



Bluetooth i problemy z bezpieczeństwem

Skrzypczyk Artur
Akademickie Stowarzyszenie Informatyczne

Wrocław 12 marca 2010
Geek's Night 2.0



Agenda

- Dlaczego Bluetooth?
- Technologia Bluetooth
- Mechanizmy bezpieczeństwa
- Rodzaje ataków
- Test bezpieczeństwa
- Ochrona
- Ciekawostki
- Ochrona
- Bibliografia

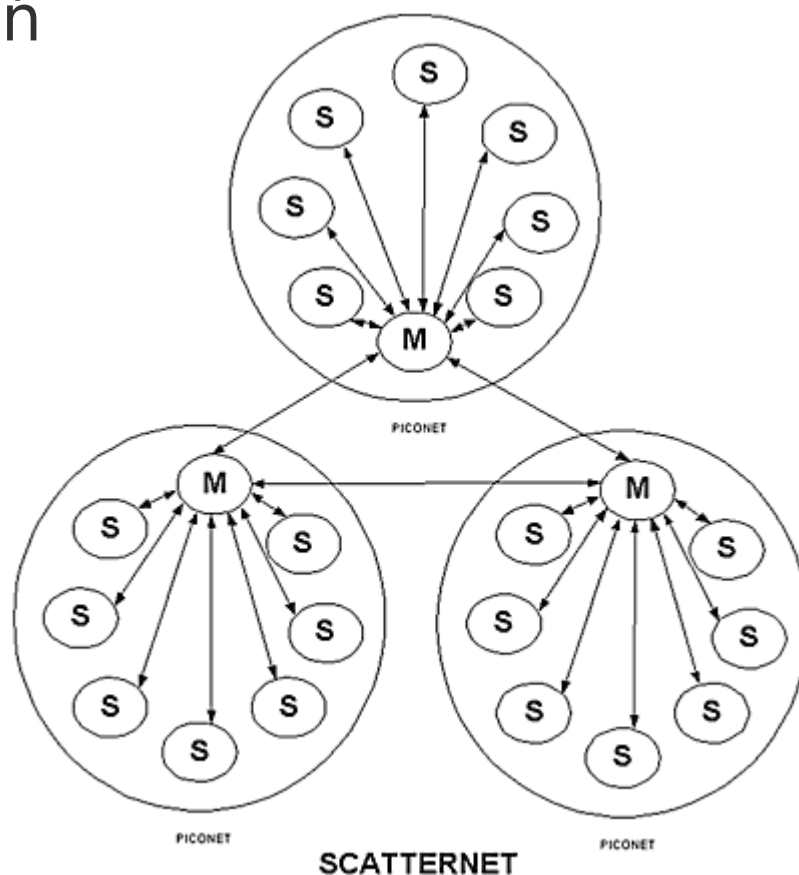
Dlaczego Bluetooth?

- ♦ 1994 - Ericsson zaczyna rozwijać technologię BT
- ♦ 1998 - Ericsson, IBM, Intel, Nokia, Toshiba
==> konsorcjum SIG
- ♦ ~ 2000 - pierwsze robaki: Cabir, Lasco, Comwar



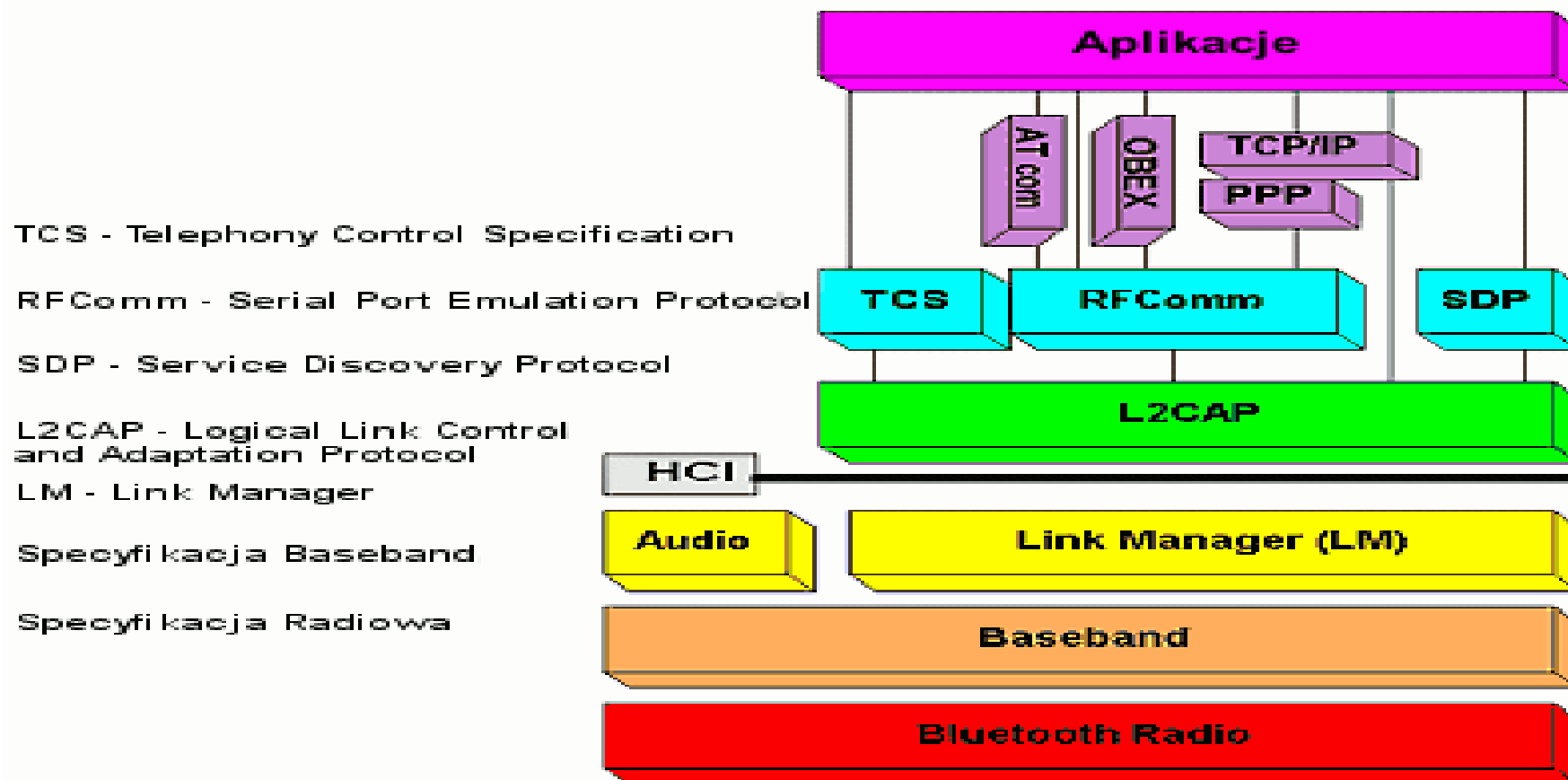
Technologia Bluetooth?

- 2,4-2,4835 GHz / 79 kanałów [1MHz]
- 1600 przeskoków częstotliwości na sekundę
- 2 rodzaje łączy (ACL, SCO)
- 3 klasy urządzeń



Technologia Bluetooth?

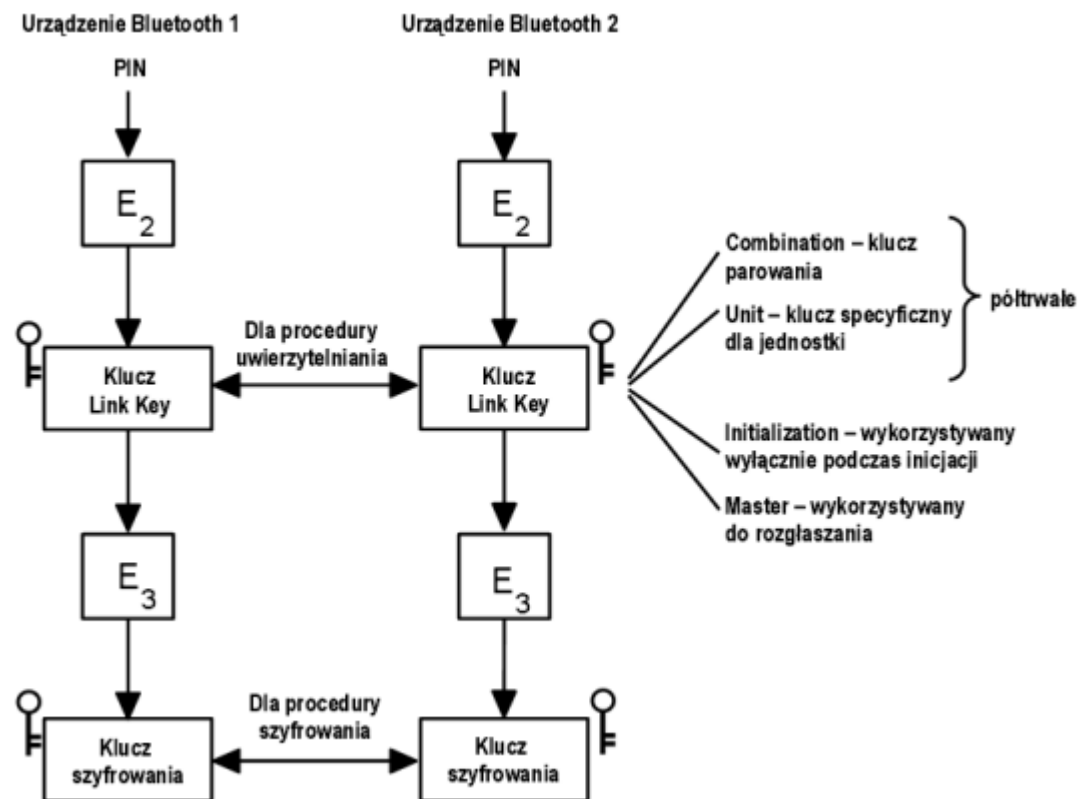
Protokoły Bluetooth



- Bluetooth Core Specification.

Mechanizmy bezpieczeństwa

- Tryb Bezpieczeństwa 1 - niechroniony.
- Tryb Bezpieczeństwa 2 - oparty na aplikacji/usłudze (L2CAP)
- Tryb Bezpieczeństwa 3 - uwierzytelnianie w oparciu o PIN/szyfrowanie adresu MAC



Rodzaje ataków

- BlueBag
- Blueprinting
- BlueSmack
- BlueSnarf
- Blue Snarf++
- HaloMoto
- BlueBump
- BlueDump
- BlueChop

Teścik se-se-se...

No właśnie...

Ochrona

- Przekształcenie na tryb niewykrywalny
- Uwierzytelnianie na podstawie kodu PIN
- Stosowanie oprogramowania antywirusowego
- Dodatkowe oprogramowanie (Bloover, Bloover II, BT Audit)

Ciekawostki



Ciekawostki



Ciekawostki

Bluejacking ;-)

Bibliografia

- ♦ www.shmoo.com
- ♦ www.bluetooth.org
- ♦ www.bluez.org
- ♦ www.ieee802.org

9. Pytania ?

Que pasa?