Systemy wykrywania włamań dla sieci bezprzewodowych Wi-Fi

Krzysztof Cabaj, Krzysztof Szczypiorski
Politechnika Warszawska
E-mail: K.Cabaj@ii.pw.edu.pl, K.Szczypiorski@tele.pw.edu.pl

Secure 2004, 20-21 października 2004 r.

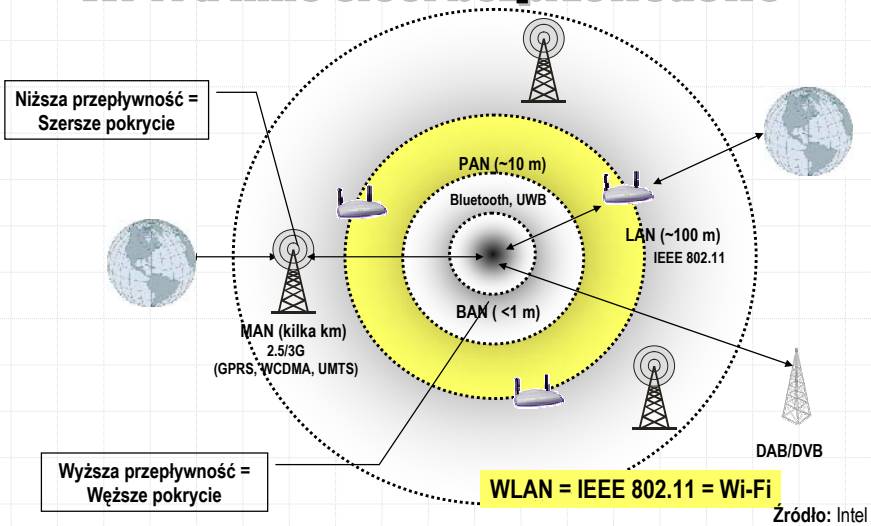
Cel prezentacji

- Przedstawienie praktycznych aspektów zastosowania systemów wykrywania włamań w bezprzewodowych sieciach Wi-Fi
- Teza: w sieciach korporacyjnych powinny być zaimplementowane systemy wykrywania włamań dla sieci Wi-Fi

Główne punkty prezentacji

- Walka z propagacją sygnału radiowego
- Podatności sieci Wi-Fi i znane lekarstwa
- Możliwe zagrożenia w sieci korporacyjnej
- Bezprzewodowi hackerzy vs. bezmyślni pracownicy
- Systemy wykrywania włamań dedykowane dla sieci Wi-Fi
  - WIDZ - Wireless IDS
  - Kismet
  - narzędzia komercyjne

Wi-Fi a inne sieci bezprzewodowe



Źródło: Intel

Propagacja sygnału radiowego

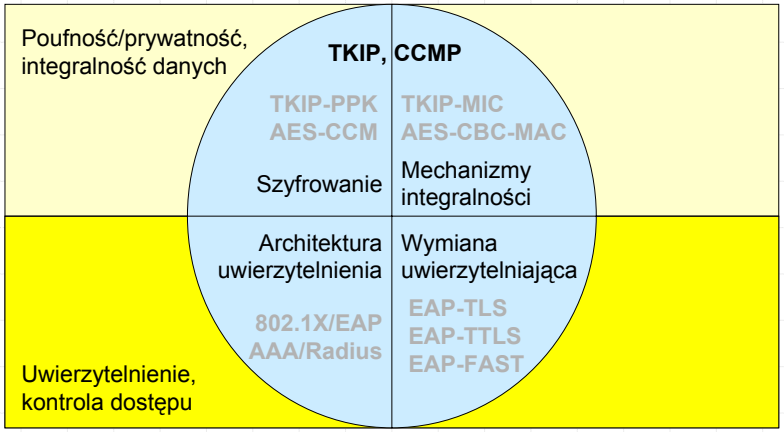
Źródło: David Wagner - Why Swiss-Cheese Security Isn't Enough

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

...i znane lekarstwa

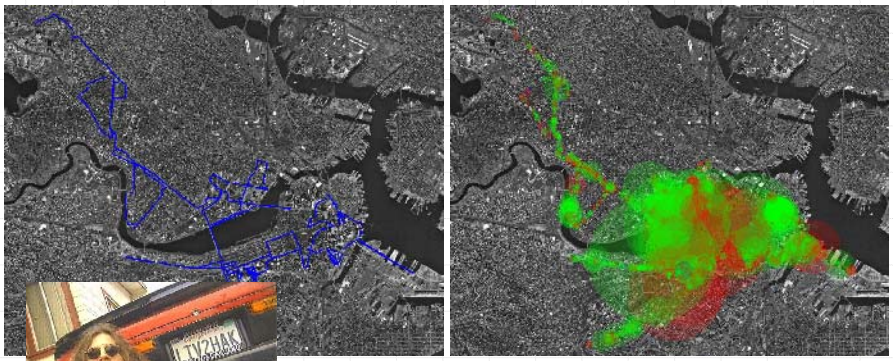
IEEE 802.11i



Możliwe zagrożenia w sieci korporacyjnej

- Dwa najczęściej występujące problemy:
  - **próby włamań przez hackerów** do sieci WiFi **(bezprzewodowi hackerzy)**
    - **pasywni: war (-driving), (-flying)...**
    - **aktywni: warchalking**
  - oraz uruchamianie przez użytkowników **nieautoryzowanych punktów dostępowych**, stających się tylnymi drzwiami do sieci **(bezmyślni pracownicy)**

Wardriving, warflying...

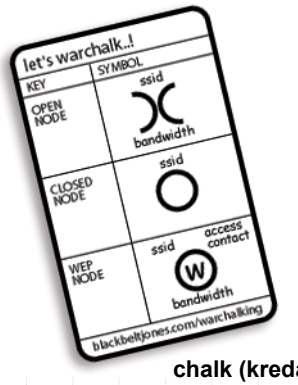


Peter Shipley - prekursor

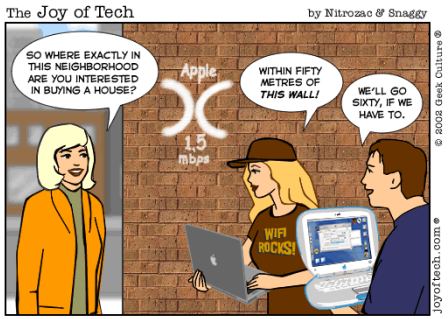
Źródło map: http://www.wardriving.com/**boston**

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

Warchalking



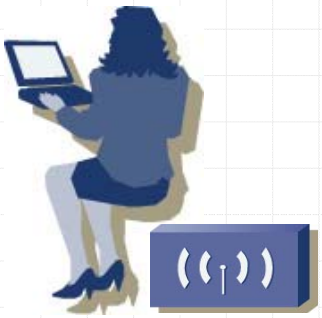
chalk (kreda)



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

Uruchamianie nieautoryzowanych punktów dostępowych

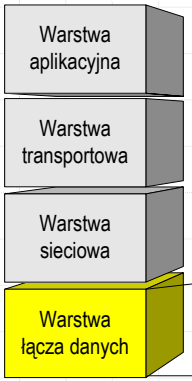
- Nagminnie pracownicy firmy, bez zgody i wiedzy osób odpowiedzialnych za bezpieczeństwo uruchamiają sieci Wi-Fi (tzw. Rogue AP)
- Ma na to wpływ: niska cena tego typu urządzeń oraz prostota instalacji
- Standardowo niebezpieczna konfiguracja (brak zabezpieczeń)
- Sieć korporacyjna staje się dostępna dla każdego posiadacza komputera przenośnego z kartą Wi-Fi



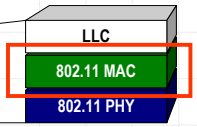
Pani Ania
z działu marketingowego
uruchomiła tzw. Rogue AP

Systemy wykrywania włamań dla sieci bezprzewodowych Wi-Fi

Stos TCP/IP

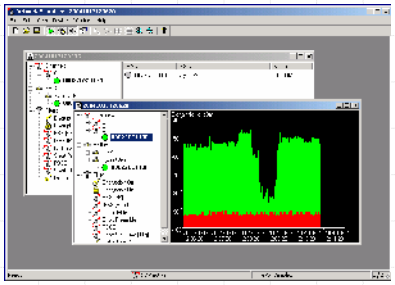


Model sieci LAN
(IEEE LAN RM)



Sygnatury skanerów wireless

- **Skanery aktywne** można wykrywać poprzez sygnatury – charakterystyczne ustawienia pól w ramkach IEEE 802.11
- **SnortWireless** – patch na Snort'a umożliwiający tworzenie sygnatur dla protokołu IEEE 802.11
- **Skanery pasywne** - aktualnie brak możliwości bezpośredniego wykrycia

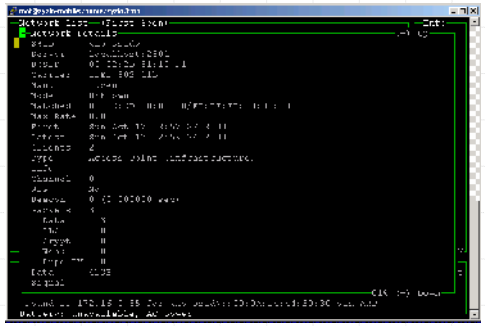


Narzędzia: WIDZ (Wireless IDS)

- Pakiet oprogramowania powstałego jako *"proof of concept"* specjalizowanego IDS dla WiFi- mimo to bardzo pomocny
- Program ***widz_apmon*** posiada dwa tryby pracy
  - Generowanie spisu widzianych AP
  - Monitorowanie środowiska, czy nie pojawiają się inne AP
- Proste rozwiązanie informujące nas o pojawiających się nowych AP. Wykrycie nowego AP może oznaczać …
  - Uruchomienie nieautoryzowanego AP
  - Próba ataku *„man in the middle"*

Narzędzia: Kismet(1/2)

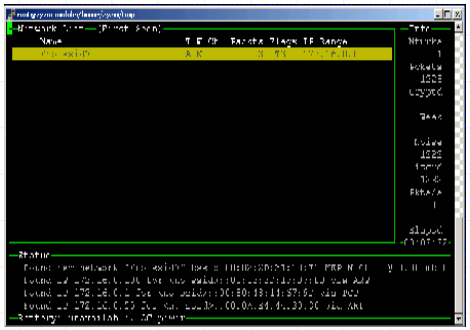
- Zaawansowany **skaner pasywny**
- Funkcje prostego systemu IDS dedykowanego sieciom Wi-Fi
- Możliwość podłączenie odbiornika GPS
- Nanoszenie na dostarczone mapy wykrytych informacji



Narzędzia: Kismet(2/2)

Możliwości programu

- Wykrywanie sieci Wi-Fi, 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)



Inne narzędzia

- **Narzędzia open-source**
  - ***SnortWireless*** (aktualnie rozwijane są nowe preprocesory dla tego systemu IDS)
  - Skanery sieciowe np. ***NetStumbler***
- **Przykładowe narzędzia komercyjne**
  - CiscoWorks Wireless LAN Solution Engine (WLSE)
  - NetworkChemistry

Podsumowanie

- Parafrazując Leonarda Cohena ("There ain't no cure for love"): **"There ain't no cure for Wi-Fi"**
- IEEE 802.11i vs. „piękny umysł" bezmyślnych pracowników
- Walka z nielegalnymi AP przypomina walkę stoczoną w przeszłości z „pracowniczymi" modemami w sieciach korporacyjnych
- Systemy IDS dla sieci Wi-Fi mogą pomóc - należy je stosować **we wszystkich** sieciach korporacyjnych

Pytania?

Krzysztof Cabaj, Krzysztof Szczypiorski

E-mail: K.Cabaj@ii.pw.edu.pl, K.Szczypiorski@tele.pw.edu.pl

Literatura

- Snort, Martin Roesch - http://www.snort.org
- Kismet, Mike Kershaw - http://www.kismetwireless.net/documentation.shtml
- Snort-Wireless, Andrew Lockhart - http://www.snort-wireless.org/
- WIDZ (Wireless IDS), Mark "Fat Bloke" Osborne - http://www.loud-fat-bloke.co.uk/w80211.html
- „Layer 2 Analysis of WLAN Discovery Applications for Intrusion Detection", Joshua Wright - http://home.jwu.edu/jwright/papers/l2-wlan-ids.pdf
- AirJack - http://sourceforge.net/projects/airjack
- NetStumbler, Marius Milner - http://www.netstumbler.com/

+ Krzysztof Cabaj, Krzysztof Szczypiorski: „Systemy wykrywania włamań dla sieci bezprzewodowych Wi-Fi", Materiały: VIII Konferencja Bezpieczeństwa IT Secure 2004, Warszawa 20-21 października 2004