Bluetooth Hacking

Full Disclosure

IT Underground

October 13rd 2005, Warsaw, Poland

by Adam Laurie, Marcel Holtmann and Martin Herfurt

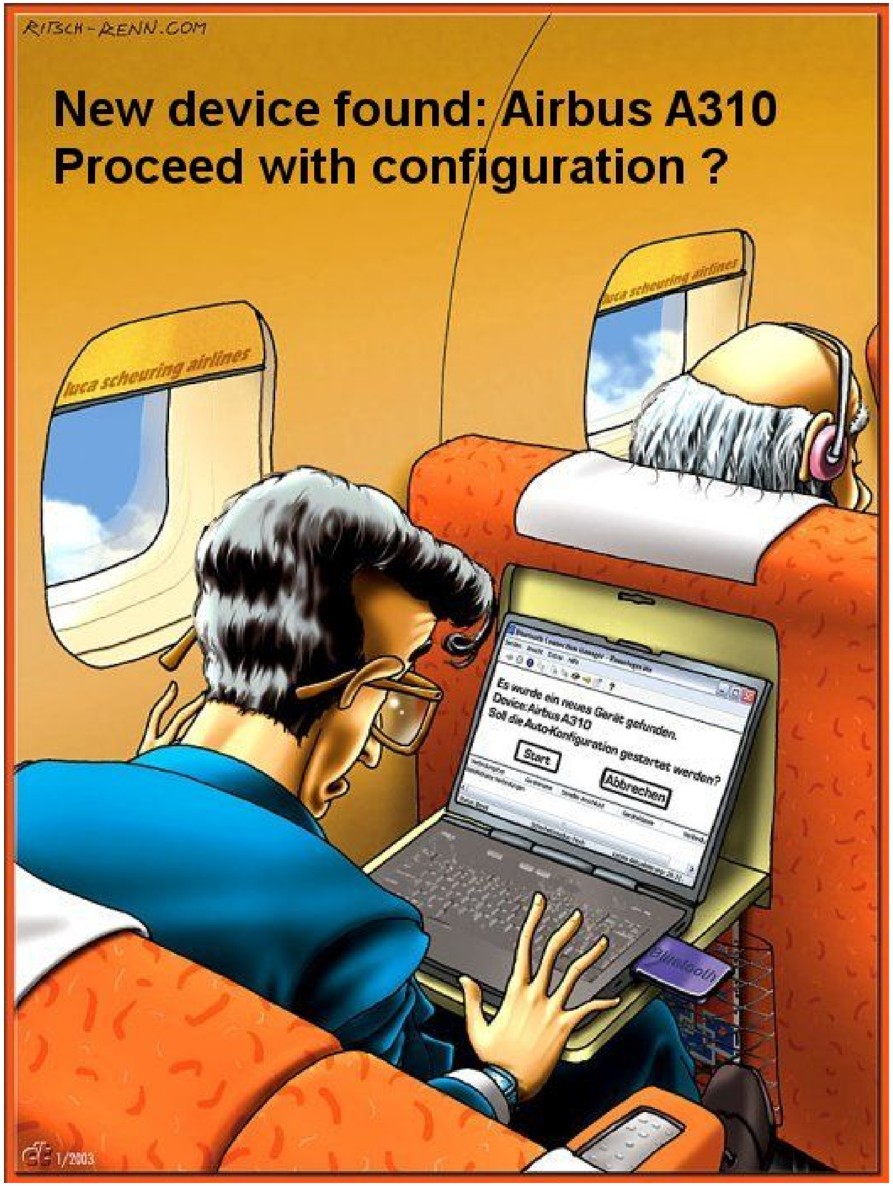
Agenda

- Bluetooth technology overview
- The security mechanisms
- Known vulnerabilities
- Tools that are used
- Live demonstration

Who is investigating

- Adam Laurie
  - CSO of The Bunker Secure Hosting Ltd.
  - DEFCON staff and organizer
- Marcel Holtmann
  - Maintainer of the Linux Bluetooth stack
- 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

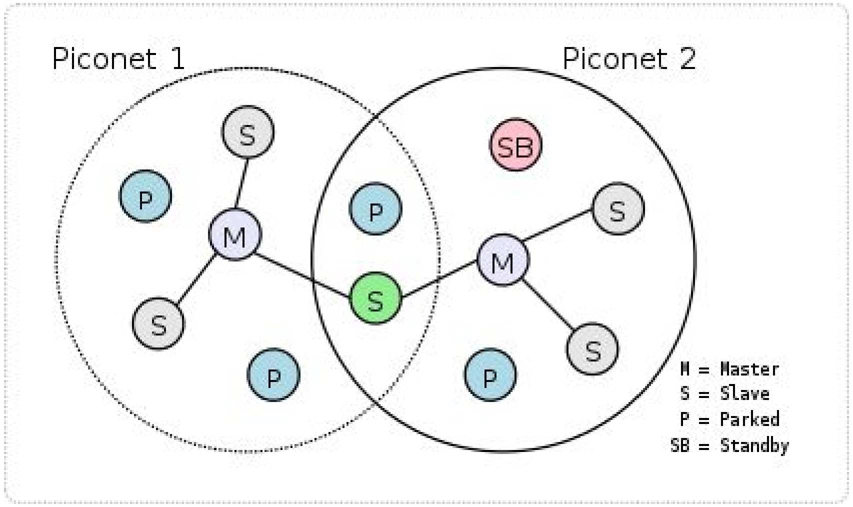
- Bluetooth SIG
  - Trade association
  - Founded 1998
  - Owns and licenses IP
- Bluetooth technology
  - A general cable replacement
  - Using the ISM band at 2.4 GHz
  - Protocol stack and application profiles

How it works

- Data and voice transmission
    - ACL data connections
    - SCO and eSCO voice channels
- Piconet and scatternet topology
- Frequency hopping
    - 79 channels
    - 1600 hops per second

Creating the topology

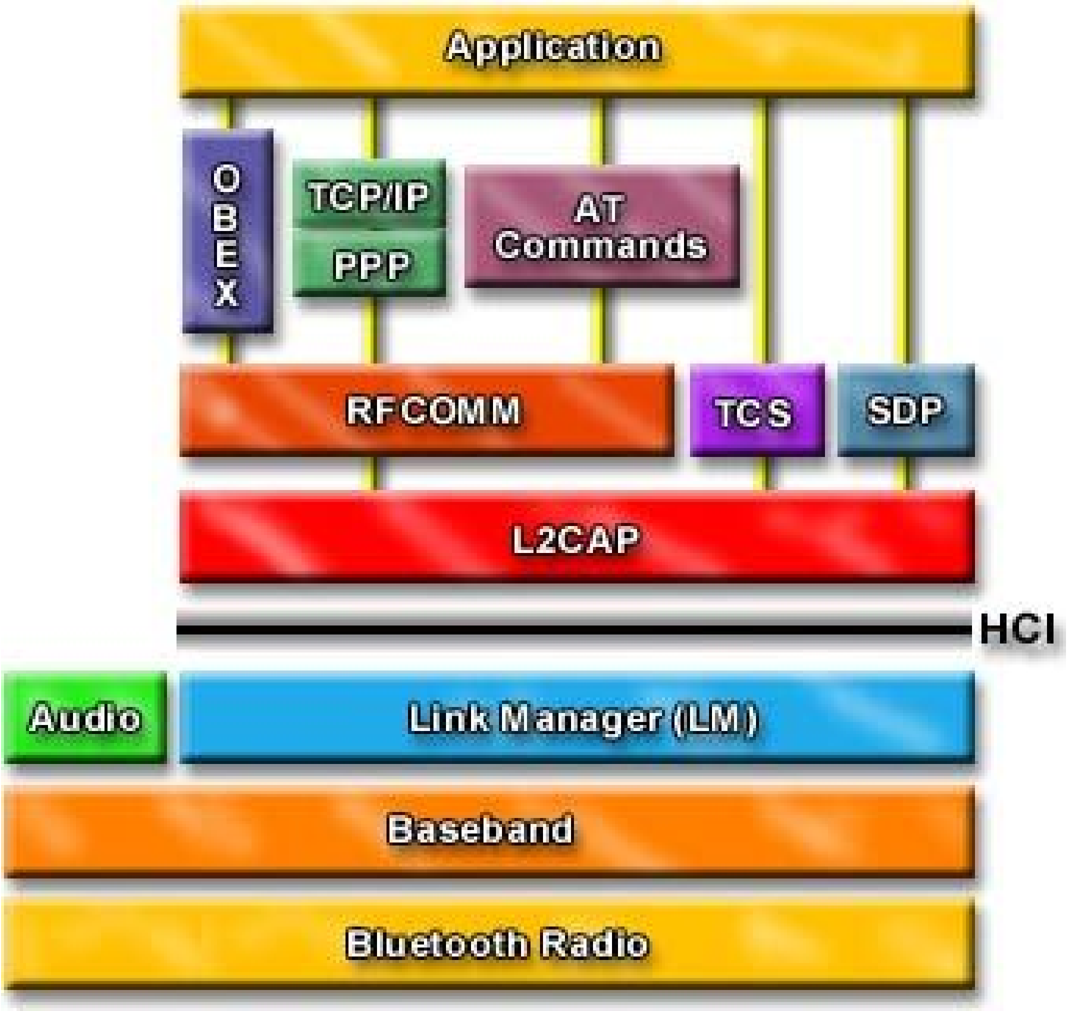
- Hopping sequence defines the piconet
  - Master defines the hopping sequence
  - Up to seven active slaves
  - Scatternet creation



Bluetooth architecture

- Hardware layer
  - Radio, Baseband and Link Manager
  - Access through the Host Controller Interface
    - Standards for USB and UART
- Host protocols
  - L2CAP, SDP, RFCOMM, BNEP, AVDTP etc.
- Application profiles
  - Serial Port Profile, Dialup, PAN, A2DP, HID etc.

Bluetooth Stack



Application specific security mechanisms

Bluetooth host security mechanisms

Security mechanisms on the Bluetooth chip

Bluetooth security

- Link manager security
    - All security routines are on-chip
    - Nothing is transmitted in “plain text”
- Host stack security
    - Interface to the link manager security
    - Part of the HCI specification
    - Easy interface
    - No further encryption of pin codes or keys

Bluetooth link keys

- Needed for authentication
- Used for encryption
    - SAFER+ (128 bit block cipher)
- Generated by pairing process
    - Passkey (1-16 alphanumeric characters)
    - Random number (from device internal clock)
    - BD_ADDR of piconet master

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

Security commands

- Settings
  - HCI_{Read|Write|Delete}_Stored_Link_Key
  - HCI_{Read|Write}_Authentication_Enable
  - HCI_{Read|Write}_Encryption_Mode
- Actions
  - HCI_Authentication_Requested
  - HCI_Set_Connection_Encryption
  - HCI_Change_Connection_Link_Key

Pairing functions

- Events
  - HCI_Pin_Code_Request
  - HCI_Link_Key_Request
  - HCI_Link_Key_Notification
- Responses
  - HCI_Pin_Code_Request_[Negative_]Reply
  - HCI_Link_Key_Request_[Negative_]Reply

How pairing works

- First connection

  (1) > HCI_Pin_Code_Request

  (2) < HCI_Pin_Code_Request_Reply

  (3) > HCI_Link_Key_Notification

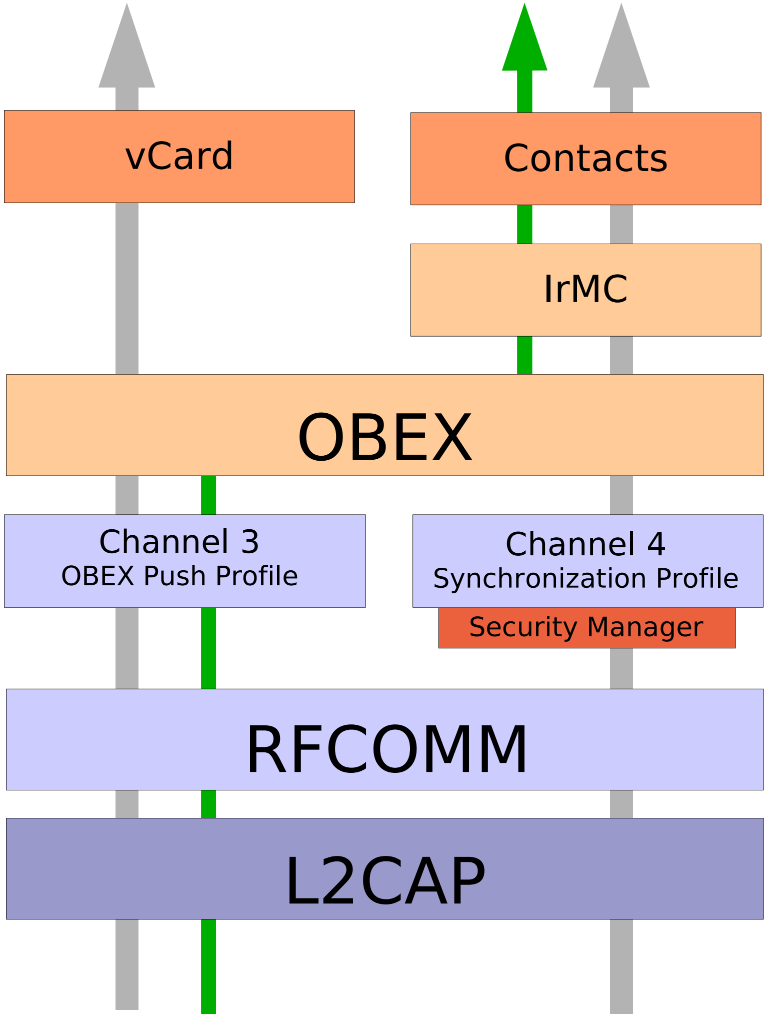
- Further connections

  (1) > HCI_Link_Key_Request

  (2) < HCI_Link_Key_Request_Reply

  (3) > HCI_Link_Key_Notification (optional)

How to avoid pairing



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.

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

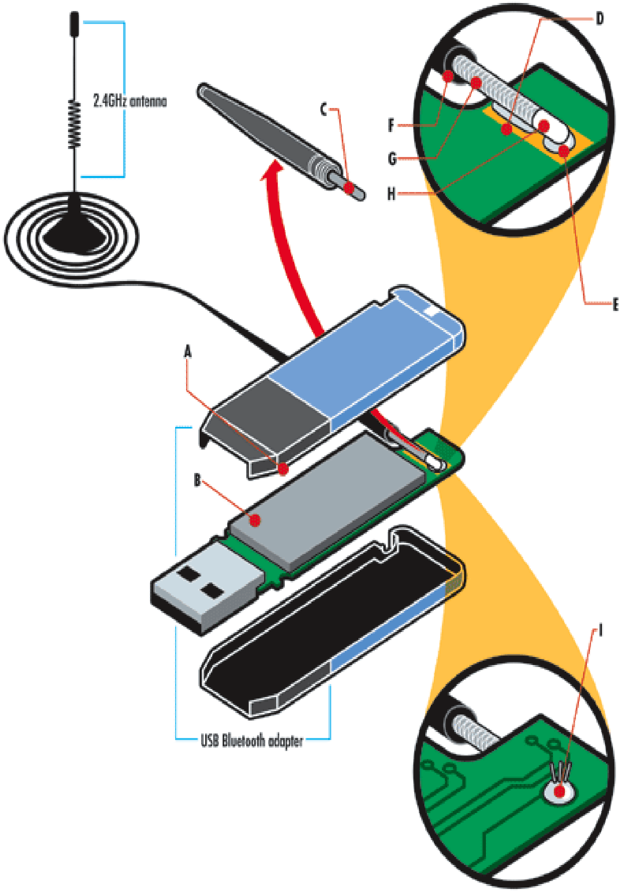
- Yanic Shaked and Avishai Wool
    - http://www.eng.tau.ac.il/~yash/Bluetooth/
    - Expands PIN attack from Ollie Whitehouse
    - Requires special hardware or firmware
- Destroy trust relationship
    - Use the BlueSpooof methods
- User interaction for pairing still needed

Blueprinting

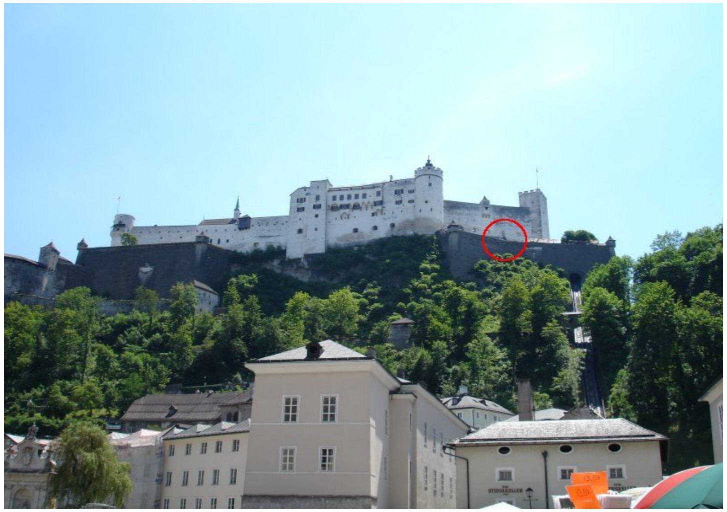
- Fingerprinting for Bluetooth
- Work started by Collin R. Mulliner and Martin Herfurt
- Based on the SDP records and OUI
- Important for security audits
- Paper with more information available

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



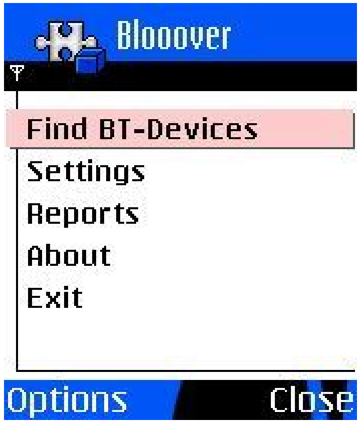
Long-Distance Attacking

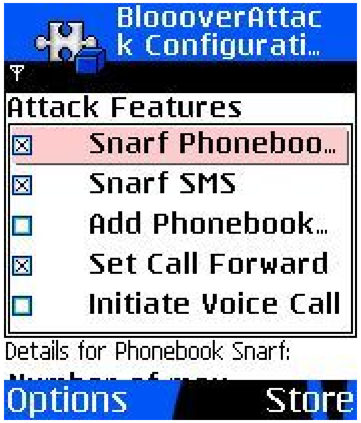
- Beginning of August 2004 (right after DEFCON 12)
- Experiment in Santa Monica California with Flexilis
- Modified Class-1 Dongle Snarfing/Bugging Class-2 device (Nokia 6310i) from a distance of 1,62 km (1.01 miles)

Blooover -What is it?

- Blooover - *Bluetooth* Wireless Technology Hoover
- Proof-of-Concept Application
- Educational Purposes only
- Phone Auditing Tool
- Running on Java
  - J2ME MIDP 2.0
  - Implemented JSR-82 (Bluetooth API)
  - Nokia 6600, Nokia 7610,
    Nokia 6670, ... Series 60
    Siemens S65
    SonyEricsson P900 ...

Blooover





Attack Features

☒ Snarf Phoneboo...

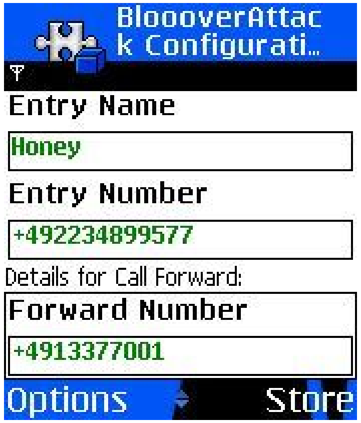
☒ Snarf SMS

□ Add Phonebook...

☒ Set Call Forward

□ Initiate Voice Call

Details for Phonebook Snarf:



Entry Name

Honey

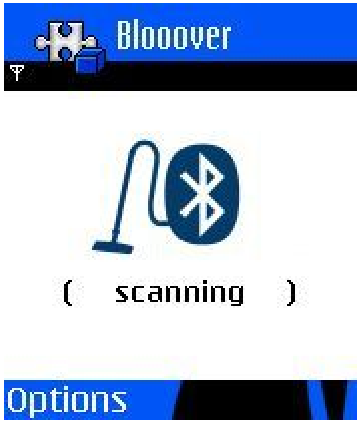
Entry Number

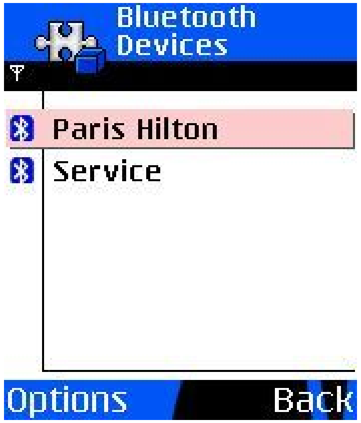
+492234899577

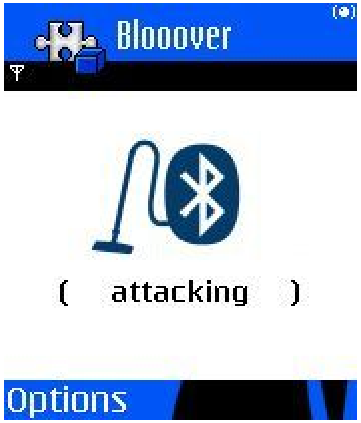
Details for Call Forward:

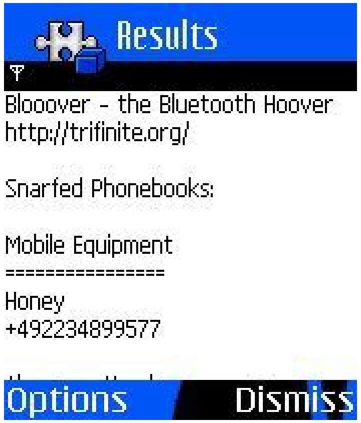
Forward Number

+4913377001









Blooover - the Bluetooth Hoover
http://trifinite.org/

Snarfed Phonebooks:

Mobile Equipment
================
Honey
+492234899577

Blooover II

- Successor of the popular Blooover application
  - More like an auditing toool for professionals
  - Included Audits
    - BlueBug
    - HeloMoto
    - BlueSnarf
    - BlueSnarf++
    - Malformed Objects
- To be released in the end of 2005

Blooonix

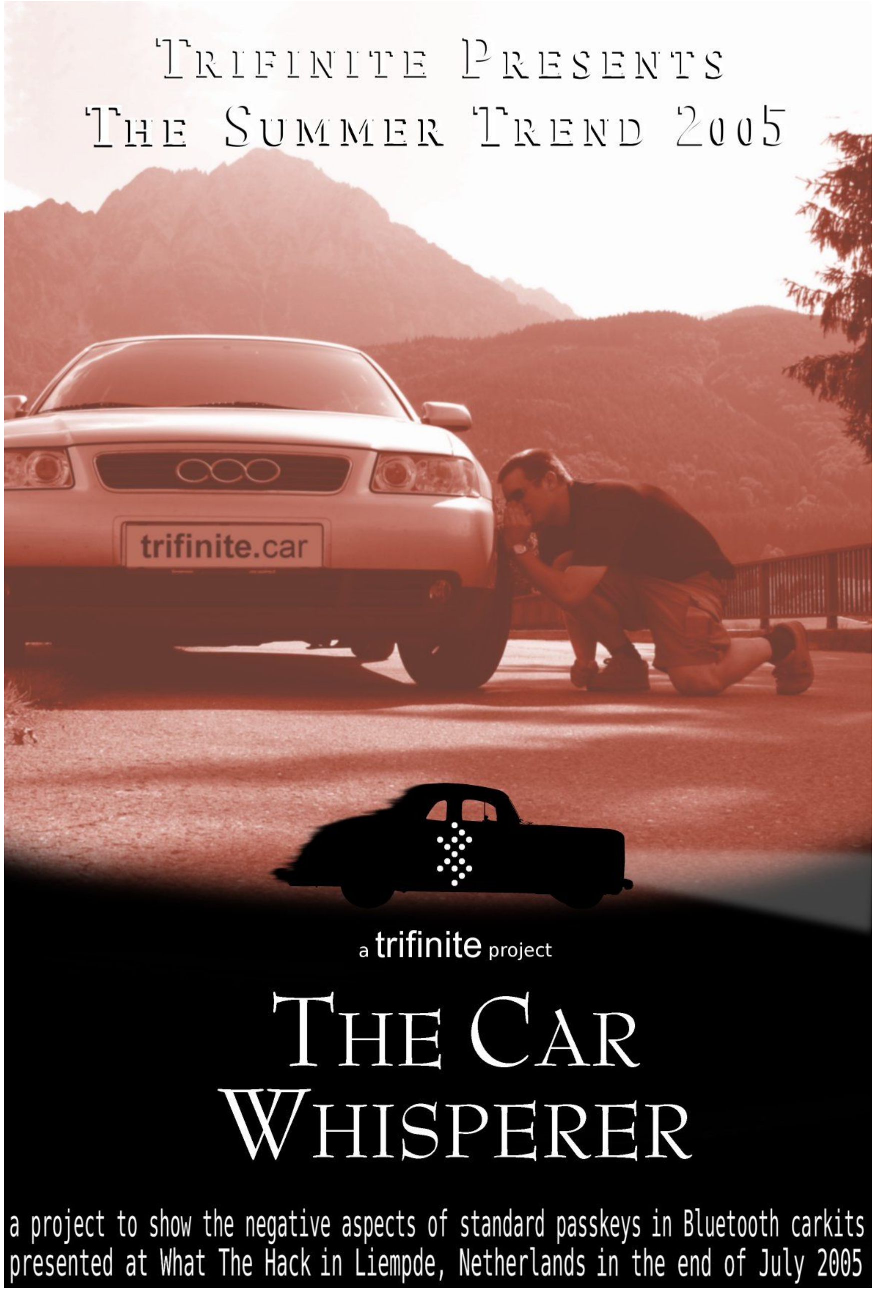
- Linux distribution for Bluetooth audits
  - LiveCD based on Morphix
  - Latest official Linux 2.6 kernel
  - Contains all latest BlueZ utilities
  - Includes also special hacker scripts
  - Graphical interface
  - Report generation
- Not available at the moment

BluePot

- Bluetooth HoneyPot
  - Runs on J2ME phones
  - Imitates vulnerable phone
  - Logs incoming attacks and device information
  - Strikeback capable
- Written by Martin Herfurt
- Not released yet

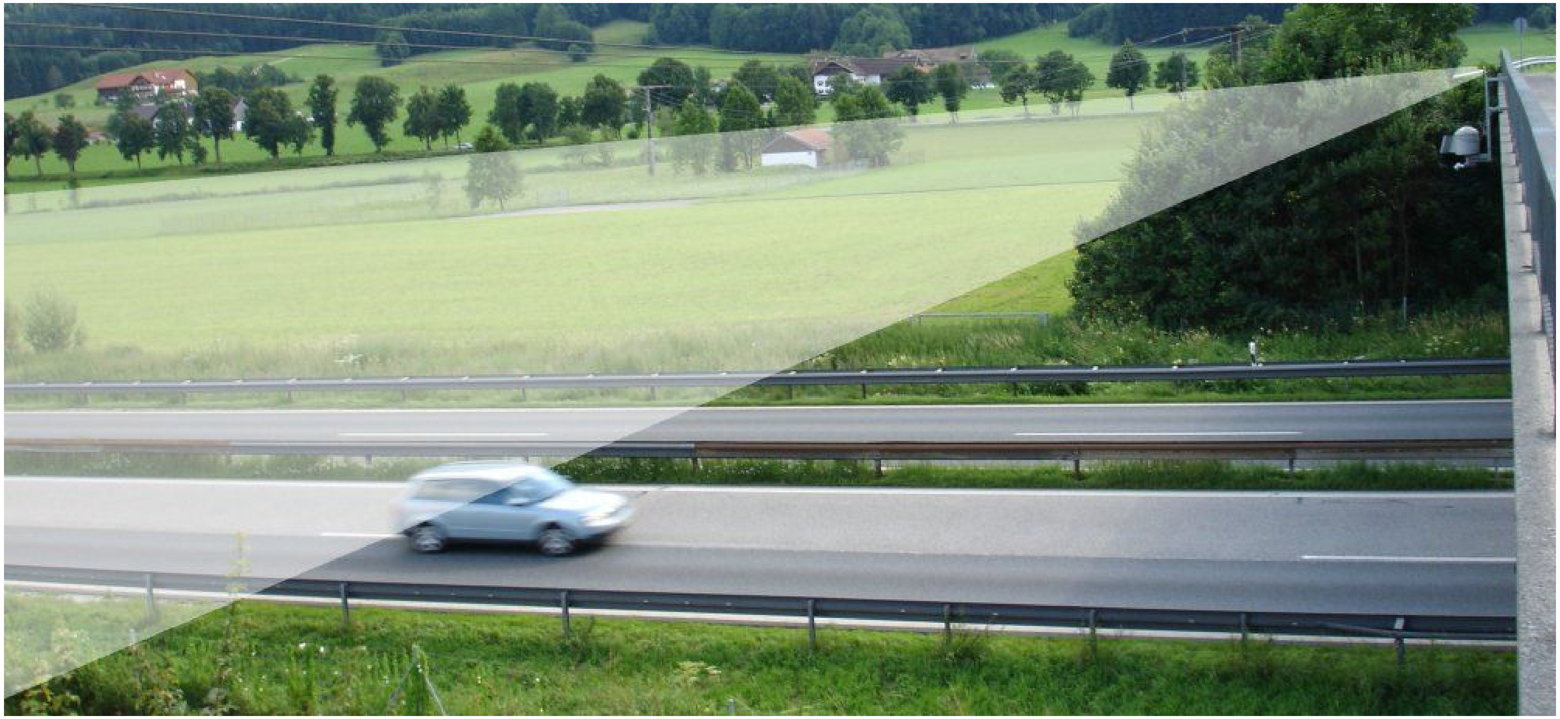
The Car Whisperer

- Use default pin codes to connect to carkits
- Inject audio
- Record audio
- Don't whisper and drive!


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



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 it-underground@trifinite.org

Questions and Feedback now!