České vysoké učení technické v Praze
Fakulta elektrotechnická

Bluetooth Security

Radek Doležal
X36MTI

Program prezentace

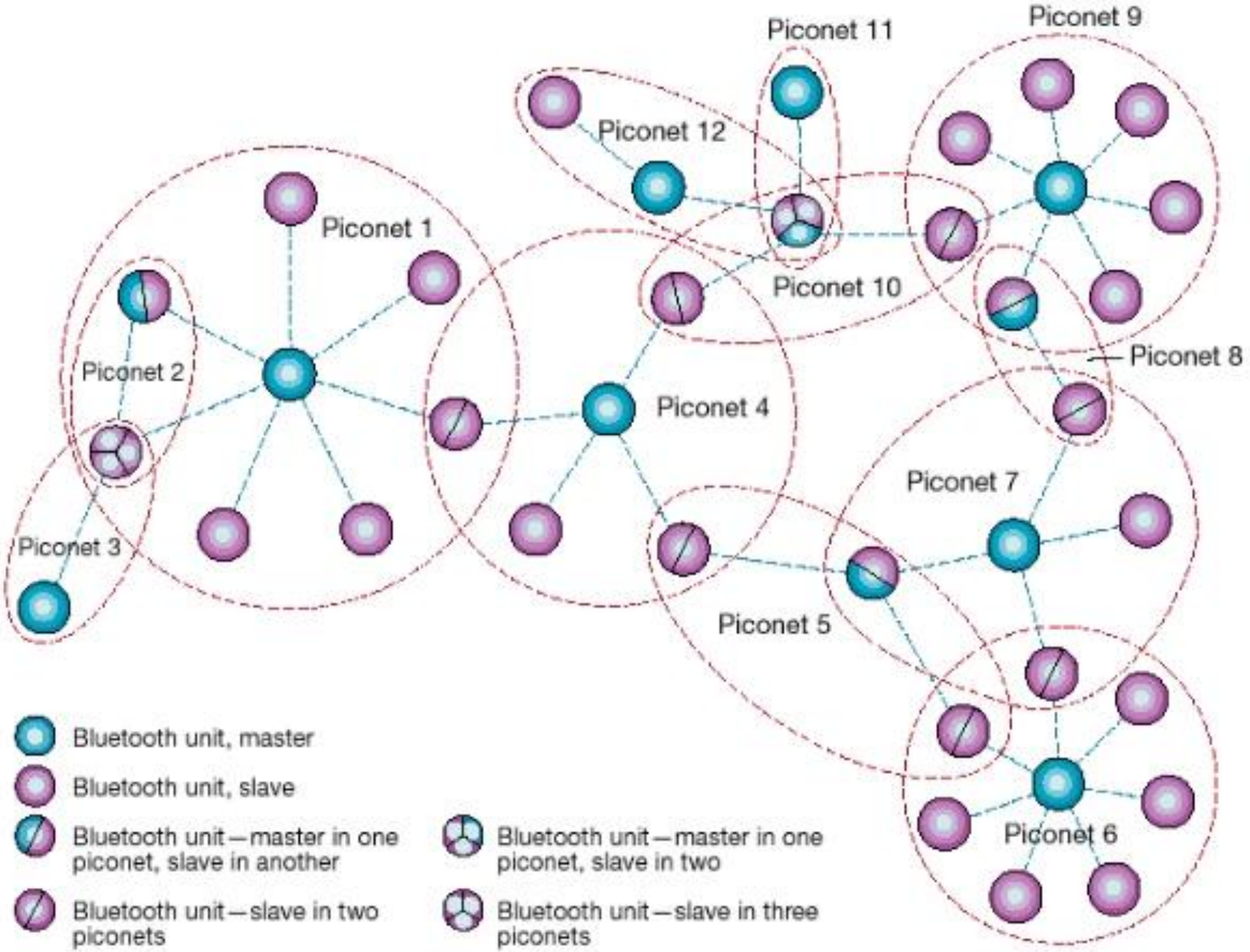
1. Základní vlastnosti
2. Bezpečnostní služby
3. Bezpečnostní režimy
4. Základní složky bezpečnosti
5. Autentizace a šifrování
6. Bezpečnostní slabiny
7. Útoky na Bluetooth

Základní vlastnosti

- **Účel**
- **Funkčnost**
- **Aplikace**

Topologie Bluetooth

- **Piconet**
- **Scatternet**


Piconet 11
Piconet 9
Piconet 12
Piconet 1
Piconet 10
Piconet 8
Piconet 2
Piconet 4
Piconet 7
Piconet 3
Piconet 5
Piconet 6
Bluetooth unit, master
Bluetooth unit, slave
Bluetooth unit—master in one piconet, slave in another
Bluetooth unit—master in one piconet, slave in two
Bluetooth unit—slave in two piconets
Bluetooth unit—slave in three piconets

Bezpečnostní služby

Bluetooth poskytuje tři základní bezpečnostní služby:

- **autentizaci** (ověření totožnosti komunikujících stran)
- **důvěrnost** (ochrana před odposloucháváním)
- **autorizaci** (povolení přístupu ke službám)

Bezpečnostní režimy

Zařízení Bluetooth může pracovat v jednom ze tří **bezpečnostních režimů:**

- **bez zabezpečení**
- **bezpečnost na úrovni služeb**
- **bezpečnost na úrovni spoje**

Základní složky bezpečnosti

- Přeskakování mezi kmitočty
- Jedinečná adresa zařízení
- Klíče odvozené z PIN
- Autentizace zařízení sdíleným 128bitovým klíčem
- Důvěrnost dat zajištěná proudovou šifrou konfigurovatelné délky(8-128 bitů)

Parametry zařízení při zabezpečení

- BD_ADDR - adresa zařízení;
- PIN - přidělený vlastníkem zařízení nebo výrobcem
- privátní klíč zařízení *(unit key)* - vygenerován při prvním použití zaříze-ní s použitím generátoru náhodných čísel

Autentizace a šifrování

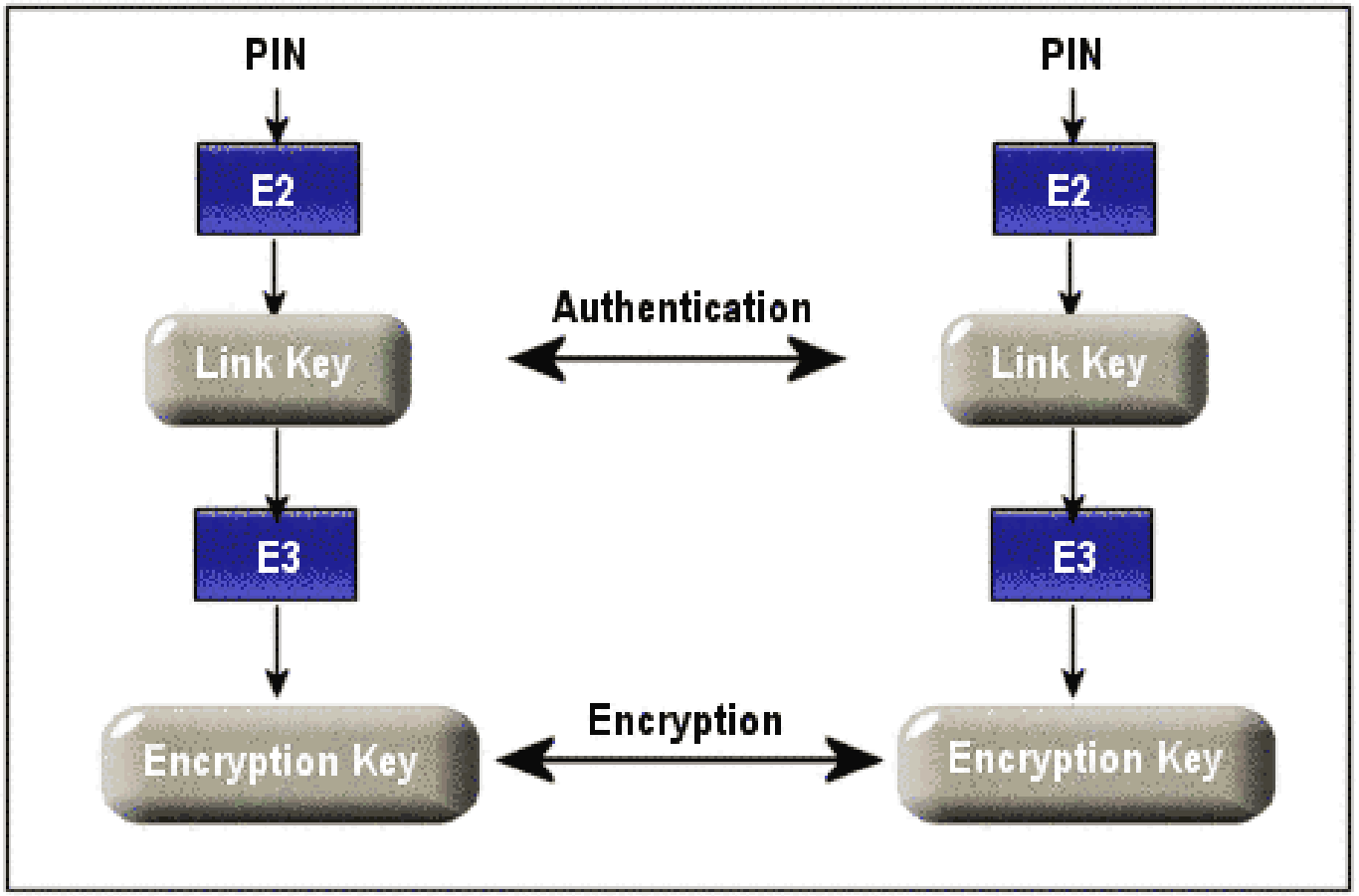
- Unit key
- Combination key
- Master key
- Autentizace – výzva odpověď
- Autentizační klíč

  inicializační klíč = BD_ADDR + PIN + náhodné číslo -> **klíč spoje** (sdílený klíč)

Šifrovací klíč

- Šifrovací klíč se odvozuje od autentizačního klíče, ovšem pro každý paket nově.
- Délka šifrovacího klíče (mezi 8 až 128 bity)
- **šifrovací klíč** = klíč spoje + náhodné číslo + BD_ADDR + hlavní takt *(master clock)*

Bezpečnostní postup



Bezpečnostní slabiny

- **krátké PIN** povoleno
- chybí metoda **distribuce PIN**
- **délka šifrovacího klíče**
- **klíč zařízení** *(unit key)* **veřejně dostupný**
- **hlavní klíč** - sdílený
- **autentizace**
- **proudová šifra Eo** - slabá
- **zabezpečení omezeno** pouze na spoj Bluetooth

Útoky na Bluetooth

- Útok formou zadních vrátek - využívající standardní párování komunikačních zařízení

- Bluesnarf – hrozí mobilním telefonům, obchází proces při párování před vlastní komunikací

Literatura a použité zdroje

- Rita Pužmanová – Bezpečnost bezdrátové komunikace, Computer Press, a.s. 2005
- http://www.bluetooth.com/dev/specifications.asp
- http://www.acm.org/crossroads/xrds9-4/blue.html
- http://articles.techrepublic.com.com/5100-1035-6139987.html