The IASTED International Conference on Communication, Network and Information Security (CNIS 2005),
Phoenix, Arizona, USA, November 14-16, 2005.

TWO PRACTICAL ATTACKS AGAINST BLUETOOTH SECURITY USING NEW ENHANCED IMPLEMENTATIONS OF SECURITY ANALYSIS TOOLS

MSc Keijo M.J. Haataja
Senior assistant
Department of CS
University of Kuopio
Finland
E-mail: haataja@cs.uku.fi

References

- **Bluetooth SIG, *Bluetooth specifications 1.0, 1.1, 1.2 and 2.0+EDR* (Technical specifications, https://www.bluetooth.org, 1999-2004).**
- **In-Stat/MDR, *Bluetooth 2004: Poised for the Mainstream* (Market Research Report, http://www.instat.com/r/nrep/2004/IN0401211MI.htm, 2004).**
- **IEEE Registration Authority, *IEEE Public OUI and Company id Assignments* (Homepage, http://standards.ieee.org/regauth/oui/oui.txt, 2005).**
- **K. Haataja, *Detailed descriptions of new proof-of concept Bluetooth security analysis tools and new security attacks* (Research report, University of Kuopio, http://www.cs.uku.fi/tutkimus/publications/reports/B-2005-1.pdf, 2005).**
- **O. Whitehouse, *@Stake - Where Security & Business Intersect* (Research report, CanSecWest/core04, http://cansecwest.com/csw04/csw04-Whitehouse.pdf, 2004).**
- **LeCroy - Protocol Solutions Group, *LeCroy Bluetooth Protocol Analyzers* (Homepage, http://www.lecroy.com/tm/products/ProtocolAnalyzers/bluetooth.asp?menuid=60, 2005).**
- **LeCroy - Protocol Solutions Group, *CATC Scripting Language Reference Manual for LeCroy Bluetooth Analyzers* (Homepage, http://www.catc.com/support/docs/pdf/BTCSLManual121.pdf, 2005).**
- **A. Laurie and B. Laurie, *The Bunker - Serious flaws in Bluetooth security lead to disclosure of personal data* (Homepage, http://www.thebunker.net/security/bluetooth.htm, 2004).**
- **SecuriTeam, *RedFang, Bluetooth Discovery Tool* (Homepage, http://www.securiteam.com/tools/5JP0I1FAAE.html, 2005).**
- **BlueZ Project, *BlueZ - Official Linux Bluetooth protocol stack* (Homepage, http://www.bluez.org, 2005).**
- **M. Herfurt, *Detecting and Attacking bluetooth-enabled Cellphones at the Hannover Fairground* (Research report, CeBIT'04, http://trifinite.org/Downloads/BlueSnarf CeBIT2004.pdf, 2004).**

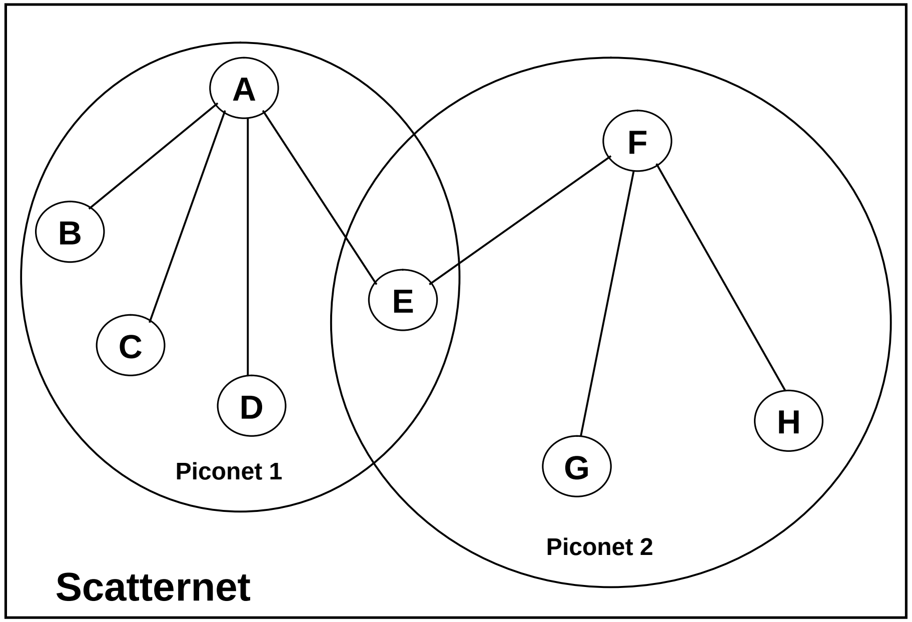
Contents

- Overview on Bluetooth technology
- Overview on Bluetooth security
- Introduction to *On-Line PIN Cracking*
- Introduction to *Brute-Force BD_ADDR Scanning*
- New Bluetooth security analysis tools
- New attacks against Bluetooth security
- Countermeasures
- Conclusions

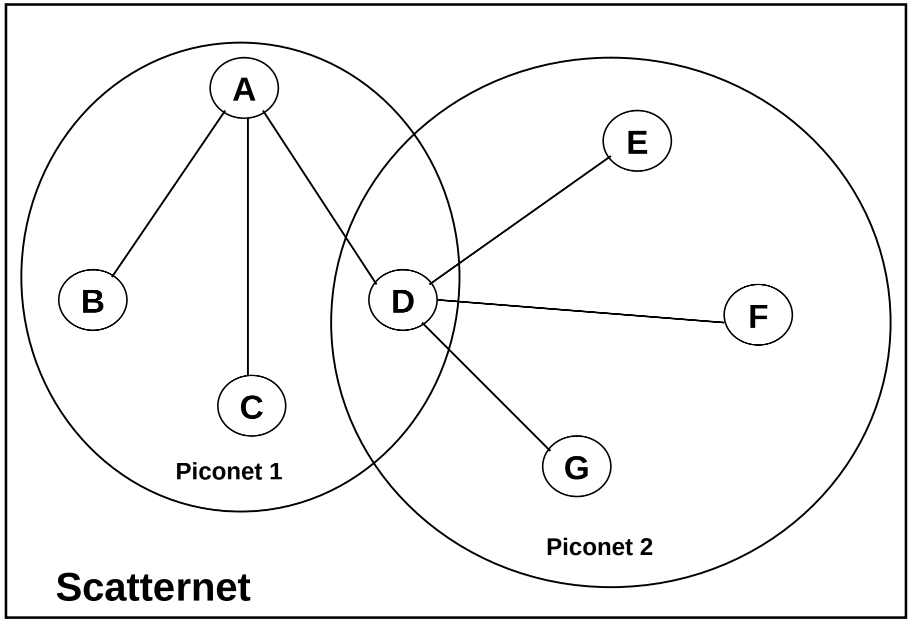
Overview on Bluetooth technology

- Wireless data transfer via ACL (Asynchronous Connection-Less) link
- Wireless two-way voice transfer via SCO/eSCO (Synchronous Connection-Oriented / Extended SCO) link
- Data rates up to 3 Mb/s
- 5x5 mm microchips form ad-hoc networks
- 2.4 GHz ISM-band (Industrial Scientific Medicine), f=2402+k MHz, k=0,…,78
- Typical communication range is 10 - 100 meters
- Bluetooth SIG (Bluetooth Special Interest Group) develops technology and brings devices to the market
- Current Bluetooth specification is 2.0+EDR (Enhanced Data Rate)

Bluetooth topology (ACL link)



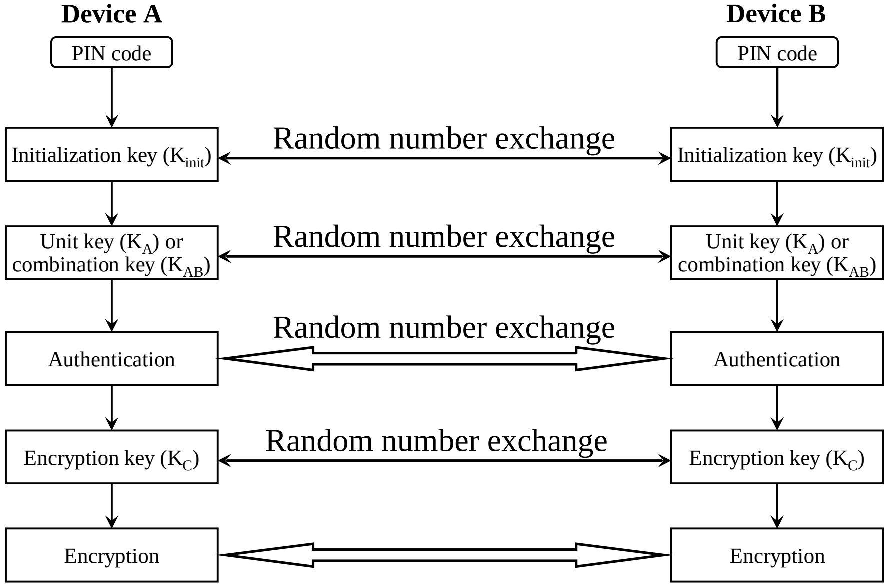
Bluetooth topology (SCO/eSCO link)



Overview on Bluetooth security

- Security within Bluetooth itself covers three major areas:
  - Authentication
  - Authorization
  - Encryption
- Security levels:
  - Silent
  - Private
  - Public
- Security modes:
  1. Nonsecure
  2. Service-level enforced security
  3. Link-level enforced security

Summary of Bluetooth security operations



Device A

PIN code

Initialization key (K_{init})

Unit key (K_A) or combination key (K_{AB})

Authentication

Encryption key (K_C)

Encryption

Device B

PIN code

Initialization key (K_{init})

Unit key (K_A) or combination key (K_{AB})

Authentication

Encryption key (K_C)

Encryption

Random number exchange

Random number exchange

Random number exchange

Random number exchange

Introduction to *On-Line PIN Cracking*

- *On-Line PIN Cracking means that:*
  - an attacker is trying to authenticate with the target device by guessing different PIN values
- *On-Line PIN Cracking* is based on:
  - the idea of changing the BD_ADDR of the attacking device every time PIN guess fails => The ever increasing delay between retries can be bypassed!
- *On-Line PIN Cracking* is possible if:
  - the target device has a fixed PIN code
  - an attacker knows the BD_ADDR of the target device

Introduction to *Brute-Force BD_ADDR Scanning*

- *Brute-Force BD_ADDR Scanning means that:*
  - an attacker is trying to discover the BD_ADDR of the non-discoverable target device via brute-force scanning
- *Brute-Force BD_ADDR Scanning* is possible if:
  - an attacker has enough scanning devices
  - an attacker has a good *Brute-Force BD_ADDR Scanning* software tool (e.g. RedFang or *Brute-Force BD_ADDR Scanning script*)
- *Brute-Force BD_ADDR Scanning* is based on:
  - the idea of brute-forcing only the last three bytes of a BD_ADDR, because the first three bytes are publicly known and can be set as fixed

New Bluetooth security analysis tools

- We call our new Bluetooth security analysis tools as:
  - *On-Line PIN Cracking script*:
    - As far as we know, our *On-Line PIN Cracking script* is the only security analysis tool for On-Line PIN Cracking so far!
    - Works only with LeCroy Bluetooth Protocol Analyzers
  - *Brute-Force BD_ADDR Scanning script*:
    - Other Brute-Force BD_ADDR Scanning security analysis tools exist, such as RedFang, but as far as we know, our *Brute-Force BD_ADDR Scanning script* is the fastest security analysis tool for Brute-Force BD_ADDR Scanning so far (**four times faster** than RedFang)!
    - Works only with LeCroy Bluetooth Protocol Analyzers

On-Line PIN Cracking script

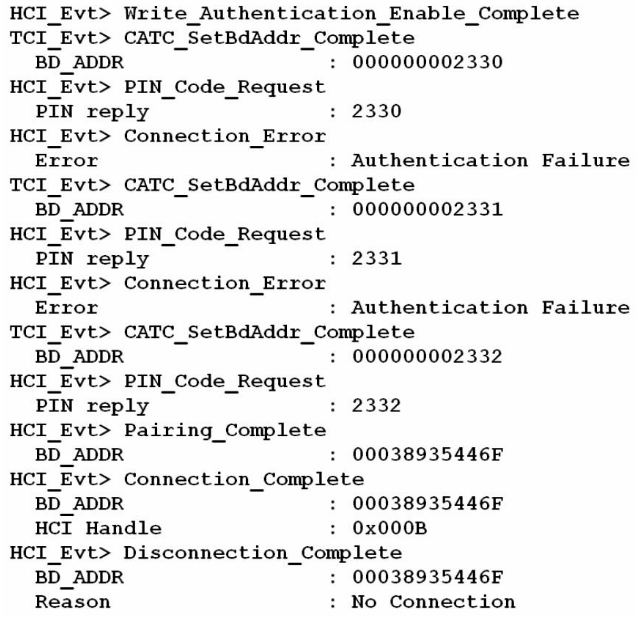
- CATC Scripting Language, which is based on C language syntax, was used for creating our *On-Line PIN Cracking script*, which works in the following way:

  1) Change the local BD_ADDR of the protocol analyzer and set a PIN value for the next PIN trial.

  2) Create basic ACL link between the protocol analyzer and the target device.

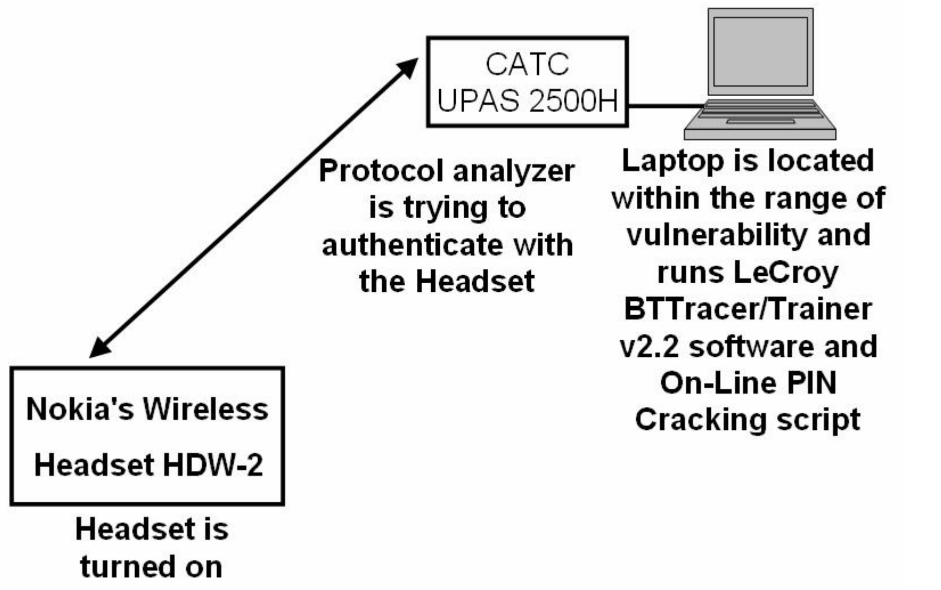
  3) Perform authentication with the target device by using the PIN value set in step 1. If authentication fails, go back to step 1. Otherwise On-Line PIN Cracking has been completed successfully!

On-Line PIN Cracking script



```
HCI_Evt> Write_Authentication_Enable_Complete
TCI_Evt> CATC_SetBdAddr_Complete
  BD_ADDR                : 000000002330
HCI_Evt> PIN_Code_Request
  PIN reply              : 2330
HCI_Evt> Connection_Error
  Error                  : Authentication Failure
TCI_Evt> CATC_SetBdAddr_Complete
  BD_ADDR                : 000000002331
HCI_Evt> PIN_Code_Request
  PIN reply              : 2331
HCI_Evt> Connection_Error
  Error                  : Authentication Failure
TCI_Evt> CATC_SetBdAddr_Complete
  BD_ADDR                : 000000002332
HCI_Evt> PIN_Code_Request
  PIN reply              : 2332
HCI_Evt> Pairing_Complete
  BD_ADDR                : 00038935446F
HCI_Evt> Connection_Complete
  BD_ADDR                : 00038935446F
  HCI Handle             : 0x000B
HCI_Evt> Disconnection_Complete
  BD_ADDR                : 00038935446F
  Reason                 : No Connection
```

On-Line PIN Cracking script



Protocol analyzer is trying to authenticate with the Headset

Laptop is located within the range of vulnerability and runs LeCroy BTTracer/Trainer v2.2 software and On-Line PIN Cracking script

Headset is turned on

Brute-Force BD_ADDR Scanning script

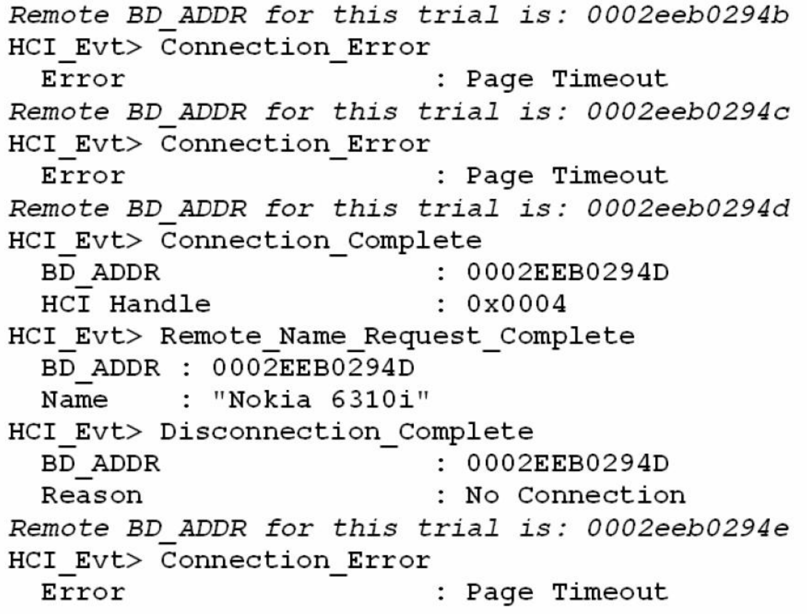
- CATC Scripting Language was used for creating our *Brute-Force BD_ADDR Scanning script*, which works in the following way:

  1) Set the scanning area.

  2) Set remote BD_ADDR for the next BD_ADDR trial.

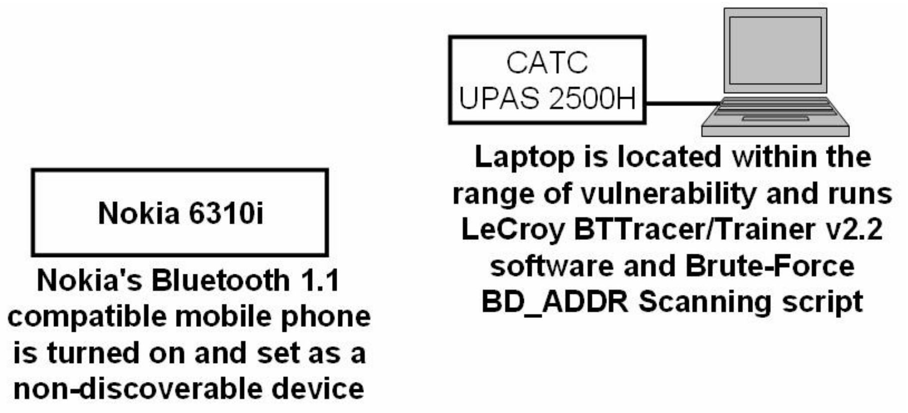
  3) Try to create basic ACL link between the protocol analyzer and a remote device by using the BD_ADDR value set in step 2. If connection attempt fails, go back to step 2. Otherwise Brute-Force BD_ADDR Scanning script has found a non-discoverable device! Perform remote name inquiry and disconnection with the target device. If there is more scanning left to do, go back to step 2.

Brute-Force BD_ADDR Scanning script



```
Remote BD_ADDR for this trial is: 0002eeb0294b
HCI_Evt> Connection_Error
  Error                  : Page Timeout
Remote BD_ADDR for this trial is: 0002eeb0294c
HCI_Evt> Connection_Error
  Error                  : Page Timeout
Remote BD_ADDR for this trial is: 0002eeb0294d
HCI_Evt> Connection_Complete
  BD_ADDR                : 0002EEB0294D
  HCI Handle             : 0x0004
HCI_Evt> Remote_Name_Request_Complete
  BD_ADDR : 0002EEB0294D
  Name    : "Nokia 6310i"
HCI_Evt> Disconnection_Complete
  BD_ADDR                : 0002EEB0294D
  Reason                 : No Connection
Remote BD_ADDR for this trial is: 0002eeb0294e
HCI_Evt> Connection_Error
  Error                  : Page Timeout
```

Brute-Force BD_ADDR Scanning script



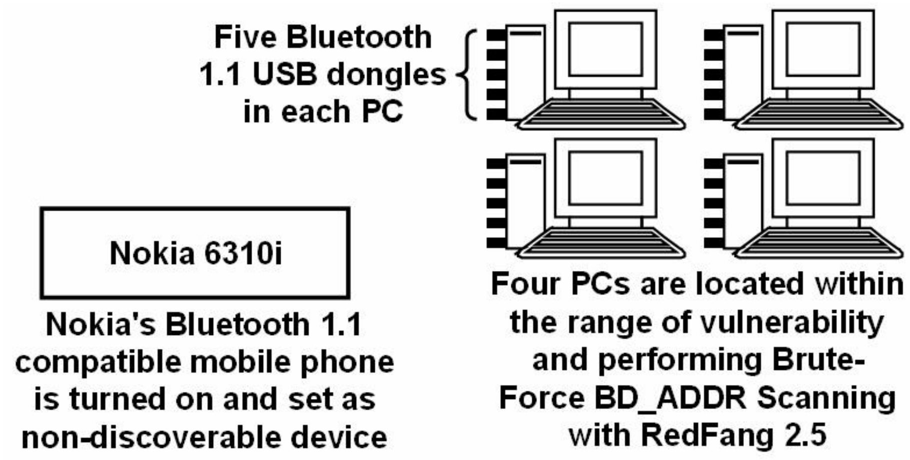
CATC UPAS 2500H

Laptop is located within the range of vulnerability and runs LeCroy BTTracer/Trainer v2.2 software and Brute-Force BD_ADDR Scanning script

Nokia 6310i

Nokia's Bluetooth 1.1 compatible mobile phone is turned on and set as a non-discoverable device

RedFang 2.5



Five Bluetooth 1.1 USB dongles in each PC

Nokia 6310i

Nokia's Bluetooth 1.1 compatible mobile phone is turned on and set as non-discoverable device

Four PCs are located within the range of vulnerability and performing Brute-Force BD_ADDR Scanning with RedFang 2.5

Brute-Force BD_ADDR Scanning script versus *RedFang 2.5*

- 24-bit address space gives 16777216 different possibilities and an attacker needs an average of 8388608 BD_ADDR guesses to discover the target device that is in the range of vulnerability:
  - If, for example, 25 compact size LeCroy Merlin II protocol analyzers are used for Brute-Force BD_ADDR Scanning attack with our *Brute-Force BD_ADDR Scanning script*, it takes an average of 20.3 days
  - For comparison, *RedFang 2.5* needs as much as 100 concurrent Bluetooth USB dongles to achieve the same result

New attacks against Bluetooth security

- We call our new attacks against Bluetooth security as:
  - *BTKeylogging* attack:
    - Extends On-Line PIN Cracking attack
    - If an attacker uses On-Line PIN Cracking attack to discover the fixed PIN code of the target Bluetooth keyboard, he/she can use the keyboard as a keylogger by intercepting all packets (i.e. all keypresses) sent via air and decrypting them!
  - *BTVoiceBugging* attack:
    - Extends On-Line PIN Cracking attack
    - When the fixed PIN code of the target device is discovered via On-Line PIN Cracking attack, it is possible to open two-way realtime SCO/eSCO link with the target device => It means that, for example, Bluetooth headset can be used as a bugging device!

New attacks against Bluetooth security

- *BTKeylogging* attack requires that:
  - the target keyboard has a fixed PIN code and its BD_ADDR is known by an attacker
  - an attacker must witness the initial pairing process between the target keyboard and the target computer => An attacker intercepts IN_RAND, LK_RAND, AU_RAND, SRES and EN_RAND => After that all intercepted information can be decrypted!
- *BTVoiceBugging* attack requires that:
  - the target device has a fixed PIN code and support for SCO/eSCO links

Countermeasures

- *Increasing user knowledge of security issues*
- *Using private or silent security level, switching Bluetooth off completely when it is not used, or switching device's power off when it is not used*
- *Purchasing only devices that have long PIN codes*
- *Automatic power-off capability or sleep mode if no successful connection attempt is made within some predestined time*
- *Requiring an additional Bluetooth-independent authentication always prior to access of a sensitive information or service*
- *Using RF signatures*
- *Careful selection of place when two devices meet for the first time and generate initialization keys*
- *The latest firmware/software update to vulnerable Bluetooth devices*
- *PIN code changing without sending the new PIN code via Bluetooth link*
- *Switching off all unnecessary SCO/eSCO links*
- *Requiring an additional Bluetooth-independent authentication prior every SCO/eSCO link establishment*

Conclusions

- Several attacks, for example, *On-Line PIN Cracking*, *BTKeylogging*, and *BTVoiceBugging*, are possible because many different kinds of Bluetooth devices, such as headsets and keyboards, have very short, often only four digits long fixed PIN codes => *We strongly recommend that 16 case-sensitive alphanumerical characters long PIN codes should always be used when possible*
- Bluetooth security has remained almost unchanged since the first Bluetooth 1.0 specification released 1999 => Based on our new enhanced security analysis tool implementations and the new attacks, security improvements are very welcome!
- Bluetooth device manufacturers should also take security issues more seriously!

ANY QUESTIONS?

?