Bluetooth Sniffing

Martin Karger

Fachhochschule Dortmund

Seminarreihe WS 2005/2006

Gliederung

1. Intro
   - Einführung in die Technik
2. Sniffing
   - Definition
   - bluez
   - Hardwareanalyser
3. Anwendung
4. Zusammenfassung

Gliederung

1. Intro
   - Einführung in die Technik
2. Sniffing
   - Definition
   - bluez
   - Hardwareanalyser
3. Anwendung
4. Zusammenfassung

Bluetooth

- Industriestandard gemäß IEEE 802.15.1 für die **drahtlose (Funk-)Vernetzung** von Geräten über kurze Distanz.
- Mobiltelefon, PDA, Computer und Pheripheriegeräte bilden **Wireless Personal Area Network** (WPAN)
- **ISM-Band** (Industrial, Scientific, and Medical Band) 2,402 GHz - 2,480 GHz, Frequency Hopping Verfahren
- Specification is developed, published and promoted by the Bluetooth **Special Interest Group** (SIG)

Bluetooth

- Industriestandard gemäß IEEE 802.15.1 für die **drahtlose (Funk-)Vernetzung** von Geräten über kurze Distanz.
- Mobiltelefon, PDA, Computer und Pheripheriegeräte bilden **Wireless Personal Area Network** (WPAN)
- **ISM-Band** (Industrial, Scientific, and Medical Band) 2,402 GHz - 2,480 GHz, Frequency Hopping Verfahren
- Specification is developed, published and promoted by the Bluetooth **Special Interest Group** (SIG)

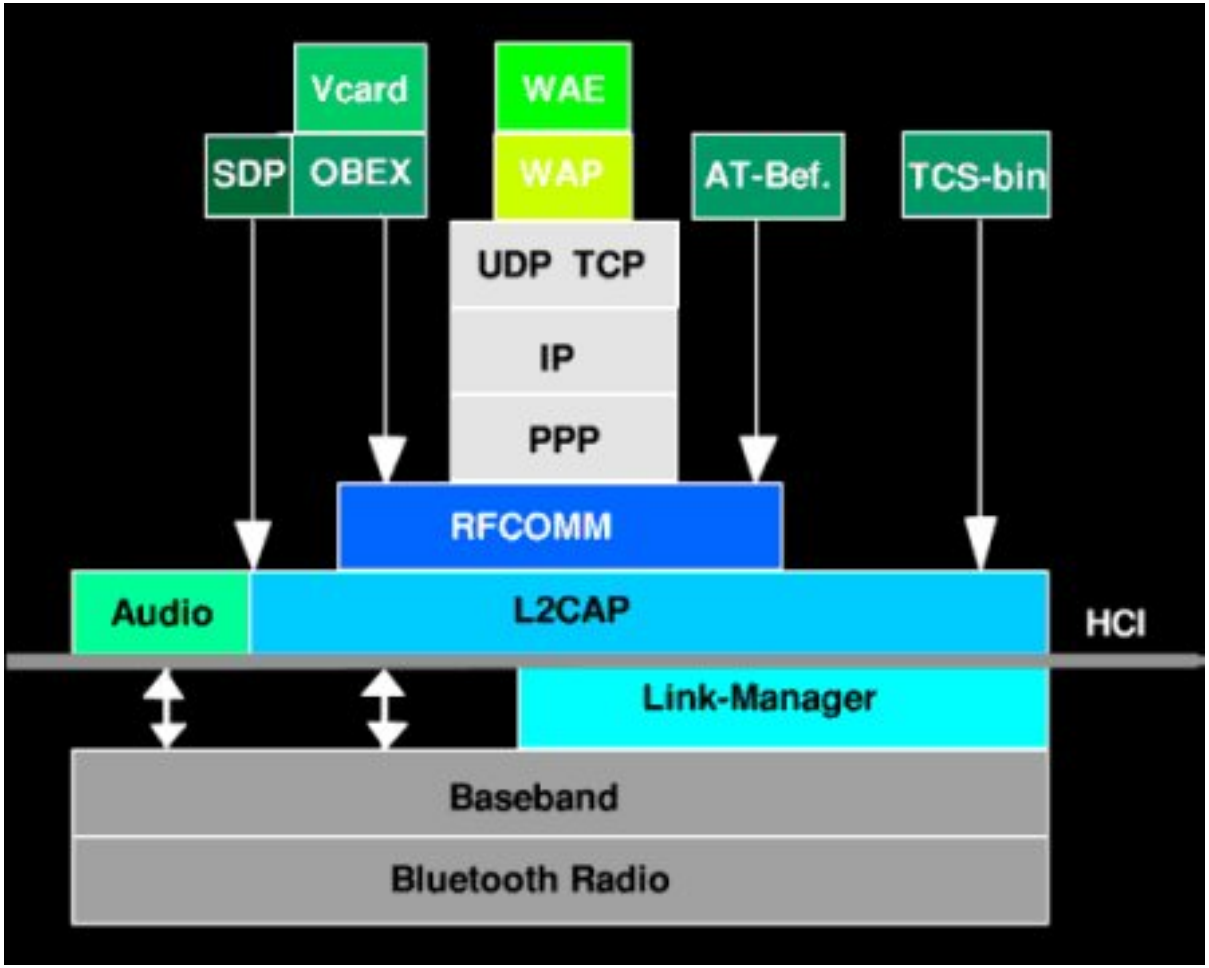
Bluetooth

- Industriestandard gemäß IEEE 802.15.1 für die **drahtlose (Funk-)Vernetzung** von Geräten über kurze Distanz.
- Mobiltelefon, PDA, Computer und Pheripheriegeräte bilden **Wireless Personal Area Network** (WPAN)
- **ISM-Band** (Industrial, Scientific, and Medical Band) 2,402 GHz - 2,480 GHz, Frequency Hopping Verfahren
- Specification is developed, published and promoted by the Bluetooth **Special Interest Group** (SIG)

Bluetooth

- Industriestandard gemäß IEEE 802.15.1 für die **drahtlose (Funk-)Vernetzung** von Geräten über kurze Distanz.
- Mobiltelefon, PDA, Computer und Pheripheriegeräte bilden **Wireless Personal Area Network** (WPAN)
- **ISM-Band** (Industrial, Scientific, and Medical Band) 2,402 GHz - 2,480 GHz, Frequency Hopping Verfahren
- Specification is developed, published and promoted by the Bluetooth **Special Interest Group** (SIG)

Bluetooth Stack



Gliederung

1 Intro
- Einführung in die Technik

2 Sniffing
- Definition
- bluez
- Hardwareanalyser

3 Anwendung

4 Zusammenfassung

Definition Packet Sniffer (aus Wikipedia)

Packet sniffers are software programs (...) that can intercept and log traffic passing over a digital network or part of a network.

Anwendungen für Sniffer (aus Wikipedia)

- Diagnose von Netzwerkproblemen
- Eindringungsversuche entdecken
- Netzwerktraffic-Analyse und Filterung nach verdächtigem Inhalt
- Datenspionage

Anwendungen für Sniffer (aus Wikipedia)

- Diagnose von Netzwerkproblemen
- Eindringungsversuche entdecken
- Netzwerktraffic-Analyse und Filterung nach verdächtigem Inhalt
- Datenspionage

Anwendungen für Sniffer (aus Wikipedia)

- Diagnose von Netzwerkproblemen
- Eindringungsversuche entdecken
- Netzwerktraffic-Analyse und Filterung nach verdächtigem Inhalt
- Datenspionage

Anwendungen für Sniffer (aus Wikipedia)

- Diagnose von Netzwerkproblemen
- Eindringungsversuche entdecken
- Netzwerktraffic-Analyse und Filterung nach verdächtigem Inhalt
- Datenspionage

Gliederung

1 Intro
- Einführung in die Technik

2 Sniffing
- Definition
- bluez
- Hardwareanalyser

3 Anwendung

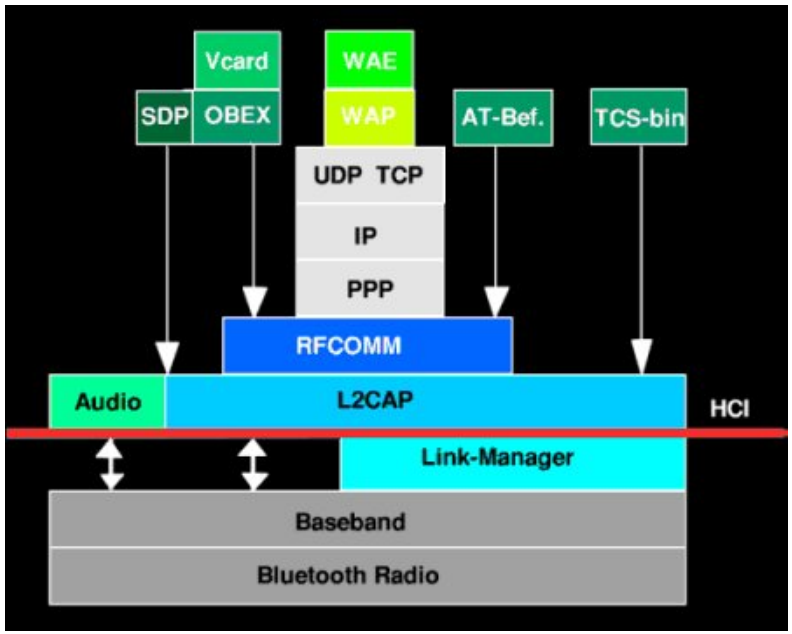
4 Zusammenfassung

bluez

- official Bluetooth-Stack since Linux 2.4.6 (July, 4th 2001)
- provides support for the core Bluetooth layers and protocols
- SIG qualified product since April, 11th 2005
- many nice »features«

hcidump

- the protocol decoding and analysis part
- reads raw **HCI data** coming from and going to a Bluetooth device



Gliederung

1 Intro
- Einführung in die Technik

2 Sniffing
- Definition
- bluez
- Hardwareanalyser

3 Anwendung

4 Zusammenfassung


LeCroy

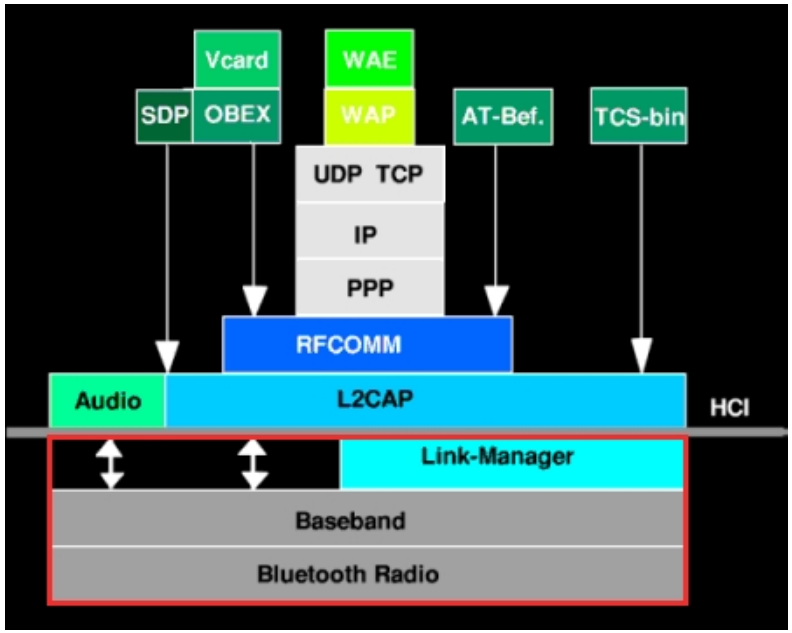

BPA 105
Bluetooth
Protocol
Analyser


LeCroy

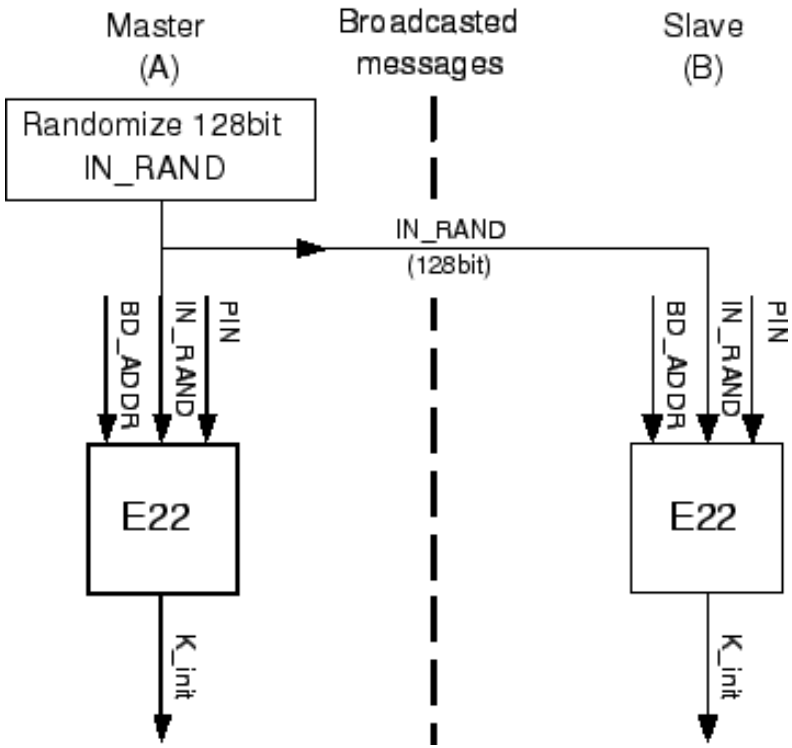

Frontline

FTS4BT

- Bluetooth v2.0 + EDR
- Bluetooth Dongle + spezielle Firmware + Software
- Capture, Filter, Decode und Anzeige in Echtzeit
- Synchronized **air** and HCI sniffing



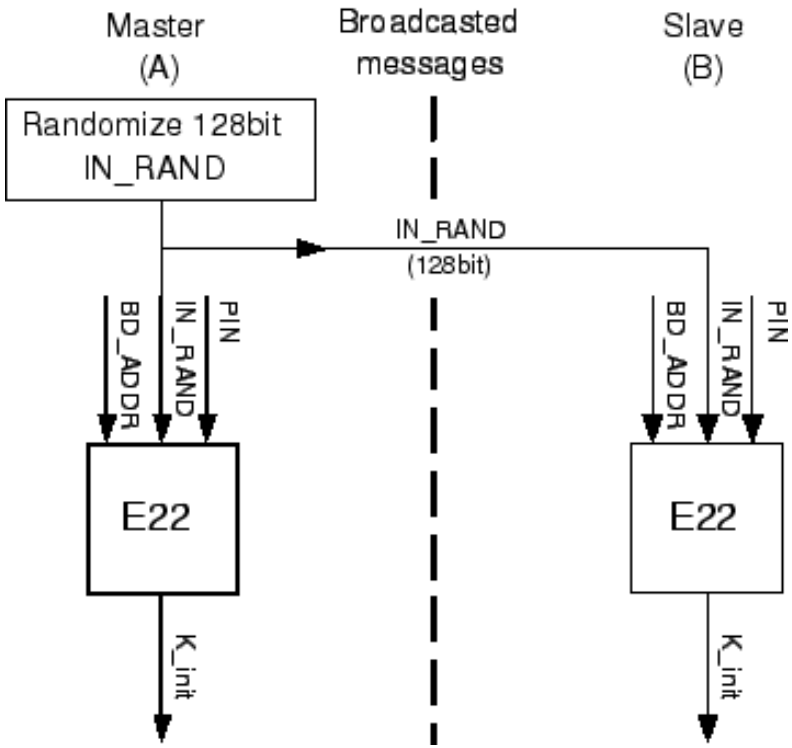
Bluetooth Pairing



Sniffing des Pairings

- BT_ADDR: bekannt
- IN_RAND: Protokollanalyser via Luftschnittstelle
- PIN: kann dann errechnet werden

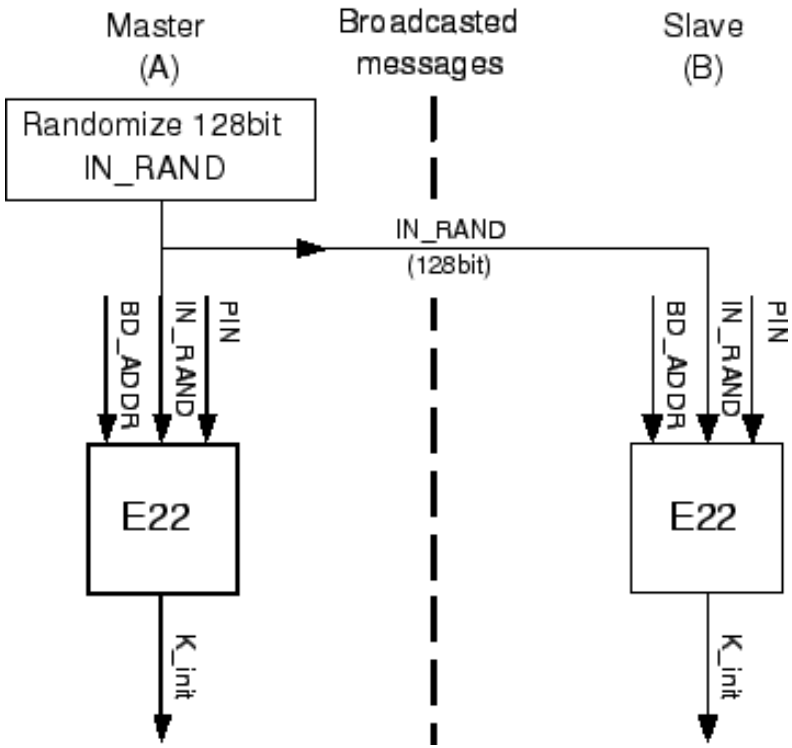
Bluetooth Pairing



Sniffing des Pairings

- BT_ADDR: bekannt
- IN_RAND: Protokollanalyser via Luftschnittstelle
- PIN: kann dann errechnet werden

Bluetooth Pairing



Sniffing des Pairings

- BT_ADDR: bekannt
- IN_RAND: Protokollanalyser via Luftschnittstelle
- PIN: kann dann errechnet werden

Zusammenfassung

- Bordmittel von bluez stellen bereits Mittel zum (lokalen) Debugging zur Verfügung
- Hardwareanalyser bieten u.A. die Möglichkeit über die Luftschnittstelle zu Sniffen
- Die Möglichkeit an der Luftschnittstelle mitzusniffen stellt ein Sicherheitsrisiko dar

- Ausblick
  - Der Angriff funktioniert eigentlich nur unter Laborbedingungen (Synchronisationsphasen des Analysers)
  - Bluetoothadresse muß bekannt sein

Weiterführende Literatur I

Bluetooth Core Specification v2.0 + EDR
Bluetooth SIG, Inc.
http://www.bluetooth.org/foundry/adopters/document/Core_v2.0_EDR/en/1/Core_v2.0_EDR.zip

Bluez
http://www.bluez.org/

Cracking the Bluetooth PIN
Yaniv Shaked and Avishai Wool
http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/

Weiterführende Literatur II

FTS4BT

Frontline Test Equipment, Inc.

http://www.fte.com/blu01.asp