How Secure Is Bluetooth?

Some issues and limitations for developers to keep in mind

written by
Karen J. Marcelo

Many of the technologies in use today can be compromised in many ways, Bluetooth among them, yet they continue to be used because the benefits are deemed to outweigh the risks.

Since Bluetooth (BT) devices will inevitably be used for transactions requiring a high degree of security, this raises obvious questions.

With the ubiquitous growth of computing, the ability to access and control various devices – some untethered – will crowd the 2.4GHz (and soon the 5GHz) spectrum. Any cabled device already in use today is a potential Bluetooth device. New devices will be manufactured to enhance Bluetooth functionality and extend access to traditional networks.

Interfaces will extend beyond that of human–computer to include autonomous device-to-device communication. Merely walking by a particular cluster of devices could have your BT device probed for information that its owner may not want to disclose. Even if a PIN were required to authorize the exchange, it would be irritating to have to enter it for different devices, and if you were mobile, you could be out of range by the time you finished entering the PIN!

Unlike infrared, direct line of sight isn't required, and unlike 802.11 not set for DHCP, nodes can be mobile, transparently joining and leaving ad hoc networks called *piconets* without users having to reconfigure their devices. Devices switch between master and slave roles and could also act as autonomous routers to other piconets, creating a random, moving "scatternet" with an unpredictable topology.

The convenience to users means they no longer need to be chained to their desks. In fact, the chain to their desks will have gotten not only longer but invisible, and with BT devices acting as routers, they could be chained to several "desks" with or without their knowledge.

There are always ways to exploit systems. The security flaws outlined in this article are based on researchers' findings. If the issues are known, care can be taken in writing and implementing applications or in device usage until the next-generation BT devices that resolve these issues become available.

Security and Access Issues

A flaw identified by Markus Jacobson and Suzanne Wetzel at Lucent is the ability to obtain the encryption key between two devices because of key exchange protocol weaknesses.

Another flaw they identified was how easy it is to obtain the address of another device that can be used to track its activities, compromising the user's privacy.

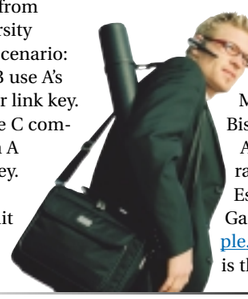
The E22 algorithm is used for key generation. The key is derived from the PIN, the length of the PIN, and a random number, all of which are sent in the clear except for the device's four-digit PIN. Some devices with no UI (such as a headset) will have the PIN set by the manufacturer to 0000 as a default. A four-digit PIN would yield only 10,000 different keys.

Once two units have exchanged keys, they can use the keys each time to authenticate.

Juha Vainio from Helsinki University describes this scenario: devices A and B use A's unit key as their link key. Later on, device C communicates with A using A's unit key. Now device B (who has A's unit key) can use that and a fake address to solve for the encryption key between A and C and listen to A and C's traffic. It can also authenticate itself to device C as A and to device A as C. For more details go to www.niksula.cs.hut.fi/~jiitv/bluesec.html.

A device's address is unique, and once a user is linked to a device, it becomes easy to monitor a person's activity. Logging and profiling will be inevitable and so will loss of privacy. Since the BD_ADDR (device address) is used to communicate within the correct piconet and is used in determining hop sequence and timing, it's not protected. The BB_PDU (baseband packet data unit) contains the device address in the header. BB_PDUs are sent when devices are in inquiry scan mode to discover other devices in the vicinity. Devices do not have to be authenticated at this point.

While the spec doesn't define how inquiry access codes are to be implemented, devices can be set to respond only to others that contain certain access codes; otherwise it will respond to all inquiry scans. Devices that connect for service discovery purposes aren't required to authenticate either (see *Bluetooth Revealed* by Brent Miller and Chatschik Bisdikian).



Another concern raised by Lamm, Estrada, Falauto, and Gadiyaram (www.people.virginia.edu/~gal4y/) is the use of the SAFER+ algorithm in the authentication process. This algorithm was submitted to the Advanced Encryption Standard (AES) and rejected. Although some minor security gaps were identified, the main reason for SAFER+ rejection was speed.

Another issue is that security can't be set on a per-service basis. This can be implemented over the existing protocol stack, but a reference implementation for it isn't available yet.

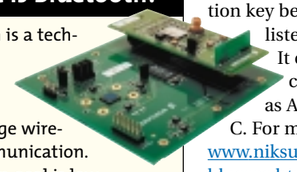
Authentication is done by device and not by user, which has implications for transactions on shared devices. The spec requires authentication but not encryption.

Members of the Bluetooth consortium have confirmed that the issues identified by Lucent's Jacobson and Wetzel are real but are fairly easy to prevent. Some of these flaws have reportedly been addressed in the next rev of the Bluetooth spec, for example, but several devices that are already or soon will be available don't implement the revisions.

I'm not advocating that Bluetooth be abandoned, but I do believe that its limitations need to be fully known and compensated for until they're resolved. Some issues relate to mobile ad hoc networks in general and are not just Bluetooth issues. Many technologies in use today can be compromised in many ways, yet they continue to be used because the benefits outweigh the risks. Doubtless, Bluetooth devices can also be used safely for transactions requiring a higher degree of security…but in the meantime proceeding with caution is advised.

> "I'm not advocating that Bluetooth be abandoned, but I do believe that its limitations need to be fully **known and compensated for until they're resolved"**

What Is Bluetooth?



Bluetooth is a technology designed to enable short-range wireless communication. The design goal is low power consumption for cheap, portable devices. It uses radio to transmit and receive data. For a thorough description, refer to the spec at www.bluetooth.com/developer/specification/specification.asp.

How Bluetooth Got Started

The idea that resulted in the Bluetooth technology was born in 1994. Ericsson Mobile Communications initiated a study to investigate the feasibility of a low-power, low-cost radio interface between mobile phones and their accessories. The aim was to eliminate cables between mobile phones and PC cards, headsets and desktop devices, etc.

Dr. Sven Mattisson (top)
Dr. Jaap Haartesen (bottom): Two of the inventors of the basic radio technology that ultimately led to the foundation of the Bluetooth specification.

Karen J. Marcelo is a researcher in the CSL Distributed Systems Group at Xerox PARC. Before that she worked as a software engineer at Frog Design, Gravity, and Intervista Software. Among the projects she's worked on are a VRML authoring tool, 3D authoring widgets, a 3D "People Finder," and a server-side real-time 3D rendering and Web-delivery system. In her spare time she is the technical contact for Survival Research Labs, a machine performance group writing Web-based telerobotic systems for various untethered lethal devices, developing the first such system using commercially available or free software written by civilians.

karen@srl.org