Finnish Data Processing Week 2005 (FDPW'05), 17.-19.5.2005

Bluetooth network vulnerability to Disclosure, Integrity and Denial-of-Service attacks

MSc Keijo Haataja
Senior assistant
Department of CS
University of Kuopio
Finland

References

- My Bluetooth research and teaching
- Keijo Haataja, *Bluetooth security threats and possible countermeasures*, Proceedings of the Annual Finnish Data Processing Week at the University of Petrozavodsk (FDPW'2004), Advances in Methods of Modern Information Technology, vol. 6, Petrozavodsk 2005.
- Bluetooth specifications 1.0/1.1/1.2/2.0+EDR. http://www.bluetooth.org
- Robert Morrow, *Bluetooth: Operation and use*, Book, New York, McGraw-Hill, cop. 2002.
- Digital Media Europe, *News: Bluetooth chipset market to double to 146m units year-on-year - report*. Newscopy, 2004. http://www.dmeurope.com/default.asp?ArticleID=4333
- In-Stat/MDR, *Bluetooth 2004: Poised for the Mainstream*. Market Research Report, 2004. http://www.instat.com/r/nrep/2004/IN0401211MI.htm
- Bluetooth SIG, *The Official Bluetooth Membership Site - About the SIG*. Homepage, 2005. https://www.bluetooth.org/foundry/sitecontent/document/About_the_SIG
- LeCroy - Protocol Solutions Group, *CATC's Universal Protocol Analyzer System (UPAS) 2500H*. Homepage, 2005. http://www.catc.com/products/upas.html
- LeCroy - Protocol Solutions Group, *CATC's BTTracer/Trainer*. Homepage, 2005. http://www.catc.com/products/bttracer_trainer.html
- Nokia, *Nokia Wireless Headset HDW-2*. Homepage, 2005. http://www.nokia.com/nokia/0,,4238,00.html
- Humphrey Cheung, *Tom's Networking - How To: Building a BlueSniper Rifle - Part 1*. Homepage, 2005. http://www.tomsnetworking.com/Sections-article106.php
- Flexilis, Inc., *Flexilis, Inc. - Wireless Research and Development*. Homepage, 2005. http://www.flexilis.com
- Defcon, *Defcon - the largest underground hacking event in the world*. Homepage, 2005. http://www.defcon.org
- Ollie Whitehouse, *@Stake - Where Security & Business Intersect*. Research report, CanSecWest/core04, Vancouver, 2004. http://cansecwest.com/csw04/csw04-Whitehouse.pdf
- LeCroy - Protocol Solutions Group, *CATC's Merlin II*. Homepage, 2005. http://www.catc.com/products/MerlinII.html
- Adam Laurie, Ben Laurie, *The Bunker - Serious flaws in Bluetooth security lead to disclosure of personal data*. Homepage, 2004. http://www.thebunker.net/security/bluetooth.htm
- BABT - Certification, *IMEI Allocation*. Homepage, 2005. http://www.babt.com/gsm-imei-number-allocation.asp
- Martin Herfurt, *Detecting and Attacking bluetooth-enabled Cellphones at the Hannover Fairground*. Research report, CeBIT 2004, March 30, 2004. http://trifinite.org/Downloads/BlueSnarf_CeBIT2004.pdf

- A. Levi, E. Cetintas, M. Aydos, C. K. Koc, and M. U. Caglayan, *Relay Attacks on Bluetooth Authentication and Solutions*. Computer and Information Sciences - ISCIS 2004, 19th International Symposium, Kemer-Antalya, Turkey, 2004. http://islab.oregonstate.edu/koc/papers/c32relay.pdf
- Sourceforge, Project info - mycrypt. Homepage, 2005. http://sourceforge.net/projects/mcrypt
- SecuriTeam, *RedFang, Bluetooth Discovery Tool by Ollie Whitehouse*. Homepage, 2005. http://www.securiteam.com/tools/5JP0I1FAAE.html
- The Shmoo Group, *BlueSniff - Proof of Concept Bluetooth Wardriver*. Homepage, 2005. http://bluesniff.shmoo.com
- LeCroy - Protocol Solutions Group, *CATC Scripting Language Reference Manual for CATC Bluetooth Analyzers*. Homepage, 2005. http://www.catc.com/support/docs/pdf/BTCSLManual121.pdf
- IEEE Registration Authority, *IEEE OUI and Company_id Assignments*. Homepage, 2005. http://standards.ieee.org/regauth/oui/oui.txt
- BlueZ Project, *BlueZ - Official Linux Bluetooth protocol stack*. Homepage, 2005. http://www.bluez.org
- Nokia, *Nokia.com - Nokia on the web*. Homepage, 2005. http://www.nokia.com
- Motorola, *Motorola.com - Morotola on the web*. Homepage, 2005. http://www.motorola.com
- Trifinite.org - The home of the trifinite.group, BlueBug. Homepage, 2004. http://trifinite.org/trifinite_stuff_bluebug.html
- Andreas Oberritter - Saftware homepage, *btxml - mobile phone backup tool using Bluetooth*. Homepage, 2003. http://www.saftware.de
- Trifinite.org - The home of the trifinite.group, *Blooover*. Homepage, 2004. http://trifinite.org/trifinite_stuff_blooover.html
- Bluejack Q, *Mobile Phone Bluejacking*. Homepage, 2005. http://www.bluejackq.com
- Benuui.Net - the harmony of mobile development, *Bluetooth (JABWT) Browser MIDlet*. Homepage, 2003. http://www.benhui.net/bluetooth/btbrowser.html
- Pentest security assurance, *Pentest Downloads - BTScanner*. Homepage, 2005. http://www.pentest.co.uk/cgi-bin/viewcat.cgi?cat=downloads&section=01_bluetooth
- BTDSD, *Bluetooth Device Security Database*. Homepage, 2005. http://www.betaversion.net/btdsd

- Trifinite.org - The home of the trifinite.group, *BluePrinting*. Homepage, 2005. http://trifinite.org/trifinite_stuff_blueprinting.html
- Martin Herfurt, Collin Mulliner, *BluePrinting - Remote Device Identification based on Bluetooth Fingerprinting Techniques*. White paper, 2004. http://trifinite.org/Downloads/Blueprinting.pdf
- Antti Kotanen, Marko Hännikäinen, Helena Leppäkoski, Timo Hämäläinen, *Experiments on Local Positioning with Bluetooth*. International Conference on Information Technology: Coding and Computing (ITCC 2003), The Orleans, Las Vegas, Nevada, USA, April 28-30, 2003, pp. 297-303.
- TDK Systems, *BlueAlert*. Homepage, 2005. http://www.tdksystems.com/software/apps/content.asp?id=4
- Nobodaddy, BlueFish - Bluetooth Surveillance System. Homepage, 2005. http://www.nobodaddy.org/portfolio/bluefish.htm
- Andreas Steinhauser, Daniel Dorau, Collin Mulliner, *The Bluetooth Location Tracker Project*. Homepage, 2004. http://www.betaversion.net/blt
- Daily Wireless, Bluetooth Viruses. Newscopy, February 2005. http://www.dailywireless.org/modules.php?name=News&file=article&sid=3626
- F-Secure Corporation, F-Secure Virus Descriptions: Cabir. Homepage, 2004. http://www.f-secure.com/v-descs/cabir.shtml
- F-Secure Corporation, *F-Secure Virus Descriptions: Bagle.Z*. Homepage, 2004. http://www.f-secure.com/v-descs/bagle_z.shtml
- F-Secure Corporation, *F-Secure Virus Descriptions: Skulls.D*. Homepage, 2005. http://www.f-secure.com/v-descs/skulls_d.shtml
- F-Secure Corporation, *F-Secure Virus Descriptions: Lasco.A*. Homepage, 2005. http://www.f-secure.com/v-descs/lasco_a.shtml
- Marcos Velasco, *Marcos Velasco Security*. Homepage, 2005. http://www.velasco.com.br
- Trifinite.org - The home of the trifinite.group, *HeloMoto*. Homepage, 2004. http://trifinite.org/trifinite_stuff_helomoto.html
- Trifinite.org - The home of the trifinite.group, *BlueSmack*. Homepage, 2004. http://trifinite.org/trifinite_stuff_bluesmack.html
- Collin R. Mulliner, *BlueSpam*. Homepage, 2005. http://www.mulliner.org/palm/bluespam.php

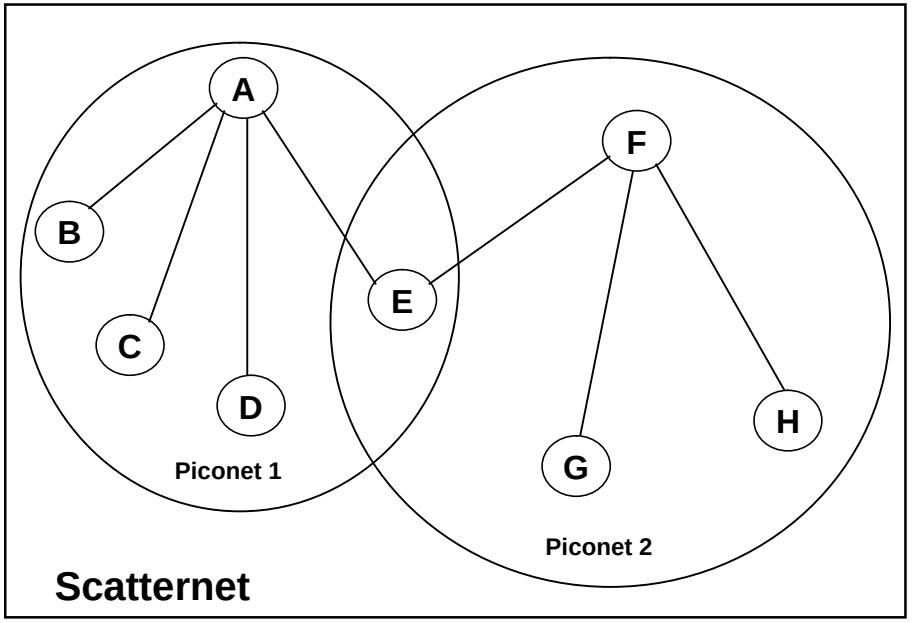
Contents

- Overview on Bluetooth technology and Bluetooth security
- Well known attacks against Bluetooth security and countermeasures
- Less known attacks against Bluetooth security and countermeasures
- Some experimental environments of attacks against Bluetooth security
- Conclusion

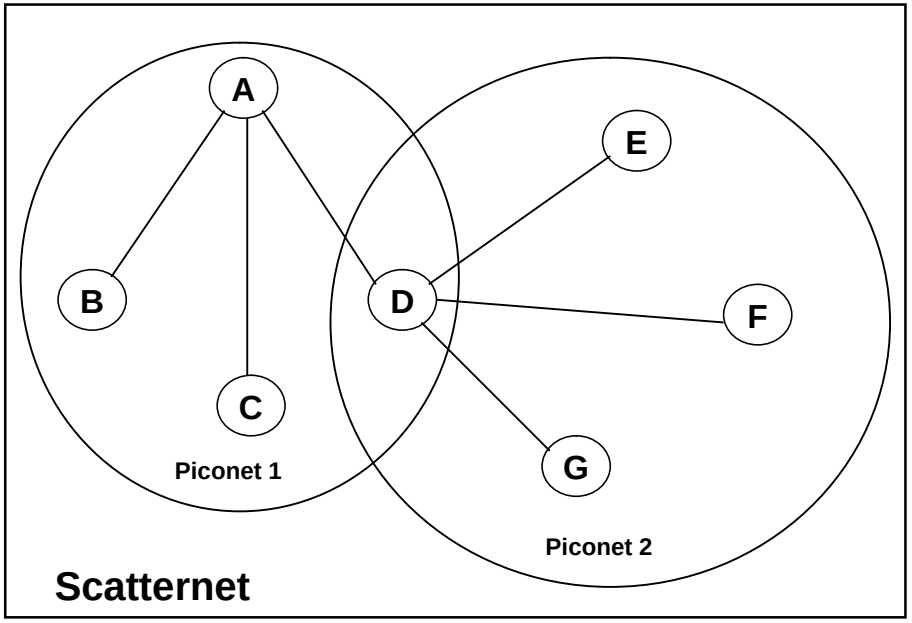
Overview on Bluetooth technology

- 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)



Security threats

- Threats in distributed networks can be roughly divided into three categories:
  - **Disclosure threat**: Leakage of information from the target system to an eavesdropper that doesn't have authorization to access the information.
  - **Integrity threat**: Deliberate alteration of information in an attempt to mislead the recipient.
  - **DoS (Denial of Service) threat**: Blocking of access to a service, making it either unavailable or severely limiting its availability to an autorized user.

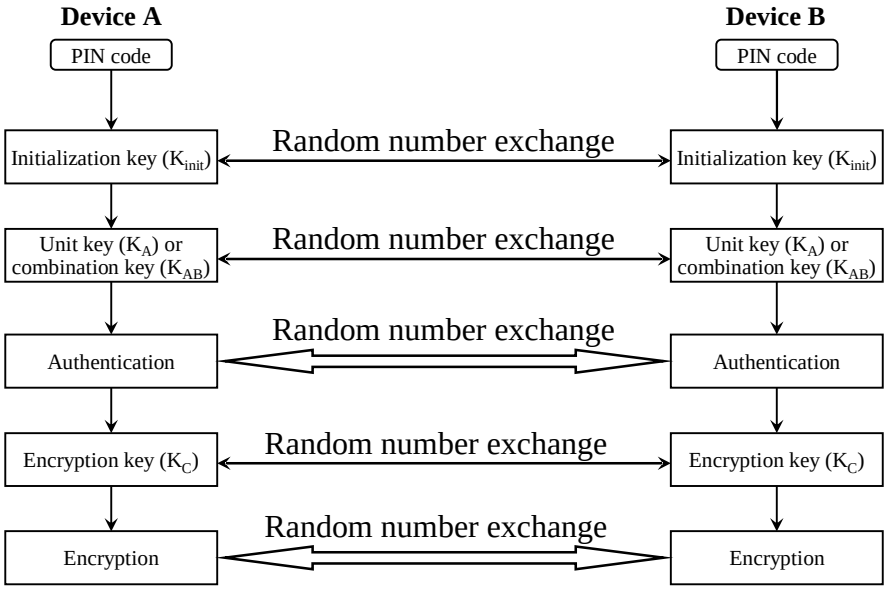
Overview on Bluetooth security

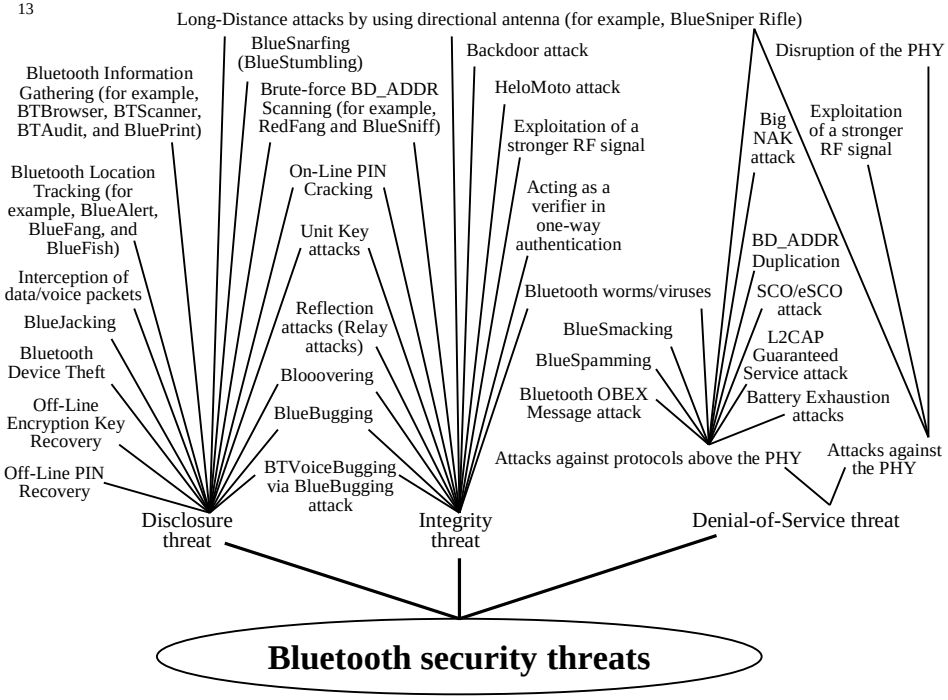
- Security within Bluetooth itself covers three major areas: **Authentication, authorization** and **encryption**
- The process of *authentication* proves the identity of one piconet member to another => The results of authentication are used for determining client's *authorization* to access various services on a server
- The process of *encryption* is used to encode the information being exchanged between devices such that eavesdroppers (even other members of the same piconet) cannot read its contents
- These three security processes are implemented within several layers of the Bluetooth protocol stack, so security is often termed as a cross-layer function

Security levels & modes

- Security begins when a user decides how a device will implement its discovery and connectability options. Different combinations of these capabilities can be divided into three general categories (*security levels*):
  - **Silent**: The device will never accept any connections. It simply monitors Bluetooth traffic.
  - **Private**: The device cannot be discovered. Connections will be accepted if the device's BD_ADDR (Bluetooth Device Address) is known by the prospective master.
  - **Public**: The device can be both discovered and connected to.
- A device can implement three different *security modes*:
  1. **Nonsecure**: A device will not initiate any security measures, so communication takes place without authentication or encryption.
  2. **Service-level enforced security**: Two devices can establish an ACL link in a nonsecure manner. Security procedures are initiated when a L2CAP (Logical Link Control and Adaptation Protocol) channel request is made.
  3. **Link-level enforced security**: Security procedures are initiated when the ACL link is being established.

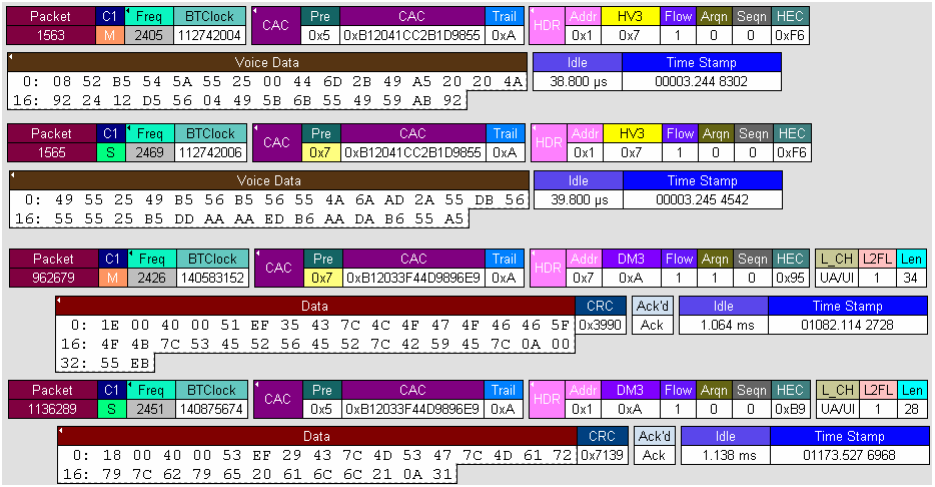
Summary of Bluetooth security operations





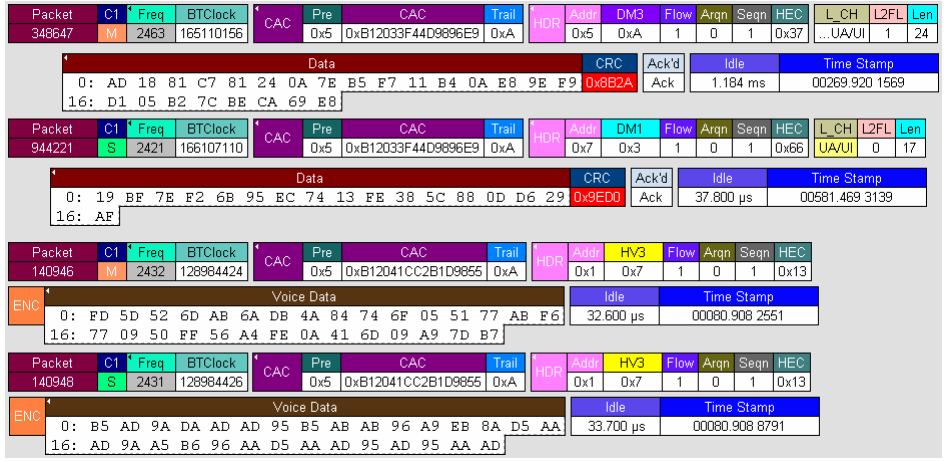
Some equipment of our Bluetooth laboratory

Interception of packets (unencrypted link)



An example of packet interception with LeCroy's Bluetooth protocol analyzer when encryption is not used.

Interception of packets (encrypted link)



An example of packet interception with LeCroy's Bluetooth protocol analyzer when 128-bit encryption is used.

```
redfang - the bluetooth hunter ver 2.5
(c)2003 @stake Inc
author:   Ollie Whitehouse <ollie@atstake.com>
enhanced: threads by Simon Halsall <s.halsall@eris.qinetiq.com>
enhanced: device info discovery by Stephen Kapp <skapp@atstake.com>
Opening logfile fangscan.txt.
Scanning 500 address(es)
Address range 00:02:ee:00:00:00 -> 00:02:ee:00:01:f3
Using 5 threads with approx 100 addresses each
Done[dev 1][total 0] - 00:02:ee:00:00:64
Done[dev 0][total 1] - 00:02:ee:00:00:00
Done[dev 3][total 2] - 00:02:ee:00:01:2c
Done[dev 2][total 2] - 00:02:ee:00:00:c8
Done[dev 4][total 4] - 00:02:ee:00:01:90
Done[dev 0][total 5] - 00:02:ee:00:00:01
Done[dev 1][total 5] - 00:02:ee:00:00:65
Done[dev 3][total 7] - 00:02:ee:00:01:2d
Done[dev 2][total 8] - 00:02:ee:00:00:c9
Done[dev 4][total 9] - 00:02:ee:00:01:91
```

An example of Brute-Force BD_ADDR Scanning attack with Ollie Whitehouse's RedFang 2.5.

An example of a successful Brute-Force BD_ADDR Scanning attack with Ollie Whitehouse's RedFang 2.5

```
Found: Nokia 6310i [00:02:ee:b0:29:4d]
Getting Device Information.. Connected.
        LMP Version: 1.1 (0x1) LMP Subversion: 0x23b
        Manufacturer: Nokia Mobile Phones (1)
        Features: 0xbf 0x28 0x21 0x00

                <3-slot packets>
                <5-slot packets>
                <encryption>
                <slot offset>
                <timing accuracy>
                <role switch>
                <sniff mode>
                <SCO link>
                <HV3 packets>
                <CVSD>
```


BlueBugging

```
<?xml version="1.0" encoding="UTF-8"?>
<phone btaddr="00:02:EE:B0:29:4D" name="Nokia 6310i">
        <manufacturer>Nokia</manufacturer>
        <model>Nokia 6310i</model>
        <revision>V 5.50    03-03-03 NPL-1 (c) NMP.  </revision>
        <imei>351453208359469</imei>
        <phonebook name="ME" size="500">
                <contact>
                        <name>Test contact number</name>
                        <number>+358501234567</number>
                </contact>
                <contact>
                        <name>Another contact number</name>
                        <number>+358447654321</number>
                </contact>
                <contact>
                        <name>Yet another number</name>
                        <number>+358112233445</number>
                </contact>
        </phonebook>
        <msgstorage name="ME">
                <message>"STO UNSENT","", This is a test message for btxml program..</message>
                <message>"STO UNSENT","", This is another test message...</message>
        </msgstorage>
        <msgstorage name="SM">
        </msgstorage>
</phone>
```

An example of a successful BlueBugging attack with (slightly modified) Andreas Oberritter's btxml (Andreas Oberritter - Saftware homepage, *btxml - mobile phone backup tool using Bluetooth*. Homepage, 2003. http://www.saftware.de). BlueBugging attack was repeated 50 times and an average time required for one successful attack (when the target mobile phone had three contact numbers and two text messages stored) was about 10.7 seconds.

Off-Line PIN Recovery

PIN code length (bytes):	An average time required (PIN code contains only digits):	An average time required (PIN code contains case-sensitive alphanumerical characters):
1	≈ 62.5 microseconds	≈ 1.6 milliseconds
2	≈ 0.6 milliseconds	≈ 0.4 seconds
3	≈ 6.3 milliseconds	≈ 1.7 minutes
4	≈ 62.5 milliseconds	≈ 7.5 hours
5	≈ 0.6 seconds	≈ 80.0 days
6	≈ 6.3 seconds	≈ 55.8 years
7	≈ 1.0 minutes	≈ 14.3 thousand years
8	≈ 10.4 minutes	≈ 3.7 million years
9	≈ 1.7 hours	≈ 0.9 billion years
10	≈ 17.4 hours	≈ 0.2 trillion years
11	≈ 7.2 days	≈ 6.1×10^{13} years
12	≈ 72.3 days	≈ 1.6×10^{16} years
13	≈ 2.0 years	≈ 4.0×10^{18} years
14	≈ 19.8 years	≈ 1.0×10^{21} years
15	≈ 198.2 years	≈ 2.6×10^{23} years
16	≈ 1981.9 years	≈ 6.7×10^{25} years

An average Off-Line PIN Recovery times for different PIN code lengths (let us assume that an attacker can perform an average of 80000 crack cycles per second). As described in "Ollie Whitehouse, *@Stake - Where Security & Business Intersect*. Research report, CanSecWest/core04, Vancouver, 2004. http://cansecwest.com/csw04/csw04-Whitehouse.pdf", by using a 850 MHz Pentium III with libmcrypt, an attacker can perform an average of 80000 crack cycles per second.

Long-Distance Attacks

- Powerful WLAN (Wireless Local Area Network) directional antennas will increase the attacking range considerably
- Requires a special long-distance attacking tool to be built
- One very good example of long-distance attacking tools is the BlueSniper Rifle (Humphrey Cheung, *Tom's Networking - How To: Building a BlueSniper Rifle - Part 1*. Homepage, 2005. http://www.tomsnetworking.com/Sections-article106.php):
  - A rifle stock, powerful WLAN directional antenna, and a small Bluetooth compatible computer
  - Powerful enough to detect devices through building walls
  - Attacking can be done over a mile away from the targets

Bluetooth Location Tracking

```
18/03/2005 :10:54,Nokia 6310i{00.02.EE.B0.29.4D},Out of range
18/03/2005 :10:54,Nokia 6230{00.E0.03.11.93.2B},Out of range
18/03/2005 :10:56,Nokia 6310i{00.02.EE.B0.29.4D},Discovered
18/03/2005 :10:56,Nokia 6230{00.E0.03.11.93.2B},Discovered
18/03/2005 :10:58,Nokia 6310i{00.02.EE.B0.29.4D},Out of range
18/03/2005 :10:59,Nokia HDW-2{00.03.89.35.44.6F},Discovered
18/03/2005 :10:59,BlueZ (0){00.A0.96.1F.02.2D},Discovered
18/03/2005 :11:00,Nokia HDW-2{00.03.89.35.44.6F},Out of range
18/03/2005 :11:00,BlueZ (0){00.A0.96.1F.02.2D},Out of range
```

An example of BlueAlert's (TDK Systems, *BlueAlert*. Homepage, 2005. http://www.tdksystems.com/software/apps/content.asp?id=4) logfile. BlueAlert is a tool for notifying Bluetooth users in advance when other Bluetooth devices go in and out of the range. It works only when the BD_ADDR of the target device is known. The source codes of BlueAlert are not released (only binaries). It only works with TDK's Bluetooth devices and runs on Windows.

BTVoiceBugging via BlueBugging attack

- This attack extends BlueBugging attack
- An attacker can use a vulnerable Bluetooth mobile phone as a bugging device by initiating a phone call from target device to any number that has voice recording capabilities (for example, answering machine or voicemail) => It means that an attacker can secretly record sensitive conversations and use them, for example, blackmailing or industrial spying purposes

Countermeasures

- Encrypting data/voice, and encrypting all sensitive material within the device
- Using private/silent security level, switching Bluetooth off completely when it is not used, or switching device's power off when it is not used
- Using only long PIN codes (16 case-sensitive alphanumerical characters), or purchasing only devices that have long PIN codes (if fixed PIN code must be used)
- Increasing user knowledge of security issues
- Minimization of transmit powers
- Careful selection of place when two devices meet for the first time and generate initialization keys
- Using additional security at software level, and an additional password to physically protect Bluetooth devices
- Requiring reauthentication always prior to access of a sensitive information/service
- Safe storage for the Bluetooth devices
- Automatic power off capability

Countermeasures

- Using RF signatures
- PIN code changing should always be possible without sending the new PIN code via Bluetooth link
- Only devices that have restricted resources should use a unit key
- Updating latest firmware/software to vulnerable Bluetooth devices
- Two-way authentication should always be required
- Watching sudden increase of transmit powers
- Keeping a list of suspicious devices
- A user should never install any unknown software
- A user should use antivirus/firewall software when possible
- Using a portable Bluetooth device to find the area where the bug captures the channel
- Switching off all unnecessary SCO/eSCO links
- Requiring reauthentication prior every SCO/eSCO link establishment
- Requiring reauthentication for every L2CAP request

Conclusion

- Many of the attacks (for example, Reflection attacks and Interception of packets) are possible because the encryption is not used by default in many different kinds of Bluetooth devices
- I strongly recommend that factory made Bluetooth settings should always enable encryption by default, because many users do not know about its existence or do not know how to set it up successfully
- Other possibility is to set Bluetooth encryption as mandatory. This of course requires minor changes to the Bluetooth specification, and would mean that older Bluetooth devices must also use encryption or communication with the new devices is not possible. On the other hand, if backward compatibility with the old Bluetooth devices must be guaranteed, then mandatory encryption is not possible.

Conclusion

- Many of the attacks (for example, On-Line PIN Cracking and Off-Line PIN Recovery) are possible because many different kinds of Bluetooth devices have very short fixed PIN codes (for example, only four digits long) which do not contain any case-sensitive alphanumerical characters
- I strongly recommend that 16 case-sensitive alphanumerical characters long PIN codes should always be used when possible
- Dozens of the attacks are also possible because many different kinds of Bluetooth devices (for example, headsets, keyboards and mice) have *public security level* as a fixed factory setting. It means that, these devices are always discoverable. This makes attacker's work much easier, because he/she can skip the most time consuming part of the attack (Brute-Force BD_ADDR Scanning attack or BD_ADDR discovery via Bluetooth protocol analyzer) and get directly down to business.

Conclusion

- I strongly recommend that the security level of Bluetooth device should never be public as default or as fixed factory setting
- A user should have at least a possibility to change the factory setting of security level somehow (for example, by pressing a particular button several seconds if a device lacks actual UI)
- Other possibility is to set *private security level* as mandatory and print the BD_ADDR of the device in every manual. This also requires minor changes to the Bluetooth specification if Bluetooth SIG wants to force device manufacturers to use it. On the other hand, some public Bluetooth services (for example, Bluetooth guidance services or Bluetooth Internet coffee bar services) are not possible if all devices must be non-discoverable.

Conclusion

- Bluetooth security has remained almost unchanged since the first Bluetooth specification released 1999 (over six years now!)
- Next major security improvements are roadmapped to two upcoming Bluetooth specifications, which will probably be released in fall 2005 and in fall 2006 by Bluetooth SIG
- Based on the attacks described in this paper, security improvements are **very** welcome
- Bluetooth device manufacturers and users should also take security issues much more seriously

THANK YOU!

ANY QUESTIONS?