Bezpieczeństwo technologii Bluetooth

CONFidence 2006

Kraków

Przemysław Frasunek

Agenda

- Charakterystyka technologii
- Problemy projektowe i implementacyjne
- Prezentacja ataku

Charakterystyka technologii (1)

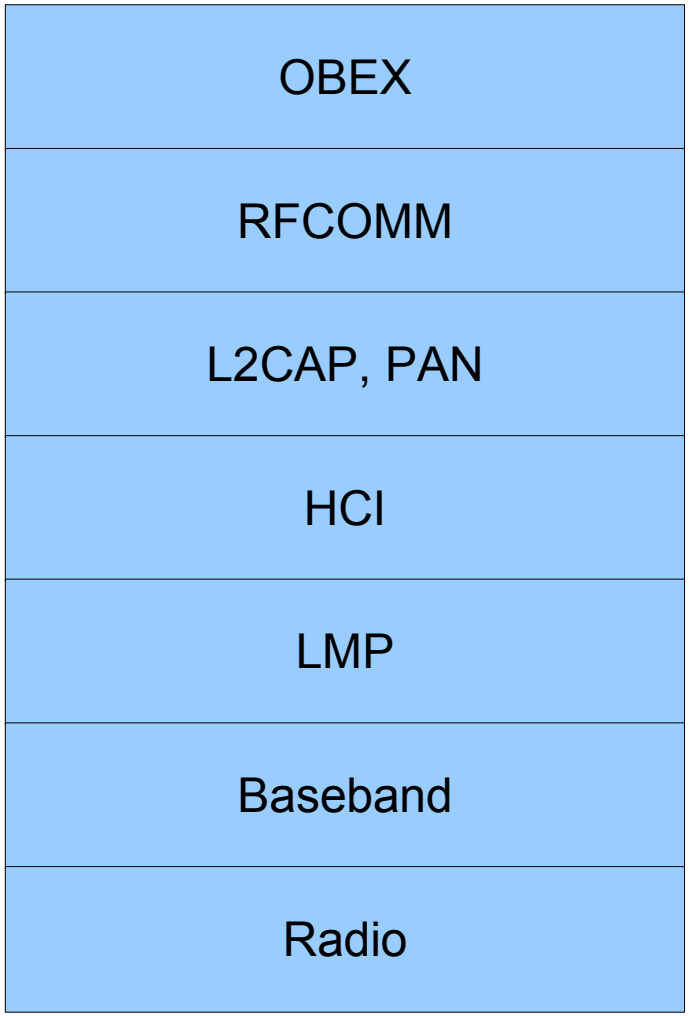
- Założenie: bezprzewodowa komunikacja dla urządzeń zasilanych z baterii
- Działa w paśmie 2,4 GHz, czyli tam gdzie WiFi 802.11b/g
  - inny dostęp do medium – FHSS vs DSSS
  - 79 kanałów, każdy po 1 MHz
  - 1600 zmian kanału na sekundę
  - efektywnie zakłóca WiFi ;)

Charakterystyka technologii (2)

- Klasy urządzeń Bluetooth
  - I klasa: 100 mW (20 dBm) ~ 100 m zasięgu
  - II klasa: 10 mW (4 dBm) ~ 10 m zasięgu
  - III klasa: 1 mW (0 dBm) ~ 10 cm zasięgu
- Szybkość transmisji danych
  - 1.1: 723 kbit/s
  - 2.0: 2,1 Mbit/s

Charakterystyka technologii (3)

- Własny stos protokołów, trochę podobny do TCP/IP



Charakterystyka technologii (4)

- Podstawowe usługi
  - wymiana plików (OBEX)
  - Transmisja głosu (słuchawka)
  - dostęp do sieci – enkapsulacja Ethernet lub PPP (DUN, PAN)

Charakterystyka technologii (5)

- Założenia bezpieczeństwa
  - przed rozpoczęciem transmisji konieczne jest parowanie
    - ustalenie klucza szyfrowania (algorytm SAFER)
    - szyfrowanie symetryczne (algorytm E0)
  - „ukrywanie” urządzenia
  - mały zasięg
  - odseparowanie użytkownika od warstwy RF

Problemy projektowe i implementacyjne (1)

- Anteny kierunkowe = większy zasięg
  - rekord – prawie 2 km
- BlueBug – ukryte kanały RFCOMM, udostepniające komendy AT
- BluePrinting – fingerprinting urządzenia

Problemy projektowe i implementacyjne (2)

- BlueSnarf – publicznie dostępne pliki na OBEX
- BlueSmack – ataki typu DoS
- BlueBump – utrzymanie otwartego połączenia pomimo skasowania autoryzacji

Problemy projektowe i implementacyjne (3)

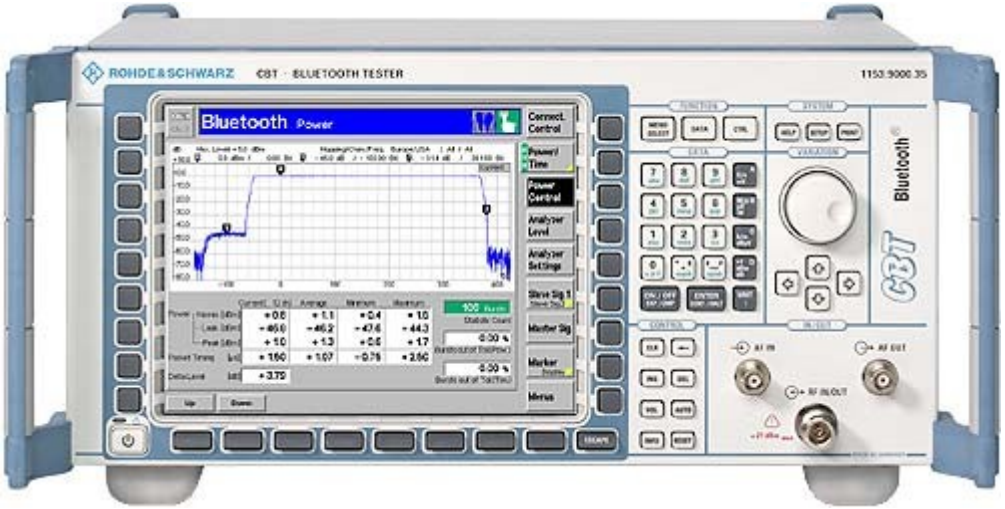
- BlueDump – urządzenie kasuje istniejące parowanie po udanym spoofingu

Inne pomysły na ataki (1)

- Ataki wykorzystujące inżynierie społeczną
  - proste i krótkie PINy
  - podszywanie się pod serwisy
  - długie i nietypowe nazwy urządzeń
- Wykrywanie ukrytych urządzeń
  - skanowanie adresów MAC

Inne pomysły na ataki (2)

- Uzyskiwanie dostępu do warstwy RF
  - gotowe analizatory
    - np. Rohde & Schwartz



Inne pomysły na ataki (3)

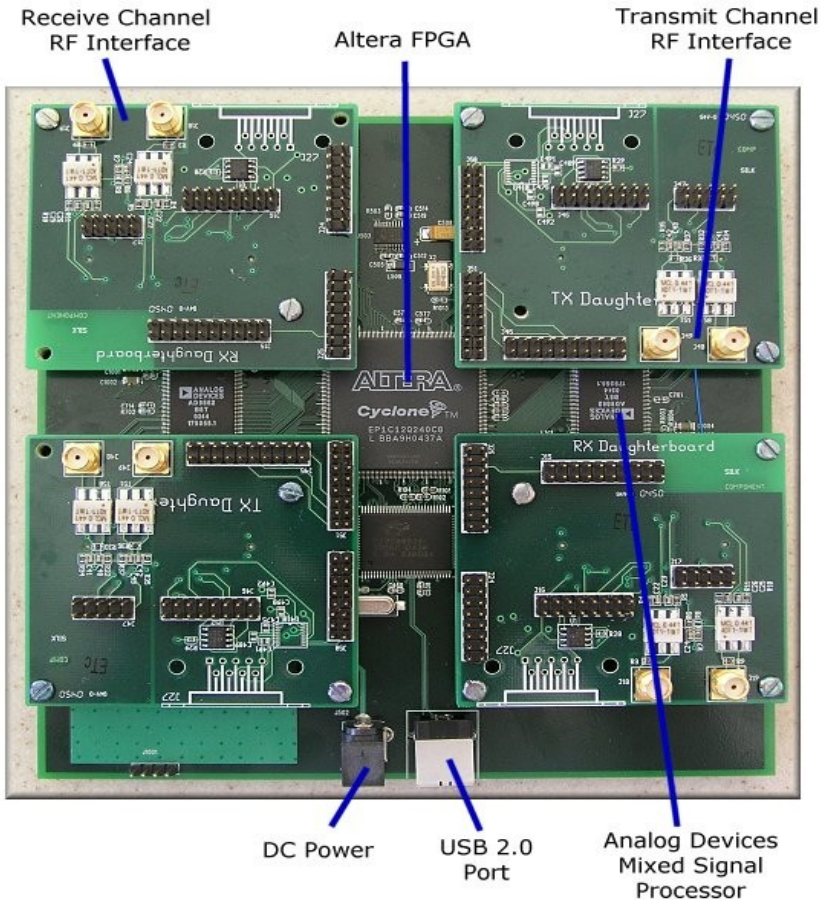
- Uzyskiwanie dostępu do warstwy RF
  - GNU Radio
    - software defined radio
    - demodulacja opisana w Pythonie lub C++
    - przykładowe demodulatory i modulatory
      - WFM i FM
      - GSM
      - AM
      - SSB
      - demodulator i modulator GMSK
        - transmisja IP do 1 Mbit/s

Inne pomysły na ataki (4)

- Uzyskiwanie dostępu do warstwy RF
  - GNU Radio
    - tak, można napisać (de)modulator dla Bluetooth
    - potrzebny sprzęt
      - przetwornik A/C i C/A
      - transreceiver na pasmo 2,4 GHz

Inne pomysły na ataki (5)

- Uzyskiwanie dostępu do warstwy RF
  - GNU Radio
    - USRP
      - zbudowany na bazie FPGA
      - interfejs USB 2.0
      - 4 przetworniki A/C
      - 4 przetworniki C/A
      - pasmo 6 Mhz
      - Open Source
      - można kupić gotowe urządzenie za 500$



Inne pomysły na ataki (6)

- Uzyskiwanie dostępu do warstwy RF
  - GNU Radio
    - USRP
      - potrzebny jeszcze odbiornik i nadajnik
        - nadajnik – 2-200 MHz – 75$
        - odbiornik – 2-300 MHz – 75$
        - odbiornik – 50-870 MHz – 100$
        - odbiornik – 800-2400 MHz – 150$
        - nadajnik/odbiornik – 400-500 MHz – 225$
        - nadajnik/odbiornik – 800-1000 MHz – 250$
        - nadajnik/odbiornik – 2400-2500 MHz - 275$

Inne pomysły na ataki (7)

- Uzyskiwanie dostępu do warstwy RF
  - co można zrobić?
    - pasywny sniffing parowania
      - off-line'owy bruteforcing PINu
        - Yaniv Shaked, Avishai Wool
        - 4-cyfrowy PIN – poniżej 1 sekundy
        - 7-cyfrowy PIN – 76 sekund
    - ataki statystyczne na E0
      - 2005 – Lu, Meier, Vaudenay – odzyskanie klucza w 2^{38} operacji przy posiadaniu 2^{23} ramek (~8 mln), znajomosci początkowych 24 bitów

Inne pomysły na ataki (8)

- Uzyskiwanie dostępu do warstwy RF
  - co można zrobić?
    - ataki aktywne – potencjalnie niezliczone błędy w zamkniętych HCI

Narzędzia Bluetooth (1)

- Przegląd narzędzi dostępnych w pakiecie BlueZ
  - hciconfig – konfigurator interfejsu hosta
  - hcitool
    - skanowanie
    - informacje o urządzeniu
    - tworzenie połączeń

Narzędzia Bluetooth (2)

- Przegląd narzędzi dostępnych w pakiecie BlueZ
  - hcidump – sniffer interfejsu hosta
  - sdptool
    - wyszukiwanie serwisów
    - publikowanie serwisów
  - l2ping
  - rfcomm – zarządzanie kanałami RFCOMM

Narzędzia Bluetooth (3)

- Przydatne dodatkowe narzędzia
  - btscanner
    - http://www.pentest.co.uk/cgi-bin/viewcat.cgi?cat=dc
    - poszukuje ukrytych urządzeń

Narzędzia Bluetooth (4)

- Przydatne dodatkowe narzędzia
  - btdsd
    - http://www.betaversion.net/btdsd/
    - skaner kanałów RFCOMM
  - Bluetooth Stack Smasher
    - http://securitech.homeunix.org/blue/
    - generuje różne typy niepoprawnych pakietów

Prezentacja praktyczna (1)

- Błąd w telefonie Nokia 6310i
- Podatność HP iPAQ h4150 na ataki DoS

Dziękuję za uwagę
i zapraszam do dyskusji