# Spaß am Gerät: Bluetooth

Hagen Paul Pfeifer

„Wir machen keinen groben Unfug - wir machen feinen fug.“
– Wau Holland

http://www.jauu.net
hagen@jauu.net

25. November 2004

# Fahrplan

# Design Ziele

- geringe Komplexität
- geringe Stromaufnahme
- geringe Herstellungskosten (ein Chip Lösung)
- minimaler Setupoverhead
- global einsetzbar (Stichwort: Frequenzen(ISM-Band))
- Standardisierte Kommunikation

# Design Ziele

- geringe Komplexität
- geringe Stromaufnahme
- geringe Herstellungskosten (ein Chip Lösung)
- minimaler Setupoverhead
- global einsetzbar (Stichwort: Frequenzen(ISM-Band))
- Standardisierte Kommunikation

# Design Ziele

- geringe Komplexität
- geringe Stromaufnahme
- geringe Herstellungskosten (ein Chip Lösung)
- minimaler Setupoverhead
- global einsetzbar (Stichwort: Frequenzen(ISM-Band))
- Standardisierte Kommunikation

# Design Ziele

- geringe Komplexität
- geringe Stromaufnahme
- geringe Herstellungskosten (ein Chip Lösung)
- minimaler Setupoverhead
- global einsetzbar (Stichwort: Frequenzen(ISM-Band))
- Standardisierte Kommunikation

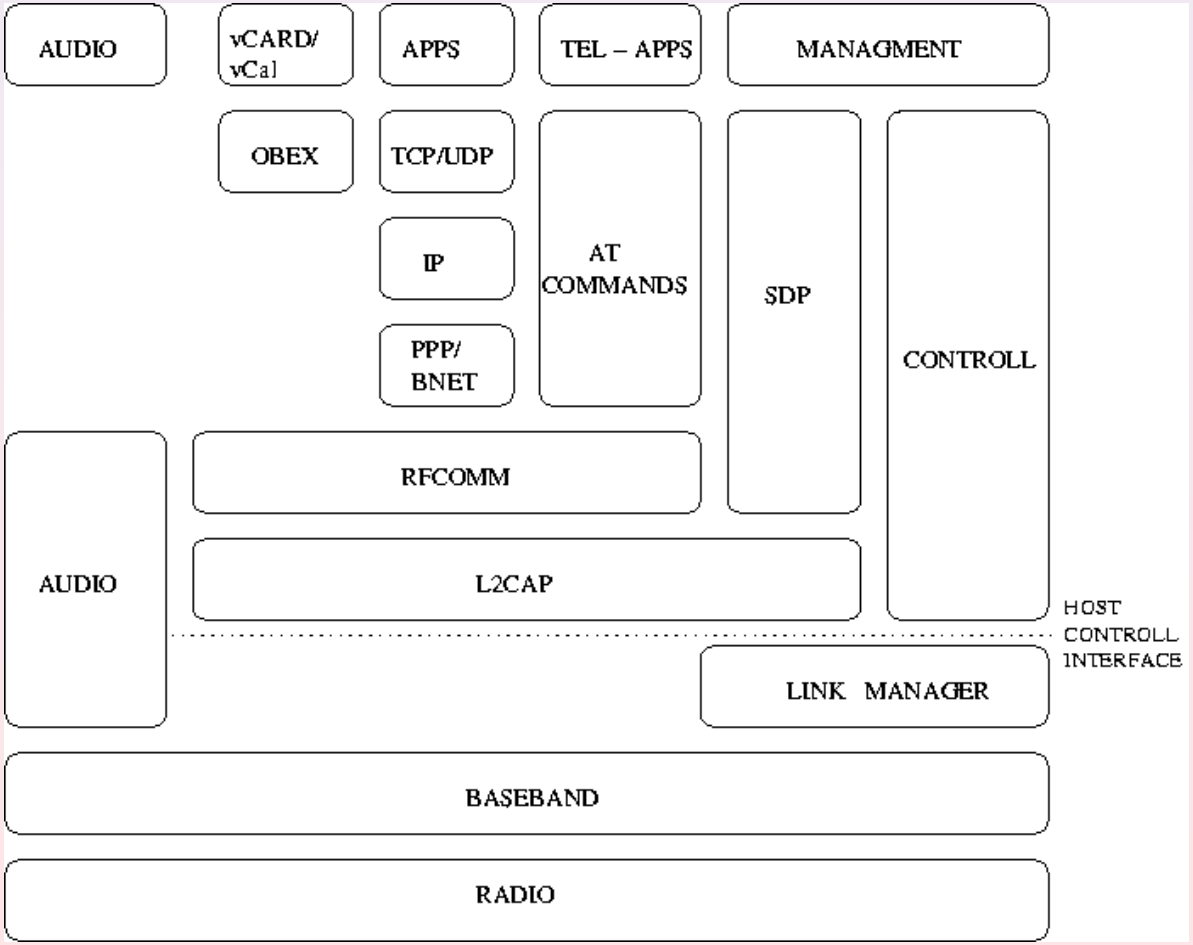
# Design Ziele

- geringe Komplexität
- geringe Stromaufnahme
- geringe Herstellungskosten (ein Chip Lösung)
- minimaler Setupoverhead
- global einsetzbar (Stichwort: Frequenzen(ISM-Band))
- Standardisierte Kommunikation

# Design Ziele

- geringe Komplexität
- geringe Stromaufnahme
- geringe Herstellungskosten (ein Chip Lösung)
- minimaler Setupoverhead
- global einsetzbar (Stichwort: Frequenzen(ISM-Band))
- Standardisierte Kommunikation

# Bluetooth Stack



# Radio

- 2.4 GHz Ism Band (2402-2480GHz)
- 79 hops (1Mhz)
- Hoprate: min. 1600 hops/s
- max. 2745 Bits pro Packet
- Raw Data Rate: 1Mbps (praktisch: 723kbps)(v1.1)
- Class 1-3 (ca. ${100m, 10m, 10cm})
- Sendestärke: 1mW bis 100mW

# Radio

- 2.4 GHz Ism Band (2402-2480GHz)
- 79 hops (1Mhz)
- Hoprate: min. 1600 hops/s
- max. 2745 Bits pro Packet
- Raw Data Rate: 1Mbps (praktisch: 723kbps)(v1.1)
- Class 1-3 (ca. ${100m, 10m, 10cm})
- Sendestärke: 1mW bis 100mW

# Radio

- 2.4 GHz Ism Band (2402-2480GHz)
- 79 hops (1Mhz)
- Hoprate: min. 1600 hops/s
- max. 2745 Bits pro Packet
- Raw Data Rate: 1Mbps (praktisch: 723kbps)(v1.1)
- Class 1-3 (ca. ${100m, 10m, 10cm})
- Sendestärke: 1mW bis 100mW

# Radio

- 2.4 GHz Ism Band (2402-2480GHz)
- 79 hops (1Mhz)
- Hoprate: min. 1600 hops/s
- max. 2745 Bits pro Packet
- Raw Data Rate: 1Mbps (praktisch: 723kbps)(v1.1)
- Class 1-3 (ca. ${100m, 10m, 10cm})
- Sendestärke: 1mW bis 100mW

# Radio

- 2.4 GHz Ism Band (2402-2480GHz)
- 79 hops (1Mhz)
- Hoprate: min. 1600 hops/s
- max. 2745 Bits pro Packet
- Raw Data Rate: 1Mbps (praktisch: 723kbps)(v1.1)
- Class 1-3 (ca. ${100m, 10m, 10cm})
- Sendestärke: 1mW bis 100mW

# Radio

- 2.4 GHz Ism Band (2402-2480GHz)
- 79 hops (1Mhz)
- Hoprate: min. 1600 hops/s
- max. 2745 Bits pro Packet
- Raw Data Rate: 1Mbps (praktisch: 723kbps)(v1.1)
- Class 1-3 (ca. ${100m, 10m, 10cm})
- Sendestärke: 1mW bis 100mW

# Radio

- 2.4 GHz Ism Band (2402-2480GHz)
- 79 hops (1Mhz)
- Hoprate: min. 1600 hops/s
- max. 2745 Bits pro Packet
- Raw Data Rate: 1Mbps (praktisch: 723kbps)(v1.1)
- Class 1-3 (ca. ${100m, 10m, 10cm})
- Sendestärke: 1mW bis 100mW

# Baseband

- Kontrolliert radio Schicht (z.b Frequenz Hop Sequenz)
- SCO (Synchronous Connection Oriented)(z.B. voice) oder ACL (Asynchronous Connection Less)(z.B. data)
- Inquerys
- Power Kontrolle
- Geräte welchen den gleichen Channel nutzen formen ein Piconet

# Baseband

- Kontrolliert radio Schicht (z.b Frequenz Hop Sequenz)
- SCO (Synchronous Connection Oriented)(z.B. voice) oder ACL (Asynchronous Connection Less)(z.B. data)
- Inquerys
- Power Kontrolle
- Geräte welchen den gleichen Channel nutzen formen ein Piconet

# Baseband

- Kontrolliert radio Schicht (z.b Frequenz Hop Sequenz)
- SCO (Synchronous Connection Oriented)(z.B. voice) oder ACL (Asynchronous Connection Less)(z.B. data)
- Inquerys
- Power Kontrolle
- Geräte welchen den gleichen Channel nutzen formen ein Piconet

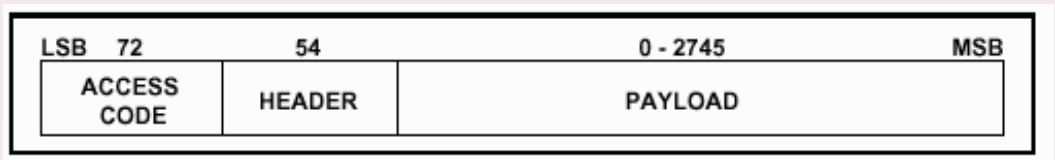
# Baseband

- Kontrolliert radio Schicht (z.b Frequenz Hop Sequenz)
- SCO (Synchronous Connection Oriented)(z.B. voice) oder ACL (Asynchronous Connection Less)(z.B. data)
- Inquerys
- Power Kontrolle
- Geräte welchen den gleichen Channel nutzen formen ein Piconet

# Baseband

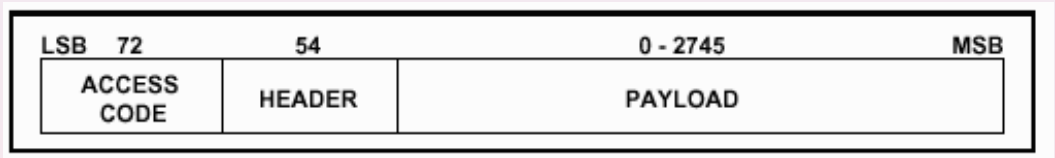
- Kontrolliert radio Schicht (z.b Frequenz Hop Sequenz)
- SCO (Synchronous Connection Oriented)(z.B. voice) oder ACL (Asynchronous Connection Less)(z.B. data)
- Inquerys
- Power Kontrolle
- Geräte welchen den gleichen Channel nutzen formen ein Piconet

# Packet Format



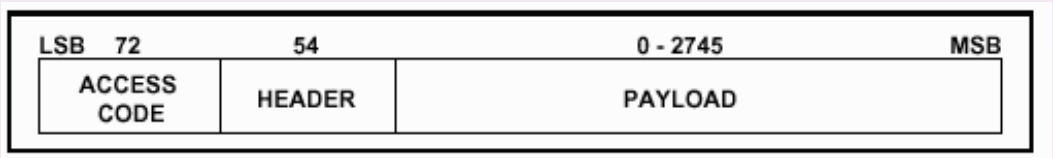

- Access Code: synchronisation, piconet id, ...
- Header: Paket Nummerierung, acks, flow controll, ...
- Payload: voice oder/und data, eigenen Header

# Packet Format




- Access Code: synchronisation, piconet id, ...
- Header: Paket Nummerierung, acks, flow controll, ...
- Payload: voice oder/und data, eigenen Header

# Packet Format




- Access Code: synchronisation, piconet id, ...
- Header: Paket Nummerierung, acks, flow controll, ...
- Payload: voice oder/und data, eigenen Header

# Link Manager Protocol

- Piconet Management
- Sicherheits Funktionen
- Link Konfiguration (QoS, Authentication)
- Power Management

# Link Manager Protocol

- Piconet Management
- Sicherheits Funktionen
- Link Konfiguration (QoS, Authentication)
- Power Management

# Link Manager Protocol

- Piconet Management
- Sicherheits Funktionen
- Link Konfiguration (QoS, Authentication)
- Power Management

# Link Manager Protocol

- Piconet Management
- Sicherheits Funktionen
- Link Konfiguration (QoS, Authentication)
- Power Management

# Abstecher: Pico Net

- Gruppe von verbundenen Geräten
- Master/Slaves (bis 8 Geräte)
- Kommunikation über SCO oder ACL

# Abstecher: Pico Net

- Gruppe von verbundenen Geräten
- Master/Slaves (bis 8 Geräte)
- Kommunikation über SCO oder ACL

# Abstecher: Pico Net

- Gruppe von verbundenen Geräten
- Master/Slaves (bis 8 Geräte)
- Kommunikation über SCO oder ACL

# L2CAP (Logical Link Controll and Adaption Protocol)

- Schnittstelle für Applikationen
- Multiplexing (Gruppenmanagment)
- Segmentation und Reassemblierung
- QoS

# L2CAP (Logical Link Controll and Adaption Protocol)

- Schnittstelle für Applikationen
- Multiplexing (Gruppenmanagment)
- Segmentation und Reassemblierung
- QoS

# L2CAP (Logical Link Controll and Adaption Protocol)

- Schnittstelle für Applikationen
- Multiplexing (Gruppenmanagment)
- Segmentation und Reassemblierung
- QoS

# L2CAP (Logical Link Controll and Adaption Protocol)

- Schnittstelle für Applikationen
- Multiplexing (Gruppenmanagment)
- Segmentation und Reassemblierung
- QoS

# HCI (Host Controller Interface)

- Zwischenschicht für Kommunikation
- glue zwischen Bus, Device und Box
- Lesen und setzen der Konfiguration
- Paket- und verbindungsorientiert

# HCI (Host Controller Interface)

- Zwischenschicht für Kommunikation
- glue zwischen Bus, Device und Box
- Lesen und setzen der Konfiguration
- Paket- und verbindungsorientiert

# HCI (Host Controller Interface)

- Zwischenschicht für Kommunikation
- glue zwischen Bus, Device und Box
- Lesen und setzen der Konfiguration
- Paket- und verbindungsorientiert

# HCI (Host Controller Interface)

- Zwischenschicht für Kommunikation
- glue zwischen Bus, Device und Box
- Lesen und setzen der Konfiguration
- Paket- und verbindungsorientiert

# RFCOMM

- simuliert serielle Schnittstelle
- AT Kommandos nutzen rfcomm
- ip ueber ppp ueber rfcomm

# RFCOMM

- simuliert serielle Schnittstelle
- AT Kommandos nutzen rfcomm
- ip ueber ppp ueber rfcomm

# RFCOMM

- simuliert serielle Schnittstelle
- AT Kommandos nutzen rfcomm
- ip ueber ppp ueber rfcomm

# OBEX

- OBject EXchange
- ähnlich http, nur binär (siehe Beispiel)
- nicht auf bluetooth beschränkt (kommt von IrDA)

# OBEX

- OBject EXchange
- ähnlich http, nur binär (siehe Beispiel)
- nicht auf bluetooth beschränkt (kommt von IrDA)

# OBEX

- OBject EXchange
- ähnlich http, nur binär (siehe Beispiel)
- nicht auf bluetooth beschränkt (kommt von IrDA)

# Verbindungsaufbau (Beispiel: emailapplikation)

1. inquiring (Suchen nach bt devices)
2. paging (synchronisieren der devices)
3. link establishment (SCO oder ACL)
4. service discovery (sdp)
5. l2cap channel
6. rfcomm Verbindung über l2cap layer
7. pairing (PIN, encryption, ...)
8. ppp, ip, tcp, ...

# Verbindungsaufbau (Beispiel: emailapplikation)

1. inquiring (Suchen nach bt devices)
2. paging (synchronisieren der devices)
3. link establishment (SCO oder ACL)
4. service discovery (sdp)
5. l2cap channel
6. rfcomm Verbindung über l2cap layer
7. pairing (PIN, encryption, ...)
8. ppp, ip, tcp, ...

# Verbindungsaufbau (Beispiel: emailapplikation)

1. inquiring (Suchen nach bt devices)
2. paging (synchronisieren der devices)
3. link establishment (SCO oder ACL)
4. service discovery (sdp)
5. l2cap channel
6. rfcomm Verbindung über l2cap layer
7. pairing (PIN, encryption, ...)
8. ppp, ip, tcp, ...

# Verbindungsaufbau (Beispiel: emailapplikation)

1. inquiring (Suchen nach bt devices)
2. paging (synchronisieren der devices)
3. link establishment (SCO oder ACL)
4. service discovery (sdp)
5. l2cap channel
6. rfcomm Verbindung über l2cap layer
7. pairing (PIN, encryption, ...)
8. ppp, ip, tcp, ...

# Verbindungsaufbau (Beispiel: emailapplikation)

1. inquiring (Suchen nach bt devices)
2. paging (synchronisieren der devices)
3. link establishment (SCO oder ACL)
4. service discovery (sdp)
5. l2cap channel
6. rfcomm Verbindung über l2cap layer
7. pairing (PIN, encryption, . . . )
8. ppp, ip, tcp, . . .

# Verbindungsaufbau (Beispiel: emailapplikation)

1. inquiring (Suchen nach bt devices)
2. paging (synchronisieren der devices)
3. link establishment (SCO oder ACL)
4. service discovery (sdp)
5. l2cap channel
6. rfcomm Verbindung über l2cap layer
7. pairing (PIN, encryption, . . . )
8. ppp, ip, tcp, . . .

# Verbindungsaufbau (Beispiel: emailapplikation)

1. inquiring (Suchen nach bt devices)
2. paging (synchronisieren der devices)
3. link establishment (SCO oder ACL)
4. service discovery (sdp)
5. l2cap channel
6. rfcomm Verbindung über l2cap layer
7. pairing (PIN, encryption, . . . )
8. ppp, ip, tcp, . . .

# Verbindungsaufbau (Beispiel: emailapplikation)

1. inquiring (Suchen nach bt devices)
2. paging (synchronisieren der devices)
3. link establishment (SCO oder ACL)
4. service discovery (sdp)
5. l2cap channel
6. rfcomm Verbindung über l2cap layer
7. pairing (PIN, encryption, . . . )
8. ppp, ip, tcp, . . .

# Probleme bei Bluetooth

- Interferenzen im ISM Band (802.11, MikroWellenKanonen)
- schnelle Anpassung auf Netzwerkinfastruktur
- einfache Verbindungsaufbau (Ergonomitaet vs. Sicherheit)
-

# Probleme bei Bluetooth

- Interferenzen im ISM Band (802.11, MikroWellenKanonen)
- schnelle Anpassung auf Netzwerkinfastruktur
- einfache Verbindungsaufbau (Ergonomitaet vs. Sicherheit)
-

# Probleme bei Bluetooth

- Interferenzen im ISM Band (802.11, MikroWellenKanonen)
- schnelle Anpassung auf Netzwerkinfastruktur
- einfache Verbindungsaufbau (Ergonomitaet vs. Sicherheit)

# Probleme bei Bluetooth

- Interferenzen im ISM Band (802.11, MikroWellenKanonen)
- schnelle Anpassung auf Netzwerkinfastruktur
- einfache Verbindungsaufbau (Ergonomitaet vs. Sicherheit)
-

# Bluetooth und Linux

- Seit 2.4.6 im Kernel (BlueZ Stack)
- Implementierung von Quallcom
- Alternativ: affix Stack

# Bluetooth und Linux

- Seit 2.4.6 im Kernel (BlueZ Stack)
- Implementierung von Quallcom
- Alternativ: affix Stack

# Bluetooth und Linux

- Seit 2.4.6 im Kernel (BlueZ Stack)
- Implementierung von Quallcom
- Alternativ: affix Stack

# der erste Start

- Kernel module:
  hci_usb bluetooth l2cap rfcomm hci_uart
- user space Applikationen:
  bluez-utils bluez-sdp bluez-hcidump
- Device starten:
  hciconfig hci0 up
- Voila: hcitool scan

# der erste Start

- Kernel module:
  hci_usb bluetooth l2cap rfcomm hci_uart
- user space Applikationen:
  bluez-utils bluez-sdp bluez-hcidump
- Device starten:
  hciconfig hci0 up
- Voila: hcitool scan

# der erste Start

- Kernel module:
  hci_usb bluetooth l2cap rfcomm hci_uart
- user space Applikationen:
  bluez-utils bluez-sdp bluez-hcidump
- Device starten:
  hciconfig hci0 up
- Voila: hcitool scan

# der erste Start

- Kernel module:
  hci_usb bluetooth l2cap rfcomm hci_uart
- user space Applikationen:
  bluez-utils bluez-sdp bluez-hcidump
- Device starten:
  hciconfig hci0 up
- Voila: hcitool scan

# Einleitung

- überwiegender Teil der Schwachstellen sind in höheren Schichten anzusiedeln

# Einleitung

- überwiegender Teil der Schwachstellen sind in höheren Schichten anzusiedeln
-

# Einleitung

- überwiegender Teil der Schwachstellen sind in höheren Schichten anzusiedeln
-

# Tools

- redfang - sucht nach non-discoverable devices
- bluesniff - ncurses sniffer
- btscanner - ncurses scanner

# Tools

- redfang - sucht nach non-discoverable devices
- bluesniff - ncurses sniffer
- btscanner - ncurses scanner

# Tools

- redfang - sucht nach non-discoverable devices
- bluesniff - ncurses sniffer
- btscanner - ncurses scanner

# bluejacking

- nicht wirklich eine technische Schwachstelle; eher „User broken“
- es geht um pseudo-anonymen Datenversand
- beruht auf der Tatsache das ein char[248] beim pairing versendet wird
- Gefahr: Verbindung wird angenohmen weil gehirn gerade „100% ideled“
  Schema: „Gehirnverkleinerung? - Drück mich!“

# bluejacking

- nicht wirklich eine technische Schwachstelle; eher „User broken“
- es geht um pseudo-anonymen Datenversand
- beruht auf der Tatsache das ein char[248] beim pairing versendet wird
- Gefahr: Verbindung wird angenohmen weil gehirn gerade „100% ideled“
  Schema: „Gehirnverkleinerung? - Drück mich!“

# bluejacking

- nicht wirklich eine technische Schwachstelle; eher „User broken“
- es geht um pseudo-anonymen Datenversand
- beruht auf der Tatsache das ein char[248] beim pairing versendet wird
- Gefahr: Verbindung wird angenohmen weil gehirn gerade „100% ideled“
  Schema: „Gehirnverkleinerung? - Drück mich!“

# bluejacking

- nicht wirklich eine technische Schwachstelle; eher „User broken“
- es geht um pseudo-anonymen Datenversand
- beruht auf der Tatsache das ein char[248] beim pairing versendet wird
- Gefahr: Verbindung wird angenohmen weil gehirn gerade „100% ideled“
  Schema: „Gehirnverkleinerung? - Drück mich!“

# bluebug

- verbindung via rfcomm zu Gerät
- Zugang via higher level protocols *rightarrow* AT commands
- Möglichkeiten: ppp, Telefonie, sms

# bluebug

- verbindung via rfcomm zu Gerät
- Zugang via higher level protocols *rightarrow* AT commands
- Möglichkeiten: ppp, Telefonie, sms

# bluebug

- verbindung via rfcomm zu Gerät
- Zugang via higher level protocols *rightarrow* AT commands
- Möglichkeiten: ppp, Telefonie, sms

# bluesnarfing

- Prinzip: Datendiebstahl ohne Spuren
- lesen, schreiben und modifizieren von Adressbuch und/oder Kalendereinträgen
- lesender Zugriff auf IMEI
- seltener: Zugriff auf kompletten Speicher
- Schwachstellen in Implementierungen
- betroffene Geräte: Nokia 6310, 7650, 8910; Ericsson T68, T610; ...

# bluesnarfing

- Prinzip: Datendiebstahl ohne Spuren
- lesen, schreiben und modifizieren von Adressbuch und/oder Kalendereinträgen
- lesender Zugriff auf IMEI
- seltener: Zugriff auf kompletten Speicher
- Schwachstellen in Implementierungen
- betroffene Geräte: Nokia 6310, 7650, 8910; Ericsson T68, T610; ...

# bluesnarfing

- Prinzip: Datendiebstahl ohne Spuren
- lesen, schreiben und modifizieren von Adressbuch und/oder Kalendereinträgen
- lesender Zugriff auf IMEI
- seltener: Zugriff auf kompletten Speicher
- Schwachstellen in Implementierungen
- betroffene Geräte: Nokia 6310, 7650, 8910; Ericsson T68, T610; . . .

# bluesnarfing

- Prinzip: Datendiebstahl ohne Spuren
- lesen, schreiben und modifizieren von Adressbuch und/oder Kalendereinträgen
- lesender Zugriff auf IMEI
- seltener: Zugriff auf kompletten Speicher
- Schwachstellen in Implementierungen
- betroffene Geräte: Nokia 6310, 7650, 8910; Ericsson T68, T610; . . .

# bluesnarfing

- Prinzip: Datendiebstahl ohne Spuren
- lesen, schreiben und modifizieren von Adressbuch und/oder Kalendereinträgen
- lesender Zugriff auf IMEI
- seltener: Zugriff auf kompletten Speicher
- Schwachstellen in Implementierungen
- betroffene Geräte: Nokia 6310, 7650, 8910; Ericsson T68, T610; . . .

# bluesnarfing

- Prinzip: Datendiebstahl ohne Spuren
- lesen, schreiben und modifizieren von Adressbuch und/oder Kalendereinträgen
- lesender Zugriff auf IMEI
- seltener: Zugriff auf kompletten Speicher
- Schwachstellen in Implementierungen
- betroffene Geräte: Nokia 6310, 7650, 8910; Ericsson T68, T610; ...

# DoS

- Korrupte bt Frames (6310i *rightarrow* reboot)

# Gegenmaßnahmen

- Stecker ziehen: bluetooth nur anschalten wenn benötigt
- non-discoverable mode

# Gegenmaßnahmen

- Stecker ziehen: bluetooth nur anschalten wenn benötigt
- non-discoverable mode

# Was gibt es noch zu sagen?

- kostengünstiger Wlan Erstatz: bnep und pand
- Sicherheitslücken werden in höheren Schichten entstehen (Stichwort: Obex, etc., Java Applikationen, )

# Was gibt es noch zu sagen?

- kostengünstiger Wlan Erstatz: bnep und pand
- Sicherheitslücken werden in höheren Schichten entstehen (Stichwort: Obex, etc., Java Applikationen, )

# Für die BWL Vorlesung bestens geeignet!

- Manual Pages
  *man {rfcomm, hcitool, hciconfig}*
- Online Ressource
  *http://www.holtmann.org*
- Online Ressource
  *http://www.palowireless.com*

# Für die BWL Vorlesung bestens geeignet!

- Manual Pages
  *man {rfcomm, hcitool, hciconfig}*
- Online Ressource
  *http://www.holtmann.org*
- Online Ressource
  *http://www.palowireless.com*

# Für die BWL Vorlesung bestens geeignet!

- Manual Pages
  *man {rfcomm, hcitool, hciconfig}*
- Online Ressource
  *http://www.holtmann.org*
- Online Ressource
  *http://www.palowireless.com*

# Für die BWL Vorlesung bestens geeignet!

- Manual Pages
  *man {rfcomm, hcitool, hciconfig}*
- Online Ressource
  *http://www.holtmann.org*
- Online Ressource
  *http://www.palowireless.com*