Bluesnarfing @ CeBIT 2004

Detecting and Attacking bluetooth-enabled Cellphones at the Hannover Fairground

Dipl.-Ing.(FH) Martin Herfurt
Salzburg Research Forschungsgesellschaft mbH, Austria
martin.herfurt@salzburgresearch.at

March 30, 2004

Abstract

A big shock went through the community when it became public, that some bluetooth-enabled handsets are disclosing personal information. The information posted on [1] introduces three basic ways to attack bluetooth-enabled devices. This report briefly describes the SNARF exploit for the recently discovered bluetooth security loophole that is not requiring any kind of preparation or prior manipulation of the devices.

1 Introduction

SNARF and bluesnarfing are words that have been spooking through the Internet during the last months. These words relate to a recently discovered security flaw in bluetooth-enabled devices. This report is about a field-trial that has evaluated this security loophole at the CeBIT 2004 in Hannover.

1.1 Bluetooth Security Issues

End of November 2003 Adam and Ben Laurie (A.L. Digital Ltd.) published a document [1] on the Internet stating that some bluetooth-enabled phones are having serious security flaws. These flaws allow attackers to connect to the device without permission (no pairing) and carry out a so-called SNARF attack.

In the beginning of February 2004, the fact that some bluetooth-enabled handsets are having security issues made it into many news-tickers around the globe. Most of the news-sites pretended that exploit-tools were available in the Internet. But even extensive research in the Internet did not bring up the location where these

tools were available.

As described in [1], the SNARF attack enables access to restricted portions of the device. SNARF is a word coming from computer-hacker jargon. To snarf something means "to grab a large document or file and use it without the author's permission"[2]. So it is possible to, for example read out the affected devices' phone books. These phone books contain numbers and associated names of persons that are either stored in the device phone-book, on the SIM card or in the lists of missed, received or dialed contacts. It is also possible to retrieve and send SMS messages from the affected phone or to initiate phone calls to any existing number (this feature is of special interest if you are the running a premium service number yourself ;-).
In theory, all supported AT-commands could be issued to the respective device, but according to statements of the manufacturers some of the commands are not permitted by means of this disallowed connection. But there would be no reason of preventing commands from a connection that the firmware discloses by accident.

1.2 CeBIT 2004

The CeBIT is one of the events, where people go that are into computers and new technologies. Compared to other groups this group of people tends to use their devices differently. It is more likely that these people are active bluetooth users. So at the CeBIT fairground optimal preconditions for the evaluation of these devices' security are given.

The CeBIT is Europe's biggest IT-exposition and takes place every year at the Hannover fairground in the north of Germany. As in the years 2002 and 2003, Salzburg Research together with the Salzburg University of Applied Sciences and Technologies had a booth at the CeBIT 2004 located in Hall 11. There, in the so-called future park, all research and education companies and institutes are located. Favorably, the Salzburg Research booth was located close to the public restrooms, where more people tend to pass by than at other places in this hall. At this location, an environment for the discovery and the attacking of bluetooth-enabled devices was set up.

2 The Bluesnarf Field Trial

The environment was build up by open-source software ran on a laptop computer.

2.1 The Environment Setup

The hardware used for this trial was a COMPAQ Evo N600c with two low-cost MSI bluetooth USB-dongles. The software used with this hardware was `linux-2.6.2`

together with Qualcomm's bluetooth stack implementation Bluez (`bluez-libs-2-.5`,`bluez-utils-2.4` and `bluez-sdp-1.5`). The actual application was implemented in PERL and C. For better data-mining capabilities, an enterprise-level SQL-DBMS (`postgresql-7.4.1`) has been used in order to store and access the collected device-information.

2.2 Collected Data Samples and Results

In total, 1269 different devices have been discovered in the period from March 18th to 21st March 2004 at the place described above. Due to the limited range of about ten meters, not all of the bluetooth-enabled devices at this place could have been detected. But still, the number of discovered devices is very high.

2.2.1 Discovered Device Vendors

Figure 1 shows a diagram that represents the distribution of manufacturers. The determination of the vendor is done by means of the bluetooth address. Similar to the hardware-address (MAC address) of Ethernet network interface cards, also the bluetooth address refers to the manufacturer of the bluetooth chip-set. Table 1 shows the vendor and the three first bytes of the bluetooth addresses that are associated with the respective vendor. Also a value expressing the distribution among the vendors is provided in this table.

The 70 percent of discovered Nokia handsets clearly represent Nokia's market-

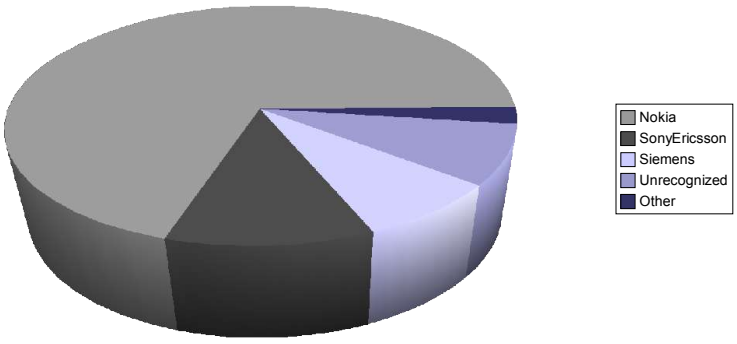

Figure 1: Device Vendor Distribution

leadership in Europe. Interestingly, many companies use the Nokia 6310i as a company phone. One possible reason for this could be the compatibility to the Nokia car-kits that have been installed over years in many company cars.

Vendor	Address-Bytes	Percentage
Nokia	00:02:EE , 00:60:57 , 00:E0:03	70
SonyEricsson	00:0A:D9	11.35
Siemens	00:01:E3	8.2
Unknown	miscellaneous	8.1
Other	miscellaneous	2.1

Table 1: Device Vendors

2.2.2 Discovered Models

It cannot be determined from the device's bluetooth address which model of the respective vendor this is. Therefore, the bluetooth name that on many devices defaults to the model number has been used to identify the model of the discovered device. The bluetooth name of the devices can be set by the user and is therefore not itself a reliable information to determine the model number. It is worth mentioning that many people use their full name as an identification for their device.

The tables 2, 3 and 4 show the numbers of models that could have been uniquely determined by their names. So, this graph is not totally correct, but gives a coarse idea on the vendor/model distribution.

The graph displayed in figure 2 supports the assumption that has been made before, that obviously many companies are using the Nokia 6310i phone for their employees.

The high popularity of the T610 phone is reflected by the diagram presented in

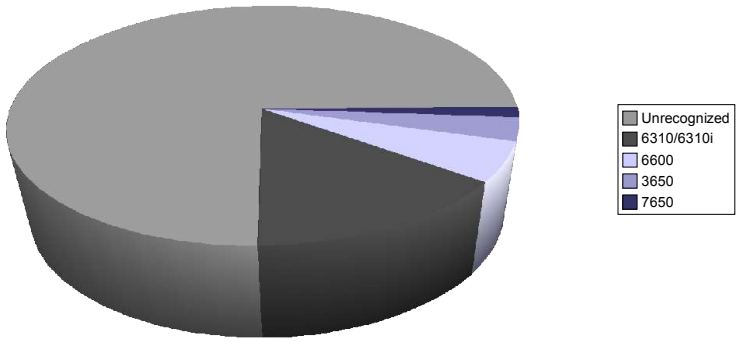

Figure 2: Nokia Model Distribution

figure 3. Also the current top-of-the-line model (the P900) has been discovered comparably often.

Device	Number	Percentage
Unrecognized	669	75.1
Nokia 6310/6310i	135	15.2
Nokia 6600	48	5.4
Nokia 3650	28	3.1
Nokia 7650	11	1.2

Table 2: Recognized Nokia Models

Characteristic for the German/European market was the relatively high presence

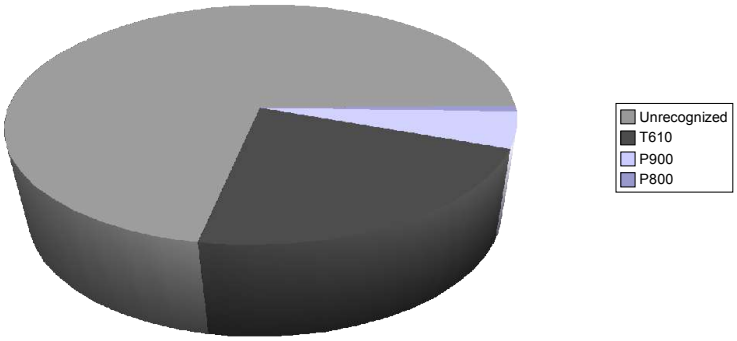

Figure 3: SonyEricsson Model Distribution

Device	Number	Percentage
Unrecognized	106	72.1
SonyEricsson T610	33	22.5
SonyEricsson P900	7	4.8
SonyEricsson P800	1	0.6

Table 3: Recognized SonyEricsson Models

of Siemens phones. At the moment, only the phones belonging to the 55 series and the new SX1 are supporting bluetooth.

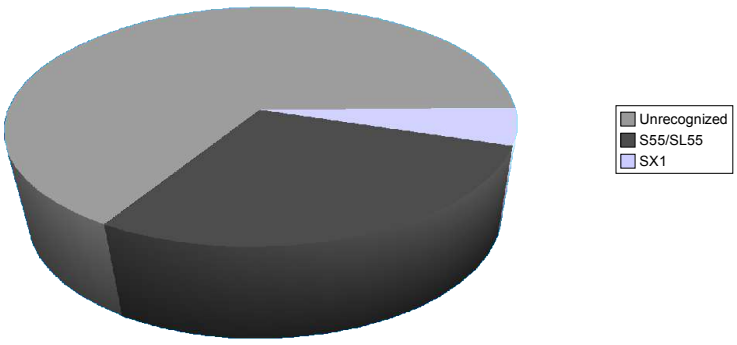

Figure 4: Siemens Model Distribution

Device	Number	Percentage
Unrecognized	69	66.3
Siemens S55/SL55	30	28.9
Siemens SX1	5	4.8

Table 4: Recognized Siemens Models

2.2.3 Discovered Vulnerable Devices

As written in [1], there are a number of devices that are vulnerable to the SNARF attack. According to this document there is the Ericsson phone T68/T68i, the SonyEricsson phones R520m, T610 and Z1010 and the Nokia phones 6310/6310i, 8910/8910i and 7650. Adam Laurie also provides information, whether the respective devices are attackable in invisible or visible mode, only. Since the setup used for this field trial did not use a brute-force approach (as presented by @stake) for detecting also invisible devices, this study only confirms the vulnerability of visible devices. Due to limited market take-up and the resulting low penetration-rate of some devices, the vulnerability of some of the listed devices cannot be confirmed by this study.

As displayed in figures 2 and 3, the two top-selling bluetooth-enabled models of SonyEricsson and Nokia are vulnerable to the SNARF attack.

Experiments with the SonyEricsson T610 showed that this model is generally not vulnerable to the SNARF attack. During an earlier presentation of the SNARF attack in February it happened that T610 phones with recent versions of the T610 firmware were disclosing personal information. Obviously, newer versions of the T610 firmware do allow SNARF attacks.

Nokia 6310/6310i As mentioned above, this study confirms that the Nokia 6310 and the more enhanced Nokia 6310i are very vulnerable to the SNARF attack. About 33 percent of all discovered devices of this type were disclosing personal phone book entries without requiring user-interaction. Since the snarf-process takes an average time of 30 seconds (from the discovery to the end of the attack), it is very likely that a lot more devices could have been read out. Too many people were just passing the location so that they left the bluetooth-covered area too early to be snarfed. Figure 5

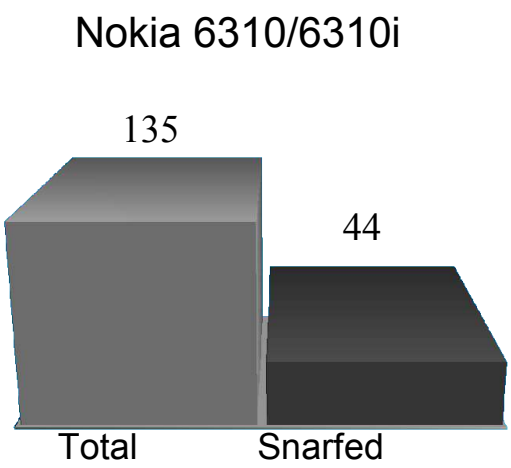

Figure 5: Snarfed Nokia Phones

displays the ratio of discovered and provenly vulnerable Nokia 6310/6310i devices. But as mentioned above, this could have been more.

SonyEricsson T610 Figure 6 shows the ratio of discovered and successfully attacked SonyEricsson T610 devices. As mentioned before, in future when the newer firmware is running on an increased number of T610-devices the success rate of the SNARF attack will also increase. In the CeBIT 2004 field trail only 6 percent of all discovered T610 devices could be read out.

Siemens phones As far as it has been observed in the CeBIT field trial, Siemens phones are not vulnerable to the SNARF attack. Bluetooth-enabled Siemens phones like the S55 merely seem to be rather paranoid. Every time a usual scan-request is received by these phones they cowardly ask for the user's confirmation. Actually, this behavior is quite annoying.

2.3 Other Experiences

In preparation for the trial-setup, the Ericsson T68i (which is also on the list of vulnerable devices) has been checked. It can be confirmed, that this phone is vulnerable

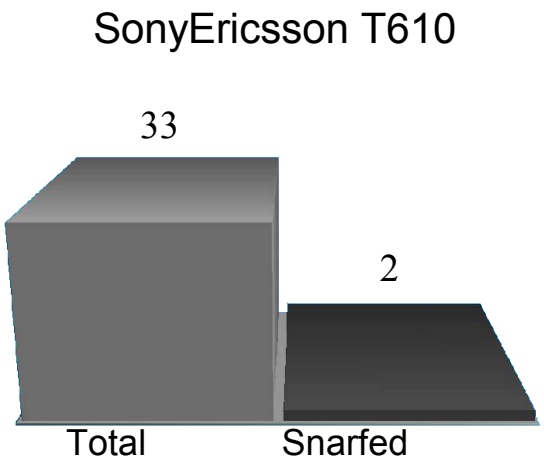

Figure 6: Snarfed SonyEricsson Phones

to the SNARF attack but switches into the hidden mode automatically (three minutes after activation of the bluetooth interface). In hidden mode this phone is not vulnerable (as mentioned in [1]).

3 Final Remarks

3.1 Proclaimer

The information gathered in this field trial will not be disclosed to anybody. Personal information that has been retrieved from vulnerable phones has been deleted. This study has been made for scientific demonstration purposes, only.

3.2 What has been done

The SNARF attack used at the CeBIT was intended to finish as fast as possible. That is why only the first 10 entries of each phone book were read out. About 50 numbers from each snarfed phone have been retrieved.

3.3 What could have been done

As mentioned in the introduction there could have been done a variety of different things with an unauthorized bluetooth connection to the phone. The following paragraphs give some ideas on the things this security flaw would also allow the attacker to do.

3.3.1 Sending a SMS

The only good way to get to know the number of the snarfed phone is to send an SMS from the attacked phone to another device. Depending on the manufacturer of the phone, SMS messages can either be provided in 7bit encoded ASCII-text and/or have to be provided as a SMS-PDU which is rather tricky to generate. For the creation of SMS-PDUs there is a tool called PDUSpy in the download section of `http://www.nobbi.com/`.

Nokia phones allow to issue text-mode and PDU-mode messages to the device, while SonyEricsson phones (and also Siemens phones) only accept PDU-encoded SMS messages. The sending of an SMS is not visible to the user. Usually, the issued SMS is not stored in the sent-box of the snarfed phone. In rare cases, the SMS settings of the snarfed phone are set to require a report that is generated at the receiving phone. In this case the sender that was not aware of having sent a message would receive a reception-report from the attacker's phone (which includes a phone number). By sending PDU encoded messages, it can be controlled by setting a flag whether a reception report is generated or not.

This method to get the victim's phone number is causing costs to the holder of the phone. That is why it has not been done in the CeBIT field-trial. But it works for sure (at least on Nokia devices).

It would also be possible to get the device's phone number by initiating a phone call to the number of a phone that is able to display the caller's number. However, this method would disclose the number of the dialed phone to the owner of the attacked phone, because every call initiation is writing an entry into the dialed contacts list (DC phone book).

3.3.2 Initiating a Phone Call

It is possible to initiate phone calls to virtually any other number. It would be very lucrative to initiate calls to a premium service number that is ran by the attacker. As mentioned before, dialed numbers are usually stored in the phone's calling lists and are also stored at the provider-site for billing purposes. Therefore, this kind of abuse is rather unlikely. It would also be very very easy to find out and sue the person being responsible for this premium service.

3.3.3 Writing a Phone Book Entry

As mentioned before, every phone call is writing an entry into the "dialed contacts" or DC phone book of the respective device. By writing a phone book entry into the DC phone book, the traces on the device that evidence that a call has been made can be replaced by any number. Since the operator also stores dialed numbers for billing purposes, this kind of obfuscation would only delay the process of finding

the responsible person.

Of course it is also possible to do some nasty phone book entries. Just imagine an entry that has 'Darling' as a name and the number of a person you dislike. This owner of the phone could then get into some trouble with his/her spouse ;)

In the CeBIT-trial no phone book entries have been done. Such entries would most likely overwrite existing ones.

3.4 Vendor Reaction

On news pages it has been stated that the respective vendors are admitting this security loophole. It has also been implied that there are no intentions to do anything against it, since it does not seriously damage the phone.

Asking representatives from the respective vendors at the CeBIT, I have been told that these problems have been solved in actual firmware-versions that can be upgraded for free. Whether this security flaw has been fixed in newer firmware versions cannot be confirmed.

4 Conclusions

It would be paranoid to imply, that it is no random incident but purposeful that the best-selling bluetooth phones of the market leaders SonyEricsson and Nokia can be easily be read out by attackers.
This test report is intended to point out this serious security flaw to bluetooth-users in order to make them act more careful in this point.

An @stake report [3] introduces some more things to consider with respect to bluetooth devices. For example, this report points out effective measures to protect devices from various attacks. Furthermore, the comparable harmless Bluejacking is another bluetooth activity that helps getting over boring times in airport terminals or other public places with a high bluetooth-device density.

5 Future Work

Ongoing experiments include a SNARF application on Java/J2ME phones. As a requirement for this, the respective phones would have to have the MIDP 2.0 API implemented together with the optionally provided Bluetooth-API. The only phone that has these features at the moment is the Nokia 6600.

6 Acknowledgments

I thank Matthias Zeitler and Peter Haber for drawing my attention to this topic, Collin R. Mulliner for providing useful information, Elfi Redtenbacher for lending me her vulnerable bluetooth enabled phone and Paul Malone and Guntram Geser for reading and correcting this report.

References

[1] Ben Laurie Adam Laurie. Serious flaws in bluetooth security lead to disclosure of personal data. Technical report, A.L. Digital Ltd., http://bluestumbler.org/, January 2004.

[2] Webopedia. What is snarf? - a word definition from the webopedia computer dictionary. Technical report, Webopedia, http://www.webopedia.com/TERM/S/snarf.html, January 2003.

[3] Ollie Whitehouse. War nibbling: Bluetooth insecurity. Research report, @stake, Inc., October 2003.