Bluetooth Hacking

The State of the Art

22C3

December 30st 2005, Berlin, Germany

by Adam Laurie, Marcel Holtmann and Martin Herfurt

... because infinite is sometimes not enough!

trifinite.org

Agenda

- Quick technology overview
- Security mechanisms
- Known vulnerabilities
- Tooools & new stuff
- Demonstrations

Who is investigating

- 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 (RHCX)
- Martin Herfurt
  - Security researcher
  - Founder of *trifinite.org*

What we are up against

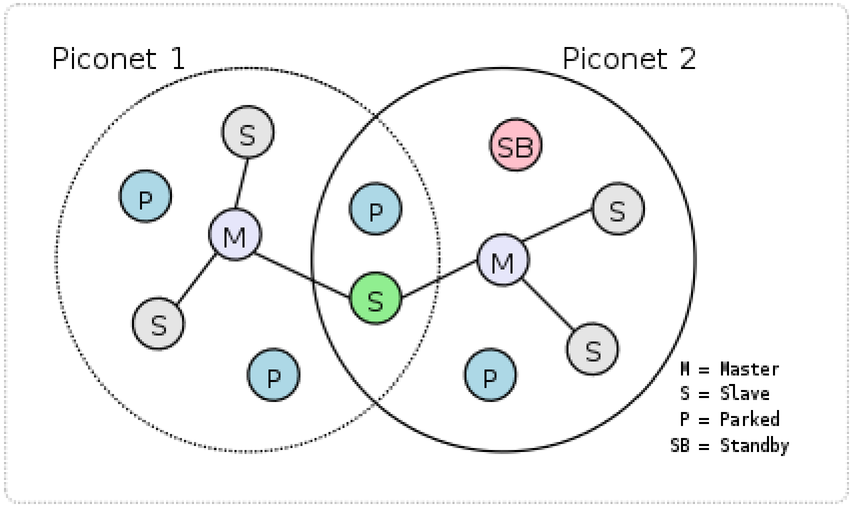
RITSCH-RENN.COM
New device found: Airbus A310
Proceed with configuration ?
luca scheuring airlines
luca scheuring airlines
Es wurde ein neues Gerät gefunden.
Device:Airbus A310
Soll die Auto-Konfiguration gestartet werden?
Start
Abbrechen
Bluetooth
1/2003

What is Bluetooth

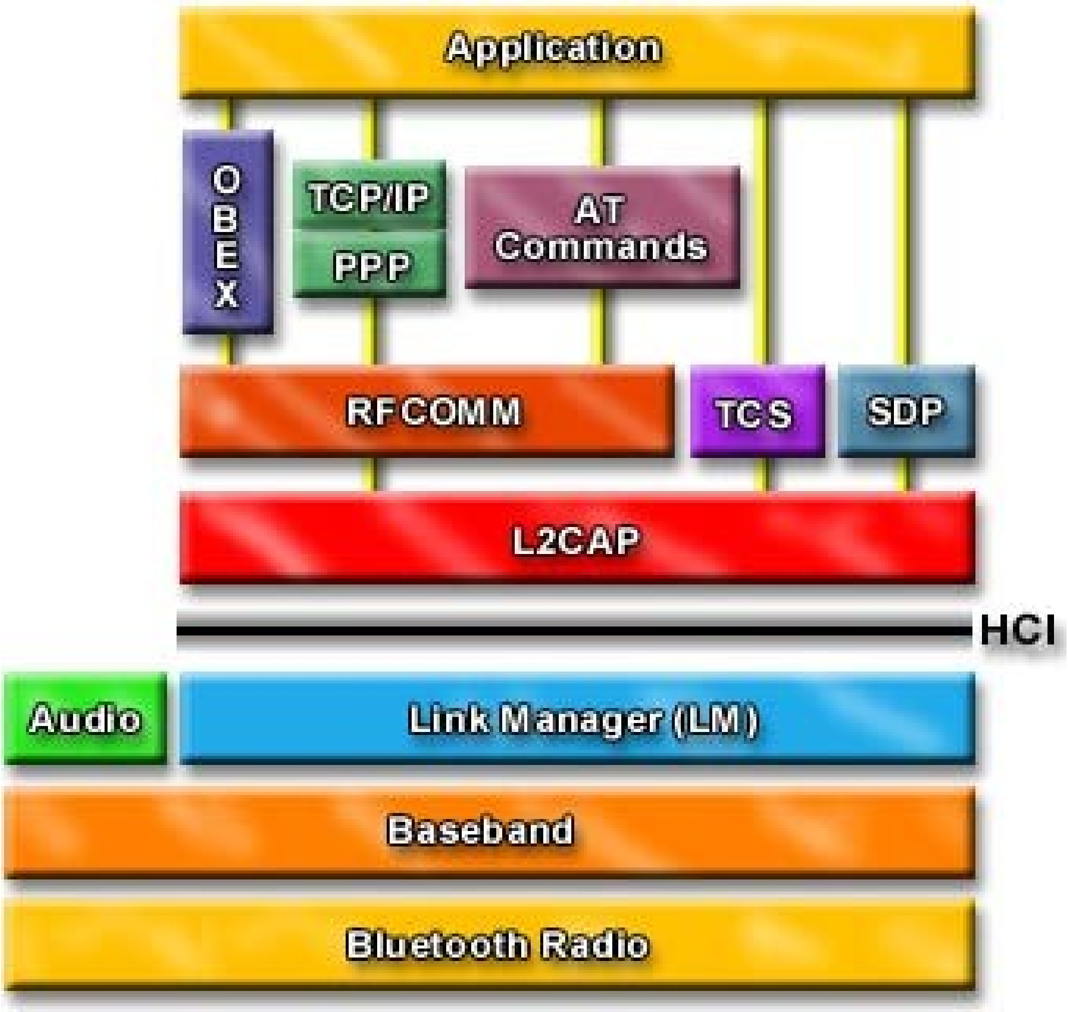
- Bluetooth SIG
  - Trade association
  - Founded 1998
  - Owns and licenses IP
- Bluetooth technology
  - A general cable replacement
  - Using the ISM band at 2.4 GHz
  - Protocol stack and application profiles

Network Topology

- Hopping sequence defines the piconet
  - Master defines the hopping sequence
    - 1600 hops per second on 79 channels
  - Up to seven active slaves
  - Scatternet creation



Bluetooth Stack



Application specific security mechanisms

Bluetooth host security mechanisms

Security mechanisms on the Bluetooth chip

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

How pairing works

- First connection
  (1) > HCI_Pin_Code_Request
  (2) < HCI_Pin_Code_Request_Reply
  (3) > HCI_Link_Key_Notification
- Further connections
  (1) > HCI_Link_Key_Request
  (2) < HCI_Link_Key_Request_Reply
  (3) > HCI_Link_Key_Notification (optional)

Principles of good Security (CESG/GCHQ)

- Confidentiality
  - Data kept private
- Integrity
  - Data has not been modified
- Availability
  - Data is available when needed
- Authentication
  - Identity of peer is proven
- Non-repudiation
  - Peer cannot deny transaction took place

Breaking all of them

- Confidentiality
  - Reading data
- Integrity
  - Modifying data
- Availability
  - Deleting data
- Authentication
  - Bypassed completely
- Non-repudiation
  - Little or no logging / no audit trails

Remember Paris

Compromised Content

- Paris Hilton's phonebook
  - Numbers of **real** Celebrities (rockstars, actors ...)

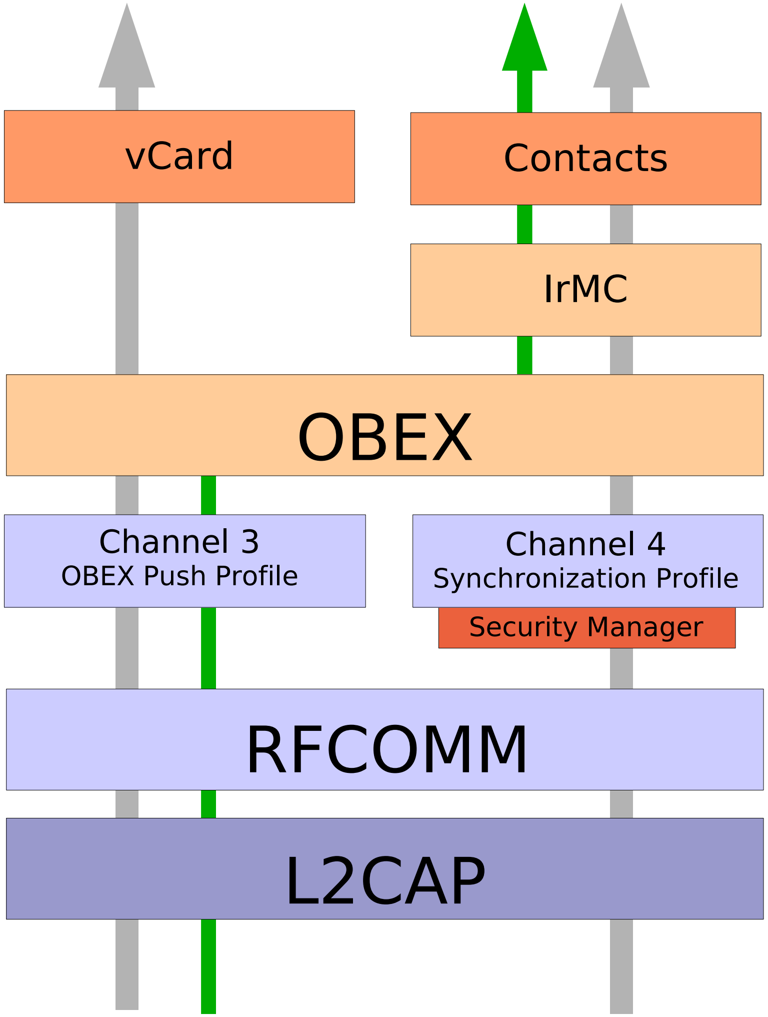
- Images

- US Secret Service
  - Confidential documents

BlueSnarf

- Trivial OBEX push attack
  - Pull knows objects instead of pushing
  - No authentication
- Discovered by Marcel Holtmann
  - Published in October 2003
- Also discovered by Adam Laurie
  - Published in November 2003
  - Field tests at London Underground etc.

How to avoid pairing



BlueBug

- Issuing AT commands
  - Use hidden and unprotected channels
  - Full control over the phone
- Discovered by Martin Herfurt
  - Motivation from the BlueSnarf attack
  - Public field test a CeBIT 2004
- Possibility to cause extra costs

HeloMoto

- Requires entry in “My Devices”
- Use OBEX push to create entry
  - No full OBEX exchange needed
- Connect to headset/handsfree channel
  - No authentication required
  - Full access with AT command
- Discovered by Adam Laurie

Authentication abuse

- Create pairing
  - Authenticate for benign task
  - Force authentication
  - Use security mode 3 if needed
- Connect to unauthorized channels
  - Serial Port Profile
  - Dialup Networking
  - OBEX File Transfer

BlueSmack

- Using L2CAP echo feature
  - Signal channel request and response
  - L2CAP signal MTU is unknown
  - No open L2CAP channel needed
- Causing buffer overflows
- Denial of service attack

BlueStab

- Denial of service attack
  - Bluetooth device name is UTF-8 encoded
  - Friendly name with control characters
  - Crashes some phones
  - Can cause weird behaviors
  - Name caches can be very problematic
- Credits to Q-Nix and Collin R. Mulliner

BlueBump

- Forced re-keying
  - Authenticate for benign task (vCard exchange)
  - Force authentication
- Tell partner to delete pairing
  - Hold connection open
  - Request change of connection link key
- Connect to unauthorized channels

BlueSnarf++

- OBEX push channel attack, again
  - Connect with Sync, FTP or BIP target UUID
  - No authentication
  - Contents are browseable
  - Full read and write access
  - Access to external media storage
- Manufacturers have been informed

BlueSpooof

- Clone a trusted device
  - Device address
  - Service records
  - Emulate protocols and profiles
- Disable encryption
- Force re-pairing

BlueDump

- Yanic Shaked and Avishai Wool
    - http://www.eng.tau.ac.il/~yash/Bluetooth/
    - Expands PIN attack from Ollie Whitehouse
    - Requires special hardware or firmware
- Destroy trust relationship
    - Use the BlueSpooof methods
- User interaction for pairing still needed

BlueChop

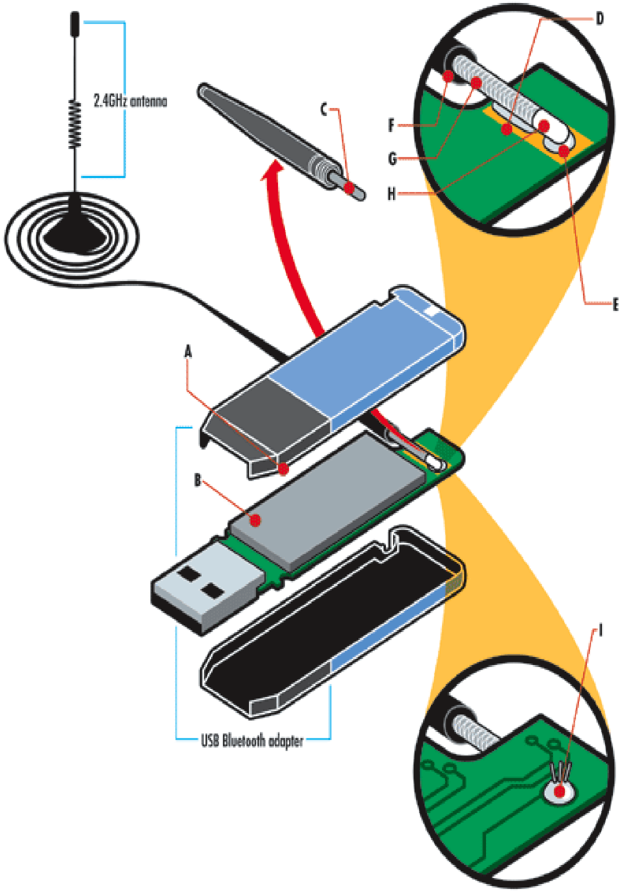
- Brandnew attack (new for 22C3)
- Disrupts established Bluetooth Piconets
- Independent from device manufacturer
  - Bluetooth standard thing
- Works for devices that are
  - Multiconnection capable (pretty much all the newer devices)
  - Page-able during an ongoing connection (very likely since more than one device can connect)

Blueprinting

- Fingerprinting for Bluetooth
- Work started by Collin R. Mulliner and Martin Herfurt
- Based on the SDP records and OUI
- Important for security audits
- Paper with more information available

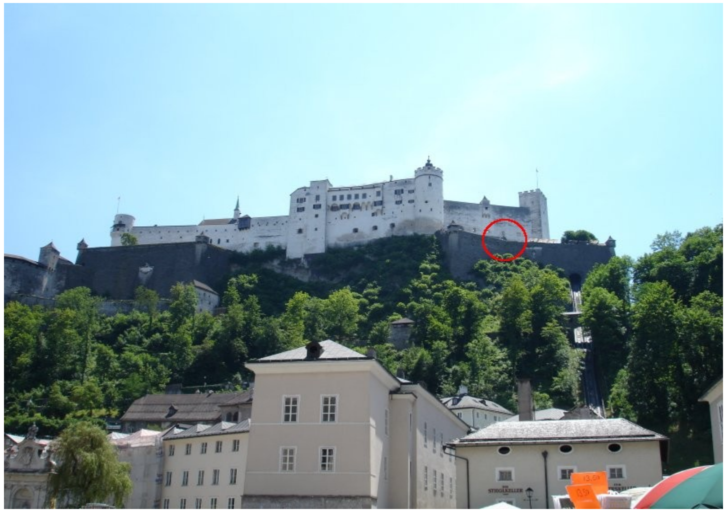
Bluetooone

- Enhancing the range of a Bluetooth dongle by connecting a directional antenna -> as done in the Long Distance Attack
- Original idea from Mike Outmesguine (Author of Book: “Wi-Fi Toys”)
- Step by Step instruction on trifinite.org



Bluetooone

Bluetooone™



Blooover

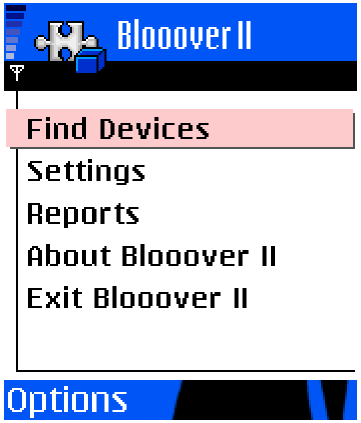
Blooover™

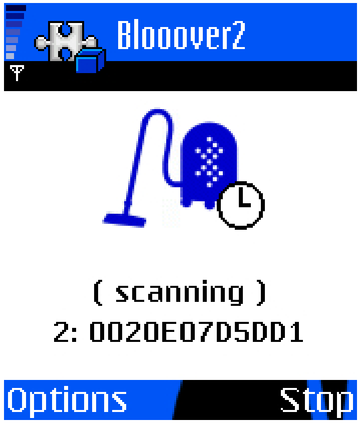
- Blooover - *Bluetooth* Wireless Technology Hoover
- Proof-of-Concept Application
- Educational Purposes only
- Java-based
  - J2ME MIDP 2.0 **with** BT-API
- Released last year at 21C3
- 150.000 + **x** downloads
  - Blooover also distributed by other portals

Blooover II

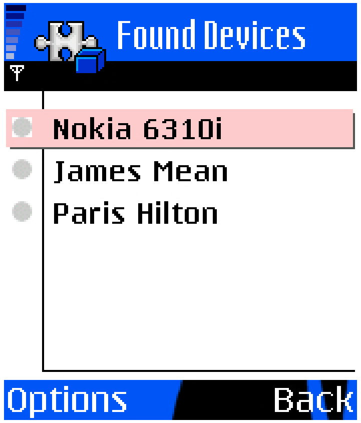
- Successor of the popular Blooover application
  - Auditing toool for professionals/researchers
  - Included Audits
    - BlueBug
    - HeloMoto
    - BlueSnarf
    - Malformed Objects
- Beta-phase starting today ;-)

Blooover II - Auditing

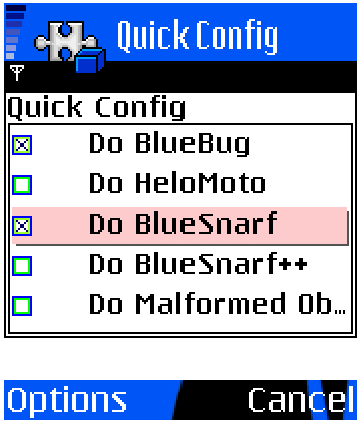




(scanning)
2: 0020E07D5DD1

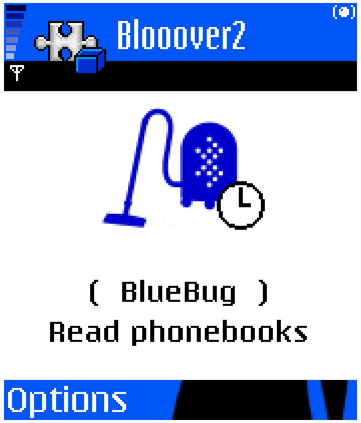


Nokia 6310i
James Mean
Paris Hilton

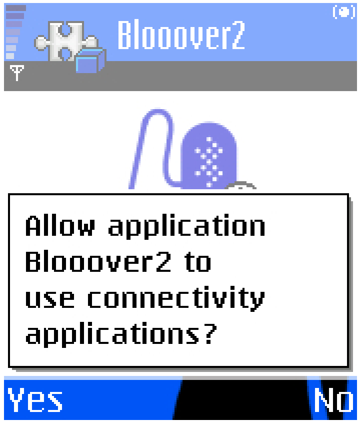


Quick Config

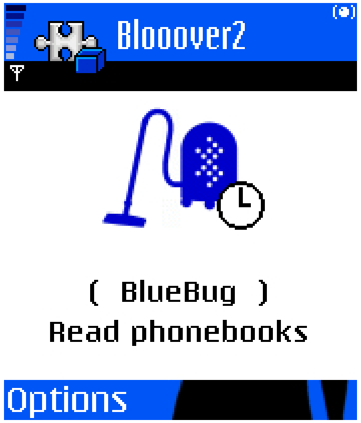
☒ Do BlueBug
□ Do HeloMoto
☒ Do BlueSnarf
□ Do BlueSnarf++
□ Do Malformed Ob…



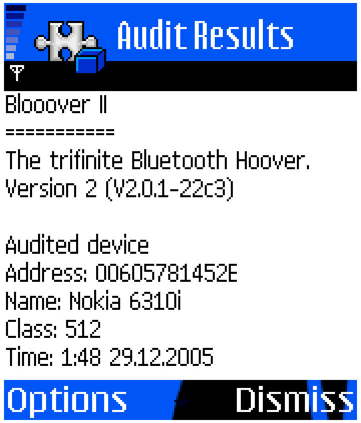
(BlueBug)
Read phonebooks



Allow application Blooover2 to use connectivity applications?

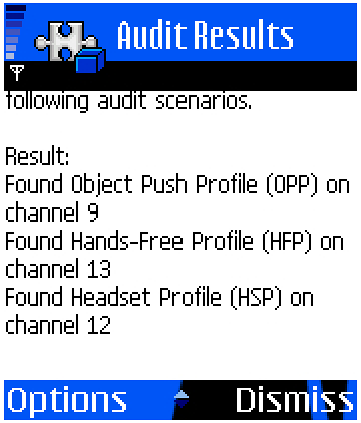


(BlueBug)
Read phonebooks



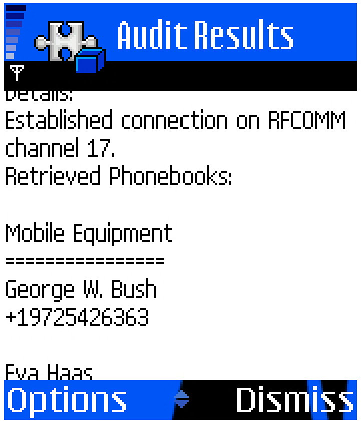
Blooover II
===========
The trifinite Bluetooth Hoover.
Version 2 (V2.0.1-22c3)

Audited device
Address: 00605781452E
Name: Nokia 6310i
Class: 512
Time: 1:48 29.12.2005



following audit scenarios.

Result:
Found Object Push Profile (OPP) on channel 9
Found Hands-Free Profile (HFP) on channel 13
Found Headset Profile (HSP) on channel 12

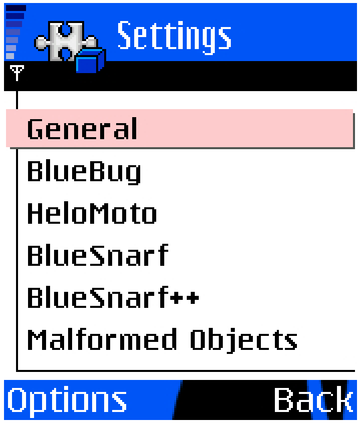


Details:
Established connection on RFCOMM channel 17.
Retrieved Phonebooks:

Mobile Equipment
================
George W. Bush
+19725426363

Eva Haas

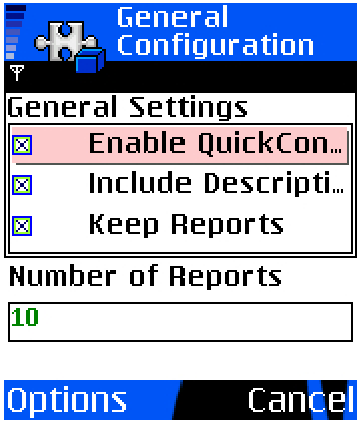
Blooover II - Settings



Settings

General
BlueBug
HeloMoto
BlueSnarf
BlueSnarf++
Malformed Objects

Options Back



General Configuration

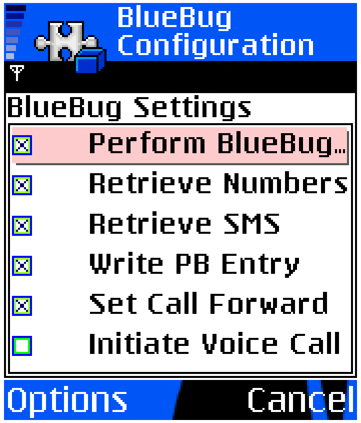
General Settings

☒ Enable QuickCon…
☒ Include Descripti…
☒ Keep Reports

Number of Reports

10

Options Cancel

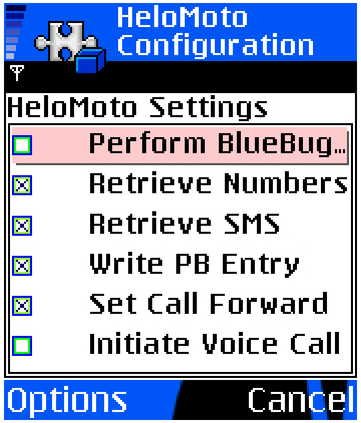


BlueBug Configuration

BlueBug Settings

☒ Perform BlueBug…
☒ Retrieve Numbers
☒ Retrieve SMS
☒ Write PB Entry
☒ Set Call Forward
□ Initiate Voice Call

Options Cancel

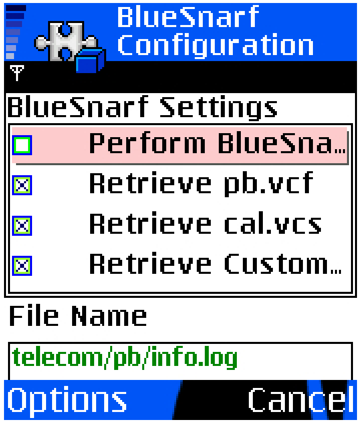


HeloMoto Configuration

HeloMoto Settings

□ Perform BlueBug…
☒ Retrieve Numbers
☒ Retrieve SMS
☒ Write PB Entry
☒ Set Call Forward
□ Initiate Voice Call

Options Cancel



BlueSnarf Configuration

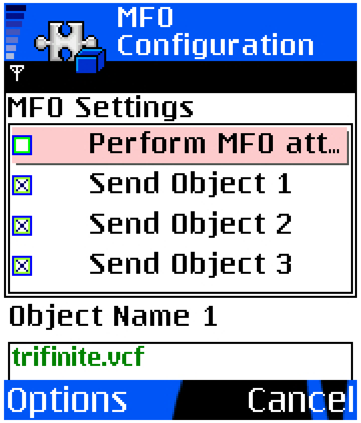
BlueSnarf Settings

□ Perform BlueSna…
☒ Retrieve pb.vcf
☒ Retrieve cal.vcs
☒ Retrieve Custom…

File Name

telecom/pb/info.log

Options Cancel



MFO Configuration

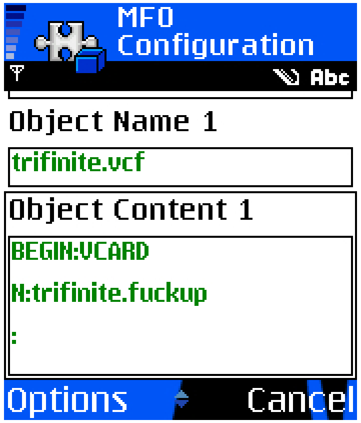
MFO Settings

□ Perform MFO att…
☒ Send Object 1
☒ Send Object 2
☒ Send Object 3

Object Name 1

trifinite.vcf

Options Cancel



MFO Configuration

Abc

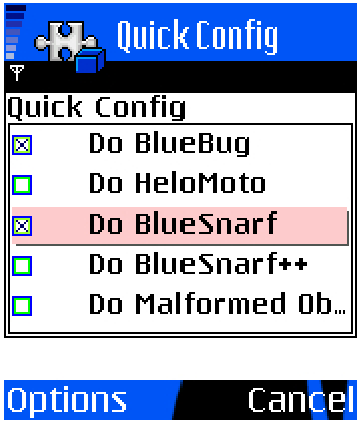
Object Name 1

trifinite.vcf

Object Content 1

BEGIN:VCARD
N:trifinite.fuckup
:

Options Cancel



Quick Config

Quick Config

☒ Do BlueBug
□ Do HeloMoto
☒ Do BlueSnarf
□ Do BlueSnarf++
□ Do Malformed Ob…

Options Cancel

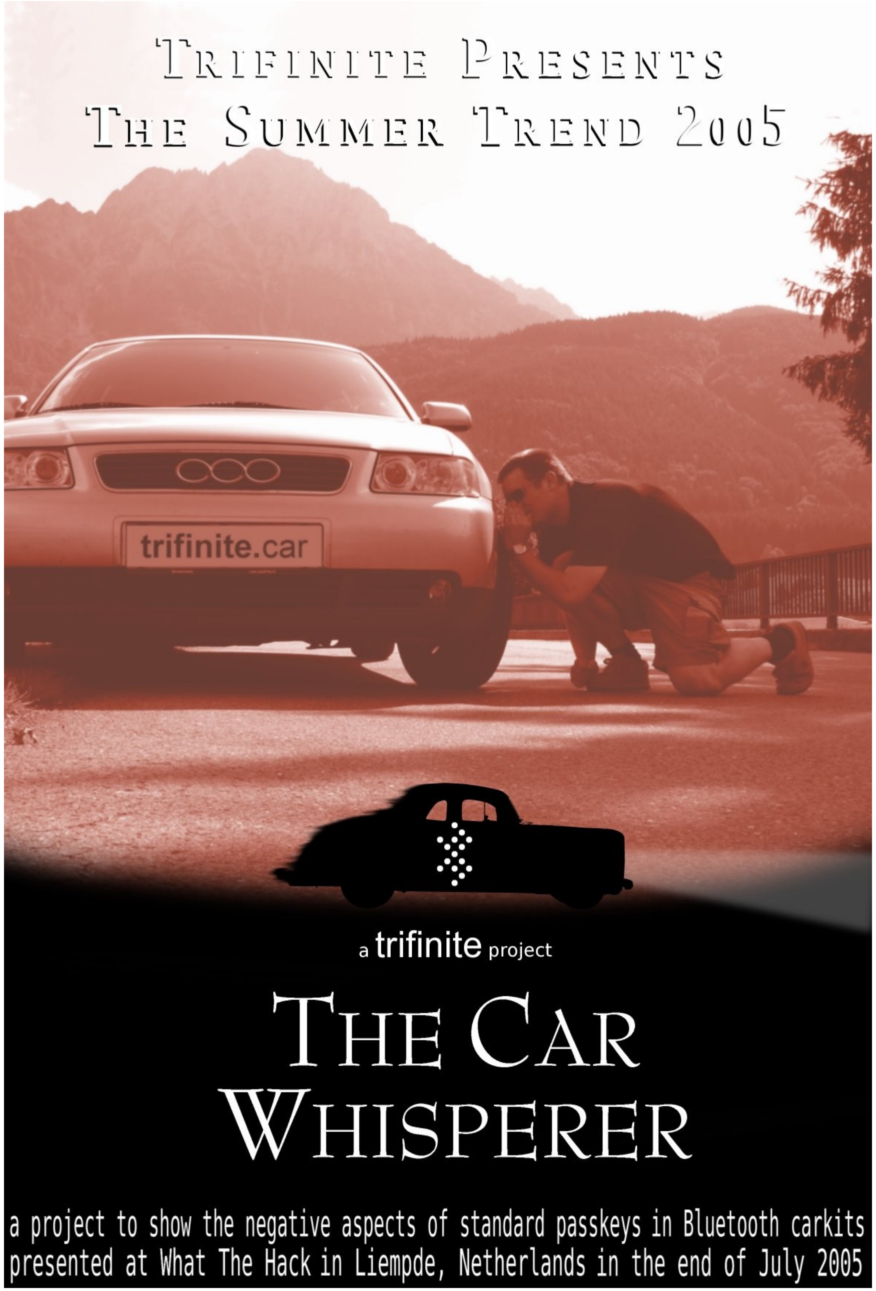
Blooover II - Breeeder

- Special edition for 22c3
- World Domination through p2p propagation
- Breeeder Version distributes 'Blooover II Babies'
  - Babies cannot breed

The Car Whisperer

- Use default pin codes to connect to carkits
- Inject audio
- Record audio

- Version 0.2 now available
  - Better phone emulation capabilities

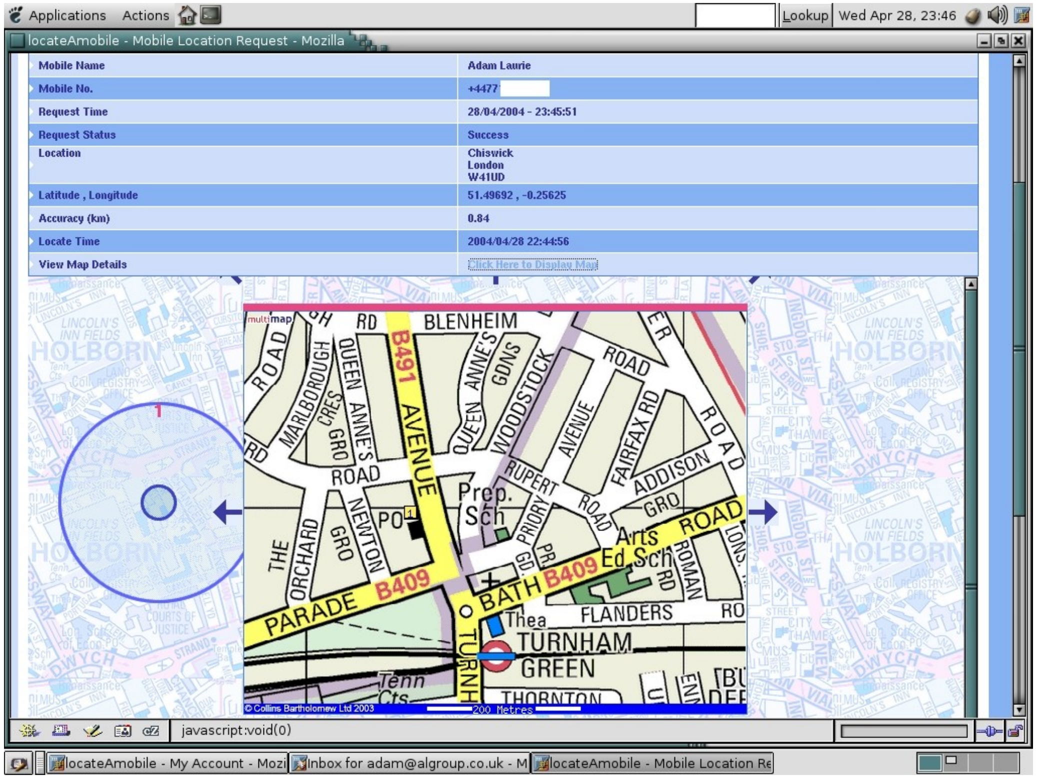

Trifinite Presents
The Summer Trend 2005
trifinite.car
a trifinite project
The Car Whisperer
a project to show the negative aspects of standard passkeys in Bluetooth carkits
presented at What The Hack in Liempde, Netherlands in the end of July 2005

The Car Whisperer

- Stationary directional antenna
    - 15 seconds visibility at an average speed of 120 km/h and a range 500 m

BlueStalker

- Commercial tracking service
  - GSM Location tracking (Accurate to about 800 meters)
- BlueBug SMS message to determine phone number and intercept confirmation message

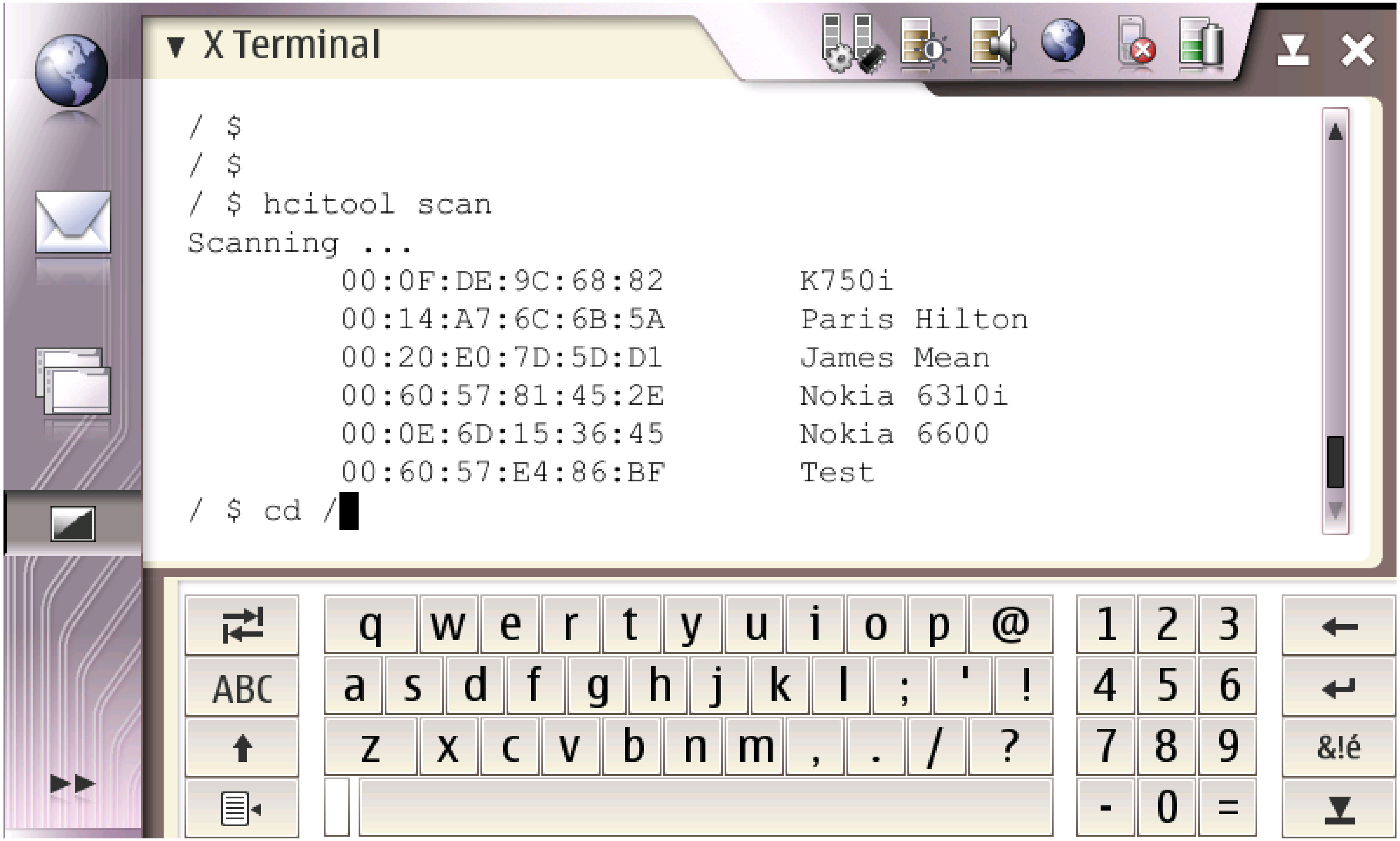

Applications
Actions
Lookup
Wed Apr 28, 23:46
locateAmobile - Mobile Location Request - Mozilla
multimap
© Collins Bartholomew Ltd 2003
200 Metres
javascript:void(0)
locateAmobile - My Account - Mozi
Inbox for adam@algroup.co.uk - M
locateAmobile - Mobile Location Re

Mobile Name	Adam Laurie
Mobile No.	+4477 [redacted]
Request Time	28/04/2004 - 23:45:51
Request Status	Success
Location	Chiswick London W41UD
Latitude , Longitude	51.49692 , -0.25625
Accuracy (km)	0.84
Locate Time	2004/04/28 22:44:56
View Map Details	Click Here to Display Map

Nokia 770

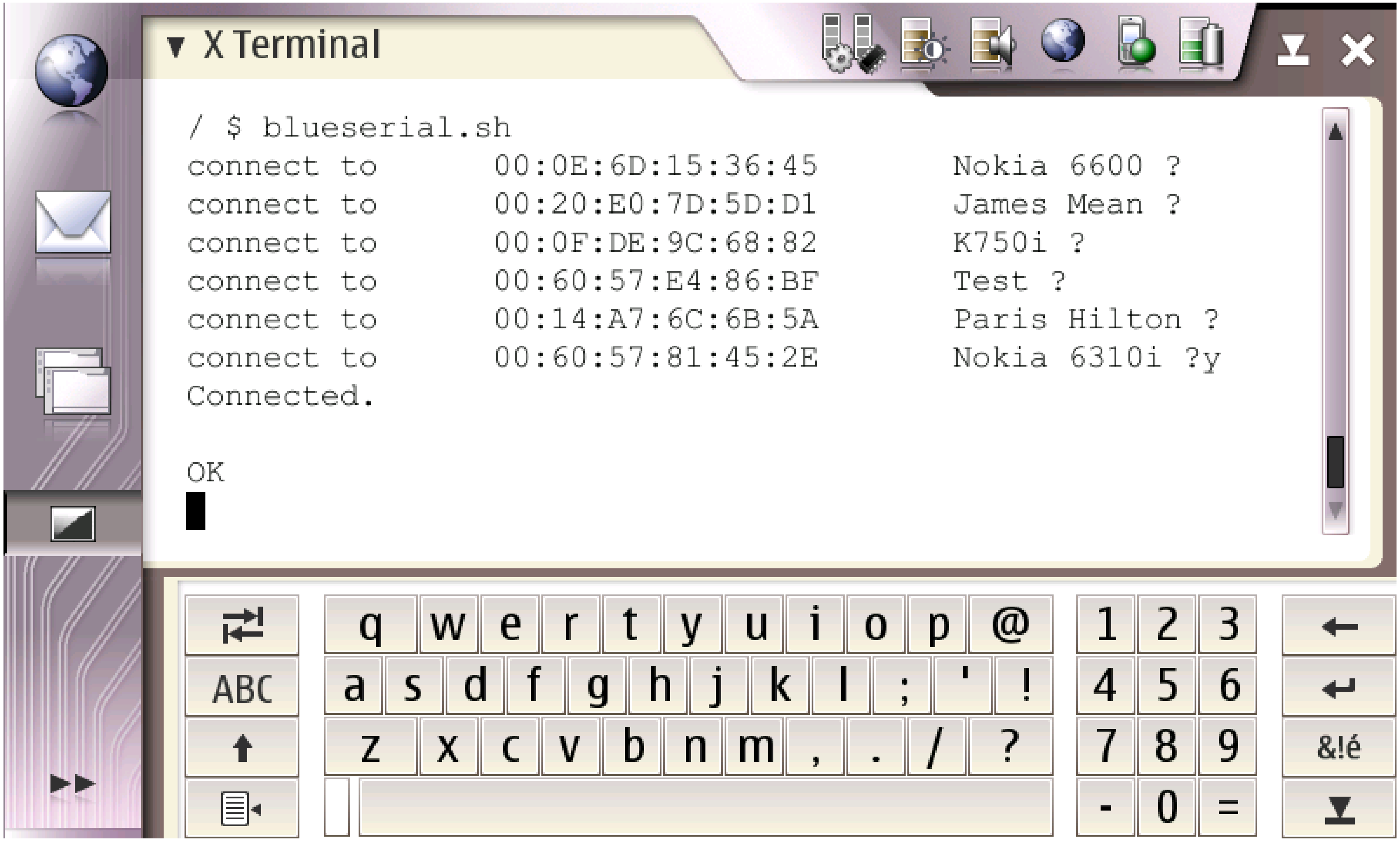
- Tablet PC
- Supports
  - Wi-Fi
  - Bluetooth
  - **No** GSM/GRPS/UMTS
- Linux-based
  - Almost open source
- Details here
  - http://www.nokia.com/770
  - http://trifinite.org/trifinite_stuff_nokia_770.html

Nokia 770



```
/ $
/ $
/ $ hcitool scan
Scanning ...
        00:0F:DE:9C:68:82       K750i
        00:14:A7:6C:6B:5A       Paris Hilton
        00:20:E0:7D:5D:D1       James Mean
        00:60:57:81:45:2E       Nokia 6310i
        00:0E:6D:15:36:45       Nokia 6600
        00:60:57:E4:86:BF       Test
/ $ cd /
```

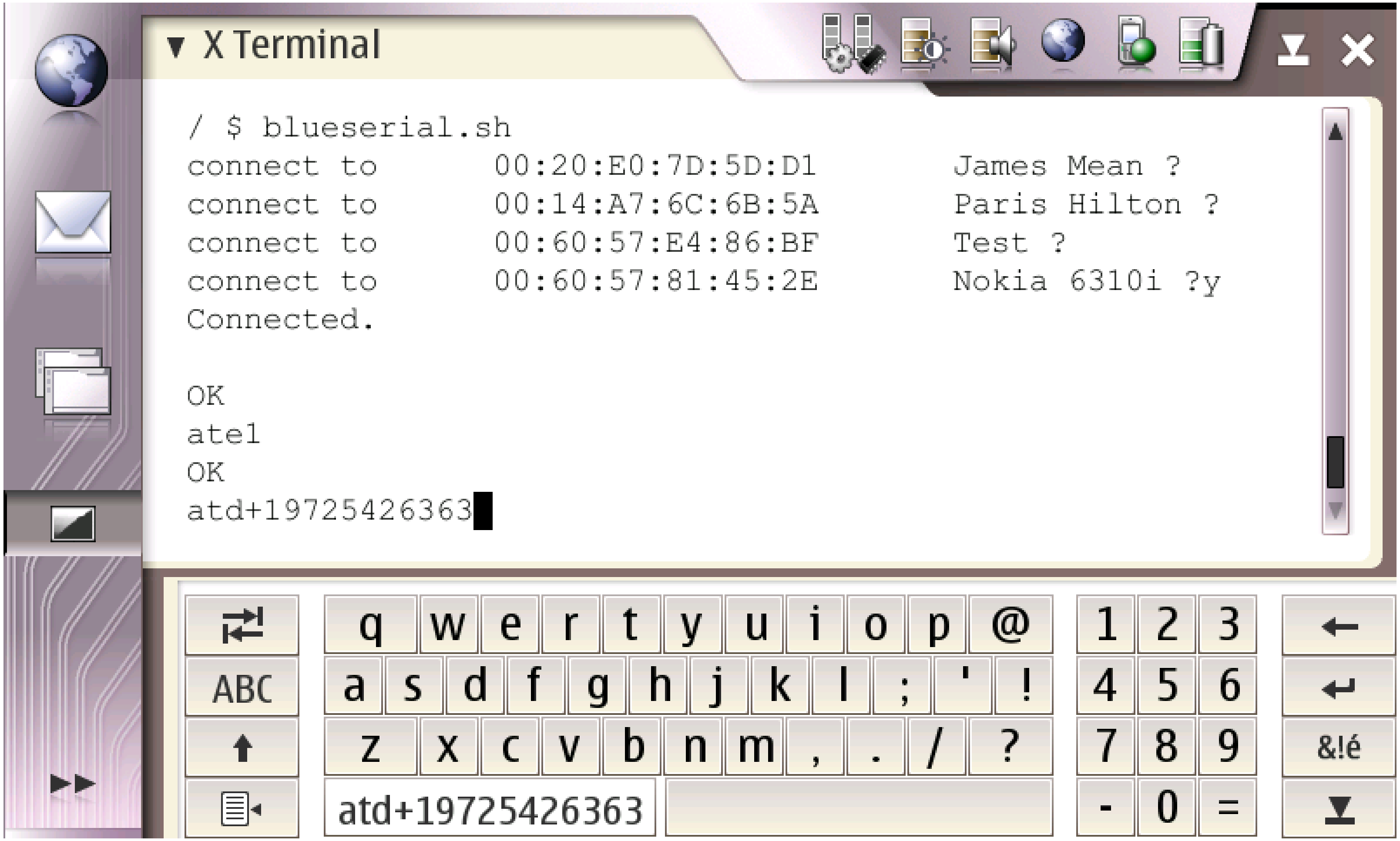
Nokia 770



```
/ $ blueserial.sh
connect to      00:0E:6D:15:36:45       Nokia 6600 ?
connect to      00:20:E0:7D:5D:D1       James Mean ?
connect to      00:0F:DE:9C:68:82       K750i ?
connect to      00:60:57:E4:86:BF       Test ?
connect to      00:14:A7:6C:6B:5A       Paris Hilton ?
connect to      00:60:57:81:45:2E       Nokia 6310i ?y
Connected.

OK
```

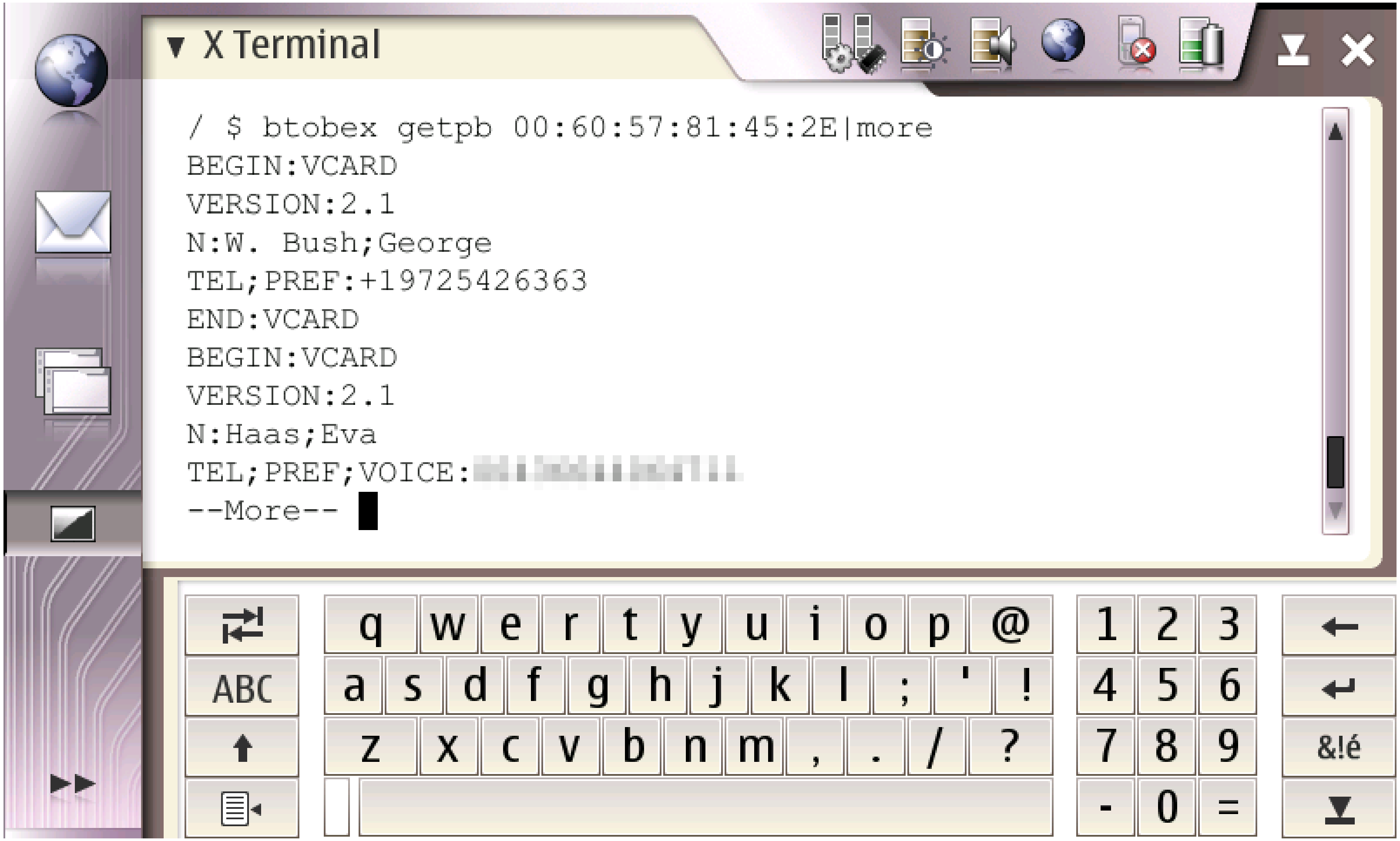
Nokia 770



```
/ $ blueserial.sh
connect to      00:20:E0:7D:5D:D1       James Mean ?
connect to      00:14:A7:6C:6B:5A       Paris Hilton ?
connect to      00:60:57:E4:86:BF       Test ?
connect to      00:60:57:81:45:2E       Nokia 6310i ?y
Connected.

OK
ate1
OK
atd+19725426363
```

Nokia 770



```
/ $ btobex getpb 00:60:57:81:45:2E|more
BEGIN:VCARD
VERSION:2.1
N:W. Bush;George
TEL;PREF:+19725426363
END:VCARD
BEGIN:VCARD
VERSION:2.1
N:Haas;Eva
TEL;PREF;VOICE:[redacted]
--More--
```

Blooonix

Blooonix

- Linux distribution for Bluetooth audits
  - Linux-based Live CD
  - Recent 2.6 kernel
  - Contains all latest BlueZ utilities
  - Dedicated auditing tools for each vulnerability
  - Report generation
- To be released early next year

Bluetooth Sniffing

- Local Sniffing
  - hcidump
- Piconet Sniffing
  - special hardware or firmware
- Air Sniffing
  - Frontline (http://www.fte.com/)
  - LeCroy/CatC (http://www.lecroy.com/)

Conclusions

- Bluetooth is secure standard (per se)
    - Problems are at the application level
- Cooperation with the Bluetooth SIG
    - Pre-release testing at UPF (UnPlugFests)
    - Better communication channels
    - Clear user interface and interaction
    - Mandatory security at application level
    - Using a policy manager

trifinite.group

- Adam Laurie (the Bunker Secure Hosting)
- Marcel Holtmann (BlueZ)
- Collin Mulliner (mulliner.org)
- Tim Hurman (Pentest)
- Mark Rowe (Pentest)
- Martin Herfurt (trifinite.org)
- Spot (Sony)

Further information

- trifinite.org
  - Loose association of security experts
  - Public information about Bluetooth security
  - Individual testings and trainings
  - TRUST = trifinite unified security testing
- Contact us via contact@trifinite.org

The Next Big Challenge

The Toy

Hacking TheToy - Just imagine all the girls freaking out when they sense the proximity of your geeky laptop ;)

Any questions?