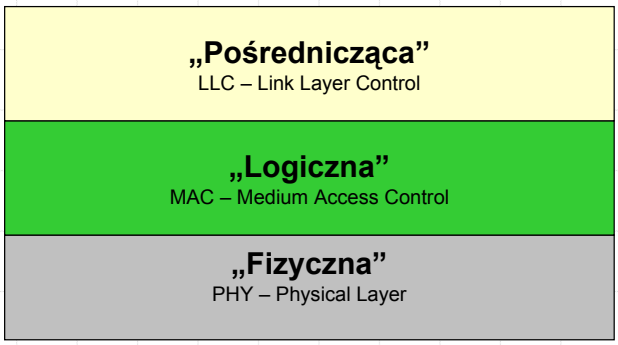
– wiosna – IEEE wydziela w ramach 802.11 grupę (TGi) poświęconą bezpieczeństwu

– 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 (???)

Warstwy WLAN



Mit bezpieczeństwa warstwy fizycznej

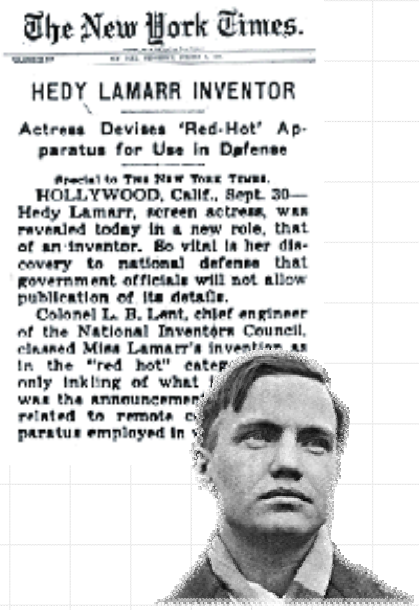
„I can't keep my eyes open - wish I had my radio."
Kate Bush

- 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**

Hedy Lamarr cz. 1/2

- Hedy Lamarr (właściwie Hedwig Eva Maria Kiesler) (1914-2000) - aktorka
- "Ecstasy" (1933) – czesko-niemiecki film; reż. Gustav Machaty
- historia młodej nieszczęśliwej kobiety (Evy) mającej za męża starszego mężczyznę; Eva zakochuje się w Adamie młodym, pełnym życia mężczyźnie
- Pierwsza „naga scena" w historii kinematografii

Hedy Lamarr cz. 2/2



The New York Times.

HEDY LAMARR INVENTOR

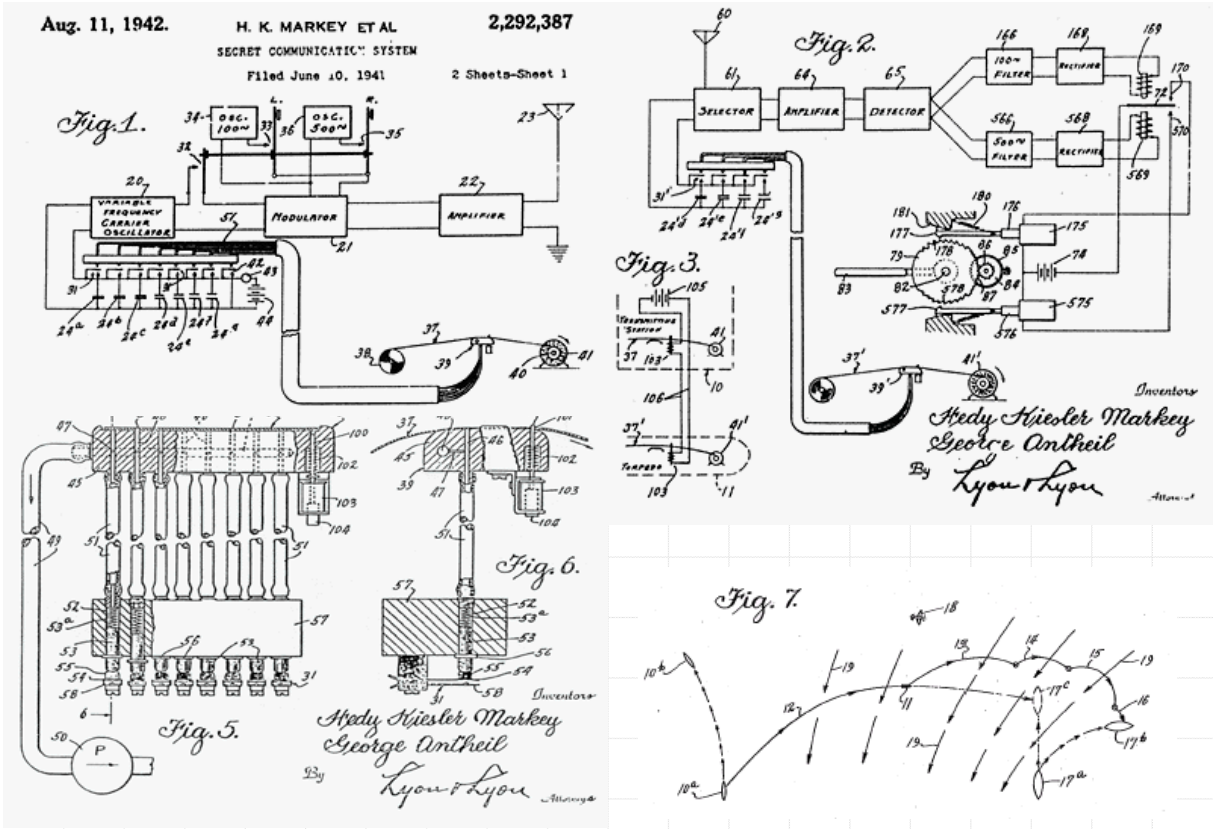
Actress Devises 'Red-Hot' Apparatus for Use in Defense

Special to THE NEW YORK TIMES.

HOLLYWOOD, Calif., Sept. 30—Hedy Lamarr, screen actress, was revealed today in a new role, that of an inventor. So vital is her discovery to national defense that government officials will not allow publication of its details.

Colonel L. B. Lant, chief engineer of the National Inventors Council, classed Miss Lamarr's invention as in the "red hot" categ... only inkling of what ... was the announcemen... related to remote c... paratus employed in ...

- Hedy Lamarr: „Any girl can be glamorous. All you have to do is stand still and be stupid”
- Hedy Lamarr: **wynalazca,** matka współczesnych technik bezprzewowodych – frequency hopping
- Radiowy system sterowania torpedami
- U.S. Patent 2,292,387 – Secret Communications System - (11 sierpnia 1942) wraz z George Antheil
- http://www.hedylamarr.at
- http://silverscreensirens.com/hedy.htm



Aug. 11, 1942. H. K. MARKEY ET AL 2,292,387

SECRET COMMUNICATION SYSTEM

Filed June 10, 1941 2 Sheets-Sheet 1

Fig. 1.

Fig. 2.

Fig. 3.

Fig. 5.

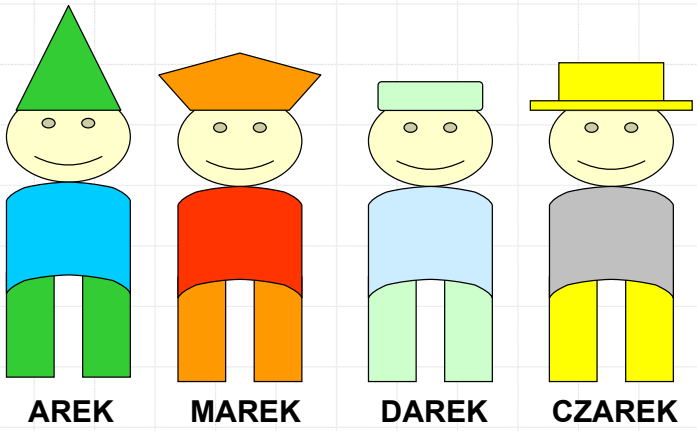
Fig. 6.

Fig. 7.

Inventors
Hedy Kiesler Markey
George Antheil
By Lyon & Lyon

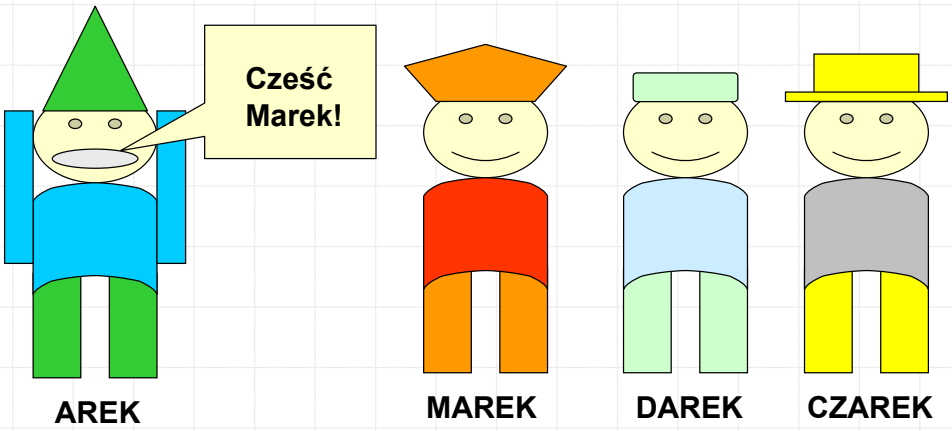
Warstwa logiczna cz. 1/8

Podstawowa metoda dostępu do medium transmisyjnego (kanału radiowego):
CSMA/CA (**C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **A**voidance)



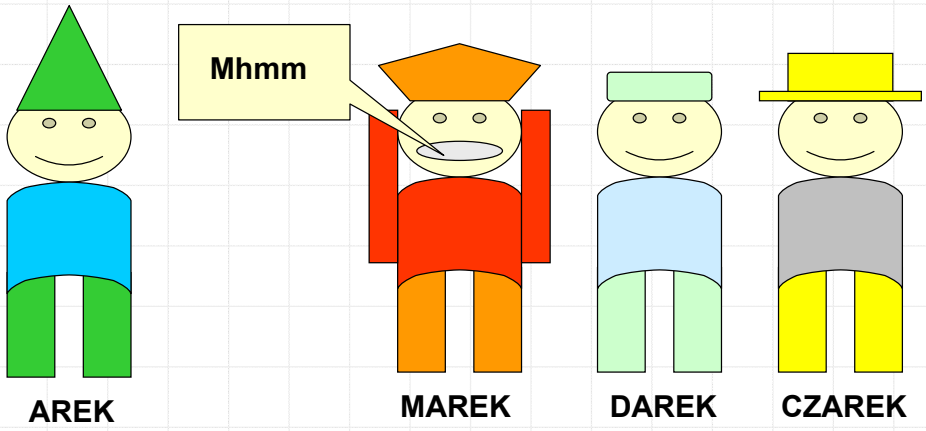
W kanale radiowym wszystkie stacje znajdujące się w zasięgu mogą słyszeć się nawzajem.

Warstwa logiczna cz. 2/8



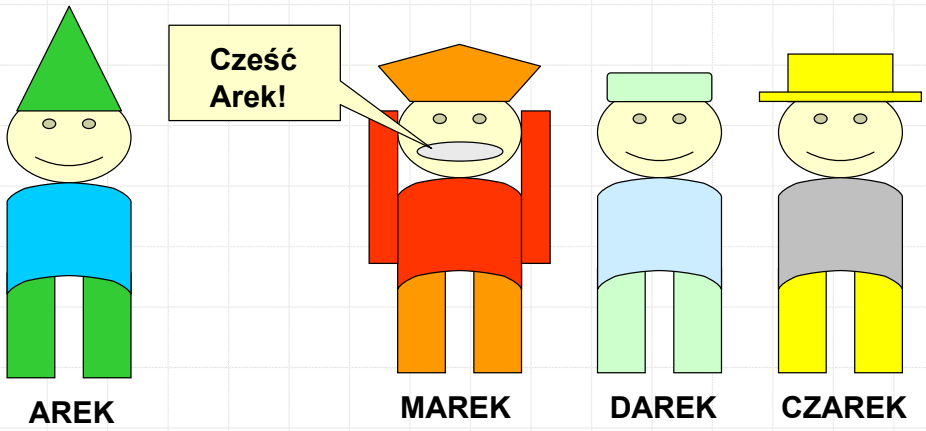
Arek sprawdza, czy nikt nie mówi, zatyka uszy (dlaczego?) i wita się z Markiem.

Warstwa logiczna cz. 3/8



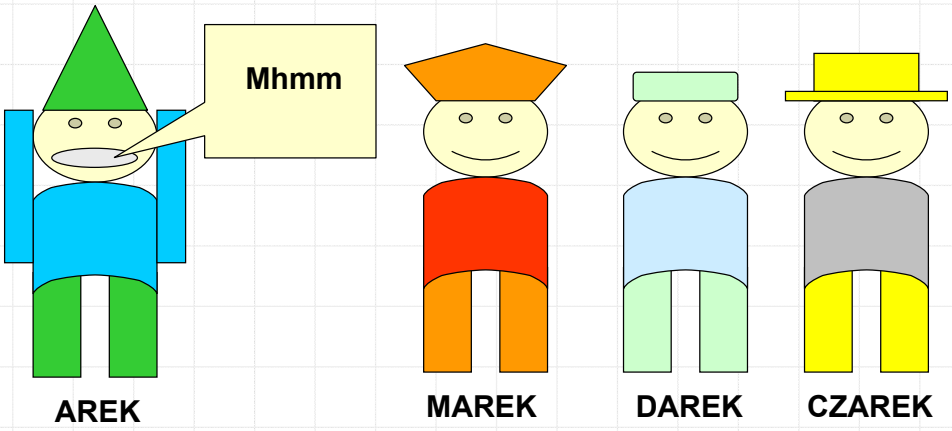
Marek sprawdza, czy nikt nie mówi, zatyka uszy i potwierdza, że usłyszał Arka.

Warstwa logiczna cz. 4/8



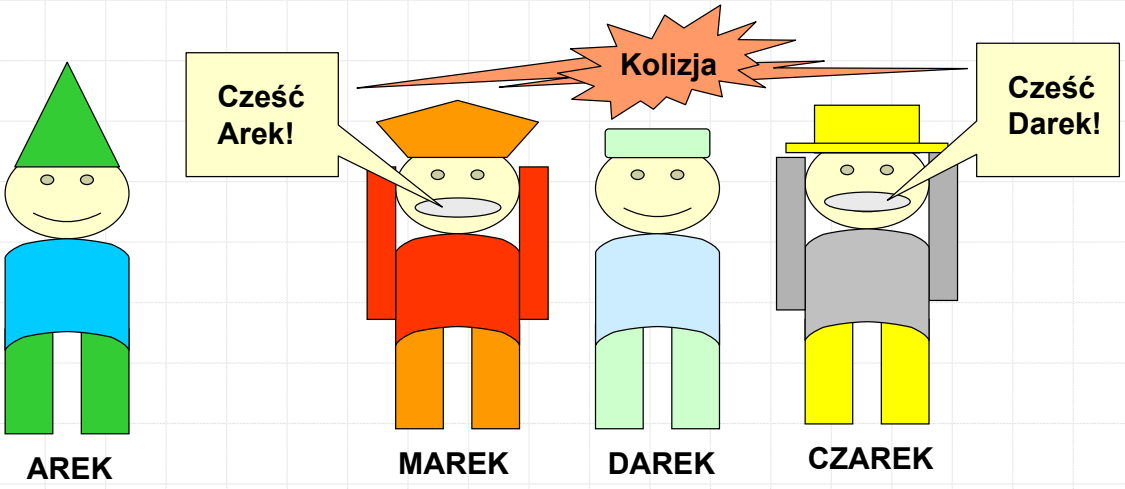
Sytuacja 1: Marek sprawdza, czy nikt nie mówi, zatyka uszy i kontynuuje rozmowę z Arkiem.

Warstwa logiczna cz. 5/8



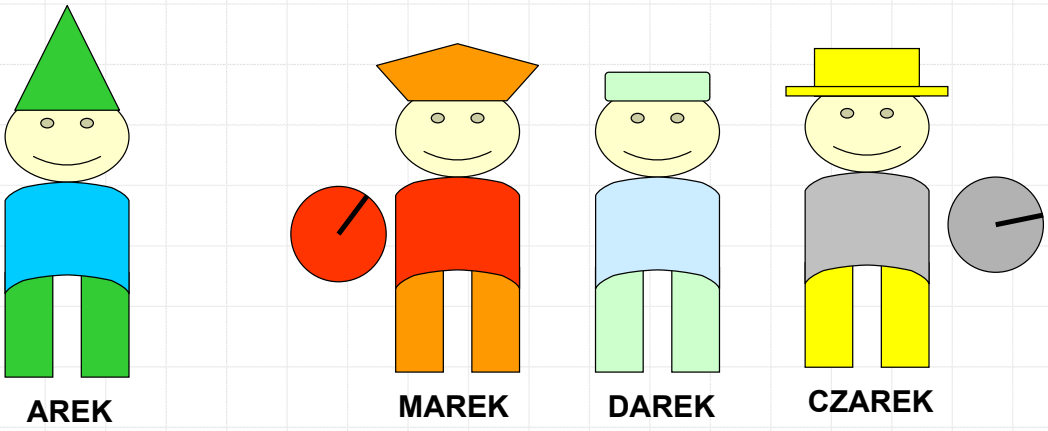
Sytuacja 1: Arek sprawdza, czy nikt nie mówi, zatyka uszy i potwierdza, że usłyszał Marka.

Warstwa logiczna 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.

Warstwa logiczna cz. 7/8

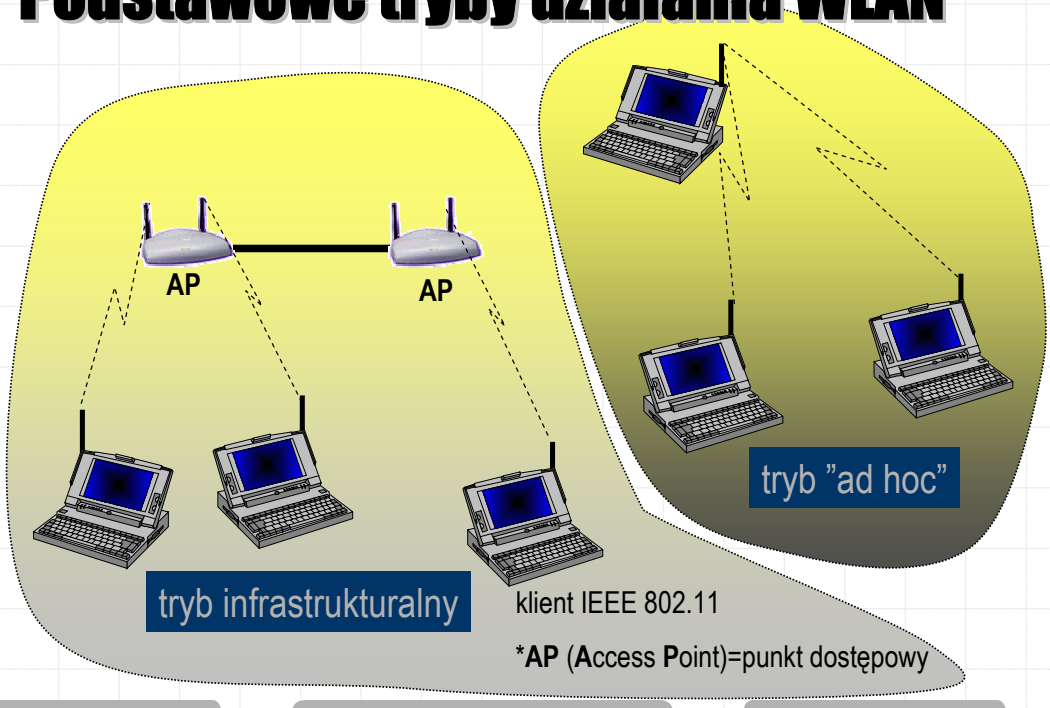


Sytuacja 2: Nikt nic nie potwierdza. Panowie, którzy mówili coś, a nie dostali potwierdzenia, milczą przez chwilę.

Warstwa logiczna 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**

Podstawowe tryby działania WLAN



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

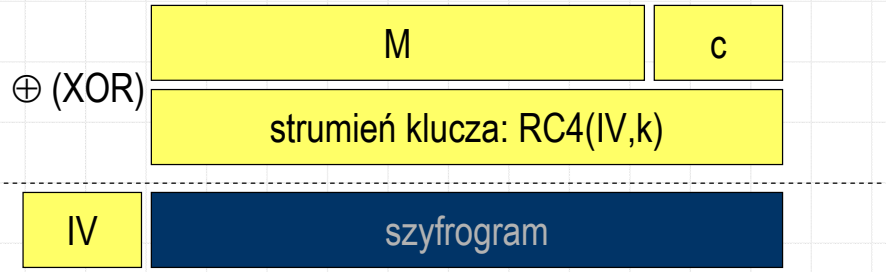
- **siła** w tajności klucza
- **samosynchronizacja** algorytmu ze względu na charakter warstwy łącza danych (“best effort” i duża bitowa stopa błędów w kanale radiowym ~10^{-5})
- **efektywność** w sprzęcie i oprogramowaniu
- **eksportowalność** algorytmu poza USA
- **opcjonalność** – implementacja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



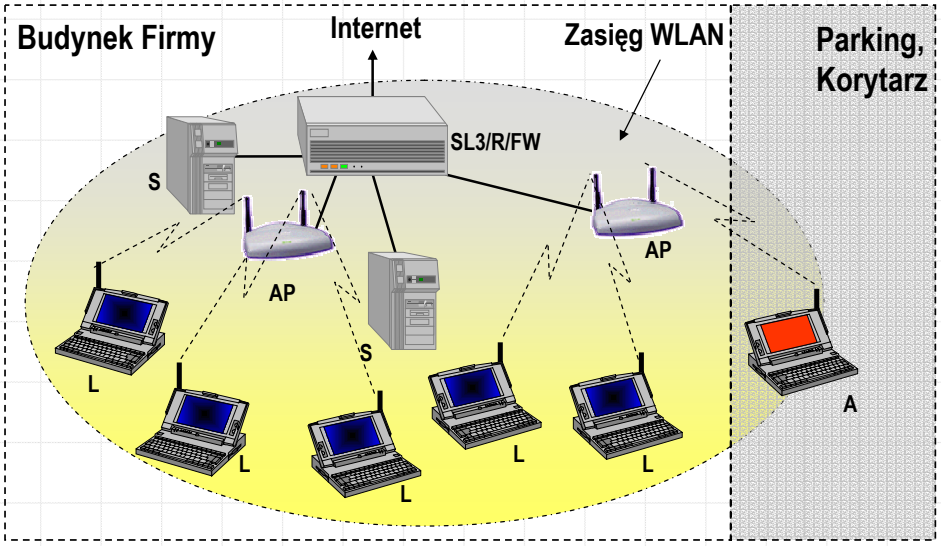
Przeszukiwanie przestrzeni klucza

- autor: Tim Newsham
- jeden z najefektywniejszych pod względem szybkości ataków
- atakujący posiada zestaw kluczy:
  - przechwycenie ramki 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 (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”

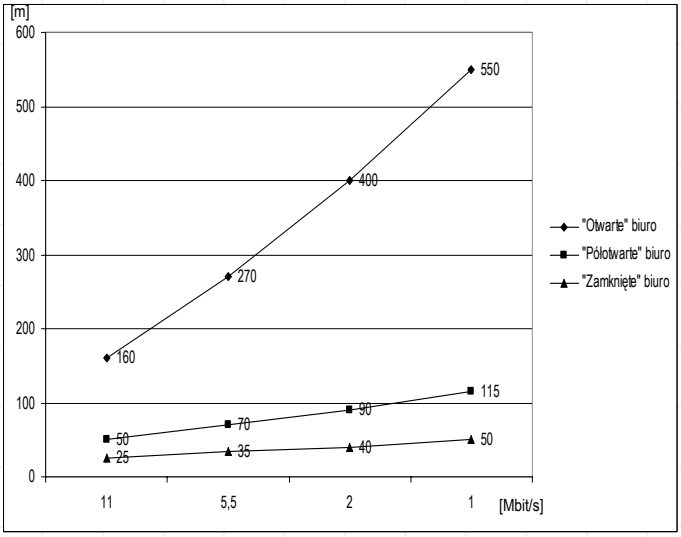
Atak parkingowy cz. 1/6



SL3/R/FW	Switch Layer 3/Router + Firewall	**L**	Legalny klient sieci IEEE 802.11
S	Serwer	**A**	Atakujący klient IEEE 802.11
AP	Punkt dostępowy		

Atak parkingowy cz. 2/6

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



Dane: Instrukcja obsługi Avaya Wireless PC Card

Atak parkingowy cz. 3/6

Atak parkingowy cz. 4/6

Atak parkingowy 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 (wykrywają to dobre systemy wykrywania włamań!)
  - punkt dostępowy będący w zasięgu wysyła:
    - swoją nazwę
    - numer kanału radiowego
    - **ESSID** – **E**xtended **S**ervice **S**et **ID**
    - adres MAC
  - narzędzia np. NetStumbler m.in. dla Windows, iPaq oraz Kismet dla Linuxa

Atak parkingowy cz. 6/6

- **Faza III:** uruchomienie protokołu warstw wyższych
  - **DHCP** (**D**ynamic **H**ost **C**onfiguration **P**rotocol)
  - lub podsłuch pakietów za pomocą sniffera aby określić nieużywany adres IP (narzędzie: np. Ethereal dla Linuxa)
  - ale jeśli jest uaktywniony WEP (**połowa przypadków!**):
    - narzędzia: AirSnort, WEPcrack
- **Faza IV:** praca w sieci
    - jeśli wszystko się powiedzie – praca jako pełnoprawny użytkownik sieci

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)

Teraźniejszość

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

Przyszłość!!!

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

802.1X/EAP

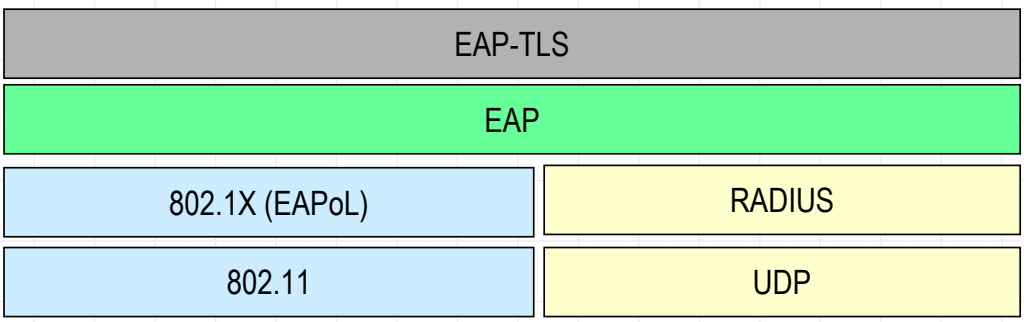
- Użycie zmodyfikowanego na potrzeby IEEE 802.11 szkieletu zarządzania kluczami 802.1X
- Nowy model:
  - **Pairwise Master Key (PMK)**
  - AP i stacja używają PMK aby ustanowić **Pairwise Transient Key (PTK)**
  - PTK jest używany do ochrony łącza
- Extensible Authentication Protocol (EAP)
  - EAPoL – EAP over LANs
  - EAP-TLS
  - EAP-TTLS
  - EAP-PEAP

Poszczególne komponenty

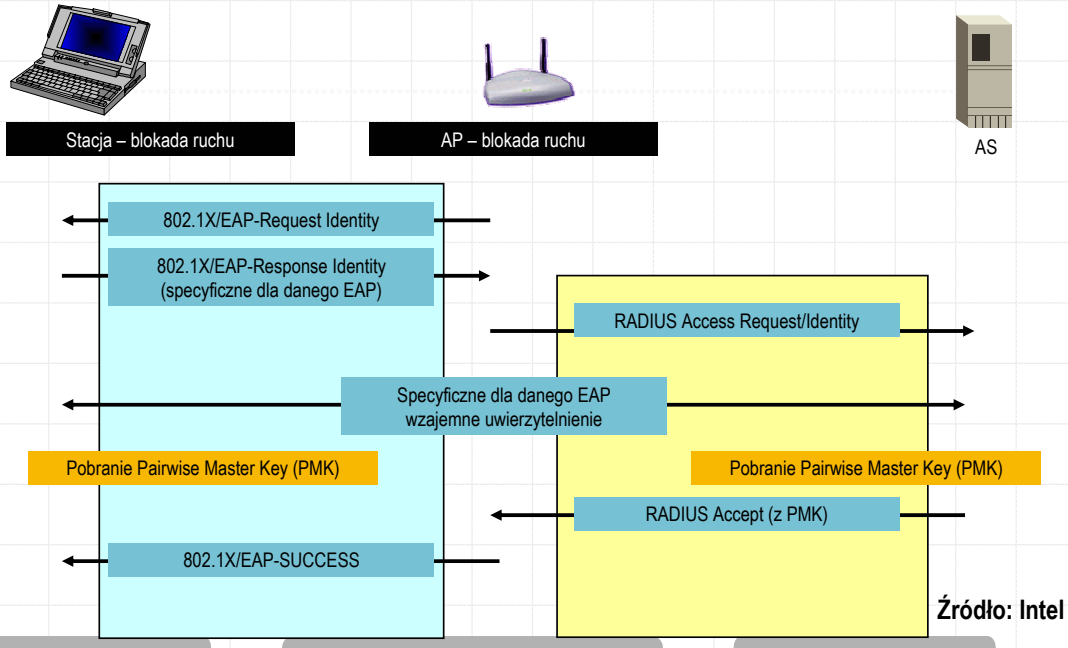
Stacja

AP

AS



802.1X/EAP – idea działania



Źródło: Intel

Wi-Fi Protected Access (WPA)

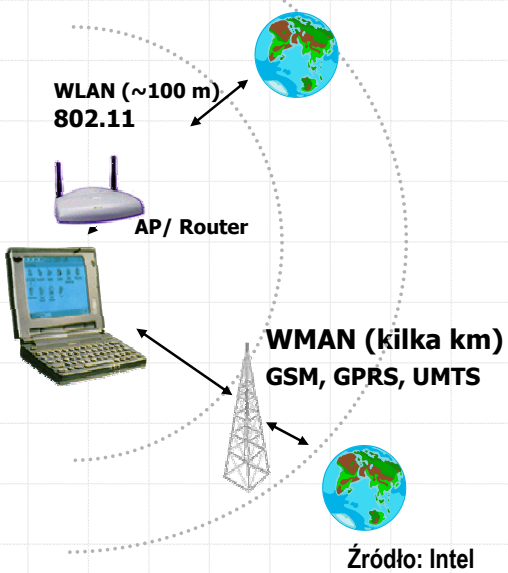
- **WPA:** 2003-2004
  - Od 2003 obowiązkowy przy certyfikacji Wi-Fi
  - Podzbiór standardu 802.11i
    - 802.1X/EAP, TKIP
- **WPA2:** 2004-???
  - 2004 (cezura: testy współpracy 802.11i) – opcjonalny
  - Od 2005 (???) - obowiązkowy
  - W pełni zgodny z 802.11i
    - WPA + Roaming + CCMP

WLAN a ...

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

EAP-SIM - Extensible Authentication Protocol - Subscriber Identity Module

- **WLAN a UMTS**



Źródło: Intel

Podsumowanie

- W obecnej chwili sieci WLAN bez należytych zabezpieczeń stanowią duże zagrożenie w korporacjach
- Standaryzacja wciąż trwa
- Liczne sygnały kompromitujące kolejne rozwiązania (w tym WEP, Cisco LEAP)
- HOT-SPOT = bezprzewodowa kawiarenka internetowa goszcząca wszystkich, którzy znajdują się w zasięgu – miejsce niebezpieczne – wyłączone wszelkie mechanizmy bezpieczeństwa

Pytania?

Krzysztof Szczypiorski
Instytut Telekomunikacji PW
E-mail: krzysztof@szczypiorski.com