Warszawska
Wyższa Szkoła
Informatyki

ANALIZA PRZEPŁYWU DANYCH W SIECIACH BEZPRZEWODOWYCH W STANDARDACH 802.11 B/G/N

Emil Wilczek

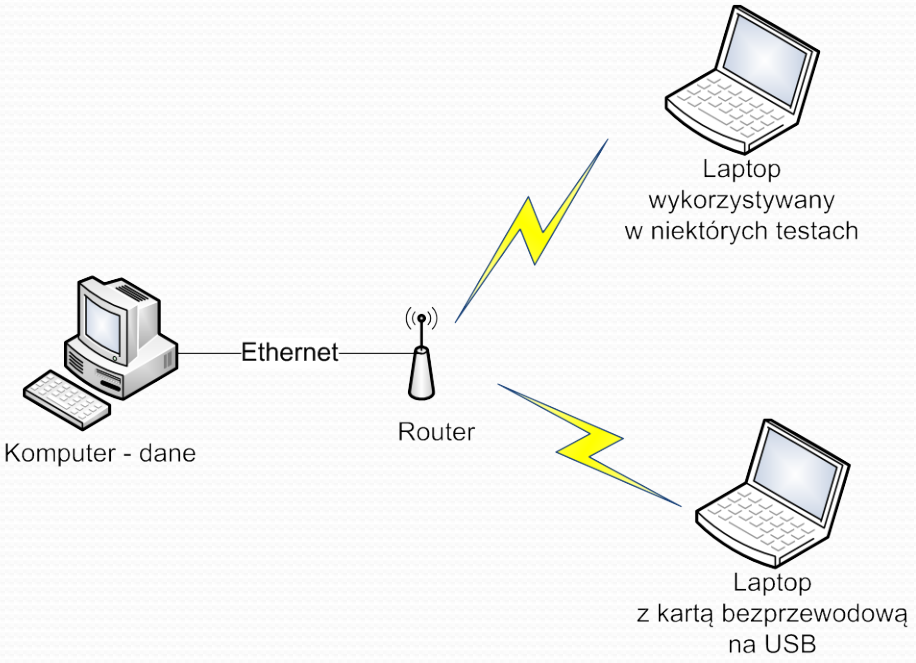
Promotor: dr inż. Dariusz Chaładyniak

Warszawa 2011

TESTY I ANALIZY

- Wydajności sieci – celem jest sprawdzenie przy jakich ustawieniach osiągane są najlepsze wydajności,
- Zasięgu sieci - sprawdzanie jak odległość i przeszkody wpływają na zasięg sieci,
- Bezpieczeństwa sieci – sprawdzenie, który mechanizm lub szyfrowanie najskuteczniej zabezpiecza sieć przed włamaniem.

ARCHITEKTURA TESTOWA



Architektura - BSS

Urządzenia:
- Router
- Laptop z zewnętrzną kartą bezprzewodową
- Laptop z wewnętrzna karta bezprzewodową
- Komputer z kartą przewodową

Wykorzystywane systemy:
- Windows Vista/7
- Linux – Backtrack 5

TESTY WYDAJNOŚCI SIECI

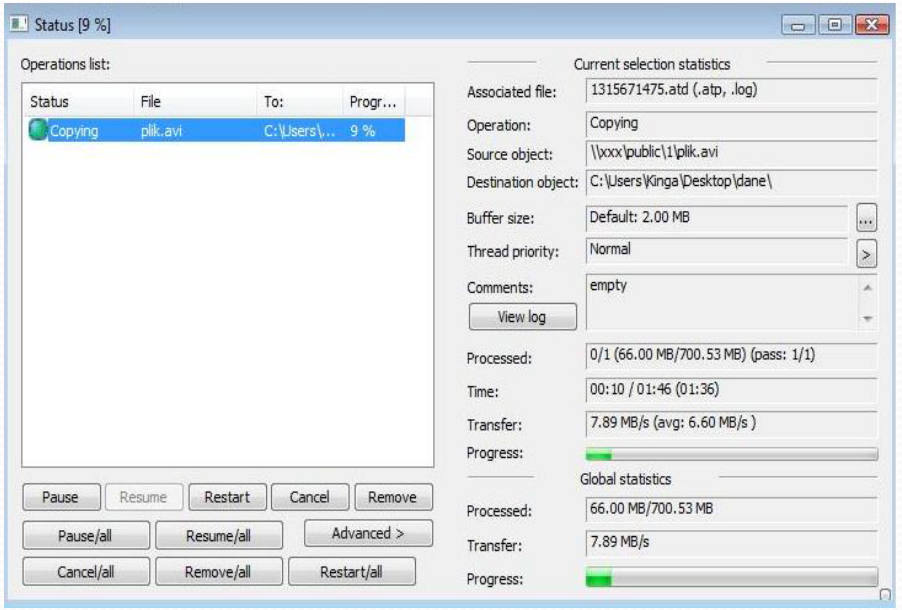
Dwa testy:

1. Kopiowanie trzech paczek plików:
   - Paczka 1: 1 plik o rozmiarze 700 MB
   - Paczka 2: 20 plików o łącznym rozmiarze 100 MB (każdy po 5 MB)
   - Paczka 3: 60 plików o łącznym rozmiarze 37,6 MB (każdy po 642 KB)

Oprogramowanie: Copy Handler

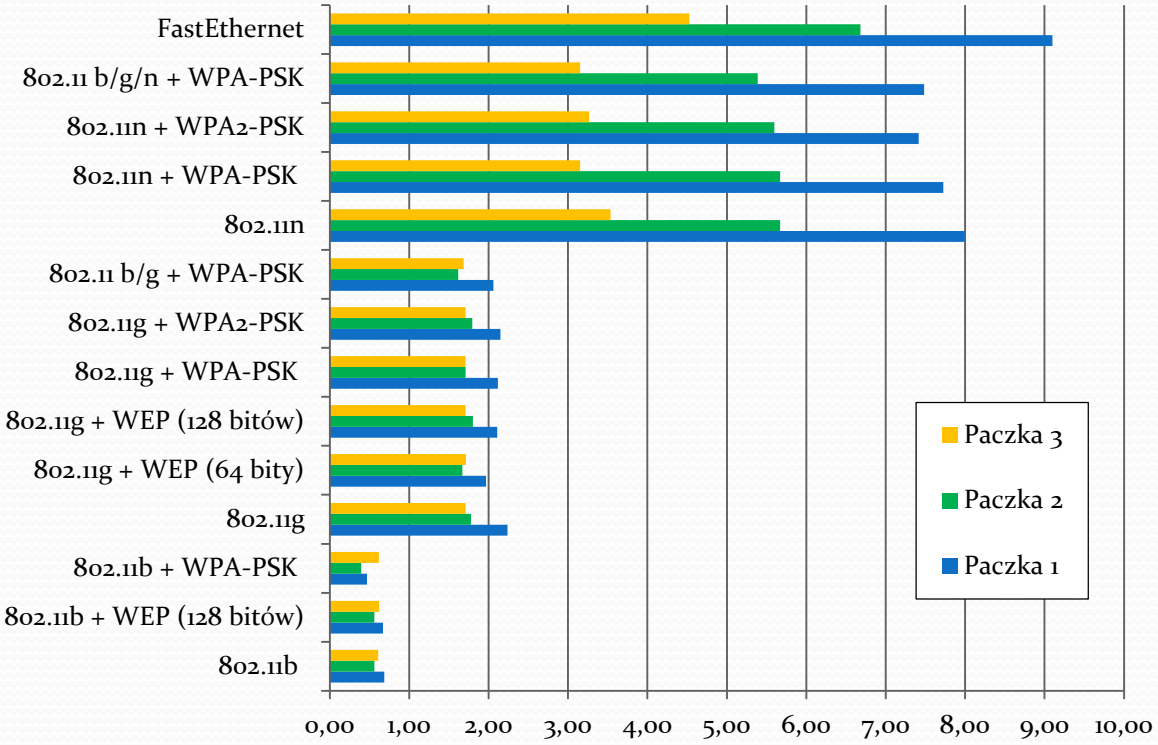
2. Badanie przepustowości - testowano na protokole TCP i rozmiarze danych 5MB

Oprogramowanie: Jperf



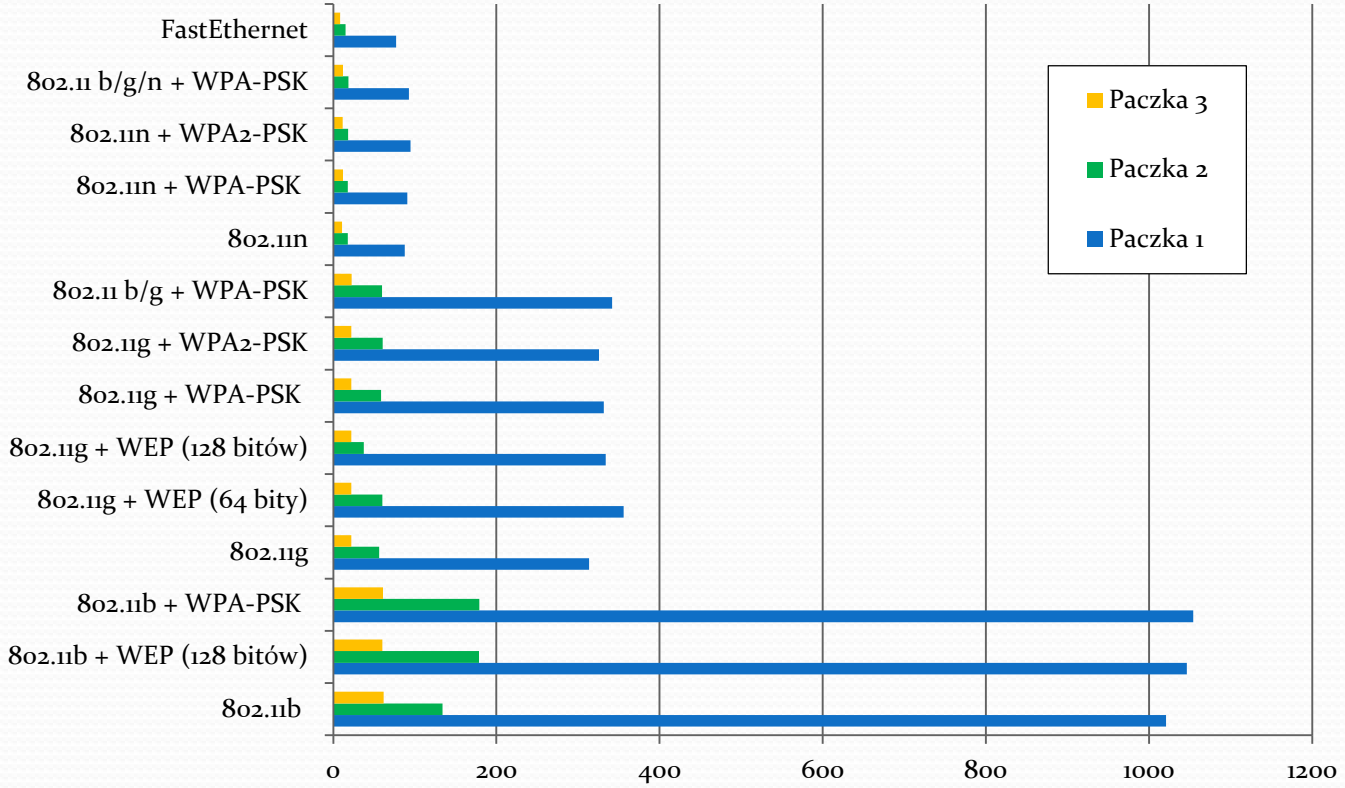
ANALIZA WYDAJNOŚCI SIECI

Szybkość kopiowania plików w MB/s (więcej = lepiej)



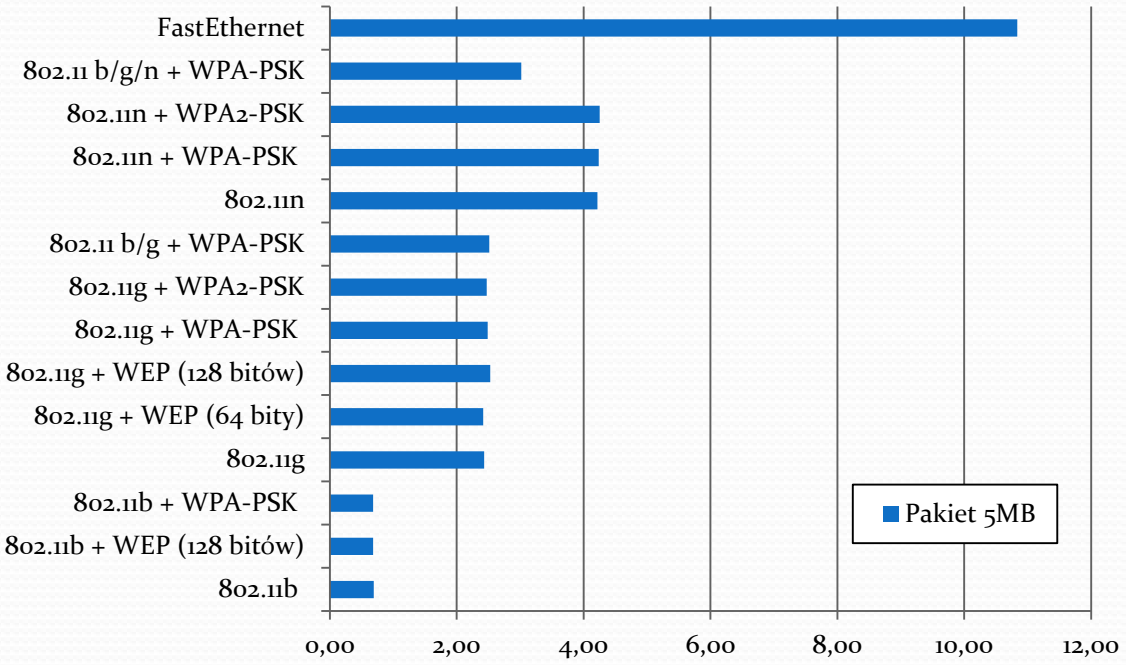
ANALIZA WYDAJNOŚCI SIECI c.d.

Czas kopiowania plików w sekundach (mniej = lepiej)



ANALIZA WYDAJNOŚCI SIECI c.d.

Wydajność łącza w MB/s

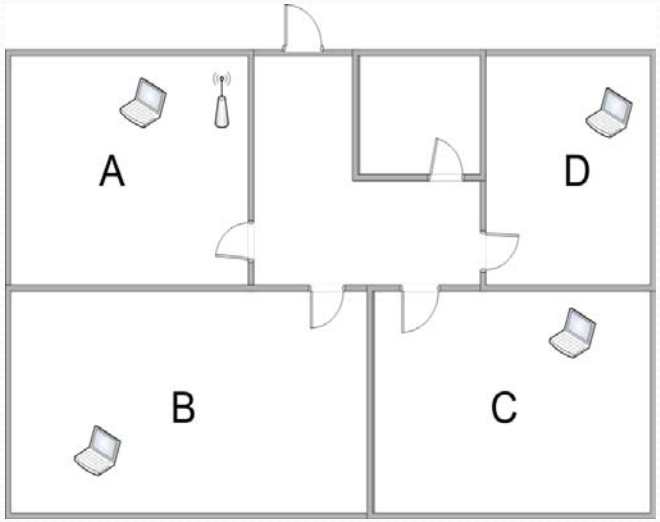


TESTY ZASIĘGU SIECI

Sprawdzenie zasięgu sieci przy zastosowaniu przeszkód oraz zwiększaniu odległości, w następujących miejscach:

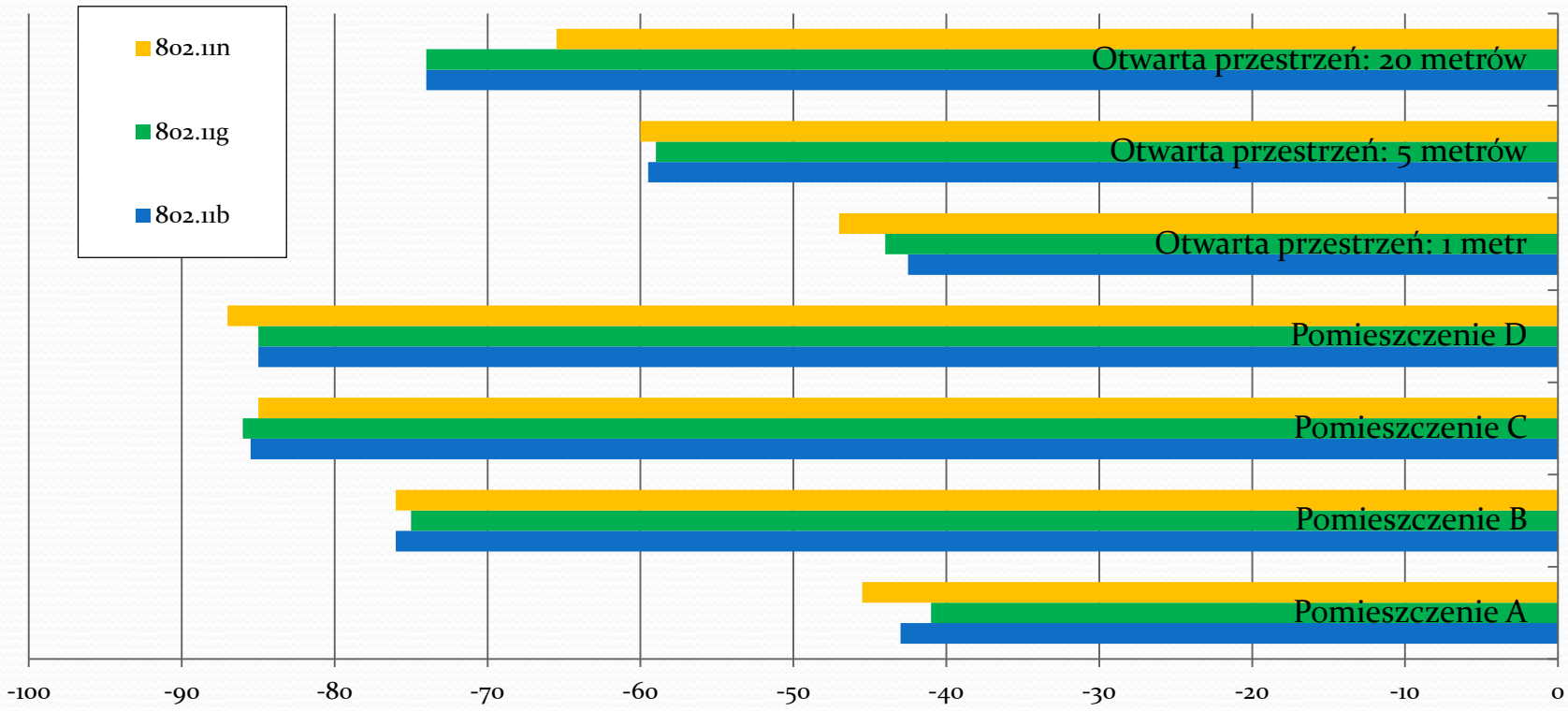
- Pomieszczenie A
- Pomieszczenie B
- Pomieszczenie C
- Pomieszczenie D
- Otwarta przestrzeń: 1 metr
- Otwarta przestrzeń: 5 metrów
- Otwarta przestrzeń: 20 metrów

Oprogramowanie: InSSIDer, WirelessMon, WirelessNetView



ANALIZA ZASIĘGU SIECI

Średnia zasięgu sieci w różnych pomieszczeniach i na otwartej przestrzeni w standardach 802.11b/g/n

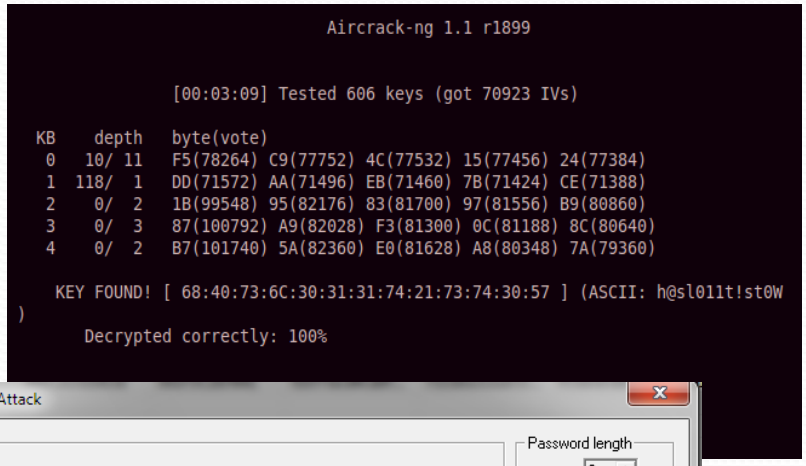


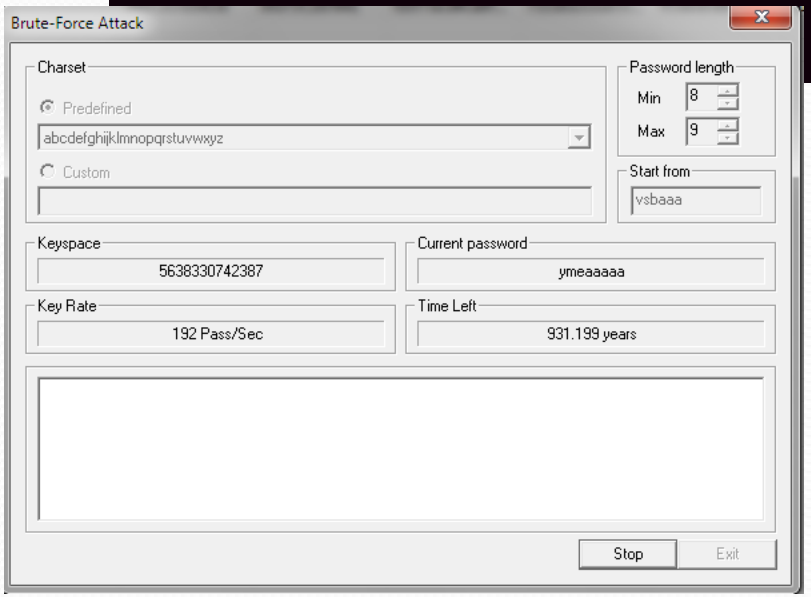
TESTY BEZPIECZEŃSTWA SIECI

Testowane podstawowe zabezpieczenia sieci:

- Ukrywanie SSID
- Filtracja MAC
- Szyfrowanie WEP
- Szyfrowanie WPA-PSK
- Szyfrowanie WPA2-PSK

Oprogramowanie: Aircrack-ng, Cain & Abel, EWSA





ANALIZA BEZPIECZEŃSTWA SIECI

- Ukrywanie SSID – czekanie aż nowy użytkownik podłączy się do sieci lub rozłączanie użytkownika,
- Filtracja MAC – zmiana adresu MAC,
- Szyfrowanie WEP - zbieranie wektorów inicjujących poprzez czekanie (nasłuchiwanie) lub wstrzykiwanie pakietów, złamane każde hasło,
- Szyfrowanie WPA-PSK/WPA2-PSK – przechwytywanie handshake zawierające wstępne tymczasowe hasło uwierzytelniające oraz SSID, następnie łamanie go. Złamane tylko hasła słownikowe.

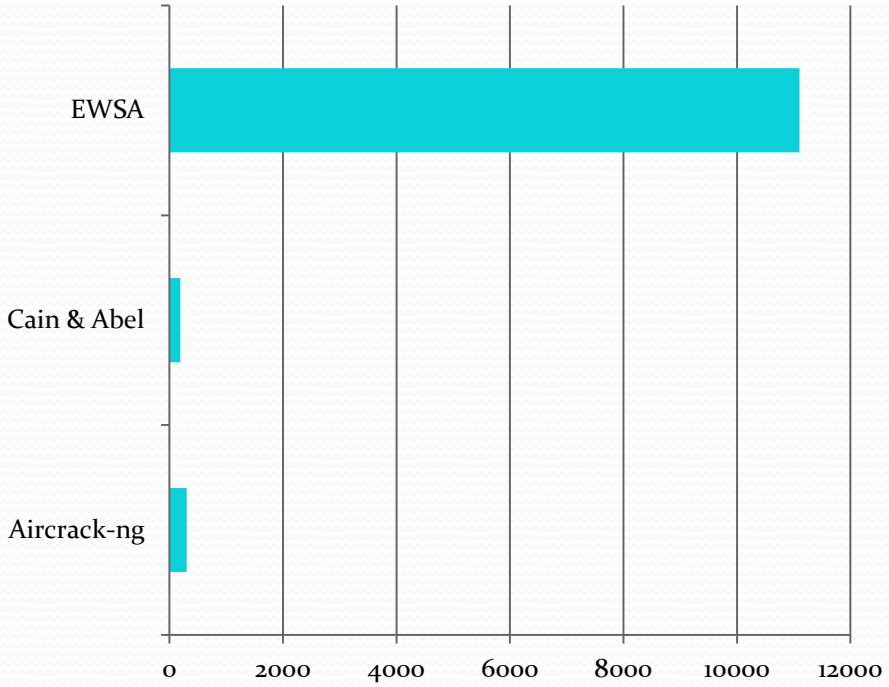
ANALIZA BEZPIECZEŃSTWA SIECI c.d.

Łamanie hasła metodą brute-force:
- dla haseł o długości 8 znaków (małe litery alfabetu) łamanie trwałoby około 40 lat,
- dla haseł o długości 8 i 9 znaków (małe litery alfabetu) około 931 lat.

Prędkość: 192 haseł na sekundę.
Oprogramowanie: Cain & Abel

Przy zastosowaniu (4xGeForce 295 GTX (CUDA)) szybkość wzrośnie do 89000 haseł na sekundę. W związku z tym szybkość łamania hasła metodą brute-force z 40 lat do 31 dni, a z 931 lat zmalałaby do około 2 lat.

Ilość sprawdzanych haseł na sekundę dla WPA-PSK



Kilka dobrych praktyk

- Ustawić szyfrowanie danych – najbezpieczniejszym obecnie szyfrowaniem jest WPA2,
- Stosować silne hasła – tu warto ustawiać hasła o minimalnej długości 12 znaków, hasło powinno zwierać małe i duże litery, cyfry, znaki specjalne. Hasło powinno się tworzyć najlepiej z przypadkowej sekwencji znaków, aby nie było można go złamać metodą słownikową,
- Zmienić identyfikator SSID – zmienić standardowy identyfikator SSID na inny, nie należy ustawiać nazwy związanej z właścicielem sieci lub z nazwą urządzenia,
- Aktualizacja oprogramowania w punkcie dostępowym – często taka aktualizacja łata dziury bezpieczeństwa w naszym punkcie dostępowym,
- Zmienić domyślne hasło w punkcie dostępowym – zmienić domyślne hasło służące do logowania się do ustawień punktu dostępowego, dodatkowo to zabezpieczenie chroni wewnątrz sieci,
- Zarządzanie tylko przez kabel – wyłączenie możliwości logowania do punktu dostępowego przez Wi-Fi,
- Zmniejszyć moc nadawania – opcja ta jest dostępna w niektórych punktach dostępowych, dzięki niej można ograniczyć zasięg sieci tylko dla danego obszaru.

WNIOSKI

- Obecnie najszybszą dostępną technologią jest standard 802.11n, niestety w szybkości 150Mbps jest wolniejszy od FastEthernet z prędkością 100Mbps.
- Standard 802.11b nie warto już używać
- Szyfrowanie ma wpływ na wydajność sieci, czym lepsze szyfrowanie tym niższa wydajność.
- Wielkość plików przy wysyłaniu ma ogromne znaczenie
- Przeszkody typu ściana wpływają bardziej na zasięg niż zwiększanie odległości na otwartej przestrzeni.

WNIOSKI c.d.

- Różne standardy nie wpływają na zasięg
- Mechanizmy typu ukrywanie SSID i filtrowanie MAC można łatwo obejść.
- Szyfrowanie WEP nie zapewnia żadnego bezpieczeństwa, gdyż złamanie tego zabezpieczenia trwa około 5 minut.
- Szyfrowanie WPA-PSK/WPA2-PSK przy haśle, które znajduje się w słowniku też łatwo złamać. W przypadku trudnych haseł (minimum 12 znakowych), które zawiera małe i duże litery, cyfry oraz znaki specjalne bardzo ciężko złamać hasło. Obecnie WPA2-PSK przy zastosowaniu silnego hasła jest najbezpieczniejszym szyfrowaniem sieci.
- Używanie programów, które wykorzystują moc obliczeniową układów graficznych znacząco przyśpiesza łamanie hasła WPA-PSK/WPA2-PSK.

Dziękuje za uwagę