

bluetooth (in)security

Pascal Steichen

25th Jan 2006 - LinuxDays 2006

- 1 bluetooth
- 2 threats
- 3 bluetooth technology
 - bluetooth stack
 - bluetooth protocols
- 4 bluetooth and gnu/linux
- 5 hacking techniques
- 6 tools and more ...
- 7 thanks
- 8 live demo

bluetooth



From the Viking-king Harald Blatand, who unified the "northmen" to today's mobile wireless technology number one (?).

threats

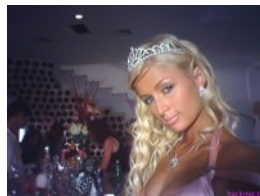
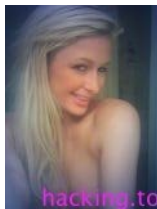
what hopefully won't be our near future:



Paris Hilton

From here hax0red mobile:

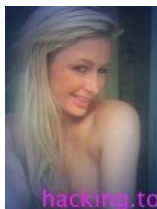
- Pictures (the least explicit ...):



Paris Hilton

From here [hax0red mobile](#):

- Pictures (the least explicit ...):



- Telephone numbers:
Aguilera, Christina: 1-310-917-9191
Eminem: 1-917-776-7643
Roddick, Andy: 1-512-228-2207

Malware

cabir/mabir



hobbes.A



latest:

- SymbOS.Sendtool.A

Malware

cabir/mabir



hobbes.A



latest:

- SymbOS.Sendtool.A
- SymbOS.Pbstealer.D

Malware

cabir/mabir



hobbes.A



latest:

- SymbOS.Sendtool.A
- SymbOS.Pbstealer.D
- SymbOS.Bootton.E

bluetooth technology

basic characteristics:

- idea and origin from Ericsson

bluetooth technology

basic characteristics:

- idea and origin from Ericsson
- developed by bluetooth-SIG (founded in 1998)

bluetooth technology

basic characteristics:

- idea and origin from Ericsson
- developed by bluetooth-SIG (founded in 1998)
- wireless using the 2.4Ghz ISM band

bluetooth technology

basic characteristics:

- idea and origin from Ericsson
- developed by bluetooth-SIG (founded in 1998)
- wireless using the 2.4Ghz ISM band
- frequency hopping technology (79 channels, 1600 hops per second)

bluetooth technology

basic characteristics:

- idea and origin from Ericsson
- developed by bluetooth-SIG (founded in 1998)
- wireless using the 2.4Ghz ISM band
- frequency hopping technology (79 channels, 1600 hops per second)
- ~1Mb/s transfer rates

bluetooth technology

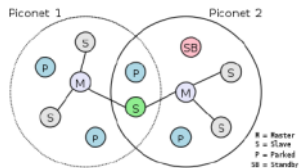
basic characteristics:

- idea and origin from Ericsson
- developed by bluetooth-SIG (founded in 1998)
- wireless using the 2.4Ghz ISM band
- frequency hopping technology (79 channels, 1600 hops per second)
- ~1Mb/s transfer rates
- theoretical range: 10m to 100m

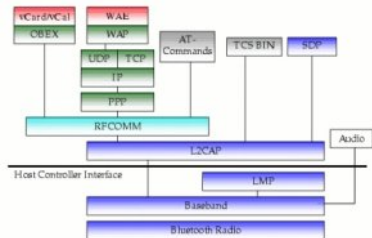
bluetooth technology

basic characteristics:

- idea and origin from Ericsson
- developed by bluetooth-SIG (founded in 1998)
- wireless using the 2.4Ghz ISM band
- frequency hopping technology (79 channels, 1600 hops per second)
- ~1Mb/s transfer rates
- theoretical range: 10m to 100m
- organizes in piconets

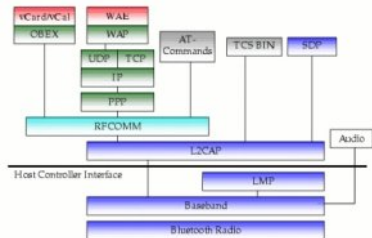


bluetooth stack



blue et rfcomm bluetooth specific

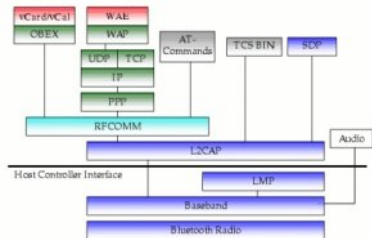
bluetooth stack



blue et rfcomm bluetooth specific

green adapted from existing technologies

bluetooth stack

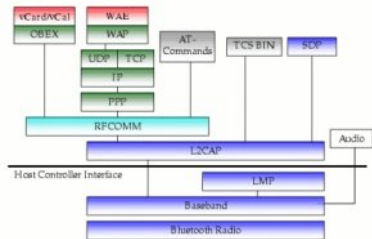


blue et rfcomm bluetooth specific

green adapted from existing technologies

gray telephony related (fax, etc.)

bluetooth stack



blue et rfcomm bluetooth specific

green adapted from existing technologies

gray telephony related (fax, etc.)

red application layer (adapted)

bluetooth protocols

LMP "Link Manager Protocol", responsible for the liaison between bluetooth equipments bt (authentication, encryption)

bluetooth protocols

LMP "Link Manager Protocol", responsible for the liaison between bluetooth equipments bt (authentication, encryption)

HCI "Host Controller Interface"

bluetooth protocols

LMP "Link Manager Protocol", responsible for the liaison between bluetooth equipments bt (authentication, encryption)

HCI "Host Controller Interface"

L2CAP "Logical Link Control and Adaptation Protocol", link to layers above

bluetooth protocols

LMP "Link Manager Protocol", responsible for the liaison between bluetooth equipments bt (authentication, encryption)

HCI "Host Controller Interface"

L2CAP "Logical Link Control and Adaptation Protocol", link to layers above

RFCOMM "Cable Replacement Protocol", transport channel for communications (emulates rs-232), necessary for almost all applications

bluetooth protocols

LMP "Link Manager Protocol", responsible for the liaison between bluetooth equipments bt (authentication, encryption)

HCI "Host Controller Interface"

L2CAP "Logical Link Control and Adaptation Protocol", link to layers above

RFCOMM "Cable Replacement Protocol", transport channel for communications (emulates rs-232), necessary for almost all applications

SDP "Service Discovery Protocol", implicit to almost all communications, gives information about available services

bluetooth protocols

LMP "Link Manager Protocol", responsible for the liaison between bluetooth equipments bt (authentication, encryption)

HCI "Host Controller Interface"

L2CAP "Logical Link Control and Adaptation Protocol", link to layers above

RFCOMM "Cable Replacement Protocol", transport channel for communications (emulates rs-232), necessary for almost all applications

SDP "Service Discovery Protocol", implicit to almost all communications, gives information about available services

AT commands commands to use modem and fax features

bluetooth protocols

LMP "Link Manager Protocol", responsible for the liaison between bluetooth equipments bt (authentication, encryption)

HCI "Host Controller Interface"

L2CAP "Logical Link Control and Adaptation Protocol", link to layers above

RFCOMM "Cable Replacement Protocol", transport channel for communications (emulates rs-232), necessary for almost all applications

SDP "Service Discovery Protocol", implicit to almost all communications, gives information about available services

AT commands commands to use modem and fax features

OBEX "Object Exchange Protocol" (adapted from IrDA), to 

bluetooth protocols

LMP "Link Manager Protocol", responsible for the liaison between bluetooth equipments bt (authentication, encryption)

HCI "Host Controller Interface"

L2CAP "Logical Link Control and Adaptation Protocol", link to layers above

RFCOMM "Cable Replacement Protocol", transport channel for communications (emulates rs-232), necessary for almost all applications

SDP "Service Discovery Protocol", implicit to almost all communications, gives information about available services

AT commands commands to use modem and fax features

OBEX "Object Exchange Protocol" (adapted from IrDA), to 

security modes

- Security mode 1
No active security enforcement

security modes

- Security mode 1
No active security enforcement
- Security mode 2
Service level security (on device level no difference to mode 1)

security modes

- Security mode 1
No active security enforcement
- Security mode 2
Service level security (on device level no difference to mode 1)
- Security mode 3
Device level security (enforce security for every low-level connection)

Pairing

- First connection

Pairing

- First connection
 - 1 Pin code request

Pairing

- First connection
 - 1 Pin code request
 - 2 Pin code request reply

Pairing

- First connection
 - 1 Pin code request
 - 2 Pin code request reply
 - 3 Link key notification

Pairing

- First connection
 - 1 Pin code request
 - 2 Pin code request reply
 - 3 Link key notification
- Further connections

Pairing

- First connection
 - 1 Pin code request
 - 2 Pin code request reply
 - 3 Link key notification
- Further connections
 - 1 Link key request

Pairing

- First connection
 - 1 Pin code request
 - 2 Pin code request reply
 - 3 Link key notification
- Further connections
 - 1 Link key request
 - 2 Link key request reply

Pairing

- First connection
 - 1 Pin code request
 - 2 Pin code request reply
 - 3 Link key notification
- Further connections
 - 1 Link key request
 - 2 Link key request reply
 - 3 Link key notification (optional)

bluetooth and gnu/linux

blueZ official gnu/linux bluetooth protocol stack (included in 2.4 and 2.6 kernel series)

bluetooth and gnu/linux

blueZ official gnu/linux bluetooth protocol stack (included in 2.4 and 2.6 kernel series)

- site: www.bluez.org

bluetooth and gnu/linux

blueZ official gnu/linux bluetooth protocol stack (included in 2.4 and 2.6 kernel series)

- site: www.bluez.org
- core developers: Marcel Holtmann, Max Krasnyansky

bluetooth and gnu/linux

blueZ official gnu/linux bluetooth protocol stack (included in 2.4 and 2.6 kernel series)

- site: www.bluez.org
- core developers: Marcel Holtmann, Max Krasnyansky
- license: GPL

bluetooth and gnu/linux

blueZ official gnu/linux bluetooth protocol stack (included in 2.4 and 2.6 kernel series)

- site: www.bluez.org
- core developers: Marcel Holtmann, Max Krasnyansky
- license: GPL

affix bluetooth protocol stack for gnu/linux (replacement for bluez)

bluetooth and gnu/linux

blueZ official gnu/linux bluetooth protocol stack (included in 2.4 and 2.6 kernel series)

- site: www.bluez.org
- core developers: Marcel Holtmann, Max Krasnyansky
- license: GPL

affix bluetooth protocol stack for gnu/linux (replacement for bluez)

- site: affix.sf.net

bluetooth and gnu/linux

blueZ official gnu/linux bluetooth protocol stack (included in 2.4 and 2.6 kernel series)

- site: www.bluez.org
- core developers: Marcel Holtmann, Max Krasnyansky
- license: GPL

affix bluetooth protocol stack for gnu/linux (replacement for bluez)

- site: affix.sf.net
- core developers: Nokia Research Center

bluetooth and gnu/linux

blueZ official gnu/linux bluetooth protocol stack (included in 2.4 and 2.6 kernel series)

- site: www.bluez.org
- core developers: Marcel Holtmann, Max Krasnyansky
- license: GPL

affix bluetooth protocol stack for gnu/linux (replacement for bluez)

- site: affix.sf.net
- core developers: Nokia Research Center
- license: GPL

bluez utils

- hciconfig, hcitool

bluez utils

- hciconfig, hcitool
- sdptool

hacking techniques

- bluesnarf, bluesnarf++

hacking techniques

- bluesnarf, bluesnarf++
- bluebug

hacking techniques

- bluesnarf, bluesnarf++
- bluebug
- helomoto

hacking techniques

- bluesnarf, bluesnarf++
- bluebug
- helomoto
- bluesmack

hacking techniques

- bluesnarf, bluesnarf++
- bluebug
- helomoto
- bluesmack
- bluestab

hacking techniques

- bluesnarf, bluesnarf++
- bluebug
- helomoto
- bluesmack
- bluestab
- bluebump, mode 3 abuse

hacking techniques

- bluesnarf, bluesnarf++
- bluebug
- helomoto
- bluesmack
- bluestab
- bluebump, mode 3 abuse
- bluespoof

hacking techniques

- bluesnarf, bluesnarf++
- bluebug
- helomoto
- bluesmack
- bluestab
- bluebump, mode 3 abuse
- bluespoof
- bluedump

hacking techniques

- bluesnarf, bluesnarf++
- bluebug
- helomoto
- bluesmack
- bluestab
- bluebump, mode 3 abuse
- bluespoof
- bluedump
- bluetooone

hacking techniques

- bluesnarf, bluesnarf++
- bluebug
- helomoto
- bluesmack
- bluestab
- bluebump, mode 3 abuse
- bluespoof
- bluedump
- bluetooone
- bluestalker

hacking techniques

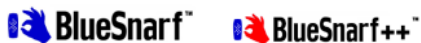
- bluesnarf, bluesnarf++
- bluebug
- helomoto
- bluesmack
- bluestab
- bluebump, mode 3 abuse
- bluespoof
- bluedump
- bluetooone
- bluestalker
- bluechop

bluesnarf, bluesnarf++



OBEX push attack

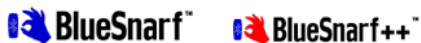
bluesnarf, bluesnarf++



OBEX push attack

- pull known objects via the (non authenticated) push channel

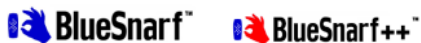
bluesnarf, bluesnarf++



OBEX push attack

- pull known objects via the (non authenticated) push channel
- bluesnarf++ (due to direct acces to the obex ftp):

bluesnarf, bluesnarf++



OBEX push attack

- pull known objects via the (non authenticated) push channel
- bluesnarf++ (due to direct acces to the obex ftp):
 - Contents are browseable

bluesnarf, bluesnarf++



OBEX push attack

- pull known objects via the (non authenticated) push channel
- bluesnarf++ (due to direct acces to the obex ftp):
 - Contents are browseable
 - Full read and write access
 - Access to external media storage

bluebug



use of AT commands

bluebug



use of AT commands

- use hidden (and unprotected) channels via a direct rfcomm connection

helomoto

the motorola bluebug-bluesnarf combination

bluesmack



DoS attack

bluestab



another DoS attack

bluebump, mode 3 abuse



social engineering attack

bluebump, mode 3 abuse



social engineering attack

- force authentication for benign task (even mode 3 -> mode 3 abuse)

bluebump, mode 3 abuse



social engineering attack

- force authentication for benign task (even mode 3 -> mode 3 abuse)
- tell partner to delete pairing

bluebump, mode 3 abuse



social engineering attack

- force authentication for benign task (even mode 3
-> mode 3 abuse)
- tell partner to delete pairing
 - hold connection open

bluebump, mode 3 abuse



social engineering attack

- force authentication for benign task (even mode 3 -> mode 3 abuse)
- tell partner to delete pairing
 - hold connection open
 - request change of connection link key

bluebump, mode 3 abuse



social engineering attack

- force authentication for benign task (even mode 3
-> mode 3 abuse)
- tell partner to delete pairing
 - hold connection open
 - request change of connection link key
- access unauthorized channels

bluespoof



social engineering attack

bluespoof



social engineering attack

- try to clone a trusted device
 - Device address

bluespoof



social engineering attack

- try to clone a trusted device
 - Device address
 - Service records

bluespoof



social engineering attack

- try to clone a trusted device
 - Device address
 - Service records
 - Emulate protocols and profiles

bluespoof



social engineering attack

- try to clone a trusted device
 - Device address
 - Service records
 - Emulate protocols and profiles
- Disable encryption

bluespoof



social engineering attack

- try to clone a trusted device
 - Device address
 - Service records
 - Emulate protocols and profiles
- Disable encryption
- Force re-pairing with devices trusting the clone

bluedump



kind of brute-force PIN attack

bluedump



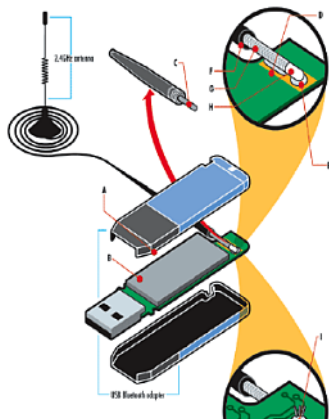
kind of brute-force PIN attack

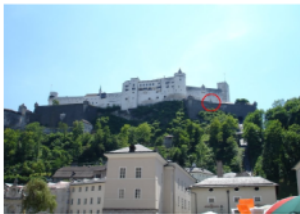
- theoretical paper:
<http://www.eng.tau.ac.il/~yash/Bluetooth/>

bluetoone



Enhancing the range of a Bluetooth dongle by connecting a





bluestalker

abuse GSM location tracking service

bluestalker

abuse GSM location tracking service

- use BlueBug to intercept SMS confirmation message

bluechop

- Brandnew attack

bluechop

- Brandnew attack
- Disrupts established Bluetooth Piconets

tools and more ...

- bloover, bloover II

tools and more ...

- bloover, bloover II
- blueprinting

tools and more ...

- bloover, bloover II
- blueprinting
- bluepot

tools and more ...

- bloover, bloover II
- blueprinting
- bluepot
- carwhisperer

tools and more ...

- bloover, bloover II
- blueprinting
- bluepot
- carwhisperer
- bloonix

tools and more ...

- bloover, bloover II
- blueprinting
- bluepot
- carwhisperer
- bloonix
- bluesniffing

bloover, bloover II



Bloover - Bluetooth Wireless Technology Hoover

bloover, bloover II



Bloover - Bluetooth Wireless Technology Hoover

- Java-based toola for mobile phones

bloover, bloover II



Bloover - Bluetooth Wireless Technology Hoover

- Java-based toola for mobile phones
 - J2ME MIDP 2.0 with bluetooth-API

bloover, bloover II



Bloover - Bluetooth Wireless Technology Hoover

- Java-based toola for mobile phones
 - J2ME MIDP 2.0 with bluetooth-API
- version II new included attacks:

bloover, bloover II



Bloover - Bluetooth Wireless Technology Hoover

- Java-based toola for mobile phones
 - J2ME MIDP 2.0 with bluetooth-API
- version II new included attacks:
 - BlueBug

bloover, bloover II



Bloover - Bluetooth Wireless Technology Hoover

- Java-based toola for mobile phones
 - J2ME MIDP 2.0 with bluetooth-API
- version II new included attacks:
 - BlueBug
 - HeloMoto

bloover, bloover II



Bloover - Bluetooth Wireless Technology Hoover

- Java-based toola for mobile phones
 - J2ME MIDP 2.0 with bluetooth-API
- version II new included attacks:
 - BlueBug
 - HeloMoto
 - BlueSnarf

bloover, bloover II



Bloover - Bluetooth Wireless Technology Hoover

- Java-based toola for mobile phones
 - J2ME MIDP 2.0 with bluetooth-API
- version II new included attacks:
 - BlueBug
 - HeloMoto
 - BlueSnarf
 - Malformed Objects

bloover, bloover II



Bloover - Bluetooth Wireless Technology Hoover

- Java-based toola for mobile phones
 - J2ME MIDP 2.0 with bluetooth-API
- version II new included attacks:
 - BlueBug
 - HeloMoto
 - BlueSnarf
 - Malformed Objects



blueprinting



Fingerprinting for Bluetooth

blueprinting



Fingerprinting for Bluetooth

- based on the SDP records

bluetooth (in)security

└ tools and more ...

└ bluepot

bluepot



Bluetooth HoneyPot

bluepot



Bluetooth HoneyPot

- Runs on J2ME phones (with bluetooth-API)

bluepot



Bluetooth HoneyPot

- Runs on J2ME phones (with bluetooth-API)
- Imitates vulnerable phone

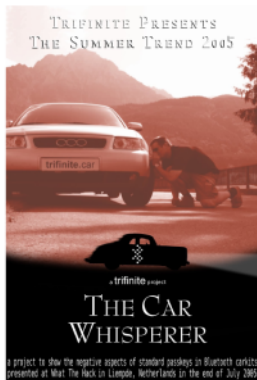
bluepot



Bluetooth HoneyPot

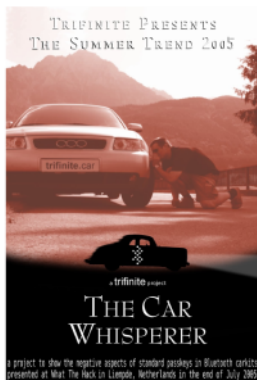
- Runs on J2ME phones (with bluetooth-API)
- Imitates vulnerable phone
- Logs incoming attacks & device info

carwhisperer



- uses default pin codes to connect to carkits

carwhisperer



- uses default pin codes to connect to carkits
- inject/record audio

bloonix



Linux distribution for Bluetooth audits



Linux distribution for Bluetooth audits

- Linux-based Live CD



Linux distribution for Bluetooth audits

- Linux-based Live CD
- Contains all latest BlueZ utilities



Linux distribution for Bluetooth audits

- Linux-based Live CD
- Contains all latest BlueZ utilities
- Dedicated auditing tools for each vulnerability



Linux distribution for Bluetooth audits

- Linux-based Live CD
- Contains all latest BlueZ utilities
- Dedicated auditing tools for each vulnerability
- Report generation

bluetooth (in)security

└ tools and more ...

└ bluesniffing

bluesniffing

Local Sniffing

bluesniffing

Local Sniffing

- hcidump

bluesniffing

Local Sniffing

- hcidump

Piconet Sniffing

bluesniffing

Local Sniffing

- hcidump

Piconet Sniffing

- special hardware or firmware

bluesniffing

Local Sniffing

- hcidump

Piconet Sniffing

- special hardware or firmware

Air Sniffing

bluesniffing

Local Sniffing

- hcidump

Piconet Sniffing

- special hardware or firmware

Air Sniffing

- Frontline (<http://www.fte.com/>)

bluesniffing

Local Sniffing

- hcidump

Piconet Sniffing

- special hardware or firmware

Air Sniffing

- Frontline (<http://www.fte.com/>)
- LeCroy/CatC (<http://www.lecroy.com/>)

thanks

to the investigators:

- Adam Laurie
CSO of The Bunker Secure Hosting Ltd.
DEFCON staff and organizer
Apache-SSL co-publisher

thanks

to the investigators:

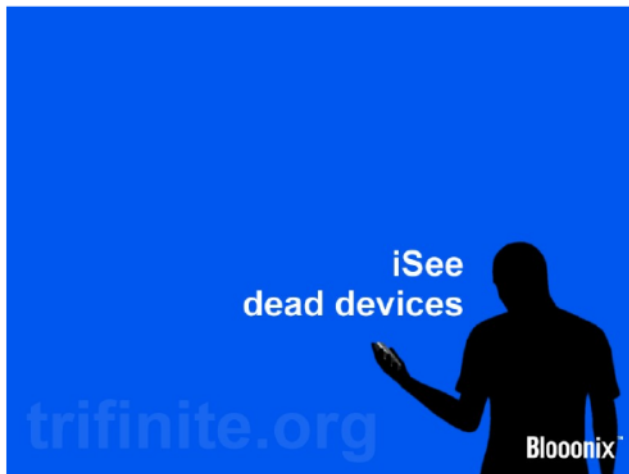
- Adam Laurie
CSO of The Bunker Secure Hosting Ltd.
DEFCON staff and organizer
Apache-SSL co-publisher
- Marcel Holtmann
Maintainer of the Linux Bluetooth stack
Red Hat Certified Examiner (RHCE)

thanks

to the investigators:

- Adam Laurie
CSO of The Bunker Secure Hosting Ltd.
DEFCON staff and organizer
Apache-SSL co-publisher
- Marcel Holtmann
Maintainer of the Linux Bluetooth stack
Red Hat Certified Examiner (RHCE)
- Martin Herfurt
Security researcher
Founder of trifinite.org

live demo



... and hoping Murphy's not around ;)