Sieci bezprzewodowe oczami hackera

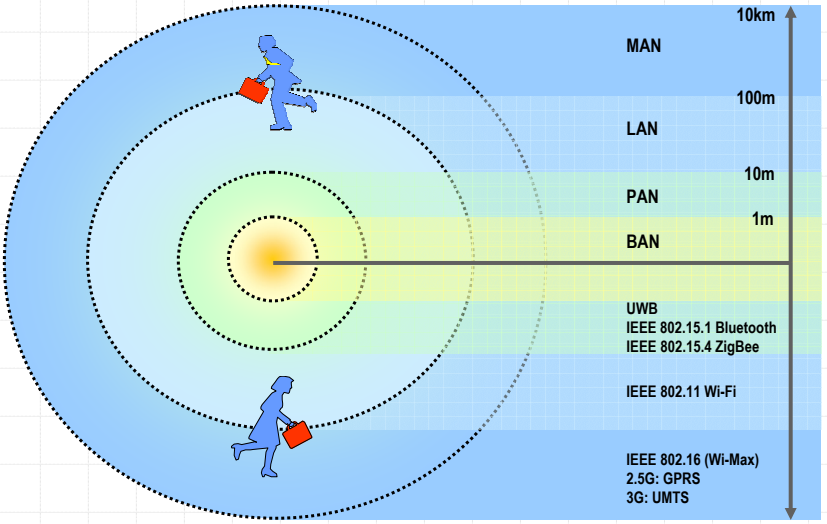
Krzysztof Szczypiorski
E-mail: krzysztof@szczypiorski.com
http://krzysztof.szczypiorski.com

VII Krajowa Konferencja Bezpieczeństwa Sieciowego
"Zabezpieczenia sieci korporacyjnych", 16 listopada 2004 r.

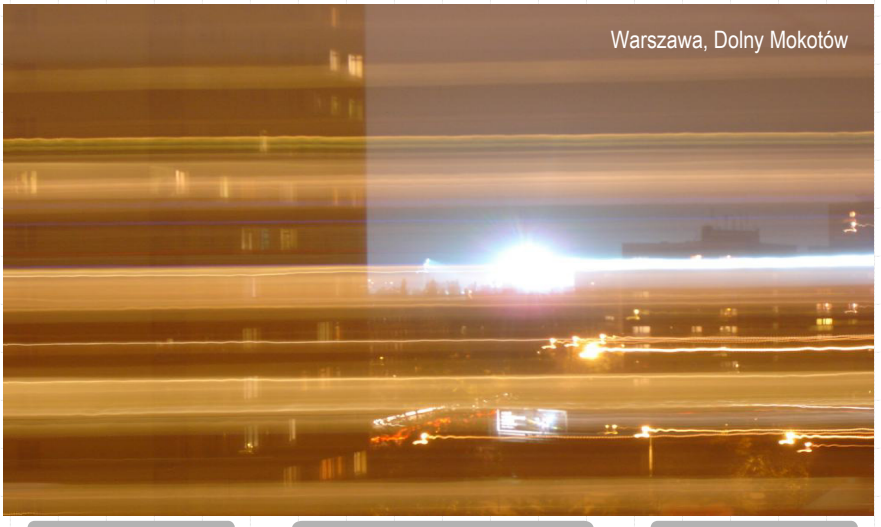
Agenda, czyli 10 pytań

- Jakie sieci bezprzewodowe widzi hacker?
- Czy wszystkiemu winny jest „zasięg”?
- …i jak wygląda ryzyko ataku z dużej odległości?
- Które sieci (nie) są podatne na ataki?
- Które sieci bezprzewodowe interesują hackerów?
- Czy zawsze winni są tylko hackerzy?
- Jakich narzędzi używają hackerzy?
- Czy możemy się chronić?
- Co nas czeka niebawem?
- Czy mają Państwo pytania? ☺

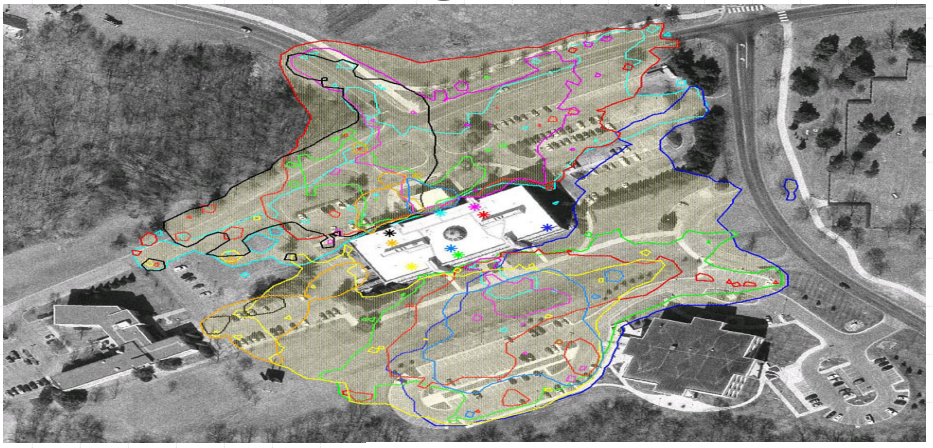
Jakie sieci bezprzewodowe widzi hacker?



Czy wszystkiemu winny jest „zasięg”?



...i jak wygląda ryzyko ataku z dużej odległości?

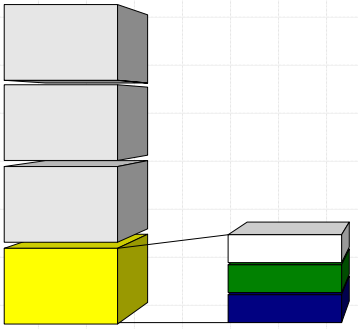


Źródło: David Wagner - Why Swiss-Cheese Security Isn't Enough

Które sieci (nie) są podatne na ataki?

Które sieci bezprzewodowe interesują hackerów?

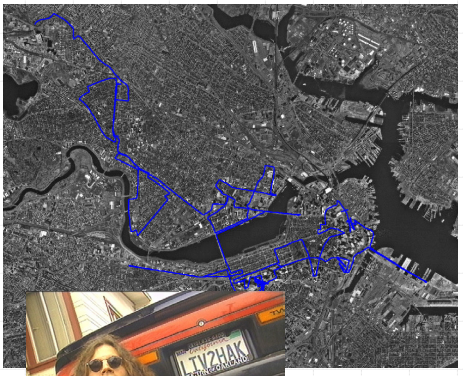
- **Wszystkie!!!**
- …ale przede wszystkim
  - WLAN - IEEE 802.11
  - Bluetooth
- dlaczego?
  - filozofia: „sieci komputerowe” vs. sieci telekomunikacyjne
  - pełny dostęp do interfejsu sieciowego - dostęp do najniższych warstw sieci, ale możliwość abstrakcji od warstwy fizycznej
  - monitor mode

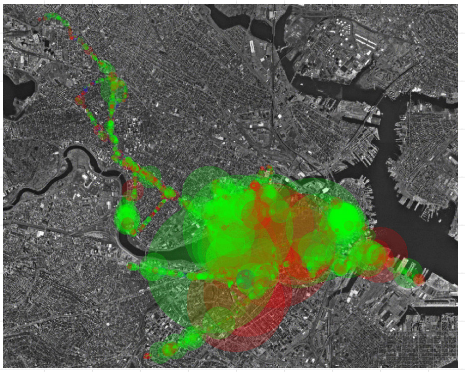


Jakie są subkultury wśród „bezprzewodowych” hackerów?

- **Hackerzy pasywni:**
  - **Motto: „Siódme: nie kradnij”**
    - przykład: wardriving - „Pokażmy światu, gdzie są sieci bezprzewodowe”
- **Hackerzy aktywni:**
  - **Motto: „Siódme: nie kradnij, ale co możesz to zgarnij”**
    - Przykład: warchalking - „Pokażmy światu, jak korzystać za darmo z bezprzewodowych sieci”
  - **Motto: „Kradnij”**
    - Przykłady:
      - > kradzieże służbowych laptopów z interfejsami bezprzewodowymi
      - > nowa subkultura: bluehacking (m.in. bluejacking) – także wysysanie informacji z telefonów komórkowych

Hackerzy pasywni: Wardriving, warflying...





Peter Shipley – prekursor Wardrivingu

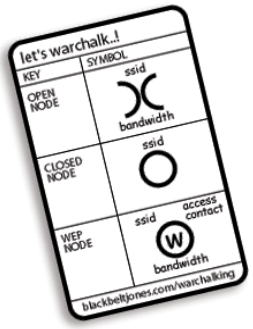
Źródło map: http://www.wardriving.com/boston

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

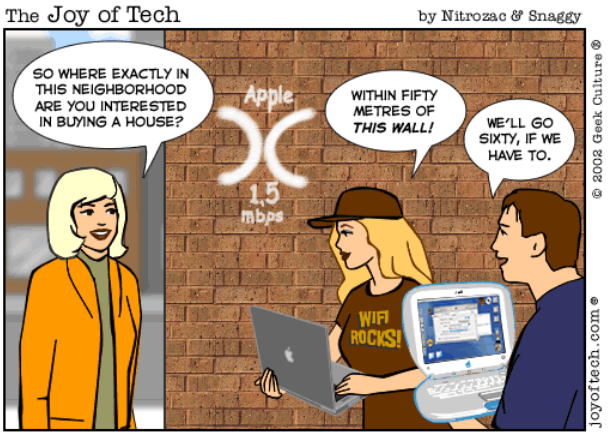
Wardriving w Polsce: Warszawa da się lubić...

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

Hackerzy aktywni: Warchalking



chalk (kreda)



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

Czy zawsze winni są tylko hackerzy?

- **uruchamianie nieautoryzowanych punktów dostępowych IEEE 802.11 przez bezmyślnych pracowników**
  - nagminnie pracownicy firmy, bez zgody i wiedzy osób odpowiedzialnych za bezpieczeństwo uruchamiają tzw. **Rogue AP**
  - niska cena tego typu urządzeń oraz prostota instalacji
  - standardowo konfiguracja bez żadnych zabezpieczeń
  - sieć korporacyjna może stać się dostępna dla każdego posiadacza komputera przenośnego z kartą WLAN
- **hot spoty**
  - najczęściej działają z wyłączonymi mechanizmami bezpieczeństwa
  - „bezprzewodowa kawiarenka internetowa”

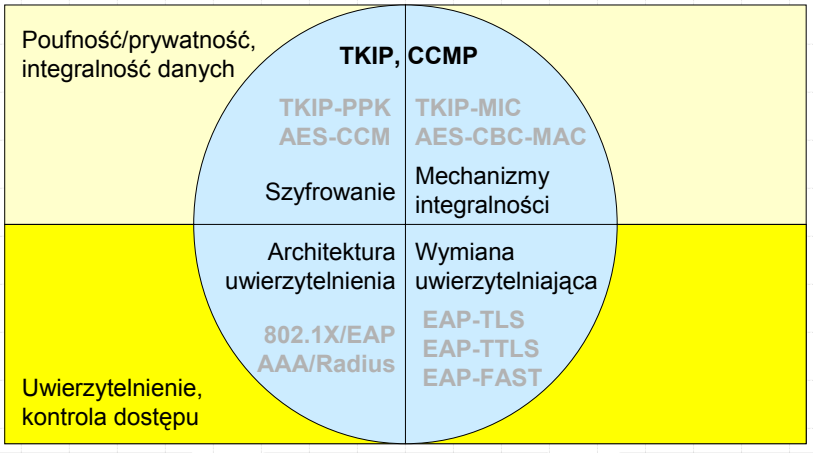

Rouge AP

Tło: Podatności WLAN...

- **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



Jakich narzędzi używają hackerzy?

- **Zasada działania hackera:**
  (1) cel należy znaleźć,
  (2) a następnie sprawdzić, czy jest tak naprawdę celem (sic!)
- **Komputer:** laptop albo palmtop z Linuxem
- **Dla WLAN – hackerzy używają przede wszystkim specjalizowanych skanerów**
  - **Skanery aktywne** (np. Netstumbler) - można je wykrywać poprzez sygnatury – charakterystyczne ustawienia pól w ramkach IEEE 802.11
  - **Skanery pasywne** (np. Kismet) - aktualnie brak możliwości bezpośredniego wykrycia
- **Dla Bluetooth** – narzędzia wciąż rozwijane: blue**stumbler**, blue**browse**, blue**jack**, blue**snarf**, blue**bug**

Przykładowe narzędzie: Kismet

- Zaawansowany skaner pasywny
- Także funkcje prostego systemu IDS dedykowanego sieciom WLAN
- Możliwość podłączenie odbiornika GPS
- Nanoszenie na dostarczone mapy wykrytych informacji
- Wykrywanie sieci WLAN, które nie rozgłaszają swojego SSID
- Wykrywanie zakresów sieci IP jedynie poprzez nasłuch transmitowanych pakietów protokołów ARP, UDP,TCP
- Praca w modelu klient-serwer (możliwość analizy w centralnym punkcie danych z wielu sensorów)

Czy możemy się chronić?

- Najprościej: nie używać sieci bezprzewodowych…
- …ale skoro już trzeba:
  - Używać sieci bezprzewodowych tylko wtedy, kiedy jest to konieczne
  - Użyć silnej kryptografia na poziomie warstwy łącza danych (AES w IEEE 802.11i) + w warstwie sieciowej (IPsec)
  - Używać systemów AAA (802.1X/EAP z IEEE 802.11i)
  - Implementować systemy wykrywania włamań dla sieci bezprzewodowych
  - Separować systemy bezprzewodowe w sieciach korporacyjnych za pomocą ścian przeciwogniowych
  - Śledzić stan wiedzy!

Co nas czeka niebawem?

- Ekspansja sieci bezprzewodowych jest faktem
- Sieci bezprzewodowe są lub będą (niebawem) wszędzie - jest to zmiana zarówno techniczna, jak i kulturowa
- Zabezpieczenia z IEEE 802.11i wzorcem dla innych sieci bezprzewodowych klasy „sieci komputerowe”
- Poprawiony szkielet zabezpieczeń GSM w UMTS – trend w sieciach telekomunikacyjnych
- Sieci bezprzewodowe trzeba wciąż zabezpieczać…

Co nas czeka niebawem?

Ilustracja z artykułu „The wireless security balancing act”: http://www.nwfusion.com/supp/2003/security/0526secwifi.html

- …chociaż przypomina to balansowanie na nieistniejącej linie…
- …a nie można zaśpiewać: **"So Just Leave Me Alone"** ☺

Czy mają Państwo pytania?

Krzysztof Szczypiorski
E-mail: krzysztof@szczypiorski.com
http://krzysztof.szczypiorski.com