DOI: 10.1145/1467247.1467282

BY ALFRED LOO

Security Threats of Smart Phones and Bluetooth

IN A RECENT SECURITY EXPERIMENT, A COMPUTER WITH a Bluetooth sniffing program[5] was hidden in a suitcase that was wheeled around public places. The objective was to ascertain the number of Bluetooth-enabled mobile devices that could be infected with viruses wirelessly. In less than 23 hours, more than 1,400 vulnerable devices were detected, most of which were mobile phones.

Although most mobile phones can only communicate by Bluetooth within a range of 10 meters, the attacking distance can be extended greatly with an inexpensive antenna. In another high-profile experiment,[7] researchers were able to attack targets in a taxi stand from the 11th floor of a hotel in Las Vegas, and they successfully retrieved 300 address books from Bluetooth-enabled devices.

These numbers of vulnerable phones reflect the low level of public awareness about the potential security threats of smart phones and Bluetooth. Phone users also underestimate the possible damage if their mobile phones are compromised. These kinds of security breaches also have serious consequences for corporations and telephone companies. However, most security teams in corporations believe that mobile phones are for individual use only, and that it is not their duty to protect these applications. Hence, mobile phones will be the next easy targets for professional hackers.

Manufacturers incorporate PDA features into mobile phones to make them "smart". As smart phones can perform the tasks of a computer, they are vulnerable to the same kind of hacking attacks. However, most smart phone owners tend to believe that:

- There are enough security features in the phones;
- Hackers are not interested in phones;
- There is no such thing as a phone virus; and
- They have little to lose even if their phones are hacked.[7]

Possible Attacks

All of the hacking problems that are related to computers are valid for smart phones. Furthermore, there are unique problems, as phones have more functions. Examples of these problems include the following.

- Hackers can retrieve address books, calendars, photos, or other files from a phone.
- SMS or MMS messages can be sent from compromised phones to other phones without any user interaction.
- Compromised phones can infect other phones that use Bluetooth or MMS.
- Hackers can remotely control a phone to make phone calls or connect to the Internet.

Consequences

These attacks seem to be harmless, so most users do not recognize their serious consequences. Some possible consequences will now be discussed.

- **Leaking calendars and address books.** Hackers could sell pieces of information from these sources to a user's competitors as the competitors could find the names of the user's clients (or potential clients). Hackers could also alter the details of a user's calendar. As a result, the user could miss important appointments with his/her clients, while competitors approach the clients with another pro-

posal. Hackers could also add entries to a user's phonebook and pretend to be his/her clients/bank representatives.

▸ **Bugging devices.**
Hackers could instruct the user's phone to make a phone call without the user's consent. They could then eavesdrop on (or even record) the user's conversation and the phone would then have become a horrible bugging device. Prudent hackers can even use pre-paid phone cards, so that it is impossible to trace their identities afterwards.

▸ **Sending SMS messages.**
Terrorists could send false bomb threats to airlines using the phones of legitimate users. This would consume government resources as the government would investigate false leads while the terrorists carried out real attacks. There would be no way to trace the terrorists, and the phone owners could be in serious trouble.

▸ **Causing financial losses.**
Hackers could send a large number of MMS messages with a user's phone. MMS services are still quite expensive for large files. Downloading large files would have the same effect. Many service providers will add charges to the phone bills of users if their phones dial a specific number or send an SMS message to the providers.

▸ **Revealing passwords.**
As mobile phone users almost always carry their phones with them, these devices are convenient places to store account numbers and passwords. Examples include corporate accounts, Internet banking accounts, ATM PINs, and the codes to deactivate the alarm systems of the companies or homes of users. The disclosure of these pieces of information would not only endanger the phone users themselves, but also jeopardize the computer systems of their employers.

▸ **Identity theft.**
There are black markets in which hackers can buy and sell personal information.

▸ **Attacks on telephone networks.**
If a virus infected a large number of phones, it could instruct all of them to make phone calls (or send SMS or MMS messages) simultaneously at a certain time. This tactic could paralyze a city's telephone networks and create chaos.

▸ **Leaking Corporation Data.**
Employees can download files from the company's computer onto their phones so that they can continue to work at home. It would be a disaster if the phones were hacked.

Improper Implementation

There are weaknesses[2] in the current Bluetooth standards. Most threats, though, come from improper implementation[4, 7] by manufacturers.

For example, one important Bluetooth security feature is the user's ability to switch between the "discoverable" and "hidden" modes. Every Bluetooth device should have a unique address. To connect to a Bluetooth device, this address would have to be known. Switching the device to the "hidden" mode would provide much better protection.

However, the default setting of some mobile phones is the "discoverable" mode. Because most users do not understand Bluetooth technology, they do not switch their phones to the "hidden" mode. Furthermore, it is difficult in some phones to find the right menu to change the "discoverable" mode to the "hidden" mode because of poor human-computer interface (HCI) design.

Another weakness is the pairing process that two Bluetooth devices need to go through before data exchange. Both devices need an identical secret PIN. A key is then generated and stored in both devices for later communications. However, the first step[6] of this pairing process is done in plain text and is not encrypted. Hackers could intercept the communication messages, which would help speed up the hacking process.

Shaked and Wool[6] have designed three methods to force devices to repeat the pairing process. Intercepting the messages during the process, they were able to determine a four-digit PIN within 0.07 second on a Pentium computer.

Improper implementation also includes the use of very short PINs instead of longer and more secure PINs. Poor HCI design also deters users from changing the default PINs in certain devices.

Manufacturer Responsibilities

A new specification,[3] Bluetooth version 2.1, has been proposed to address the above weaknesses. However, it would be pretty long until devices supporting the new Bluetooth specification are out to the market. Till then, all devices are vulnerable to the existing attacks. Furthermore, hackers will always find new ways to attack. Measures should be adopted to make devices safer which include:

▸ Logs of pairing activities should be maintained so that users can detect any intrusion attempts as soon as possible.
▸ The default security setting should be set at the maximum level.
▸ Manufacturers should pay attention to HCI design so that users can fine-tune the security settings easily.
▸ Security issues should be discussed in the user's manual.
▸ Devices with fixed PINs should be long enough (at least 64 bits).

Corporate Responsibilities

Corporations should take a proactive approach. Examples of the countermeasures they could take include the following.

▸ Devise a policy for the use of mobile devices by their employees.
▸ Learn and monitor the latest developments in phones and other related technologies.
▸ Provide a list of phones with good security features and HCI design to their employees. If large numbers of corporations offer such advice, manufacturers will be forced to develop proper security features.
▸ Educate employees to select and use their phones properly. For example, a short seminar could be offered to employees, and up-to-date guidelines could be issued. The content of these guidelines could change over time. Examples of the guidelines include the following.

- Switch the Bluetooth security setting to the "hidden" mode.
- Activate Bluetooth only when it is needed.
- Do not accept any unsolicited pairing requests.
- Minimize pairing operations in public areas.
- Monitor the numbers and names of the paired devices on the phone to discover any suspicious connections.
- Update the phone's firmware when a new version becomes available.
- Pay attention to whether the phone is consuming power at a rate that is faster than usual and to any other anomalies.
- Use long PINs whenever possible (at least 64 bits).

User Responsibilities

It is the duty of phone users to protect themselves and the data of their

employers. In addition to adhering to these guidelines, it would be useful for users to do the following.

- Be vigilant and treat a smart phone as a computer. Almost all of the precautionary measures for computers can be applied to phones. Bluetooth is not the only threat.
- Invest in the time to update knowledge, for example, by attending seminars.
- Be aware of social engineering techniques.[1]

Conclusion

Every technology has its weaknesses. The risks of using Bluetooth and smart phones are relatively low compared with those of other technologies, provided that they are used properly. Most of the existing threats come from the ignorance of users, improper security implementation by some manufacturers, and the inactive attitude of many corporations.

There is no silver bullet or panacea in the fight against hacking. However, it is interesting to note the sad but true "tiger" theory: *"To survive in the jungle, one does not need to run faster than the tiger. All one needs to do is to run faster than the other people. The tiger is not interested in chasing the fastest runner."* If an organization has a reasonable level of security measures, rational hackers will attack other, weaker organizations, where their hacking will be more cost effective. It always pays to be the leader in the implementation of proper security measures. C

References

1. Berghel, H. Phishing Mongers and Posers. *Commun. of the ACM, 49*, 4, (2006).
2. Bialoalowv, M. Bluetooth Security Review, Security Focus, 2005; (www.securityfocus.com/infocus/1830).
3. Bluetooth SIG, Bluetooth SIG Improves User Experience, March 2007. (http://www.bluetooth.com/Bluetooth/Press/SIG/BLUETOOTH_SIG_IMPROVES_USER_EXPERIENCE.htm)
4. Laurie, B. and Laurie, A. Serious flaws in bluetooth security lead to disclosure of personal data. L. A. Digital Ltd., 2004; (http://www.thebunker.net/security/bluetooth.htm).
5. McMillan, R. BlueBag PC Sniffs Out Bluetooth Flaws. IDG News Services, 2006.
6. Shaked, Y. and Wool, A. Cracking the Bluetooth PIN. *Proceedings of 3rd USENIX/ACM Conference on Mobile Systems, Applications and Services*, 2005, 39-50.
7. Zetter, Kim. Security cavities ail Bluetooth. *Wired News*, 2004. (http://www.wired.com/news/privacy/1,64463-0.html)

Alfred Loo (alfred@ln.edu.hk) is an associate professor in the Lingnan University, Hong Kong.