+

All your Bluetooth is belong to us

The rest too.

Kevin Finistere & Thierry Zoller
Hack.lu - 2006

Bluetooh – Please just turn it off

Turn off your BT please,

,no really.

Who we are ? – Hippies

- Kevin Finistere
  - Former Head of Research of SNOSoft
  - Found Vulnerabilities in Apple, IBM, SAP, Oracle, Symantec…
  - Has contributed **a lot** to this talk
  - Not here today ☹

Mad Hax0r

- Thierry Zoller
  - Welcome home
  - Security Consultant @ N.runs
  - Found vulnerabilities in Checkpoint, Symantec, Citrix, F-Secure, MySQL4, MacAfee, Nod32…
  - Don‘t like to talk about me, see for yourself.

The Goal of this Talk ?

- The Goal of this talk is <u>not</u> to:
  - Build myths
  - Show off – and not show how

- The Goal of this talk is to :
  - Raise awareness
  - Make risks transparent
  - Paradigm Shift – Bluetooth is not only for toys
  - Clear the air about InqTana

What are we talking about today ?

- [0x00] – Introduction : What is Bluetooth ?
  - How does it work and hold together ?
  - Security Modes, Paring modes
  - Scatternets, Piconets..
  - What‘s the difference to WiFi (802.11a/b/g) ?
  - Common Implementations of the Protocol
- [0x01] – Get ready to rumble : Extending the Range
  - Extending the range of Bluetooth devices
  - Building automated reconnaissance and attack devices
  - Bluetooth War driving (GPS, 360° Camera)
  - More..
- [0x02] – Attack! : Getting dirty with it
  - Attacking Mobile Phones / Handhelds / PDAs
  - Attacking Cars / Headsets / Free Hands kits
  - Attacking Internal Networks (0day)
  - Attacking the Protocol, braking the encryption (0day)
  - Tracking the un-trakeable and more..

[0x00] Introduction

- What is Bluetooth ?
  - Invented 1995 by Ericsson, SIG formed 1998 (Bluetooth Special Interest Group)
  - Bluetooth 1.0 - 1.7.1999, first devices sold in mid 2000
  - Named after “Harald Blauzahn”
  - Goal was, low-cost “cable replacement”
  - Personal Area Networks

- Tech Specs
  - 2.400-2.4835 GHz (WiFi, Cameras, etc..)
  - Frequency Hopping, up to 3200 times per second ! (1600 in connection state)

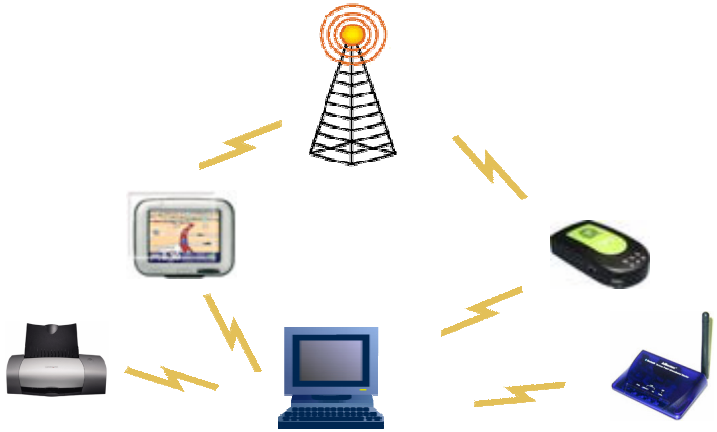
[0x00] Introduction

- The difference and similarities with WiFi :
  - Operate on the same ISM band : 2,4Ghz
  - WiFi 11 Channels, Bluetooth 79 Channels
  - Both do frequency hopping (WiFi 600 times slower)
  - WiFi broadcasts it's presence every x ms
  - Bluetooth is a complete Framework with Profiles and layers of protocols
  - Obvious: Range

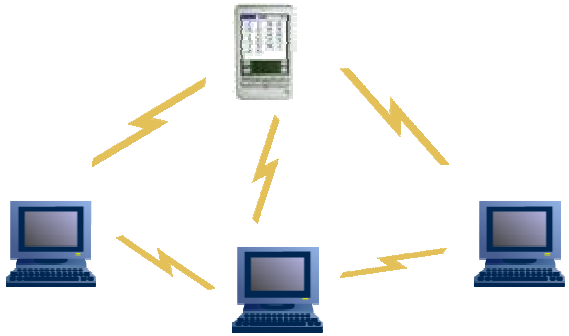
[0x00] Introduction

- What does it do for me ?

Cable Replacement



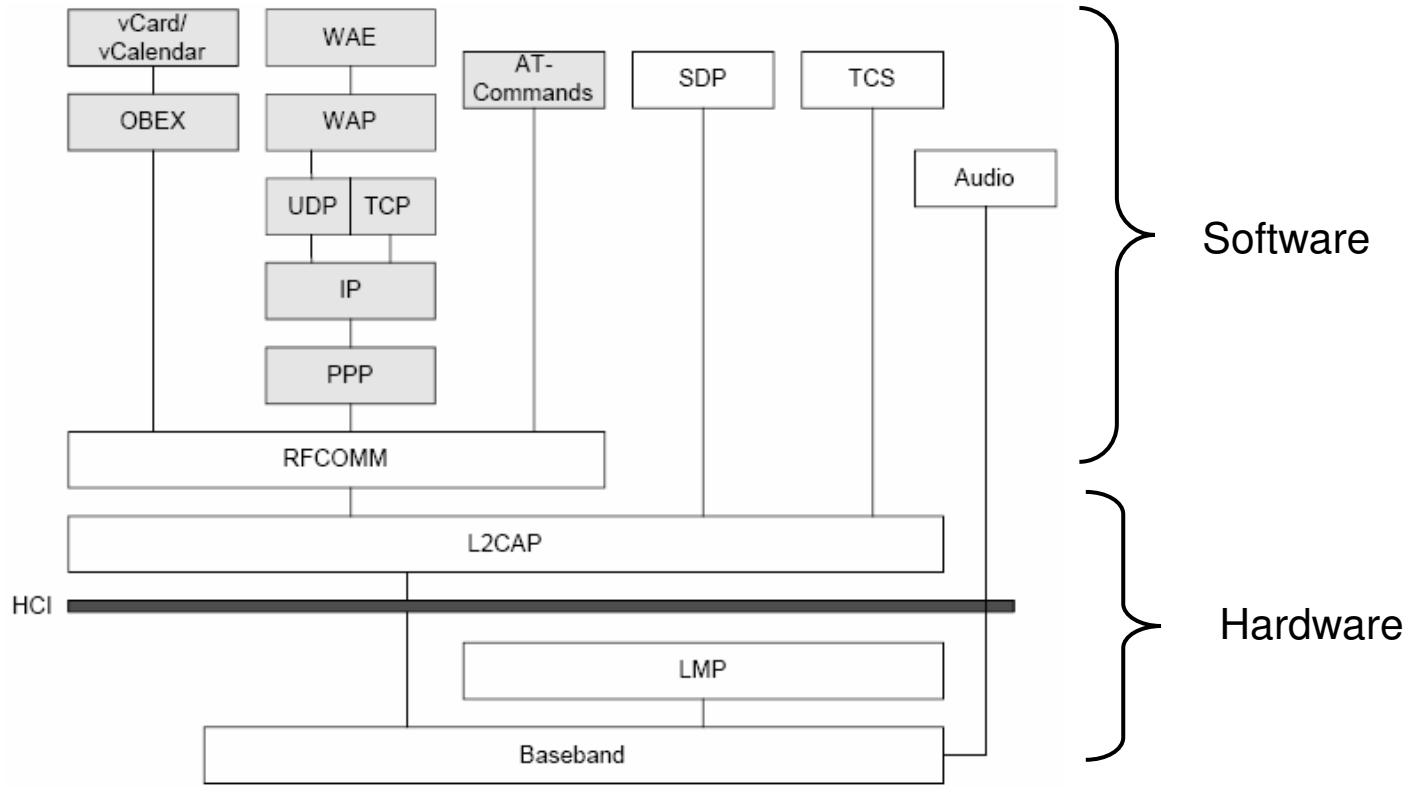
Data/Voice



Personal Area Networks

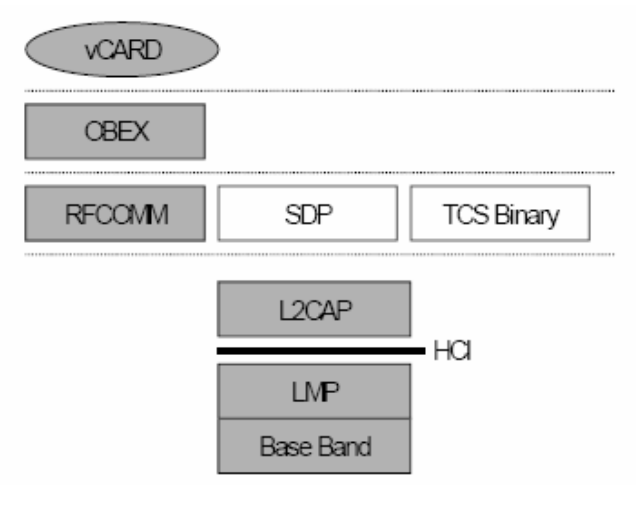
[0x00] Introduction

- The foundation – Protocol Stack



[0x00] Introduction

- The Bluetooth Profiles
  - Represent a group and defines mandatory options
  - Prevent compatibility issues, modular approach to BT extensions
  - Vertical representation of BT layer usage, handled through SDP



Object Push Profile

```
Service Name: OBEX Object Push
Service RecHandle: 0x10001
Service Class ID List:
  "OBEX Object Push" (0x1105)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 9
  "OBEX" (0x0008)
Language Base Attr List:
  code_ISO639: 0x656e
  encoding:    0x6a
  base_offset: 0x100
Profile Descriptor List:
  "OBEX Object Push" (0x1105)
    Version: 0x0100
```

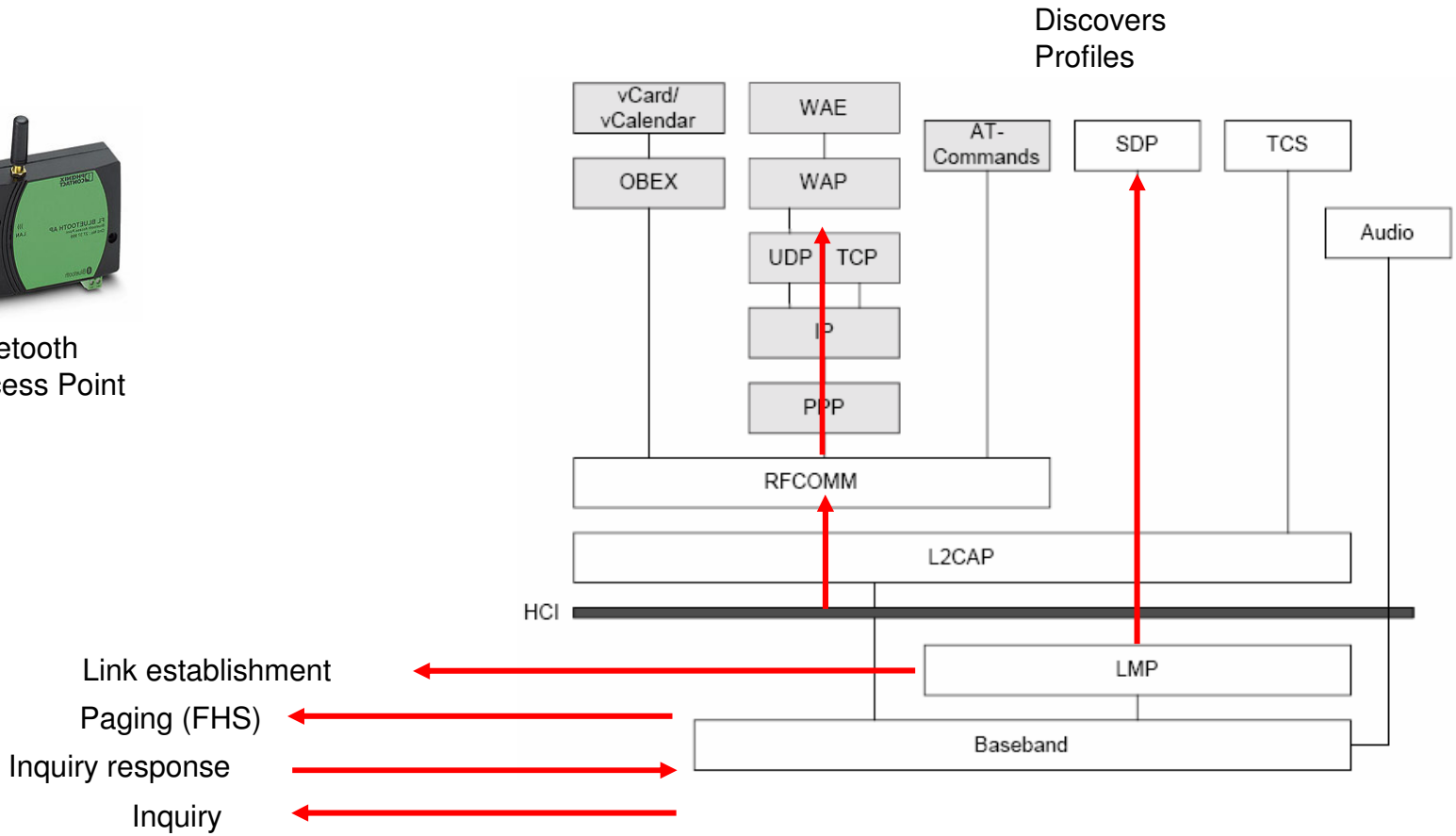
[0x00] Introduction

- Typical Bluetooth Scenario (1)
  - Simplistic Model (ignoring security for now)
    - 1 - User goes into a lobby and wants to read email
    - 2 - Clicks on the PDA Email application
    - 3 - Sends and receives Email

[0x00] Introduction

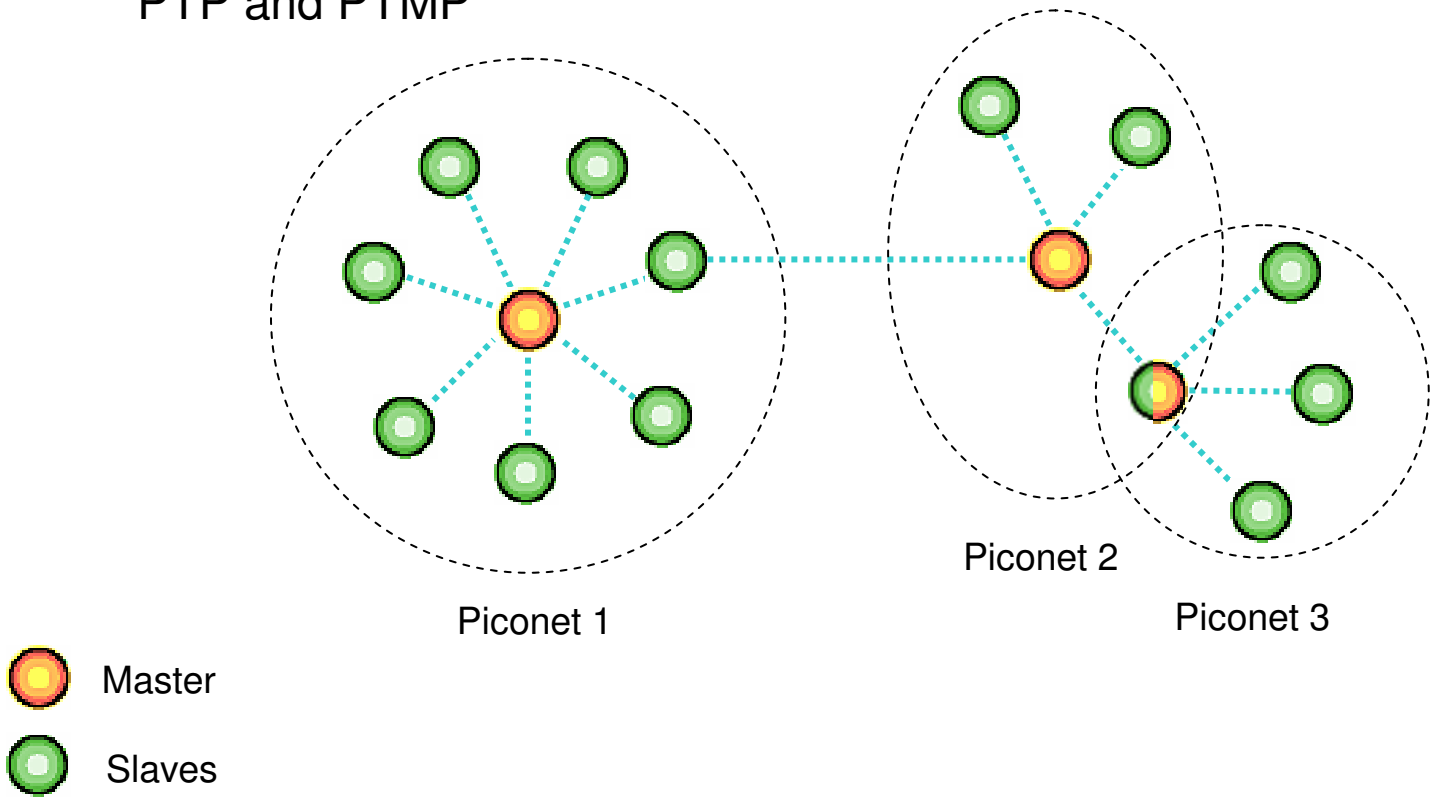
- Typical Bluetooth Scenario (2)

Bluetooth
Access Point



[0x00] Introduction

- Piconets / Scatternets
  - A Piconet can hold 7 active (and 255 parked) slaves and 1 master, PTP and PTMP



[0x00] Introduction

- Frequency Hopping
  - Slaves always sync to the Master
  - Hop up-to 3200 times a second over 79 channels using 625 µs length
  - Piconet agrees to a Sequence based on the BD_ADDR and Clockoffset of the master. (Now THIS is a unique fingerprint)

  - This procedure called “Paging” in Bluetoohesque
  - FH is the reason you can not easily sniff these BT connections. You have to sync to the Master (or use a Spectral Analyzer and reconstruct afterwards – Good luck)

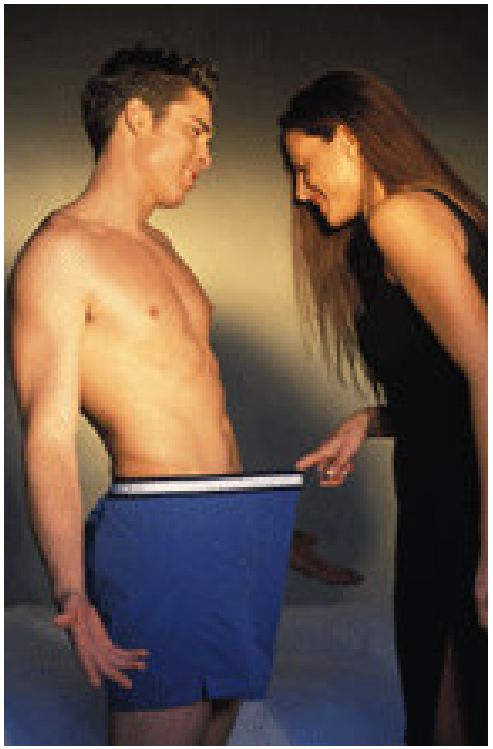
[0x00] Introduction

- Discoverable modes :
  - **Discoverable** :
    Sends inquiry responses to all inquiries.
  - **Limited discoverable**:
    Visible for a certain period of time (Implementation bugs..)
  - **Non-Discoverable**:
    Never answers an inquiry scan (in theory)

- Pairing modes :
  - **Non-pairable mode :**
    Rejects every pairing request (LMP_not_accepted) (Plantronics)
  - **Pairable mode :**
    Will pair up-on request

[0x01] Get ready to rumble

- Extending the Range



[0x01] Get ready to rumble

- Extending the Range

Specification defines 3 classes :
- Class 1 - 100 mW (20 dBm)
- Class 2 - 2.5 mW (4 dBm)
- Class 3 - 1 mW (0 dBm)

Class 3 — 10 M

Class 2 — 25 M

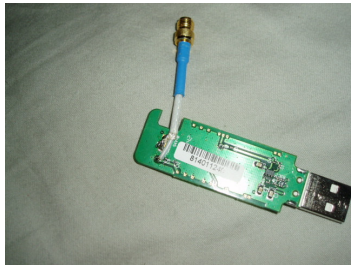
Class 1 — 100 M

Home Grown — 788 M

Home Grown — Up to 2,6km are possible

[0x01] Get ready to rumble

- HOW-TO
  - Modify class 1 dongle to accept an aftermarket antenna.
  - Basic soldering skills required
  - Provides much more flexibility when testing
  - Connects to an Laptop that supports USB
  - Instant Ownage

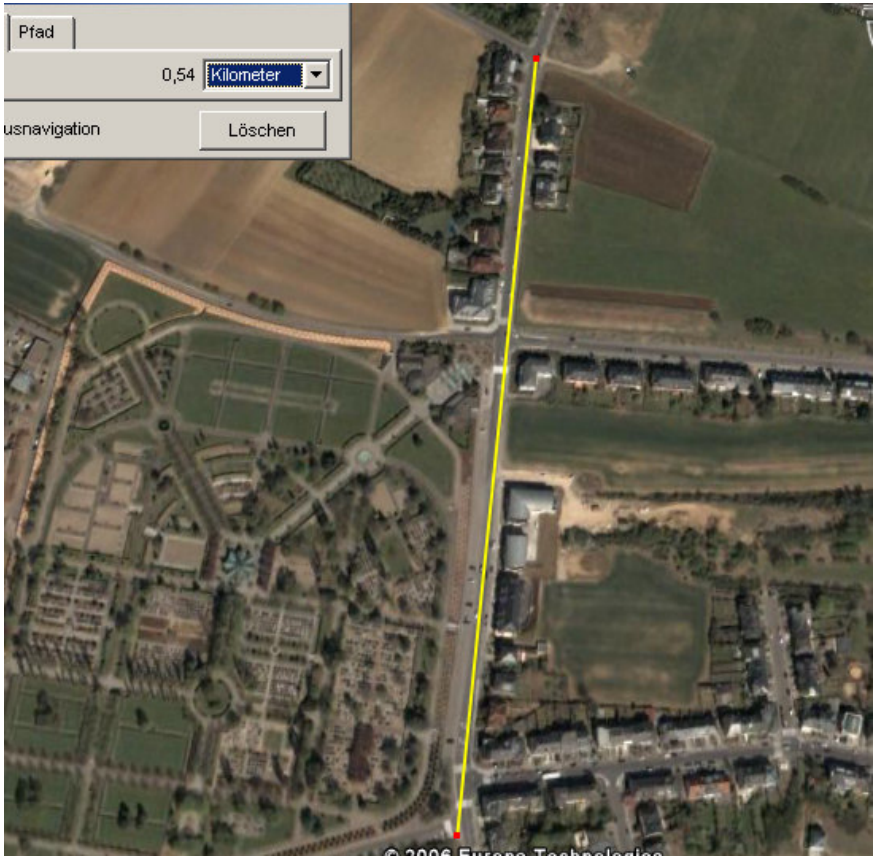


[0x01] Get ready to rumble

- Long Distance - Datasets
  - Antrum Lake, water reflection guarantees longer ranges.
  - 788 Meter !
  - An old Man stole my phone during this test! I tracked him with the yagi.

[0x01] Get ready to rumble

- Long Distance - Datasets
  - Strassen, Luxembourg
  - 550 Meter
  - Thanks Jerome Carrère



[0x01] Get ready to rumble

- Long Distance - More More
  - New World record attempt by Kevin
  - Use of high precision Trimble GPS receivers will be used.
  - DGPS data correction for centimeter accuracy
  - 2,6 km !
  - Needs narrow antenna beam

[0x01] Get ready to rumble

- Optimizing for Penetration (1)
  - Integrated Linksys Dongle
  - Integrated USB Cable
  - Metal Parabola
  - 10 * Zoom
  - Laser (to be done)

[0x01] Get ready to rumble

- Optimizing for Penetration (2)
  - Bundling (Parabola)
  - Higher penetration through walls
  - Glass is your friend
  - On board embedded device. (NSLU2)
  - Auto scan and attack toolkit

  - Experiment : Went through a building found the device on the other side IN another building.

[0x01] Get ready to rumble

- PerimeterWatch – Bluetooth Wardriving
  - Perl Script by KF
  - Searches Bluetooth Devices
  - Takes 360° pictures
  - GPS coordinates

[0x02] Attack !

- Attacking Bluetooth Devices – Bypassing security

[0x02] Attack !

- Menu du Jour :
  - Bluebug (AT over RFCOMM)
  - Bluesnarf (Obex)
  - Car Whisperer
  - Limited time, sorry..

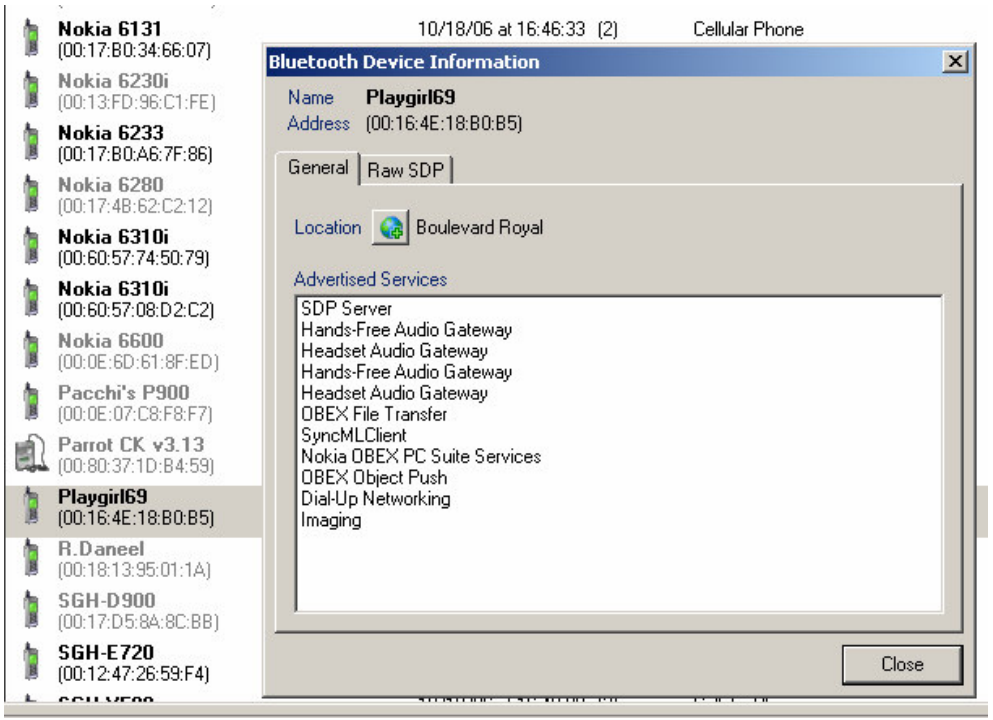
- Some 0-day :
  - Owning internal Networks over Bluetooth
  - Attacking the Protocol:
    Bluecrack - BT Pin and Link key cracker
  - Widcomm Overflow (Broadcom merger leaves lots of vuln users that can not patch) BTW 3.0.1.905 (../ attacks) and up to BTW 1.4.2.10 has (overflows)

[0x01] Get ready to rumble

- Luxembourg – 1 hour Bluetooth Scan
  - Boulevard Royal
  - 295 unique discoverable Bluetooth devices
  - Lots of vulnerable ones

Type

- Smart Phone (33)
- Cellular Phone (195)
- Hands Free (24)
- Headset (10)
- Unclassified (4)
- Cordless Phone (10)
- Unclassified Phone (5)
- Miscellaneous (1)
- Palm Computer (3)
- Handheld Computer (1)



[0x01] Get ready to rumble

- Luxembourg – 1 hour Bluetooth Scan
  - 00:0E:9F - Audi UHV – Pin 1234

Unknown (00:0E:9F:20:FB:C0)	10/18/06 at 16:25:41 10/18/06 at 16:25:41	(1)	Hands Free	Boulevard Royal
Unknown (00:0E:9F:20:F4:3C)	10/18/06 at 16:30:16 10/18/06 at 16:30:16	(1)	Hands Free	Boulevard Royal
Unknown (00:0E:9F:22:51:42)	10/18/06 at 16:34:07 10/18/06 at 16:34:07	(1)	Hands Free	Boulevard Royal

  - Nokia 6310 - Disaster

Nokia 6310i (00:60:57:74:50:79)	10/18/06 at 16:40:30 10/18/06 at 16:45:51	(6)	Cellular Phone SDP	Boulevard Royal
Nokia 6310i (00:60:57:08:D2:C2)	10/18/06 at 16:45:04 10/18/06 at 16:48:22	(7)	Cellular Phone SDP	Boulevard Royal
Nokia 6310i	10/18/06 at 17:05:29	(2)	Cellular Phone	Boulevard Royal

[0x02] Attack !

- Implementation - Issues Galore
  - **Pairing always enabled**
    Rare – few devices
    Headsets (Plantronix) – Pairing Button is useless
    Default Pins (0000, 1111 …)
  - **Discovery enabled**
    Lots of Devices
    Siemens T60 – stays in discover mode if you ping it, might be attacked forever.
  - **Hidden (non advertised) Services**
    ObexIRDA, etc Nokia, others..

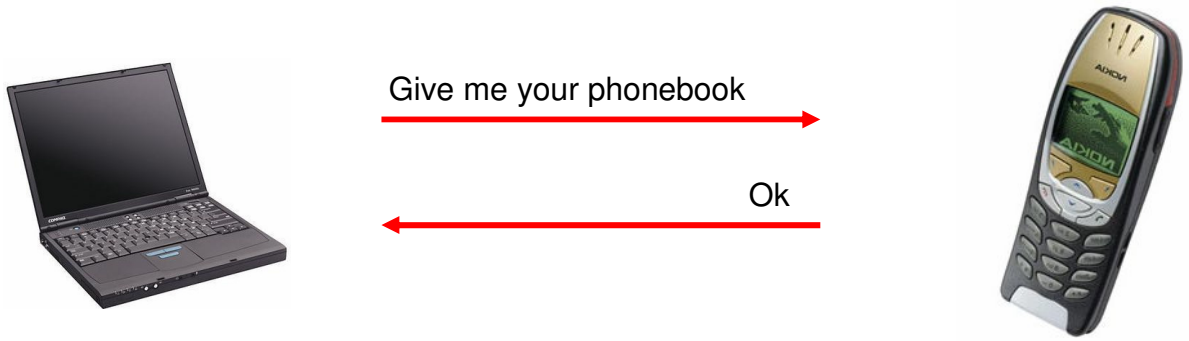
[0x02] Attack !

- Bluebug Attack – Trifinite Group
  - The Service that shouldn't be there
    - Read phonebook
    - Read / Send SMS
    - Dial Number
    - Redirect Calls
    - Etc…

  - Vulnerable devices :
    - Nokia 6310, Nokia 6310i, Nokia 8910i, Nokia 8910, T68, Sony Ericsson T68i, T610, T68, T68i, R520m, T610, Z1010, Z600, Motorola V80, V5xx, V6xx and E398 and others…

[0x02] Attack !

- Bluesnarf Attack – Trifinite Group
  - Basically a “get” request over OBEX Push
  - Obex Push usually not authenticated
  - Request for known files, telecom/pb.vcf



  - Vulnerable devices :
    - Nokia 6310, Nokia 6310i, Nokia 6650, Ericsson T610, Ericsson T68, Ericsson T68i, Ericsson T630, Ericsson Z600 others…

[0x02] Attack !

- CarWhisperer – Martin Herfurt
  - Listen and Record Conversations
  - Eavesdrop on Headsets, Hands-Free kits
  - Works against Widcomm < BTW 4.0.1.1500 with no pincode required!
  - Root Cause :
    Paring mode, discoverable, hard coded Pin.

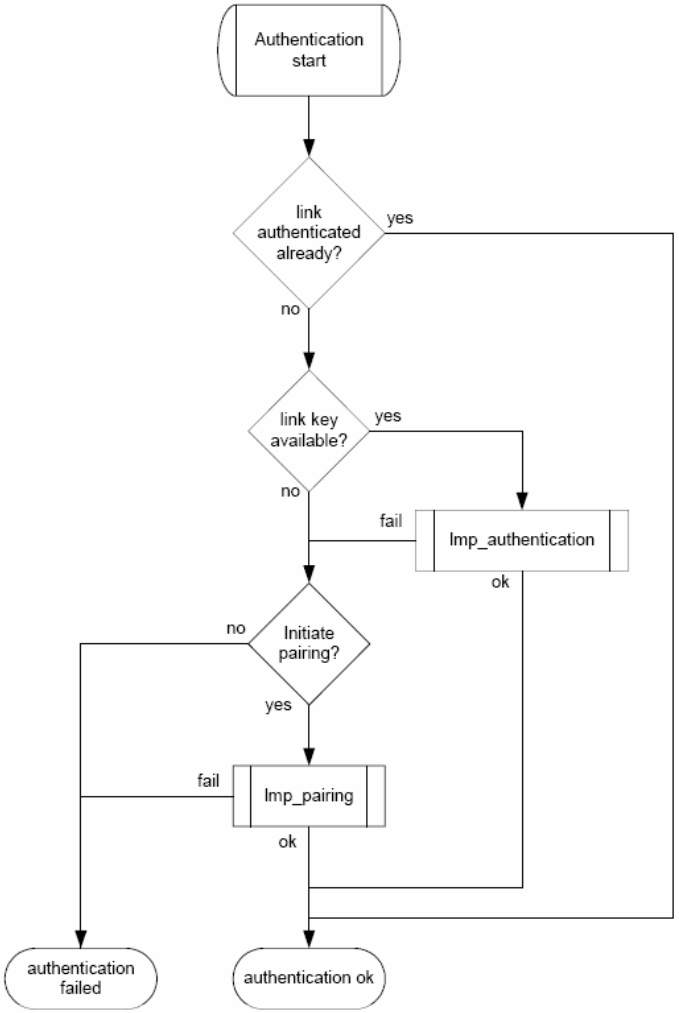
```
SWITCH: for ($bdaddr) {
        /00:02:EE/      && do { $pin="5475"; last;}; # Nokia
        /00:0E:9F/      && do { $pin="1234"; last;}; # Audi UHV
        /00:80:37/      && do { $pin="8761"; last;}; # O'Neill
        /00:0A:94/      && do { $pin="1234"; last;}; # Cellink
        /00:0C:84/      && do { $pin="1234"; last;}; # Eazix
        $pin="0000"; # 0000 is the default passkey in many cases
        }
```

[0x02] Attack !

- Wireless Keyboards
  - If HID server (PC) accepts connections, you might remotely control the PC. (Collin R. Mulliner)
  - If you have the link key :
    - decryption of packets i.e. capture the keystrokes.
    - connect to the PC and remotely control it

[0x02] Attack !

- The PIN is not really that useful
  - The link key is !
  - Here's why :



  - Protocol 1.2 Authentication :

[0x02] Attack ! – 0day

- InqTana - Setting the Record straight
  - Kevin created a cribbled PoC Worm named InqTana
  - It's real, it's here and it's not an invention of the AV industry, KF handed it over in order for them to protect you against these types of attacks.

  - ObexFTP server directory traversal exploit,malicious InputManager and a local root exploit = remote login tty over rfcomm
  - NO user interaction required
  - Media completely missed the point and invented an obscure conspiracy theory
  - **Points were :**
    - Macs are NOT invulnerable (the flaw is patched now)
    - You can own internal networks over Bluetooth

[0x02] Attack ! – 0day

- Obex ../../../ - Owning internal networks
  - Apple
    - OSX 10.3 Tiger
    - OSX 10.4 Jaguar
      Vanilla, delayed release
  - Windows
    - Widcomm, Toshiba,
      Bluesoil, others ?
  - Pocket PC

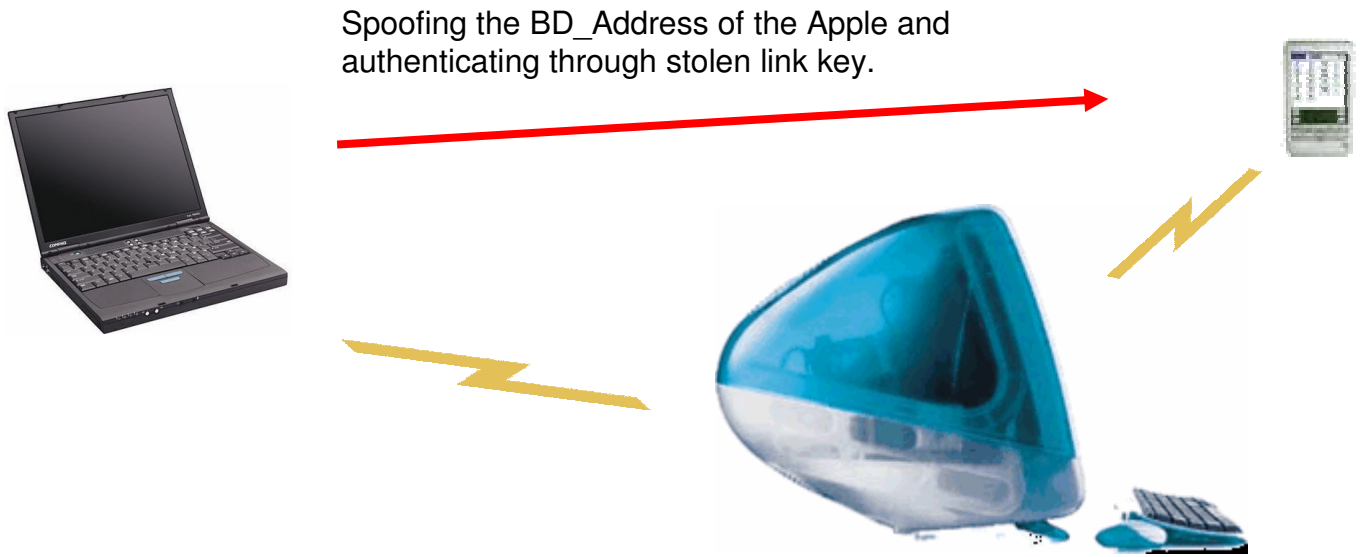
- Kevin: Apple asked me to not tell 10.4 was shipping vulnerable
- OSX 10.3.9 patched, OSX 10.4 shipped vulnerable patched a month after OSX 10.3.9

[0x02] Attack ! – 0day

- MAC OS 10.3 & 10.4 Vanilla
  - Multi-Staged attack :
    - Step 1 – ObexFTP ../../../ Attack
    - Step 2 – Using Input Manager launches Root exploit (then binds getty to the pda sync port)
    - Step 3 – Connecting to Port 3 over Rfcomm
    - Step 4 – Harvesting Keys
    - Step 5 – Owning the network, scanning for other BT devices, compromising them.

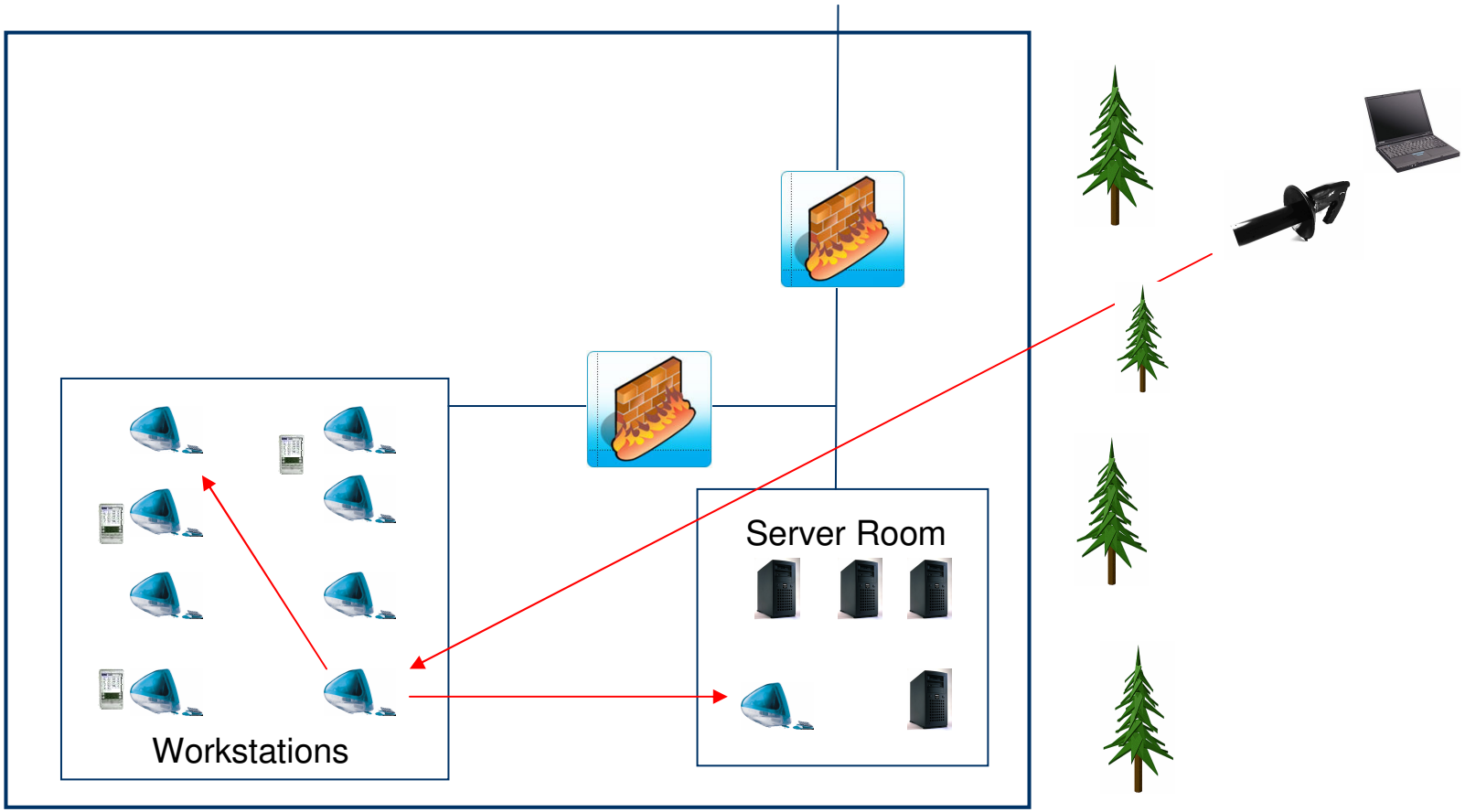
[0x02] Attack ! – 0day

- MAC OS 10.3 & 10.4 Vanilla
  - Multi-Staged attack :



[0x02] Attack ! – 0day

- Transposed to a Company



[0x02] Attack ! – 0day

- Get the Code
  - For Hack.lu, Inqtana code release : http://www.digitalmunition.com
  - Presented also in the upcoming Hacking Exposed : Wireless

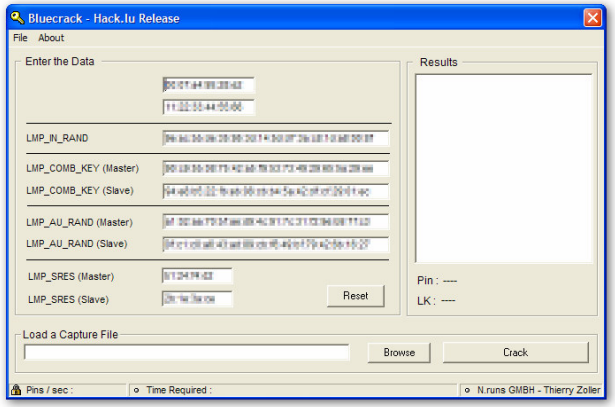
[0x02] Attack !

- BUT – The misconception vault
  - we have an USB policy
  - BT is only 10 meters
  - we have automatic patches
  - we have preset policies disabling all Wireless devices

- Your internal networks are at risk.
  - Implement Mitigation / Monitoring
  - RFProtect and similar Products

[0x02] Attack ! – 0day

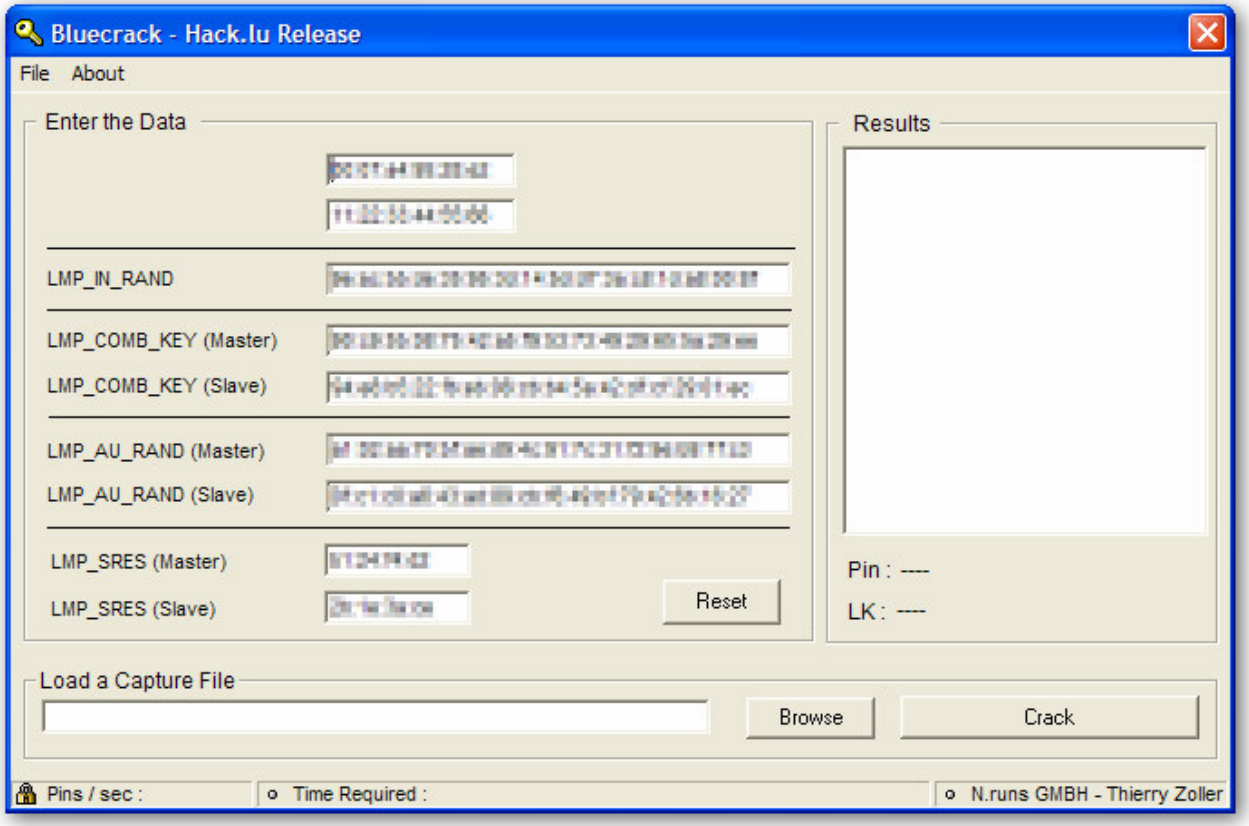
- Introducing BTCrack
  - Hack.lu release
  - Cracks PIN and Linkkey
  - Requires values from a Pairing sniff
  - We can force repairing by using various Methods
  - Based on the research of Shaked and Wool



  - 4 digits pin – 0,25 seconds

[0x02] Attack ! – 0day

- Introducing BTCrack



[0x02] Attack ! – 0day

- BT Crack – Behind the scenes (1)
  - Pairing

E22 = Connection key
E21 = Device key

Device A		Device B
Step1 Generates (RAND) K = E22(RAND, PIN, PIN_LEN)	Rand →	**Step1** K = E22(RAND, PIN, PIN_LEN)
Step2 Generates (RANDA) CA = RANDA xor K	CA →	**Step2** Generates (RANDB) CB = RANDB xor K
	← CB	
Step3 RANDB=CA xor K LKA=E21(RANDA, ADDRA) LKB=E21(RANDB,ADDRB) LKAB=LKA xor LKB		**Step3** RANDB=CA xor K LKA=E21(RANDA, ADDRA) LKB=E21(RANDB,ADDRB) LKAB=LKA xor LKB
Step4 SRESA = E1(CH_RANDA,ADDRB,LKAB)	CH_RANDA →	**Step4** SRESB = E1(CH_RANDA,ADDRB,LKAB)
	← SRESB	
Step5 SRESA = SRESB		

[0x02] Attack ! – 0day

- BT Crack – Behind the scenes

  Right : Shaked and Wool logic
  Bottom: Pseudo code by Tomasz Rybicki

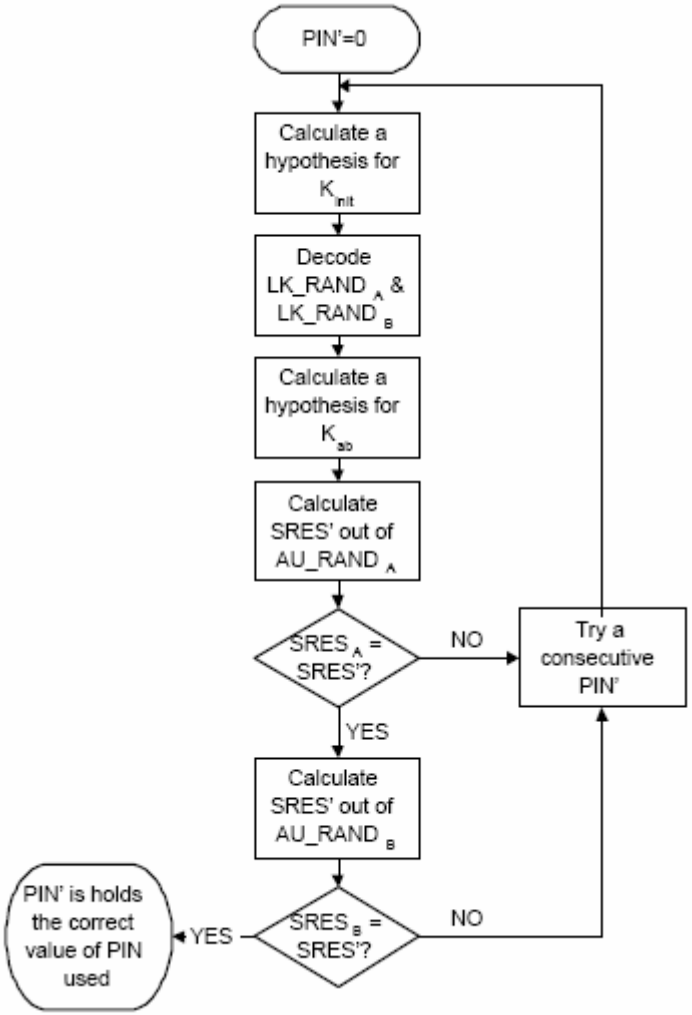
```
Pin =-1;
Do
{
   PIN++;
   CR_K=E22(RAND, PIN, length(PIN));

   CR_RANDA = CA xor CR_K;
   CR_RANDB = CB xor CR_K;

   CR_LKA = E21 (CR_RANDA, ADDRA);
   CR_LKB = E21 (CR_RANDB, ADDRB);

   CR_LKAB = CR_LKA xor CR_LKB;

   CR_SRES = (CH_RAND, ADDRB, CR_LKAB);
}
 while (CR_SRES == SRES)
```



- Hackin9 04/2005 - Tomasz Rybicki

[0x02] Attack ! – 0day

- BT Crack – Demo

[0x02] Attack ! – 0day

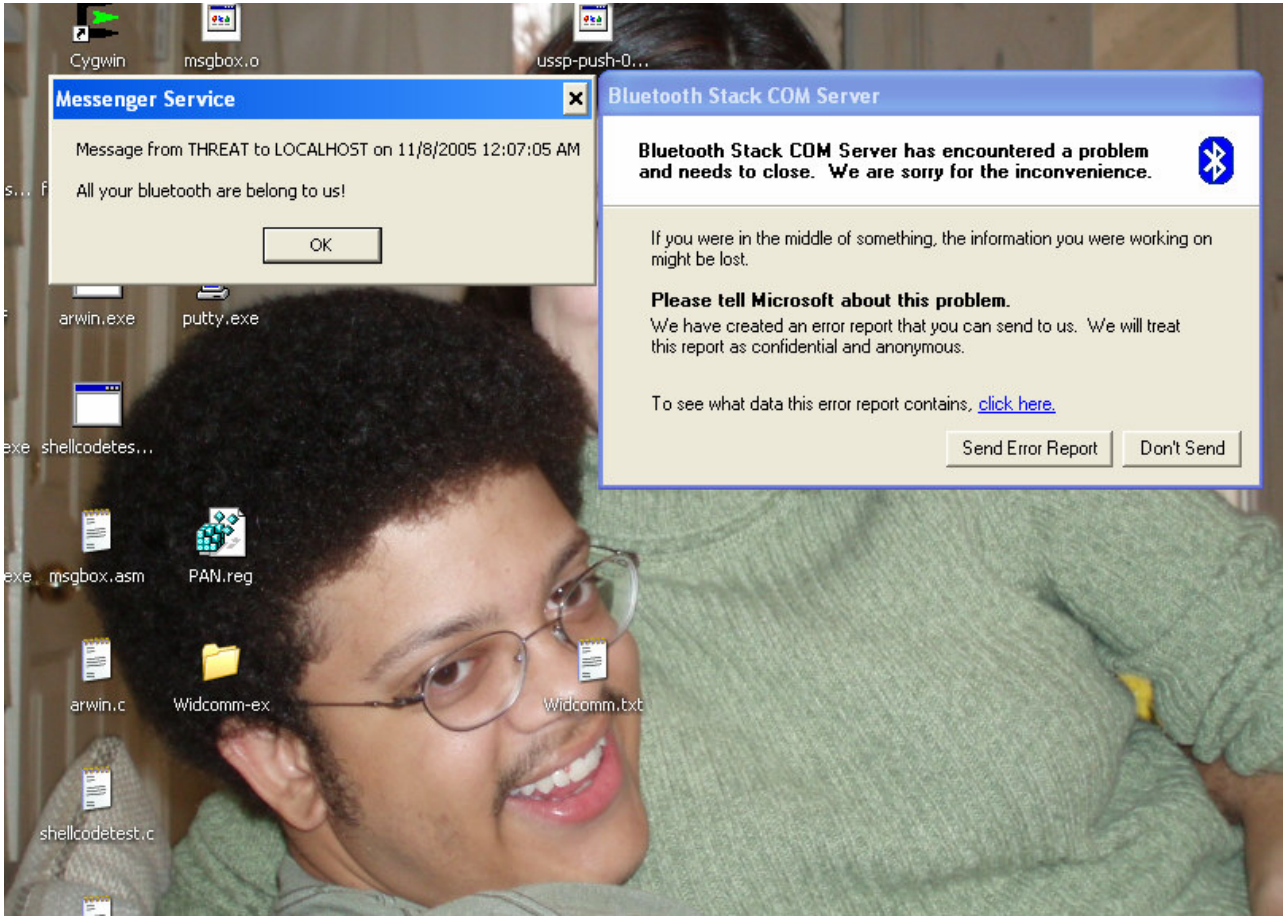
- BT Crack – Download
  - Give me a bit of time to fix the bugs
  - Will be available at http://www.nruns.com

[0x02] Attack !

- Windows Widcomm - Buffer overflows
  - Video
    - http://www.digitalmunition.com/Widcomm.avi
    - File
  - Vulnerable versions
    - Widcomm Stack up to 3.x is vuln
    - Widcomm BTStackServer 1.4.2 .10
    - Widcomm BTStackServer 1.3.2 .7
    - Widcomm Bluetooth Communication Software 1.4.1 .03
    - HP IPAQ 2215
    - HP IPAQ 5450

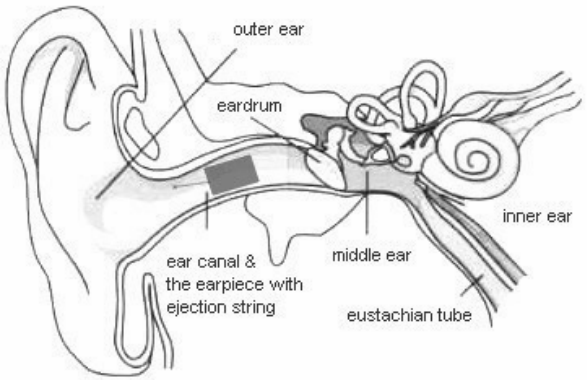
[0x02] Attack !

- Windows Widcomm - Buffer overflows



[0x02] Attack ! – 0day

- Owning the Secret Service ? ;)
  - MicroEarpiece – worlds smallest
  - Goes **into** the ear Tunnel



Your phone then asks if you want to pair with it. Accept by pressing 'Yes' or 'OK' on the phone and confirm with the **passkey or PIN[3] = 0000 (4 zeros).**

  - Jabra Headset - Pin Code : 0000
  - Seriously: You can get it at MicroEarPiece.com
  - Not discoverable, not in Pairing mode, got it yesterday evening, no time

[0x02] Attack !

- Things to Remember :
  - Bluetooth might be a risk for your Company
  - Don’t accept every file you are being send, just click NO.
  - Disable Bluetooth if not required
  - Pair in “secure” places (SIG Recommendations)
  - Hold your Bluetooth vendor accountable for vulnerabilities!