Detailed descriptions of new proof-of-concept Bluetooth security analysis tools and new security attacks

Keijo M.J. Haataja

Report B/2005/1

UNIVERSITY OF KUOPIO

Department of Computer Science

P.O.Box 1627, FIN-70211 Kuopio, FINLAND

Detailed descriptions of new proof-of-concept Bluetooth security analysis tools and new security attacks

Keijo M.J. Haataja
Department of Computer Science
University of Kuopio
P.O.Box 1627
FIN-70211 Kuopio, Finland
E-mail: haataja@cs.uku.fi

Abstract

This report describes the details of two new proof-of-concept Bluetooth security analysis tools and two new attacks against Bluetooth security. On-Line PIN Cracking script is a security analysis tool for on-line Bluetooth device PIN cracking. Brute-Force BD_ADDR Scanning script is a security analysis tool for brute-force discovery of the addresses of Bluetooth devices that want to be private. Scripts of both our security analysis tools exist and can be demonstrated to Bluetooth device manufacturers or press if required, but they will not be released in any public domain because due to their efficiency they can be very dangerous. Our new attacks, BTKeylogging and BTVoiceBugging, extend On-Line PIN Cracking attack.

1 Introduction

Section 2 describes our On-Line PIN Cracking script, which is as far as we know, the only security analysis tool for On-Line PIN Cracking so far. Section 3 describes our Brute-Force BD_ADDR Scanning script. BTKeylogging and BTVoiceBugging attacks are described in Sections 4 and 5 respectively. Finally, Section 6 concludes the report.

2 On-Line PIN Cracking script

The On-Line PIN Cracking is described in [1, 2]. We successfully performed a On-line PIN Cracking attack by using:

- CATC Protocol Analyzer System 2500H [3]: CATC Protocol Analyzer System 2500H is flexible and efficient integrated environment providing, for example, 512 MB of recording memory, Hi-Speed USB 2.0 Interface to host PC/laptop, upgradeable firmware/ BusEngine/Baseband, and support for plug-in modules.

- Bluetooth Analyzer and Test Generator Plug-In Module [3]: We used LeCroy Bluetooth 1.1 compatible radio unit as a plug-in module for the CATC Protocol Analyzer System 2500H.
- Nokia's Wireless Headset HDW-2 [4]: We used the Bluetooth 1.1 compatible Nokia HDW-2 as a victim device. It has a fixed 4-digit PIN code.
- LeCroy BTTracer/Trainer v2.2 software [3]: We installed a LeCroy BTTracer/Trainer v2.2 software to our laptop, which was connected to the CATC Protocol Analyzer System 2500H via a USB cable.
- On-Line PIN Cracking script [2]: CATC Scripting Language [5] was used to create our On-Line PIN Cracking script, which makes the On-Line PIN Cracking attack possible.

Figure 1 illustrates our On-Line PIN Cracking laboratory experiment. Our *On-Line PIN Cracking script*, an example of a successful On-Line PIN Cracking attack, and average On-Line PIN Cracking time calculations are described in [2].

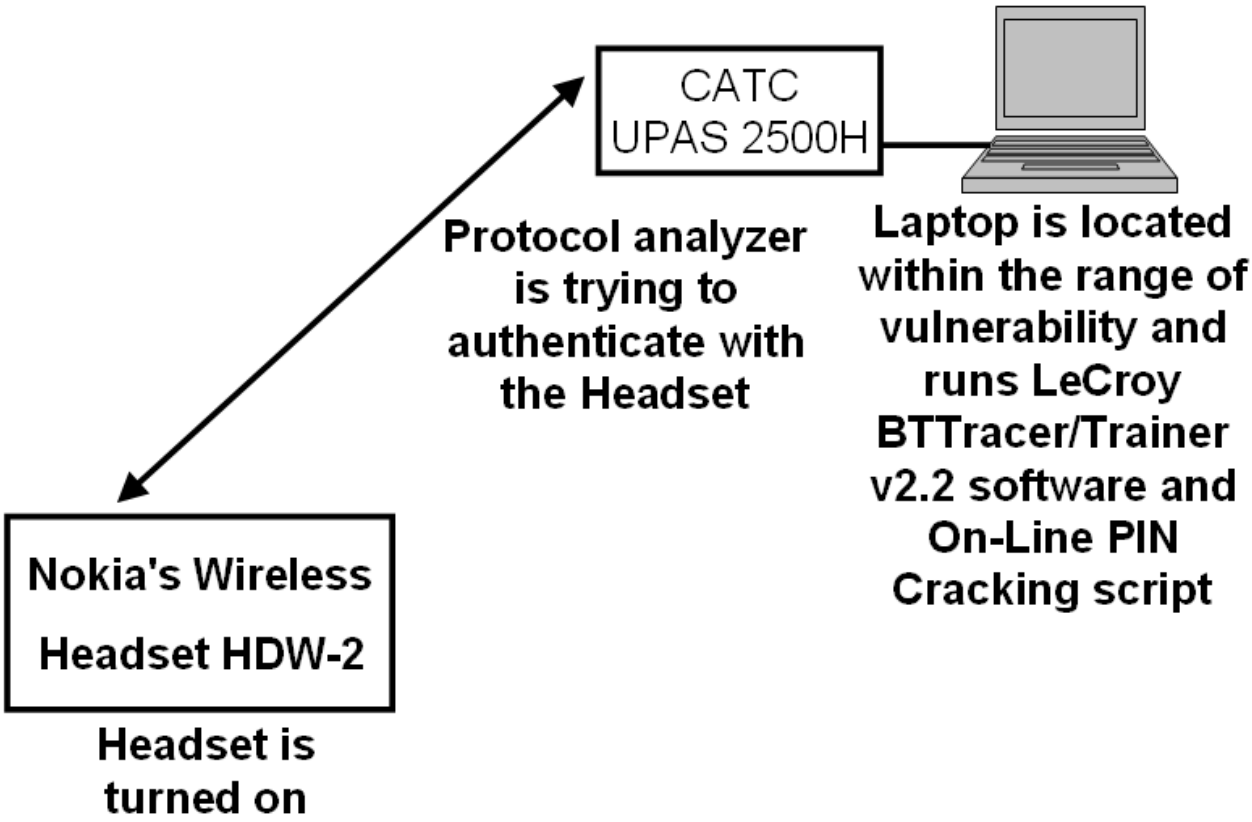

Figure 1: An example of the On-Line PIN Cracking laboratory experiment

3 Brute-Force BD_ADDR Scanning script

The Brute-Force BD_ADDR Scanning is described in [1, 2]. We successfully performed a Brute-Force BD_ADDR Scanning attack by using:

- The CATC Protocol Analyzer System 2500H.
- A Bluetooth Analyzer and Test Generator Plug-In Module: We used a LeCroy Bluetooth 1.1 compatible radio unit as a plug-in module for the CATC Protocol Analyzer System 2500H.
- A Nokia 6310i [6] mobile phone: We used an unmodified Bluetooth 1.1 compatible Nokia 6310i mobile phone as a victim device.
- The LeCroy BTTracer/Trainer v2.2 software.
- A Brute-Force BD_ADDR Scanning script: The CATC Scripting Language was used to create our Brute-Force BD_ADDR Scanning script, which makes the Brute-Force BD_ADDR Scanning attack possible.

Figure 2 illustrates our Brute-Force BD_ADDR Scanning laboratory experiment. Our *Brute-Force BD_ADDR Scanning script*, an example of a successful Brute-Force BD_ADDR Scanning attack, average Brute-Force BD_ADDR Scanning time calculations, and comparison to another Brute-Force BD_ADDR Scanning security analysis tool (RedFang 2.5) are described in [2].

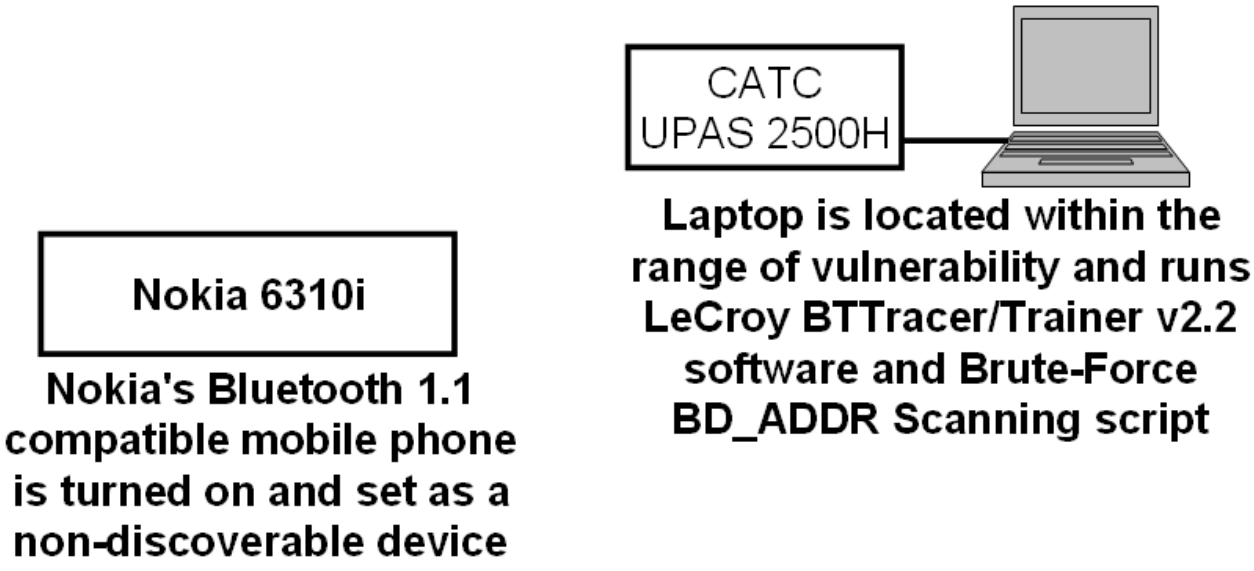

Figure 2: An example of the Brute-Force BD_ADDR Scanning laboratory experiment

4 BTKeylogging attack

The BTKeylogging attack is described in [2]. We successfully performed a BTKeylogging attack by using:

- The CATC Protocol Analyzer System 2500H.
- A Bluetooth Analyzer and Test Generator Plug-In Module: We used a LeCroy Bluetooth 1.1 compatible radio unit as a plug-in module for the CATC Protocol Analyzer System 2500H.
- A Microsoft Bluetooth keyboard and a Microsoft Bluetooth USB Transciever [7]: We used Microsoft's Bluetooth 2.0 compatible keyboard and Microsoft's Bluetooth 2.0 compatible USB dongle in the victim device (PC).
- The LeCroy BTTracer/Trainer v2.2 software.
- An On-Line PIN Cracking script: We used an On-Line PIN Cracking script to discover the PIN code of the keyboard.

We used a protocol analyzer to intercept all required information (IN_RAND, LK_RAND, AU_RAND, SRES and EN_RAND) for the attack. After that we used a keyboard as a keylogger by intercepting all keypresses, and finally we successfully decrypted all intercepted information.

5 BTVoiceBugging attack

The BTVoiceBugging attack is described in [2]. We successfully performed a BTVoiceBugging attack by using:

- The CATC Protocol Analyzer System 2500H.
- A Bluetooth Analyzer and Test Generator Plug-In Module: We used a LeCroy Bluetooth 1.1 compatible radio unit as a plug-in module for the CATC Protocol Analyzer System 2500H.
- Nokia's Wireless Headset HDW-2: We used the Bluetooth 1.1 compatible Nokia HDW-2 as a victim device.
- The LeCroy BTTracer/Trainer v2.2 software.
- An On-Line PIN Cracking script: We used an On-Line PIN Cracking script to discover the PIN code of the headset.

We used a protocol analyzer to open a two-way realtime SCO connection with the headset, i.e. the headset was used as a bugging device. We also intercepted all voice packets for later use. Recorded voice packets can be exported to a WAV file and stored for later use.

6 Conclusion

This report described the details of two new proof-of-concept Bluetooth security analysis tools and two new attacks against Bluetooth security. The purpose of this report is to give some additional details for our research paper [2] about Bluetooth security analysis tools (On-Line PIN Cracking script and Brute-Force BD_ADDR Scanning script) and attacks (BTKeylogging attack and BTVoiceBugging attack).

References

[1] O. Whitehouse, *@Stake - Where Security & Business Intersect.* Research report, CanSecWest/core04, Vancouver, Canada, April 21-23, 2004. http://cansecwest.com/csw04/csw04-Whitehouse.pdf

[2] K. Haataja, *Two practical attacks against Bluetooth security using new enhanced implementations of security analysis tools.* Proceedings of the IASTED International Conference on Communication, Network and Information Security (CNIS 2005), Phoenix, Arizona, USA, November 14-16, 2005.

[3] LeCroy - Protocol Solutions Group, *LeCroy Bluetooth Protocol Analyzers.* Homepage, 2005. http://www.lecroy.com/tm/products/ProtocolAnalyzers/bluetooth.asp?menuid=60

[4] Nokia, *Nokia Wireless Headset HDW-2.* Homepage, 2005. http://www.nokia.com/nokia/0,,4238,00.html

[5] LeCroy - Protocol Solutions Group, *CATC Scripting Language Reference Manual for LeCroy Bluetooth Analyzers.* Homepage, 2005. http://www.catc.com/support/docs/pdf/BTCSLManual121.pdf

[6] Nokia, *Nokia 6310i Phone.* Homepage, 2005. http://www.nokia.com/cda7/0,1106,133,00.html

[7] Microsoft, *Microsoft Mouse and Keyboard Hardware - Optical Desktop Elite for Bluetooth.* Homepage, 2005. http://www.microsoft.com/hardware/mouseandkeyboard/ ProductDetails.aspx?pid=033&active_tab=overview