Hacking the Bluetooth Stack for Fun, Fame and Profit

HITBSecConf2007 - MALAYSIA

3RD - 6TH SEPTEMBER 2007 - KUALA LUMPUR

DEEP KNOWLEDGE SECURITY CONFERENCE

CAPTURE THE FLAG COMPETITION
ZONE-H HACKING CHALLENGE
LOCK PICKING VILLAGE

DUAL TRACK SECURITY CONFERENCE
HANDS-ON TECHNICAL TRAINING
4 KEYNOTE SPEAKERS

Contents

- Who Are We?
- Why Bluetooth?
- What security Mechanisms ?
- Bluetooth Attacks
- Newer Bluetooth attacks and nifty tricks
- Protection
- Further reading and information

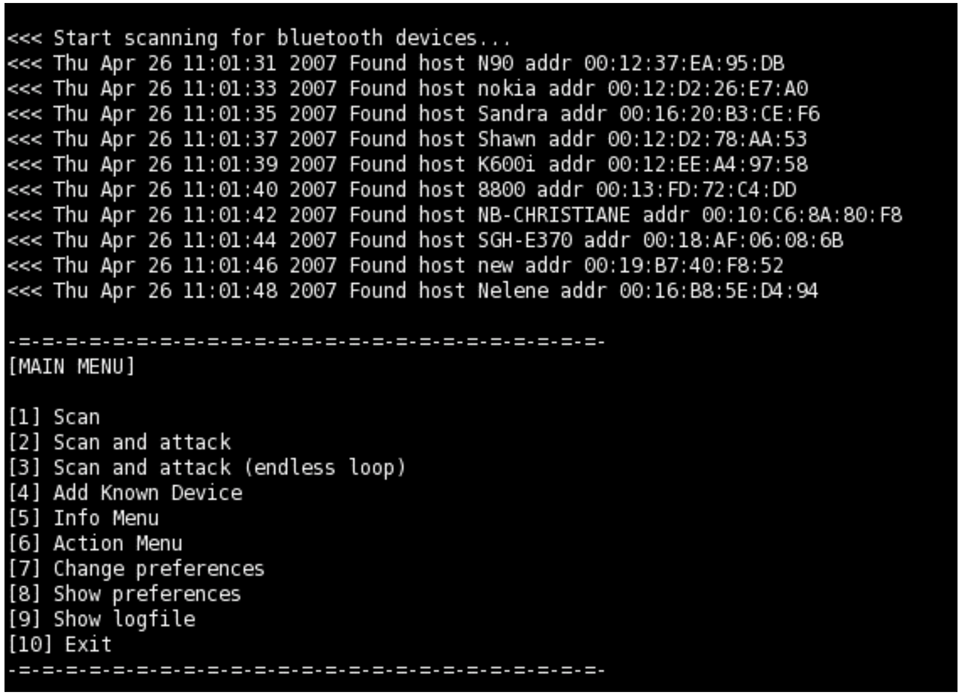
Who are we?

- Information Security Company – South Africa
- Operating since 2002
- Give back to the open source community – Responsible reporting and disclosure (Latest Advisories)
- Speak at local (.za) and international conferences

Awareness

- ➢Airports/Offices/Malls/etc

- ➢Raise awareness levels

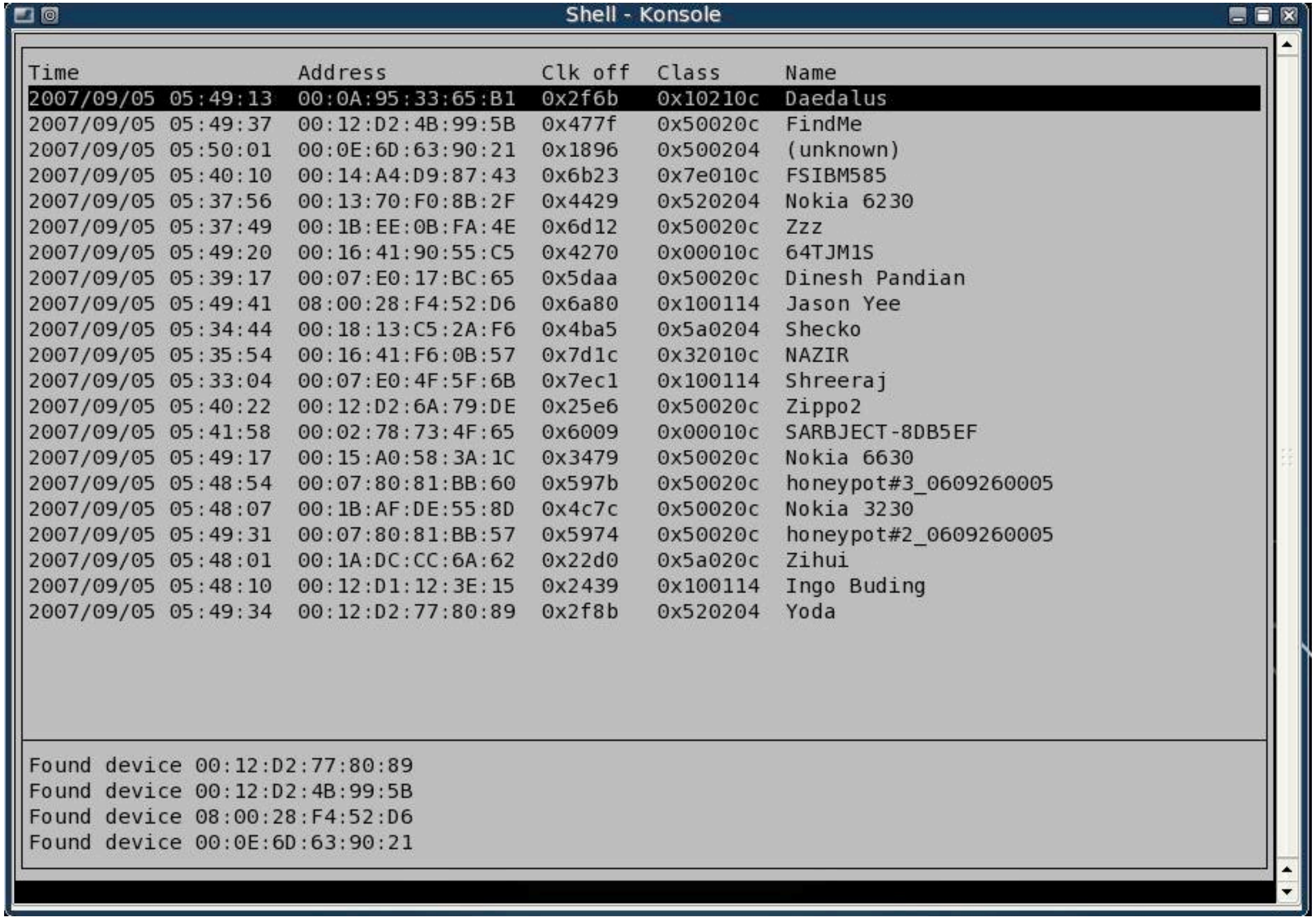


```
<<< Start scanning for bluetooth devices...
<<< Thu Apr 26 11:01:31 2007 Found host N90 addr 00:12:37:EA:95:DB
<<< Thu Apr 26 11:01:33 2007 Found host nokia addr 00:12:D2:26:E7:A0
<<< Thu Apr 26 11:01:35 2007 Found host Sandra addr 00:16:20:B3:CE:F6
<<< Thu Apr 26 11:01:37 2007 Found host Shawn addr 00:12:D2:78:AA:53
<<< Thu Apr 26 11:01:39 2007 Found host K600i addr 00:12:EE:A4:97:58
<<< Thu Apr 26 11:01:40 2007 Found host 8800 addr 00:13:FD:72:C4:DD
<<< Thu Apr 26 11:01:42 2007 Found host NB-CHRISTIANE addr 00:10:C6:8A:80:F8
<<< Thu Apr 26 11:01:44 2007 Found host SGH-E370 addr 00:18:AF:06:08:6B
<<< Thu Apr 26 11:01:46 2007 Found host new addr 00:19:B7:40:F8:52
<<< Thu Apr 26 11:01:48 2007 Found host Nelene addr 00:16:B8:5E:D4:94

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[MAIN MENU]

[1] Scan
[2] Scan and attack
[3] Scan and attack (endless loop)
[4] Add Known Device
[5] Info Menu
[6] Action Menu
[7] Change preferences
[8] Show preferences
[9] Show logfile
[10] Exit
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
```

- ➢Show nifty tricks and cool Bluetooth implementations

Awareness

- Hack in the box BT devices, Are any of these yours?



```
Time                 Address            Clk off   Class     Name
2007/09/05 05:49:13  00:0A:95:33:65:B1  0x2f6b    0x10210c  Daedalus
2007/09/05 05:49:37  00:12:D2:4B:99:5B  0x477f    0x50020c  FindMe
2007/09/05 05:50:01  00:0E:6D:63:90:21  0x1896    0x500204  (unknown)
2007/09/05 05:40:10  00:14:A4:D9:87:43  0x6b23    0x7e010c  FSIBM585
2007/09/05 05:37:56  00:13:70:F0:8B:2F  0x4429    0x520204  Nokia 6230
2007/09/05 05:37:49  00:1B:EE:0B:FA:4E  0x6d12    0x50020c  Zzz
2007/09/05 05:49:20  00:16:41:90:55:C5  0x4270    0x00010c  64TJM1S
2007/09/05 05:39:17  00:07:E0:17:BC:65  0x5daa    0x50020c  Dinesh Pandian
2007/09/05 05:49:41  08:00:28:F4:52:D6  0x6a80    0x100114  Jason Yee
2007/09/05 05:34:44  00:18:13:C5:2A:F6  0x4ba5    0x5a0204  Shecko
2007/09/05 05:35:54  00:16:41:F6:0B:57  0x7d1c    0x32010c  NAZIR
2007/09/05 05:33:04  00:07:E0:4F:5F:6B  0x7ec1    0x100114  Shreeraj
2007/09/05 05:40:22  00:12:D2:6A:79:DE  0x25e6    0x50020c  Zippo2
2007/09/05 05:41:58  00:02:78:73:4F:65  0x6009    0x00010c  SARBJECT-8DB5EF
2007/09/05 05:49:17  00:15:A0:58:3A:1C  0x3479    0x50020c  Nokia 6630
2007/09/05 05:48:54  00:07:80:81:BB:60  0x597b    0x50020c  honeypot#3_0609260005
2007/09/05 05:48:07  00:1B:AF:DE:55:8D  0x4c7c    0x50020c  Nokia 3230
2007/09/05 05:49:31  00:07:80:81:BB:57  0x5974    0x50020c  honeypot#2_0609260005
2007/09/05 05:48:01  00:1A:DC:CC:6A:62  0x22d0    0x5a020c  Zihui
2007/09/05 05:48:10  00:12:D1:12:3E:15  0x2439    0x100114  Ingo Buding
2007/09/05 05:49:34  00:12:D2:77:80:89  0x2f8b    0x520204  Yoda

Found device 00:12:D2:77:80:89
Found device 00:12:D2:4B:99:5B
Found device 08:00:28:F4:52:D6
Found device 00:0E:6D:63:90:21
```

Please turn them off !

Why Bluetooth?

- New technologies

- Developed by Ericsson 1994

- Household appliances, paypoints, cellphones , car kits etc

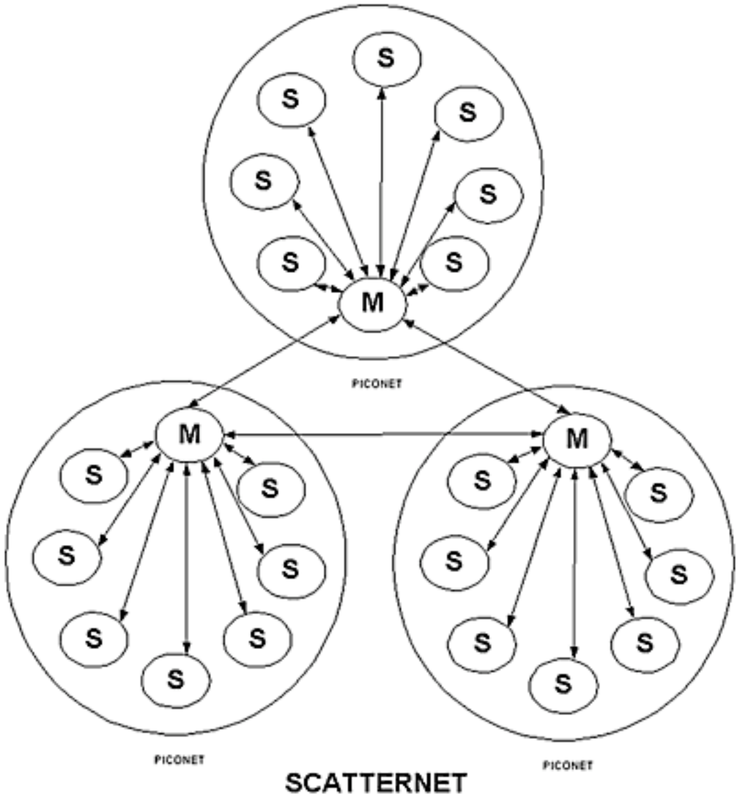
- Antivirus and worms spread using bluetooth, Cabir , Lasco and Comwar

- Many people still misunderstand bluetooth security risks

Why Bluetooth?

- Based on Piconets, 1 master unit and 7 slave units

- Piconets can be united into scatternets



Why Bluetooth?

➢Unlicensed frequency band between 2.4 to 2.4835 GHz.

➢Frequency hopping algorithm with 1600 frequency hops per second.

➢ Two types of connection: ACL (asynchronous connectionless) and SCO (synchronous connection-oriented).

➢ The first type of connection is used to transfer data that can be handled at any time. A slave unit can have only one ACL connection to the master unit.

➢The second link type is used for transferring data in real time, e.g. for transmitting voice data. A slave unit can have up to 3 SCO links with the main unit, each with a rate of 64 kb/sec.

Why Bluetooth?

The Bluetooth specification divides Bluetooth devices into three groups:
Class 1 100 mW 100m
Class 2 2.5 mW 10m
Class 3 1 mW 1m

Bluetooth Core Protocols

TCS - Telephony Control Specification

RFComm - Serial Port Emulation Protocol

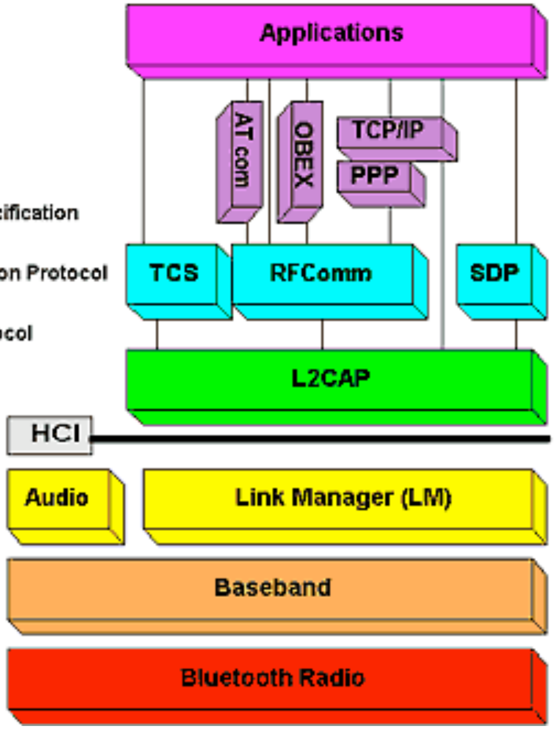
SDP - Service Discovery Protocol

L2CAP - Logical Link Control and Adaptation Protocol

LM - Link Manager

Baseband Specification

Radio Specification



Security Mechanisms

Bluetooth can operate in one of three Security Modes:

Security Mode 1 – unprotected (no security) In this mode, no encryption or authentication is used, while the device itself operates in a non-discriminating, i.e. broadcasting (promiscuous) mode.

Security Mode 2 – application/service based (L2CAP) In this mode, once a connection is established, Security Manager performs authentication, thereby restricting access to the device.

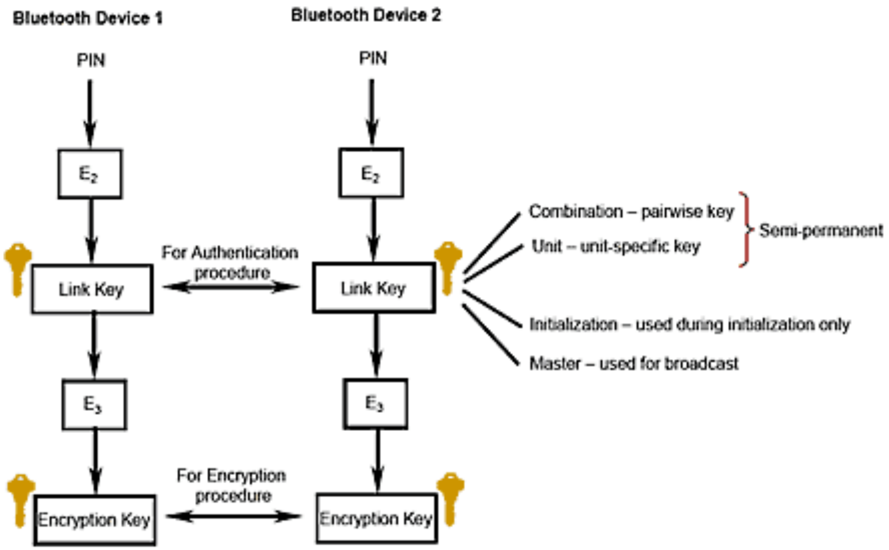
Security Mode 3 – link-layer PIN authentification/ MAC address encryption. Authentication is performed prior to a connection be established. Although transparent encryption is used, even in this mode the device can be compromised.

Security Mechanisms

Bluetooth security is based on the generation of keys using a PIN code, which can be 1 to 16 bytes in length.

Most devices currently use 4-byte PINs. First, the E2 algorithm is used to generate a 16-byte Link Key based on the PIN code.

Then an Encryption Key based on the Link Key is calculated using the E3 algorithm. The first key is used for authentication, the second for encryption.



Security Mechanisms

The authentication process is as follows:

The device initiating the connection sends its address (BD_ADDR). This 48-bit address is unique, like a network adaptor's MAC address. A device's manufacturer can be determined by this address.

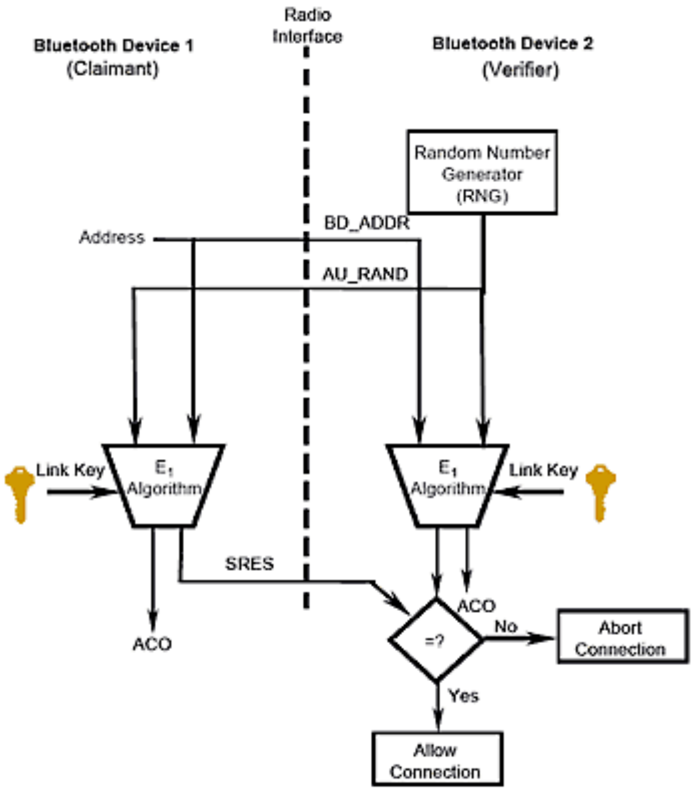
In response a random 128-bit challenge sequence is sent (AU_RAND).

Both devices generate an authentication response string called SRES based on BD_ADDR, Link Key and AU_RAND.

The device trying to establish the connection sends its SRES.

The other device compares the SRES received with its own and if the two strings match, establishes a connection.

Security Mechanisms



Although the PIN code is not transmitted openly, it can be cracked if BD_ADDR, AU_RAND and SRES are intercepted.

Types of Attacks, Bluetooth

BlueChop

Disrupting a Piconet, by utilising a device which is not part of the network. This attack is valid, due to the fact that the master unit supports multiple connections which can be used to create a bigger network (i.e. scatternet).

This entails spoofing a random device which is part of the Piconet.

BlueDump Attack

The attacker needs to know the BDADDR of a set of paired devices. The address of one of the devices is spoofed and the attacker connects to the other. Since the attacker has no link key, when the victim device requests authentication, the attacker's device will respond with an 'HCI_Link_Key_Request_Negative_Reply', which will, in some cases, cause the target device to delete its own link key and go into pairing mode.

Types of Attacks, Bluetooth

BlueBump

Social engineering attack to establish a trusted connection with a device of choice. Such as sending a business card via bluetooth to perform authentication, then taking advantage of the target device. Victim is not aware that the device is still connected and active.

BlueSmack

This is a DoS attack, which can be performed using standard tools provided with Linux Bluez. The attack is as L2CAP level, where its possible to request an echo from another Bluetooth device. Similar to ICMP, it checks connectivity between bluetooth devices. You can specify the length of the packets to be sent using l2ping. To achive DoS, a size of about 600 bytes is used.

Types of Attacks, Bluetooth

BlueBug attack:

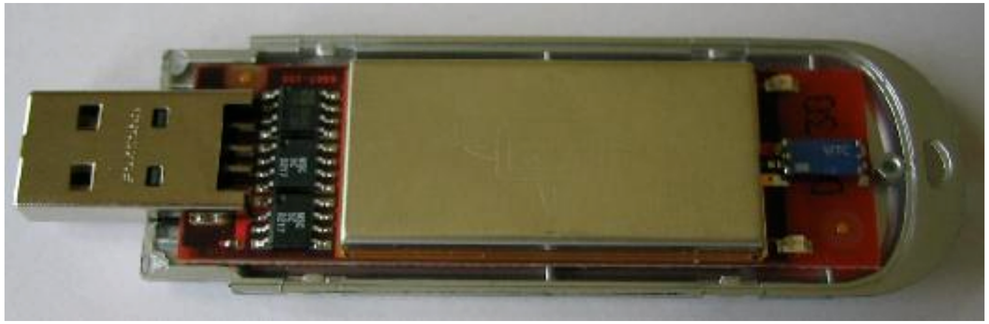
Vulnerabilities in certain implementations allow attackers to perform unauthorised actions on target devices.

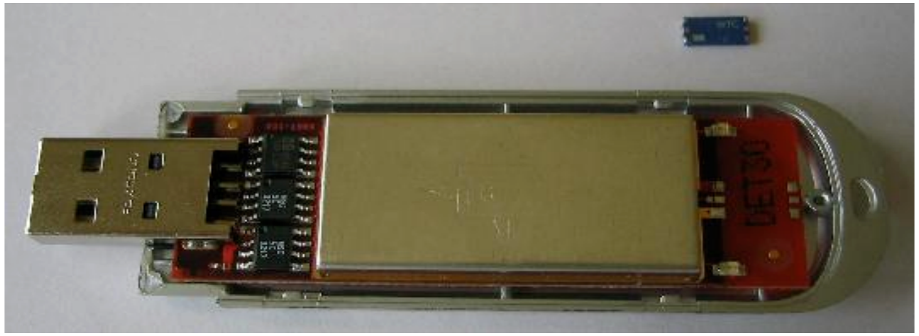
The attack is limited by transmitting power of class 2 radio’s, which , as mentioned previously is 10-15 metres, but can be extended by using a directional antenna.

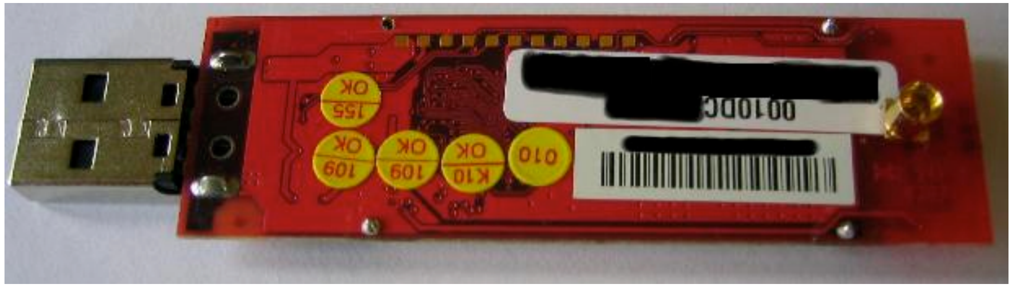
Some mobile phones allow the issuing of AT commands, meaning we can initiate calls, send sms’s , read stored sms’s , read and write phonebook entries, configure call forwarding and more.

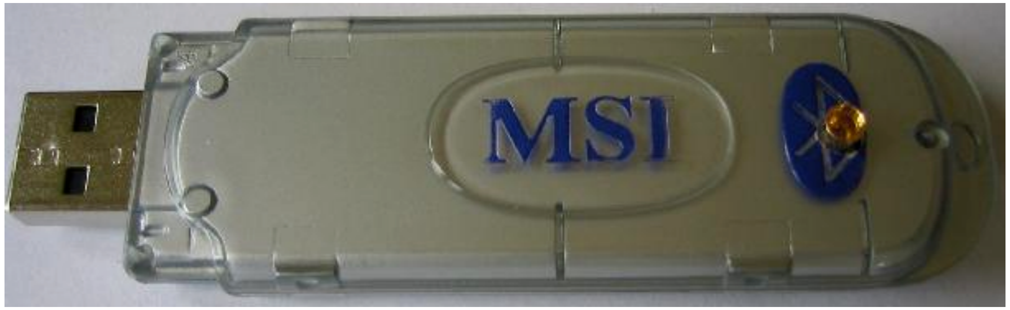
Types of Attacks, Bluetooth

Simple dongle modification:









Pigtail connectivity possible

Types of Attacks, Bluetooth

BluePrinting:

Bluetooth devices have a range of services that can be listed and obtained via the service discovery protocol(SDP). The resultant information is in a specific format which can be utilised to identify the device model.

HelloMoto:

Combination of BlueSnafing and Bluebugging. Attack is based off incorrect processing of trusted device handling, on specific Motorola phones.

Attacker creates a connection using OBEX Push and mimics sending Vcard. The attack is purposefully interrupted but remains trusted on the device. AT commands can then control the device accordingly.

Types of Attacks, Bluetooth

BlueSnarf:

Most definatly the most well known Bluetooth attack. OBEX Push Profile is utilised which in most cases does not require authentication. The attack conducts OBEX GET for well known filenames such as:

Telecom/pb.pcf
Telecom/cal.vcs

If the firmware on the device has not been implemented correctly, attackers are able to access all files on the device.

BlueSnarf++:

Similar to BlueSnarf , differential is in the methodology used. BlueSnarf++ provides the attacker with FULL RW access via OBEX Push Profile. If OBEX Ftp server is running, a connection can be made without pairing. Attackers can use standard commands like “ls” “rm” and so fourth.

Types of Attacks, Bluetooth

Car Whisperer Project

- Some Preset standard passkey on headsets and handsfree units is '0000' or '1234'.

- Carwhisperer binary can start sending audio to, and recording audio from the headset. This even allows attackers to inject audio data into the car.

- In Bluetooth communication scenarios the link key is used for authentication and encryption of the information that is exchanged between the counterparts of the communication.

- The cw_scanner script is repeatedly performing a device inquiry for visible Bluetooth devices of which the class matches the one of Bluetooth Headsets and Hands-Free Units.

Types of Attacks, Bluetooth

- Once a visible Bluetooth device with the appropriate device class is found, the cw_scanner script executes the carwhisperer binary that connects to the found device (on RFCOMM channel 1) and opens a control connection and connects the SCO links.

- The carwhiperer binary connects to the device found by the cw_scanner. The passkey that is required for the initial connection to the device is provided by the cw_pin.pl script that replaces the official Bluez PIN helper (graphical application that usually prompts for the passkey).

- The cw_pin.pl script provides the passkey depending on the Bluetooth address that requests it. Depending on the first three bytes of the address, which references the manufacturer, different passkeys are returned by the cw_pin.sh script.

Types of Attacks, Bluetooth

- Attackers are also able to eavesdrop conversations among people sitting in the car. Ideally, the carwhisperer is used with a toooned dongle (http://trifinite.org/trifinite_stuff_bluetooone.html) and a directional antenna that enhances the range of a Bluetooth radio quite a bit.

- Manufacturers should not use standard passkeys in their Bluetooth appliances.

- There should also be a direct interaction with the device that allows a device to connect. It should also change the device to invisible mode, when no authorized device connects to it within a certain time frame.

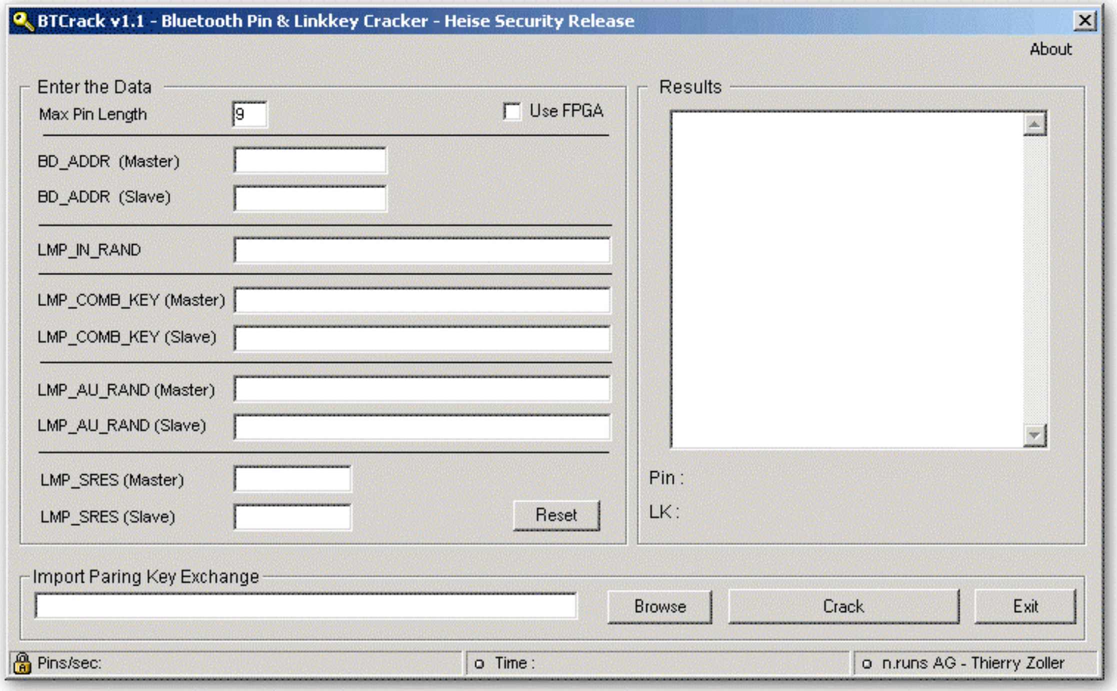
- Not all Bluetooth carkits are subject to this threat. There are a few Bluetooth carkits that use random passkeys that are generated for every individual device during the production process.

Newer Bluetooth attacks and nifty tricks

BT Crack:

BTCrack is a Bluetooth Pass phrase (PIN) Brute force Proof of Concept tool

Aimed at reconstructing the Passkey and the Link key from captured Pairing (Pairing takes place when 2 devices enter the Passkey (PIN)) exchanges.



BTCrack v1.1 - Bluetooth Pin & Linkkey Cracker - Heise Security Release

Max Pin Length: 9

Newer Bluetooth attacks and nifty tricks

BT Crack (http://www.nruns.com/_en/security_tools_btcrack.php):

Attack scenario:

- Attacker reconstructs BD_ADDR of both Master and Slave through Passive (Reconstructing through a preamble sniff) or Active means (Redfang POC)

- Attacker changes his BD_ADDR to the one of the Slave device

- Attacker asks to pair with the Master indicating it has no key, the Master will more then often discard the old pairing data and request a new link key from the genuine slave

- Attacker now captures the key (pairing) exchange taking place between the two devices as the users try to re-establish a connection

- Attacker can export data to CSV format and import into BTCrack

- Has access to the Master and Slave through usage of the cracked Linkkey

- May decrypt communications from that moment on between these 2 devices

Newer Bluetooth attacks and nifty tricks

The BlueBag Project - www.computer.org/security/

Current Bluetooth worms pose relatively little danger compared to Internet scanning worms. However, our belief is that things could change soon.

The authors’ of the BlueBag project show targeted attacks through Bluetooth malware using proof-of-concept codes and devices that demonstrate their feasibility. This shows results that are applicable in real life scenario’s.

The total cost to build such a device is approximately US $750 , demonstrating just how economical and dangerous it is to create a Bluetooth attack device.

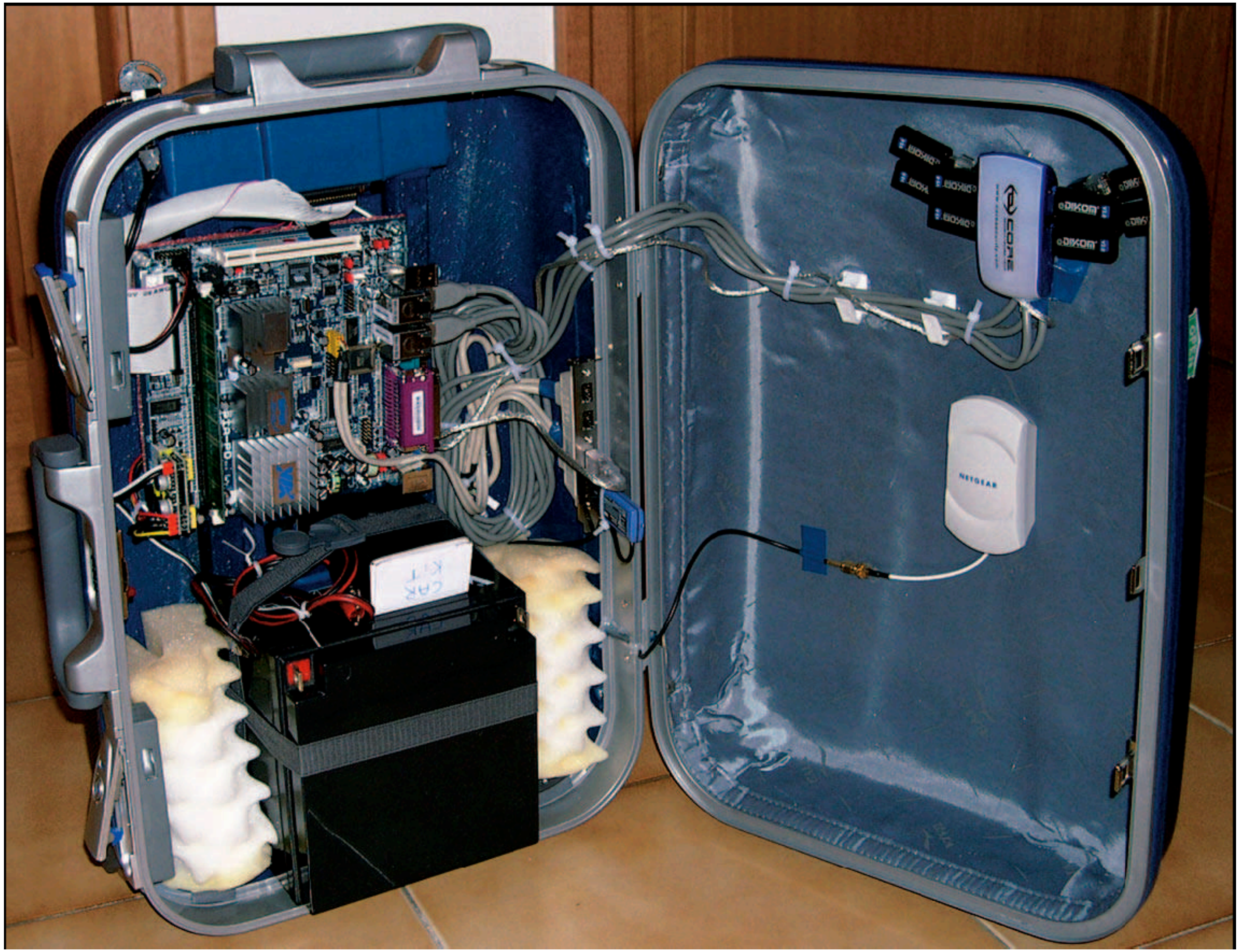
Newer Bluetooth attacks and nifty tricks

Components required:

A VIA EPIA Mini-ITX motherboard (model PD6000E; because it doesn’t have a fan, its power consumption is reduced);.

- 256 MBytes of RAM in a DDR400 DIMM module;
- EPIA MII PCI backplate to extend the available onboard USB connections from two to six;
- a 20-Gbyte iPod, with a 1.8-inch hard drive that can resist an acceleration of up to 3gs;
- eight class-1 Bluetooth dongles with Broadcom chipsets (some were connected to a four-port USB hub);
- a modified class-1 Linksys Bluetooth dongle (Cambridge Silicon Radio chipset) modified with a Netgear omnidirectional antenna with 5dBi gain.
- a picoPSU, DC-DC converter (this small power supply can generate up to 120 watts at over 96 percent efficiency);
- a 12V-26Ah lead acid battery to power our lengthy surveying sessions (up to 8 hours).

Newer Bluetooth attacks and nifty tricks



The completed project: Note the motherboard, battery, dongles and the antenna.

Newer Bluetooth attacks and nifty tricks

- By utlising this as a tool (and transmitting a specific image file), the authors found that an astounding 7.5 percent of device owners carelessly accepted unknown file transfers from unknown sources and were thus highly vulnerable to social engineering attacks.

- Attackers could create a botnet of Bluetooth enabled, remotely controlled zombie Machines/phones, which they could then use to perform further attacks on devices they couldn’t normally reach.

- A barrier for mobile malware propagation has, historically, been the differences among various operating systems and hardware platforms. This is now easier to overcome because of the growing popularity of Java 2 Micro Edition (J2ME), This enables authors (and the bad guys) to create cross-platform software (or malware for mobiles).

Newer Bluetooth attacks and nifty tricks

Bluetooth attack demonstration:

The following Video depicts:

- Very common and easy prime-rate number attack, achieved via Bluetooth attacks.
- How many people are still actually vulnerable to this attack
- Awareness value
- How easily it can actually be pulled off!!

Newer Bluetooth attacks and nifty tricks

Bluetooth attack demonstration:

Newer Bluetooth attacks and nifty tricks

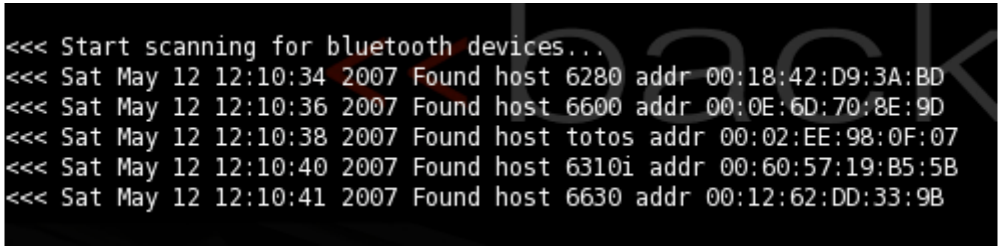
Case Study:

- Bank background - .ZA
- Awareness of issues – Non existent awareness campaigns (i.e. social engineering etc)
- Challenge of obtaining RVN

Newer Bluetooth attacks and nifty tricks

Case Study:

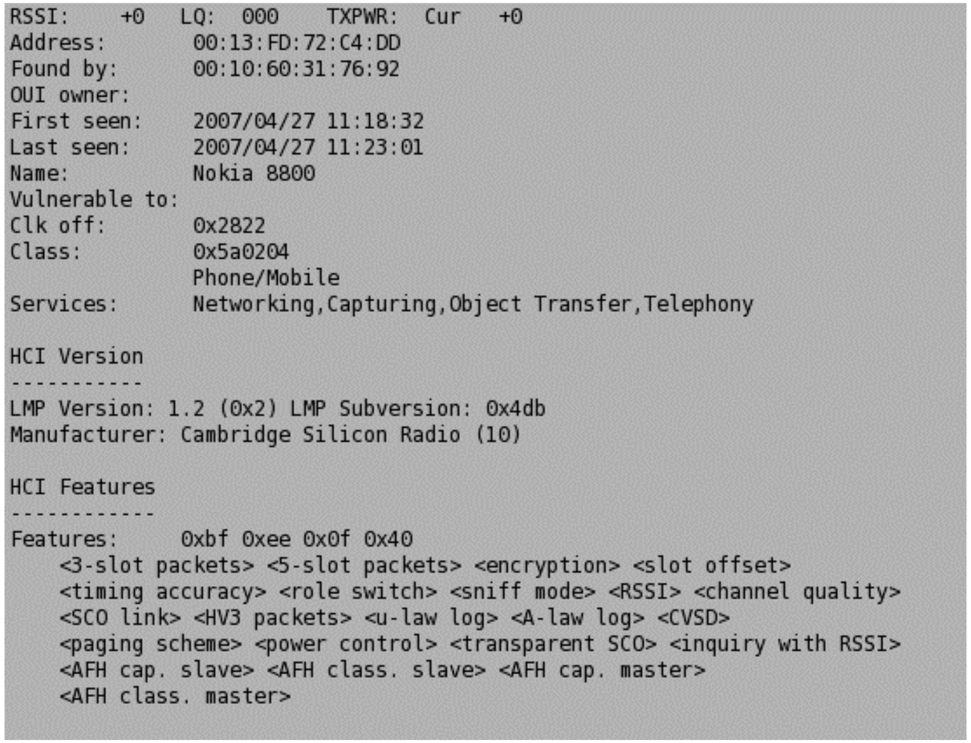
- Internet Kiosk and Challenges
- Past RVN Nightmare (i.e. email)
- Challenge of obtaining RVN via their mobile



```
<<< Start scanning for bluetooth devices...
<<< Sat May 12 12:10:34 2007 Found host 6280 addr 00:18:42:D9:3A:BD
<<< Sat May 12 12:10:36 2007 Found host 6600 addr 00:0E:6D:70:8E:9D
<<< Sat May 12 12:10:38 2007 Found host totos addr 00:02:EE:98:0F:07
<<< Sat May 12 12:10:40 2007 Found host 6310i addr 00:60:57:19:B5:5B
<<< Sat May 12 12:10:41 2007 Found host 6630 addr 00:12:62:DD:33:9B
```

Newer Bluetooth attacks and nifty tricks

Case Study:



```
RSSI:     +0   LQ:  000     TXPWR:  Cur    +0
Address:        00:13:FD:72:C4:DD
Found by:       00:10:60:31:76:92
OUI owner:
First seen:     2007/04/27 11:18:32
Last seen:      2007/04/27 11:23:01
Name:           Nokia 8800
Vulnerable to:
Clk off:        0x2822
Class:          0x5a0204
                Phone/Mobile
Services:       Networking,Capturing,Object Transfer,Telephony

HCI Version
-----------
LMP Version: 1.2 (0x2) LMP Subversion: 0x4db
Manufacturer: Cambridge Silicon Radio (10)

HCI Features
------------
Features:      0xbf 0xee 0x0f 0x40
    <3-slot packets> <5-slot packets> <encryption> <slot offset>
    <timing accuracy> <role switch> <sniff mode> <RSSI> <channel quality>
    <SCO link> <HV3 packets> <u-law log> <A-law log> <CVSD>
    <paging scheme> <power control> <transparent SCO> <inquiry with RSSI>
    <AFH cap. slave> <AFH class. slave> <AFH cap. master>
    <AFH class. master>
```

- ➢Bluetooth specification
- ➢Bluebag concept scanning throughout branch
- ➢Bluebugging and social engineering trusted device (pairing)
- ➢Success in obtaining RVN, log in and transfer (Simple POC)

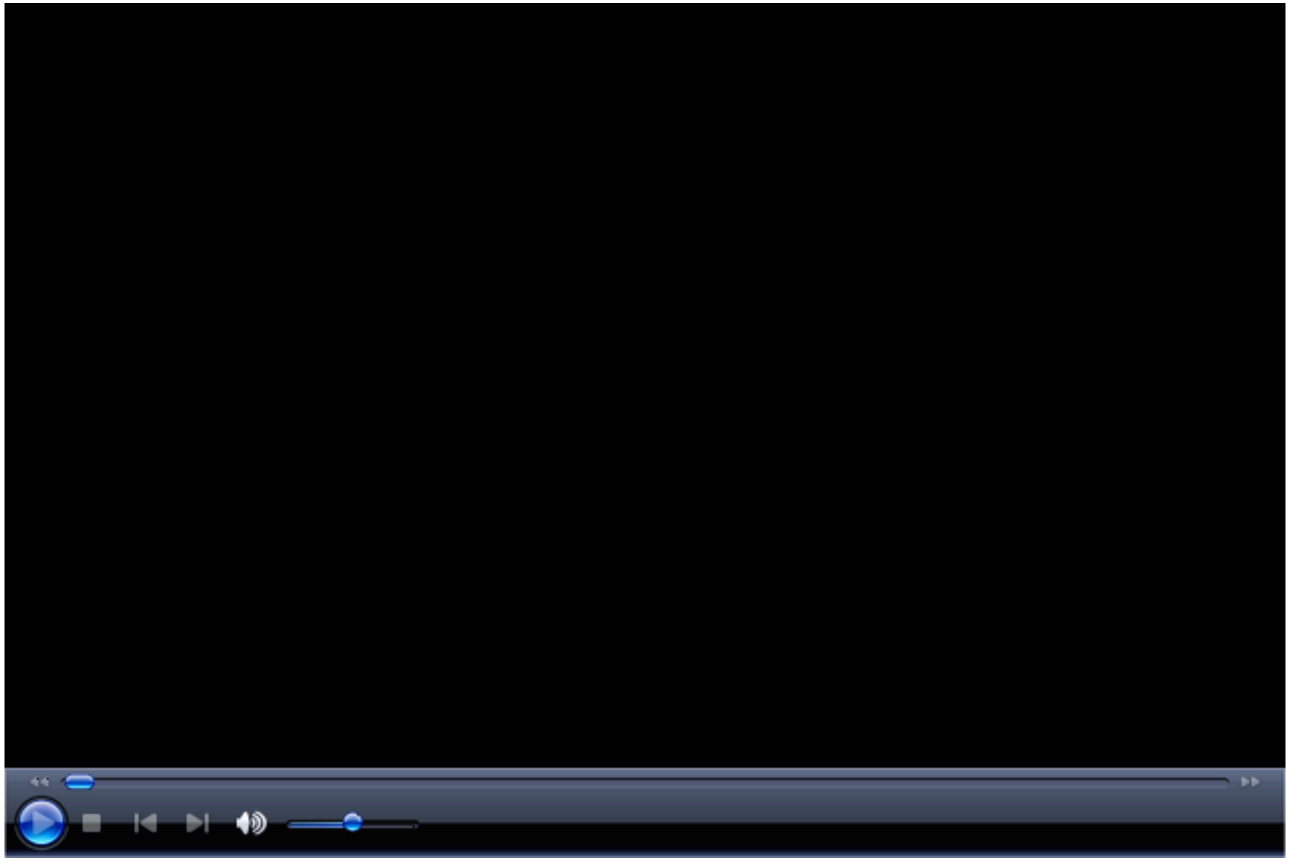
Newer Bluetooth attacks and nifty tricks

PS3 Sixaxiz controllers - Is it possible to pair them and control _other_ devices?

- ➢ Bluetooth mode with Linux
- ➢ Operates as a regular HID device in UDB mode
- ➢ Document explains how to configure Linux to recognize the SIXAXIS as a Bluetooth HID device.
- ➢ Demonstration Videos

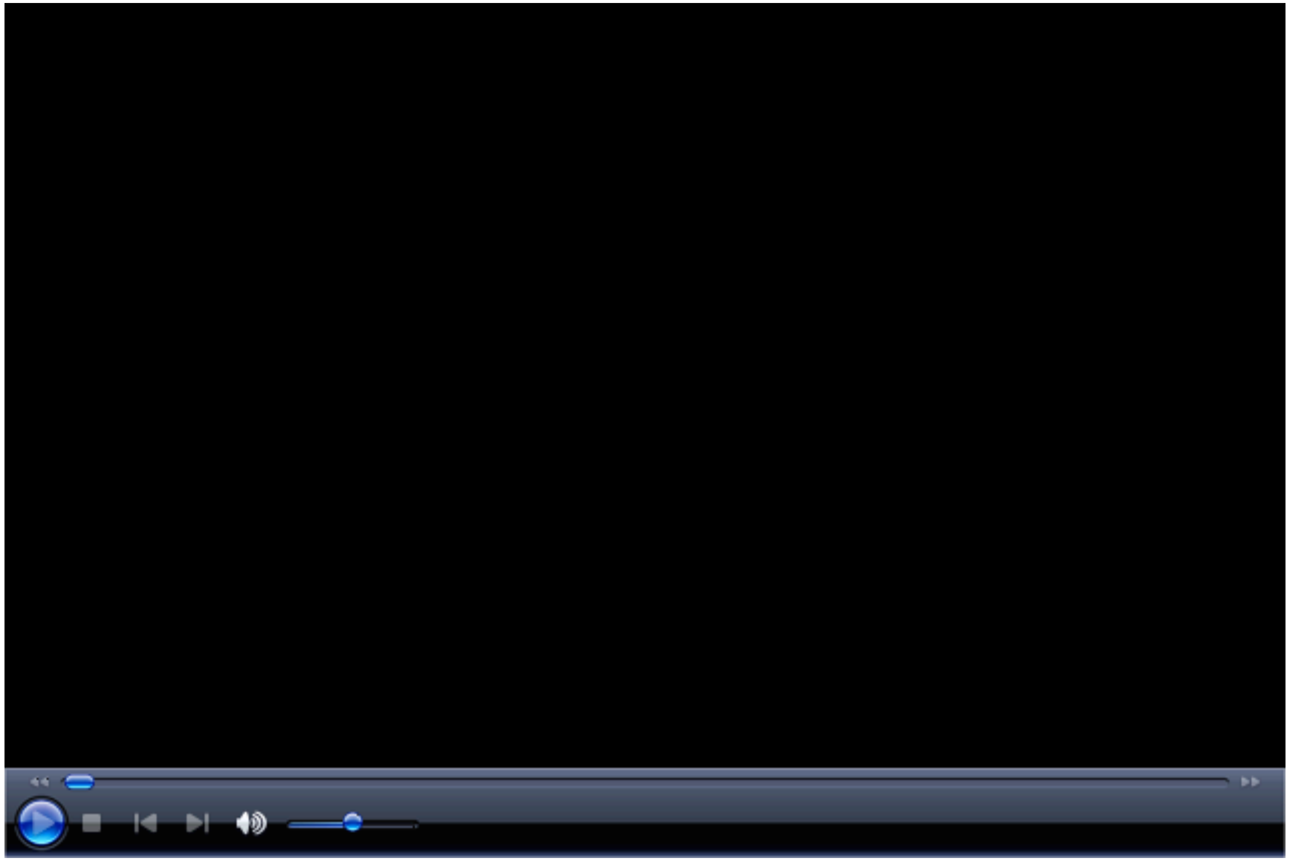
Newer Bluetooth attacks and nifty tricks

Demonstration Video 1:



Newer Bluetooth attacks and nifty tricks

Demonstration Video 2:



Protection

➢Set the device to non-discoverable mode.

➢Enable PIN-based authentication.

➢Use antivirus software

➢Leading antivirus vendors already have products for mobile devices. Vendors such as F-Secure, Kaspersky, Symantec all offer applications for mobile phone protection.

Protection

- Use additional software (Blooover, Blooover II, BT Audit)

- Blooover is a free application written in Java. It can be used only if the phone supports J2ME MIDP 2.0 VM with JSR-82 API.

- BT Audit scans open RFCOMM channels and L2CAP PSM and generates reports on their status.

Summary

In a world where technology is making our lives much easier, we often forget about the possible dangers we face.

With the release of lower cost devices and built in functionality, hackers are continually devising new methods to change devices to work in ways that they were not intended.

Turn off your bluetooth!

Thank you!

http://www.telspace.co.za

Thanks to the following for their extensive research.

Thierry Zoller

Kevin Finistere

Luca Carettoni, Claudio Merloni & Stefano Zanero

http://www.pabr.org/sixlinux/sixlinux.en.html - PS3 Research

Telspace Systems Research Team

Bibliography

Q & A