

Bluetooth Security Review, Part 2

Marek Bialoglwy 2005-05-26

In [part 1](#) of this article, we introduced Bluetooth and some of its security and privacy issues, including how it is detected and some implementation issues from various mobile phone vendors. Now in part 2 we look at Bluetooth viruses, several unpublished vulnerabilities in Symbian based phones, and then moves on to discuss "Blue tag" tracking, positioning, and privacy issues.

Bluetooth fauna

When the Cabir mobile worm started to attack mobile devices and used Bluetooth to spread, many people were caught by surprise. It first appeared as a proof-of-concept virus written by the A29 group, was provided to an anti-virus company, and then later appeared in the wild. The worm started spreading from infected mobile phones using the Bluetooth wireless capabilities to search for the next victim and infect it based. This infection was based on a vulnerability in the Bluetooth implementation of several Nokia and Sony Ericsson phones. The virus was not dangerous, however, as it only drained the phone's battery and it still required the user to accept installation of the file. However, it showed that it is possible to write mobiles viruses that spread via Bluetooth, which may encourage a number of virus writers to take the same approach. Future Bluetooth viruses may very well be much more damaging. A good example of the potential damage that can be caused first appeared in Japan in 2001, where the virus blocked the ability to call emergency numbers. Recent vulnerabilities in Java, discovered by famous Polish security researcher Adam Gowdiak, could also be used by mobile virus writers to break the Java mobile security model and get access to the phone's memory, affecting many things including changing the very way the phone works.

Increased popularity of mobile worms and viruses would certainly have an impact on the GSM operator as well. Blocking certain phone numbers and making customers frustrated with any inability to make phone calls on infected handsets would direct cause a lost of revenue. The added possibility of installing a backdoor on the handset would also have an impact on the privacy of the users, as malicious hackers could easily use Bluetooth or GPRS to read the Phonebook, Calendar, any SMS messages, and download photos from the phone.

The recent attack of the newer Mabir worm shows not only that mobile viruses are a growing trend but also that mobile viruses are getting more sophisticated. Cabir used only Bluetooth to spread, whereas its successor Mabir.A uses both Bluetooth *and* MMS to replicate, which is quite an improvement. The worm also sends an MMS in a reply to any received SMS, which is clever

technique to fool the user into installing the received application. However, besides interesting techniques such as this, overall the Mabir worm is still relatively simple and does not use any sophisticated attacks on specific application or system vulnerabilities. Compare this to the most dangerous worms affecting personal computers today, which tend to benefit from vulnerabilities in the PC's operating system or applications in order to propagate. This area has not yet been explored by the mobile virus writers. Could this be a future attack vector for a mobile viruses? This author believes it is quite possible, and that such an approach can even include vulnerabilities in Bluetooth related applications on mobile phones. To prove this point, let's look at some simple yet unpublished vulnerabilities that exist today.

OS and application vulnerabilities

In order to prove that Bluetooth related application vulnerabilities can and do exist on mobile phones, this article now presents a previously unpublished vulnerability in the Beamer application found on Sony Ericsson P900. Other headsets such as the SE P800 may be affected as well.

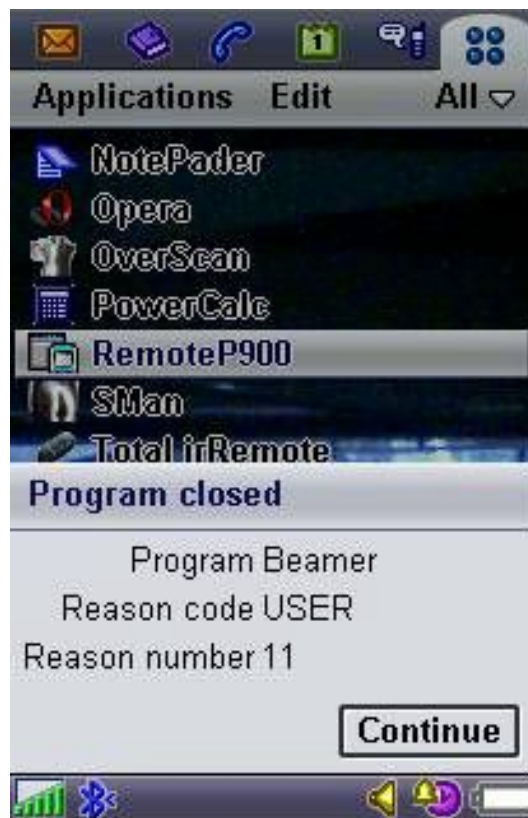


Figure 1. Vulnerability in Sony-Ericsson P900.

The vulnerability itself is trivial. When sending (pushing) a file to a vulnerable phone using obexftp and Obex File Transfer or OBEX Object Push, and when using a remote filename longer than 197 characters, the Beamer application crashes and USER Panic 11 is raised, as shown in Figure 1.

To see the effect yourself simply modify the 743 line (obexftp 0.10.6 version) of obexftp client.c file to send more than 197 characters as remotename in obexftp_put_file function, as shown below.

```

---- snip ---
object = build_object_from_file (cli->obexhandle, localname, \
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA \
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA \
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA" );
---- snip ---

```

After compilation of the modified code, simply execute the obexftp (set the right BT address and chose any existing file):

```
# ./obexftp -b 00:0A:D9:E7:0B:1D --channel 2 -p /etc/passwd -v
```

Then after the execution of obexftp, the Beamer thread on the P900 handset will result in a USER Panic 11, which usually occurs when an operation that moves or copies data to a 16 bit variant descriptor causes the length of that descriptor to exceed its maximum length. The offending thread is also immediately killed when the panic is raised.

The descriptor overflow vulnerabilities are surprisingly common on various mobile phones.

Nokia 9500 vCard Bug

A similar descriptor overflow bug can be observed on Nokia 9500 handsets, which occurs when the viewer reads a specially crafted vCard. To this author's knowledge this bug was also never previously published, thus it will be briefly described.

Lets start by introducing [vCard](#). Simply stated, it is an electronic business card. It contains information such as someone's name, address, phone number, and so on. The vCard is also commonly used for contact information exchange between handsets using the Bluetooth PIM Item Transfer (OBEX Object Push), which is also supported by the Nokia 9500 Communicator. However, the vCard viewer application on Nokia 9500 has quite a trivial bug.

When opening the vCard with a name (N: field) longer than 245 characters, the Nokia 9500

vCard viewer (Text message viewer) will crash resulting in a USER Panic 11 -- the same error as in previously described P900 Beamer application bug.

The sample corrupted vCard file looks as follow:

```

--- Nokia9500.vcf ---
BEGIN:VCARD
VERSION:2.1
N:AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA \
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA \
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA \
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA \
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA;BIALOGLOWY
FN:Marek Bialoglowy
ORG:INDEPENDENT
TITLE:COO
TEL;WORK;VOICE:+6221
TEL;WORK;FAX;
ADR;WORK;ENCODING=QUOTED-PRINTABLE:;;Indonesia
LABEL;WORK;ENCODING=QUOTED-PRINTABLE:Indonesia
URL;WORK;
EMAIL;PREF;INTERNET:bialoglowy@gmail.com
REV:20050430T1958490
END:VCARD
--- Nokia9500.vcf ---

```

In order to observe the effect of the vulnerability, we have to first import the vCard to a contact manager and send it via Bluetooth to the handset. During my tests I simply imported the vCard to Microsoft Outlook and used the Send to Bluetooth feature to send it to the Nokia 9500. Transferring the vCard as a file will not work.

At this stage, interaction with the phone's user is required. The authorization for a vCard transfer will be requested by the phone, as shown below in Figure 2.

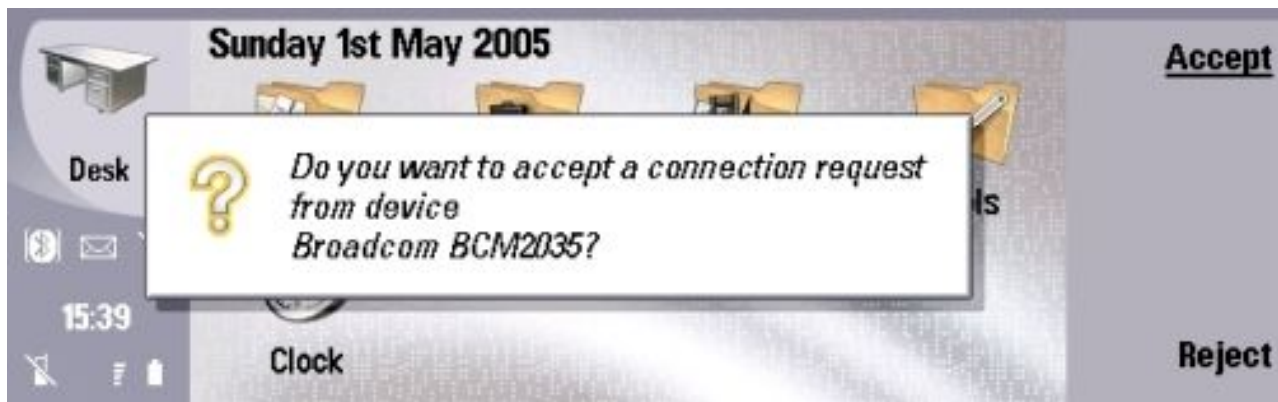


Figure 2. Requesting authorization.

If the transfer was accepted by the user, the new business card will appear in the phone. Here, one more interaction with the user will be required, where user has to open the Business card, as showing in Figure 3.

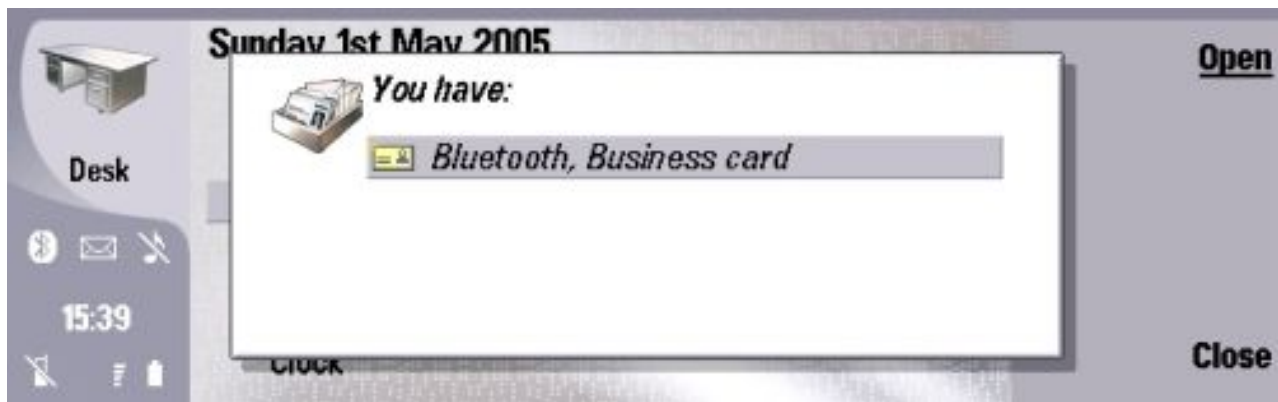


Figure 3. More user interaction required.

A few seconds after confirmation, the viewer will automatically open the vCard and crash due to the name field exceeding descriptor length shown in Figure 4, resulting in previously described USER Panic 11.

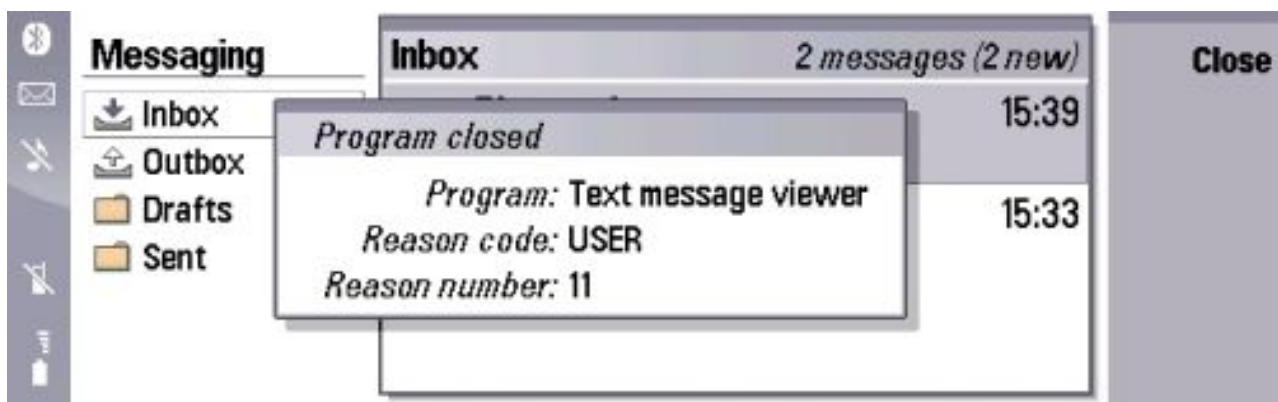


Figure 4. USER Panic 11.

Fortunately for users, true exploitation of this type of vulnerability on Symbian based phones

seems not to be possible. The use of descriptors prevents smashing of the stack, more commonly known as buffer overflow exploitation. Additionally, the corresponding Symbian application runs at low privilege level. Therefore, the Symbian OS design prevents one from compromising the device's security even under the condition that a running application may be incorrectly programmed. However, there is always a chance that sometime in the near future someone may still benefit from this type of vulnerability in some other way. This would be an interesting discussion but is outside of the scope of the current article.

Service authorization issues

To examine this type of vulnerability, let's take a look at the SE P900 again. In addition to the presence of the Beamer vulnerability, it is important to notice that the SE P900 phone accepts Bluetooth file transfers/beams without any authorization from the user.

During the author's tests on the SE P900, the phone sometimes requests a PIN exchange during a file transfer, yet after canceling the transfer 2 or 3 times from the phone interface it will not try to pair anymore and will simply accept the file. However, this is not the only way to transmit an arbitrary file. Most of the time the file is simply accepted if it is sent through OBEX Object Push (channel 2), without any confirmation from the user -- even if the list of authorized Bluetooth devices is empty. The inconsistent results seem to be due to the obexftp application rather than to the Symbian OS itself or the Beamer application. Nevertheless, it is clear that malicious hackers can transfer a file to a phone or cause Beamer application to panic without any interaction with the user, provided Bluetooth is enabled and discoverable.

A Bluetooth service generally has three modes. Mode 1 allows all connections by any device without authentication and authorization. Mode 2 provides basic service-level of security, usually requiring authorization. Mode 3 requires security procedures before the communication channel is established. To achieve a basic level of security, normally a minimum of mode 2 is required. However, mobile device manufacturers more often provide mode 1 (non-secure mode) functionality for an OBEX file transfer.

The problem in having the OBEX file transfer available without authorization (Mode 1) occurs with several Bluetooth enabled smart-phones and PDAs on the market. For instance, the XDA O2 phone with the old WinCE operating system by default accepts all incoming Bluetooth file transfers. The newer version of Bluetooth for Windows CE (BTW-CE) provides an, "Authorization required" setting which enforces the authorization request upon incoming Bluetooth file transfers. However, one will note that the majority of PDA users have this feature disabled. This has

significant impact on the security as the users may simply execute any received application or file, especially if the file has tempting name such as `naked_in_bed.jpg`, for example, and if a vulnerability exists in the graphic files viewer. From a security perspective it is always better to make a request such as, "Do you want to receive a file from an unknown device?" rather than skip this stage and go directly to "Do you want to open the received application: `naked_in_bed.sis`?". Thus, the minimal security mode for all sort of file transfer should always be Mode 2.

At this point we can clearly see that Bluetooth application related security issues can provide malicious hackers with the means to attack Bluetooth devices. However, are there any security and privacy threats related directly to the Bluetooth protocols themselves? Let's try to find answer by reviewing the lower layers of Bluetooth communication, and by looking at the use of some interesting Bluetooth positioning technology.

Bluetooth positioning and tracking

Denmark's largest zoological gardens, the Aalborg Zoo was one of the first to implement a Bluetooth positioning and tracking technology. The special "Bluetags" given to visitors are specially body tags pinned to children, which allow parents to position and track the movement of their child within the Zoo -- and greatly prevents lost children. The method of detecting the position of a "Bluetag" is based on a simple concept of Bluetooth zones, whereby a short range receiver installed at a known location detects a signal of a Bluetooth tag and reports the presence of a Bluetooth tag in the nearest location. For example, a Bluetooth receiver installed near the lion cage detects the Bluetag and reports the presence of the tag (identified by Bluetooth MAC address) as being near the lion cage. When the child moves to the tiger cage the short range receiver located near tiger cage reports the presence of a Bluetag device, within its short 10m proximity, and allows the positioning system to inform security about the new position of a child within the Zoo. Additionally, it also allows one to track a child's movements, for example, from the lion cage to the tiger cage. The data can be later used to draw a map of the movement inside the Zoo within a 10 meter accuracy range, and then inform Zoo staff about the length of stay at each location. In addition to the safety factor, this also provides statistics to management on which animals or parts of the Zoo's facilities are the most popular among children. Overall, this solution is an example of a beneficial use of the Bluetooth technology, which in this case helps to ensures the safety of the children visiting the Zoo. Yet, as one might anticipate, this beneficial idea of using Bluetooth in positioning and tracking can also have a dark side.

Bluetags and privacy issues

As described in [Part 1 of this article](#), each BT enabled device has an unique address assigned to it, allowing one to identify the device. We also already know that one can freely connect to the vast majority of discoverable Bluetooth devices out there without the need for any user authorization, unless we want to access particular service (OBEX, Dial-up etc.) that requires it. The lack of authorization and authentication for a basic LMP (Link Manager Protocol), L2CAP (Logical Link Control and Adaptation Protocol) communication, combined with the fact that each device has a unique Bluetooth address, results in one important problem -- the Bluetooth device itself becomes a Bluetag.

One could simply build a special device with a short range Bluetooth receiver that performs a scan for discoverable Bluetooth devices every minute, and then reports all discovered devices to the monitoring system. If more then one receiver is installed at various distances, the network of such devices (nodes) could record the device's position and additionally, the movement of a Bluetooth device -- all this without the device owner's knowledge. The non-discoverable device could be also reported if we know the MAC address and make a request to it every 1 minute and report any response.

Such system could have a number of interesting uses. For instance, if we carry a Bluetooth enabled handset (in discoverable mode) with us while shopping at the local supermarket, the supermarket owner could easily track our movements as we walk through the supermarket, record how long we spend in certain areas, and eventually create a map of our movements within the supermarket. Based on gathered data, it would be possible to analyze our shopping behavior as market research, and as result change positions of certain products or advertisements, or worse, sell the marketing data to research companies. RFID might seem to be more efficient in such a system, however this would require the supermarket to issue RFID tags to their customers, which most people would not accept. By using the Bluetooth technology on the phone they are already carrying, companies can avoid issuing special tracking cards or badged to customers yet still be able to track their movements.

BT positioning based on zones and is not necessary limited to an indoor environment or a small area. It can also be used for the surveillance of citizens within a city. The perfect example of such a system exists as the [Loca project](#). It is an artistic project run in Helsinki which explores various aspects of Bluetooth surveillance and mobile media, and also raises public awareness of pervasive surveillance. It consists of small network of Bluetooth receivers (nodes) deployed in public spaces within the Helsinki city, connected to the central Loca server via GPRS. The nodes report the position of any Bluetooth devices within proximity to the server, which then is capable of responding with a messages to the Bluetooth device's owner, such as "you were last seen here

yesterday at 21:45" or "we have seen you 6 times in 3 days." This is an excellent, albeit spooky, example of analyzing people's routines and eventually predicting people movements. The presence of such system shows that in fact it is possible to build a basic Bluetooth based surveillance system used to report presence and movement of Bluetooth users within the city.

However, Loca network provides only a limited coverage of the city and does not allow accurate tracking of the movement itself. Would it be possible to make it more accurate? Does one have to cover an area of 10km x 10km Bluetooth receivers (nodes) every 20m to create a true Bluetooth monitoring zones? Well, with current technology we would need at least 250,000 Bluetooth receivers, and therefore it's not truly feasible on a larger scale to use this technique.

Trilateration for tracking and positioning

Unfortunately for users, tracking and positioning using Bluetooth is relatively easy to implement and the cost is also relatively low. In order to track position and movement of a Bluetooth device within a large area, we have to use a different positioning technique from the one previously described. The technique is called Trilateration and yes, it is the same technique used by the GPS system and by police to track the position of a mobile phone or a radio device. Using trilateration, we can calculate a location of a mobile phone base on a distance of a phone to a three different GSM base stations of a known location, as showing below in Figure 5.

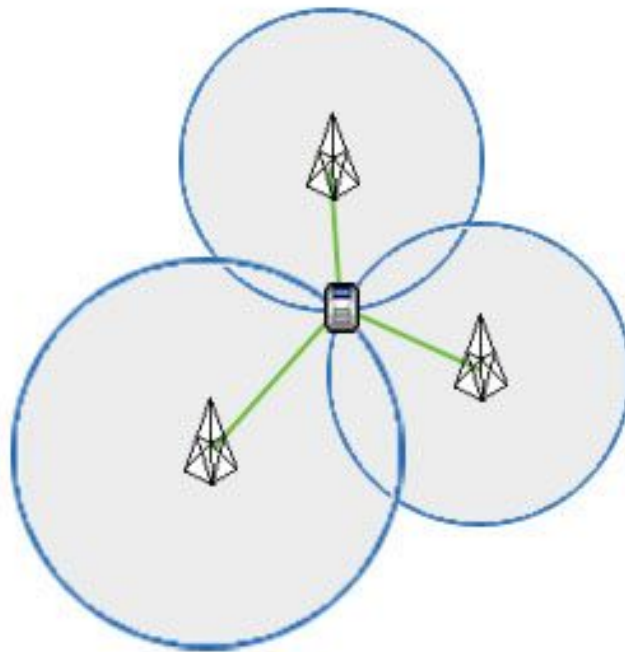


Figure 5. Trilateration using GSM base stations.

The same method also applies to a Bluetooth, but instead of using GSM base stations as receivers, the Bluetooth receivers are being used. Based on calculations involving signal levels and other analysis, it is possible to calculate a distance of a Bluetooth enabled phone from a given receiver.

If you are interested in the technical details of the Bluetooth positioning, I strongly recommend reading two excellent research papers which describe the subject:

An indoor Bluetooth-based positioning system: concept, Implementation and experimental evaluation, by Silke Feldmann, Kyandoghene Kyamakya, Ana Zapater and Zighuo Lue from Institute of Communications Engineering in Hanover.

Bluetooth Positioning, Josef Hallberg, Marcus Nilsson, Kåre Synnes from Luleå University of Technology / Centre for Distance-spanning Technology.

In general, when at least three Bluetooth receivers are installed in known locations, using the trilateration technique it is possible to locate a Bluetooth device and track the device's movement with a good accuracy -- and four receivers can provide an even greater accuracy.

However, the maximum range of a standard Bluetooth dongle available on the market today is a Class 1 device with up to 100m range. In order to achieve a full coverage of the area it would be necessary to install a receiver at least every 100m. To fully cover 100km² it would be still a great challenge and require thousands of Bluetooth receivers, which today is still too difficult to implement. In order to solve this problem, the simplest method is to just extend the range of a receiver beyond 100m.

Bluetooth range extension

A standard Class 1 Bluetooth USB dongle, shown below in Figure 6, has a small antenna allowing it to communicate with a Bluetooth device within a range up to 100m. This is the maximum range of a Bluetooth device as defined in the Bluetooth specification.



Figure 6. Standard USB Bluetooth dongle.

However, the range can be extended with a very basic modification of the Bluetooth dongle itself. To extend the range of a Class 1 Bluetooth adapter we simply replace the small built-in antenna with a more efficient one. Installation of a 5 dBi 2.4GHz antenna in a USB Bluetooth Class 1 dongle could provide us with range or at least 200m or more, though it depends on the type of antenna, soldering and the cable. According to an article entitled, *Bluetooth a Mile Away* in Popular Science, installation of a 5 dBi antenna can extend the range of a Bluetooth USB Class 1 dongle to a mile. Unfortunately, the author of this article was not able to reproduce these results, and with a 5 dBi antenna the maximum distance between the dongle and a SE P900 phone was 230m. Other approaches, such as the popular [Bluetooth gun](#) displayed at the 2004 DEFCON conference, is also possible for extending line-of-sight Bluetooth range.



Figure 7. Typical Bluetooth antenna.

Overall, use of more efficient and bigger antennas provides better results, however in general the low power of a Bluetooth device limits this approach. The D-Link ANT24-1400 14dBi high gain

directional panel antenna, connected directly to a Class 1 Bluetooth dongle, in my tests allowed connection to P900 phone to a maximum distance of 500m. The range above 1km can be achieved using 2.4GHz amplifiers.

Large area Bluetooth positioning

With a modified 1.5km range Bluetooth adapter, it would require only approximately 36 such devices (every 1.5km in a grid) to track a Bluetooth device's movement within a 100km² range, possibly achieving up to 50m accuracy using trilateration (estimated). Greater positioning accuracy can be achieved with a mixed use of trilateration and zone positioning. Special 20m range nodes could be installed within buildings, main junctions and popular locations to provide additional position readings when trilateration could not be accurately used, due to the large objects within the line of sight, within an enclosed space, or other noise. The best option today is certainly to build a series of customized, low-cost, short and long range nodes designed for the sole purpose of a Bluetooth positioning. The total cost of such surveillance equipment used to monitor Bluetooth devices with a good accuracy within a 100km² city today for less than \$10,000USD.

Bluetooth is already so pervasive that these positioning and tracking approaches warrant discussion. Considering the fact that now even the car manufacturers such as BMW, Toyota, Ford and Lexus are producing Bluetooth enabled cars, one could even trace a car using a Bluetooth tracking system, or attack it with a "drive by" Bluetooth spread worm.

Conclusion

Almost any standardized technology such as Bluetooth goes through a number of development and improvement stages which, along the course of time, makes it better, faster and safer for users. The Bluetooth Special Interest Group (SIG) works intensively to make Bluetooth technology safe for its users. While Bluetooth technology itself is relatively secure, the problems mentioned in this article are primarily to do with various implementations by software developers and phone manufacturers. The newest Bluetooth specification addresses certain problems such as a lack of encryption of the Bluetooth address itself during communication, and can add better access control or firewall functionality. However, with the improvements in security we will also see improvements in hacker knowledge of Bluetooth security. New attacks affecting both old and new Bluetooth specification will undoubtedly emerge. In general, the risk of security incident while using Bluetooth technology can still be considered low, as long as users are following the simple Bluetooth security tips as listed at the bottom of this article.

Easy Bluetooth security tips

- Enable Bluetooth only when you need it,
- keep the device in non-discoverable (hidden) mode,
- Use long and difficult to guess PIN key when pairing the device (key such as 1234 is unacceptable),
- Reject all unexpected pairing requests,
- Check list of paired devices from time to time to ensure there are no unknown devices on the list,
- Update your mobile phone firmware to a latest version,
- Enable encryption when establishing BT connection to your PC.

References

1. Bluetooth SIG - <http://www.bluetooth.com>
2. Research of trifinite group - <http://trifinite.org>
3. Research of Ollie Whitehouse - <http://www.blackops.cn>
4. Research of The Shmoo Group - <http://www.shmoo.com>
5. BlueZ Project - <http://www.bluez.org>
6. BlueLon (Bluetooth BodyTag producer) - <http://www.bluelon.com>
7. FTE (producer of BT Sniffer) ? <http://www.fte.com>
8. Bluetooth Device Discovery (presentation) - by Bruce Potter
9. Bluetooth Vulnerabilities Fact and Fiction (WiCon 2004 presentation) by Pentest Limited
10. Bluetooth ? The universal radio interface for ad hoc, wireless connectivity by Jaap Haartsen
11. Positioning and Location Technologies (presentation) by Peter Ørbæk, WorkSPACE, PalCom projects
12. Positioning using Bluetooth (presentation) - IT University of Copenhagen

Finally, thanks to Tabloid Pulsa and Jim Geovedi for help with equipment.

About the author

[Marek Bialoglowy](#) is an independent IT Security Researcher from Poland who provides information security advisory and training services to private enterprises and government in Indonesia and Singapore. He has discovered several critical security vulnerabilities appearing on the SANS/FBI TOP 20 Vulnerabilities list, including one of the first critical vulnerabilities in

Windows 2003.

[Privacy Statement](#)

Copyright 2006, SecurityFocus