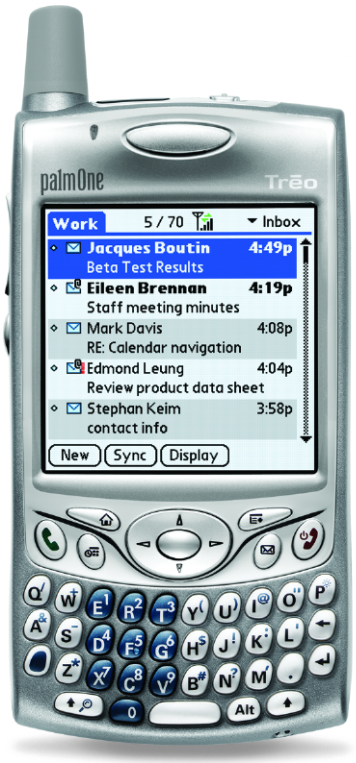
Connecting devices wirelessly with Bluetooth wireless technology.

This paper presents an overview of best practices for using Bluetooth® wireless technology and for addressing security concerns when using Bluetooth services.



What is Bluetooth technology?

Bluetooth technology is a set of specifications that allow devices to talk to other devices, or to accessories, wirelessly over short distances. Bluetooth technology allows devices to communicate with each other without cables. As of the writing of this paper (Fall 2005), Bluetooth technology is being used in significant numbers by cell phone manufacturers to do things like connect a hands-free headset to a mobile phone or connect a mobile phone to a computer.

More specifically, Bluetooth technology is a wireless standard developed by the Bluetooth Special Interest Group, or Bluetooth SIG, an industry association of electronics manufacturers. Bluetooth technology is used primarily in personal area networks (PANs). PANs are spontaneous, or ad hoc, and require no infrastructure. Bluetooth technology is ideal for PANs because of its short range and low power consumption.

The Bluetooth standard ensures that many various types of devices with wireless capabilities (Bluetooth handhelds, Bluetooth headsets, PCs with Bluetooth cards, Bluetooth mobile phones, and so on) can communicate with each other without extensive setup by the user. Bluetooth devices usually talk to each other seamlessly and automatically or semi-automatically.

NOTE: Several versions of Bluetooth technology are currently in use, including versions 1.1, 1.2, and 2.0. This paper covers general features that are applicable across versions. Information specific to Palm® Treo™ 650 smartphones applies to Bluetooth technology version 1.1, the version supported by Treo 650 smartphones.

Different versions of Bluetooth technology offer version-specific security measures as well. For example, version 1.2 has added an anonymity Mode to bolster the security of Bluetooth wireless connections by masking the physical address of a radio so as to prevent identity attacks and snooping.

Contents

Bluetooth transmission details

The Bluetooth specification supports transmissions between Bluetooth transceivers operating in the 2.4 GHz ISM (industrial, scientific, and medical) band, the same band used by Wi-Fi® networks and household microwaves. Bluetooth devices transmit a 1 mW (milliwatt) signal that travels about 10 meters (about 33 feet).

Bluetooth technology employs "spread-spectrum frequency hopping": It regularly switches transmitting among 79 individual random frequencies. The switch happens 1,600 times per second, so it's improbable that two Bluetooth devices will use the same frequency at the same time. This makes it possible to have many different Bluetooth- enabled devices running in close proximity at the same time without interfering with each other.

NOTE: The ISM radio bands were originally reserved internationally for non-commercial use of electromagnetic fields for ISM purposes. Over the years they have come to be used for license-free communications applications such as Bluetooth technology.

What are Bluetooth profiles?

Bluetooth technology is actually a conglomeration of many different types of wireless communication methods, all of which have their own features and capabilities. Bluetooth profiles organize the various technologies according to their function to ensure that various devices can work together on certain operations. Profiles are a way to offer and use services that various devices can understand because they are based on recognized standards. For example, a Treo™ 650 smartphone may offer the dial-up networking (DUN) service, and a partnered handheld or computer can understand this offer and use it if it also supports the DUN service.

Manufacturers can add features to a basic Bluetooth profile, but their devices must, at the very minimum, offer the basic services described in the profile's official specification from the Bluetooth SIG. For example, the PAN profile explains how data can be transferred directly between two Bluetooth devices.

Dial-up networking on the Treo 650 smartphone

If your computer is enabled with Bluetooth wireless technology and supports the DUN profile, you have a data plan with your wireless carrier, and your carrier supports the Bluetooth DUN profile, you can use your Treo 650 smartphone as a wireless modem to access the Internet from your computer. You can browse the web or download email on your computer when you are away from your desk, for example, at an airport.

To set up your smartphone as a wireless modem, you create a trusted pair between your smartphone and your computer and then enable dial-up networking (DUN) on both your computer and your smartphone. From that point, you can access the Internet from your computer using your smartphone as a wireless modem.

Each Bluetooth profile has a specialized use. There is a Bluetooth profile just for headsets when used with mobile phones. This headset profile defines how a Bluetooth mobile phone user can use a Bluetooth headset for a wireless hands-free calling experience. This profile can move audio signals to and from a phone and knows how to control calls. Another profile is devoted to connecting to LANs. This profile knows how to handle file transfers and secure logins. When a device says it has "Bluetooth," this only means that the device has some variety of Bluetooth technology and uses at least one Bluetooth profile.

Discovering devices available for pairing.

Pairing Bluetooth devices

Pairing two Bluetooth devices the first time requires setup of both devices. Once you have done this, typically the devices have the option of becoming "trusted" with one another, allowing for a simplified pairing process in the future.

The typical initial setup includes these four general steps:

1. The Bluetooth functionality on each device is turned on.
2. The devices are put into "discoverable" mode.
3. A shared code or keystroke is entered.
4. The connection is made.

Within these broad steps, the specific instructions for pairing differ with each device.

Treo™ 650 smartphones have a straightforward setup screen that leads the user through the steps, including selecting the profile. Headsets, since they have no screens for feedback, generally accomplish the same sequence by means of a set of button pushes listed in the user documentation.

When two devices have been paired, each device can remember the other as "trusted." There can be several trusted device pairings. For example, a smartphone can have a trusted headset, a trusted notebook computer, a trusted printer, and a trusted GPS receiver. In subsequent use, connecting is just a matter of turning on the Bluetooth functionality and selecting the desired trusted device from a list.

The security provided by these steps is covered in later sections of this paper.

Security concerns

Palm® Bluetooth devices have been developed and are provisioned to help minimize security risks. Various types of hacking have been labeled as bluejacking, bluesnarfing, and bluebugging.

- Bluejacking allows phone users to send personal messages anonymously to other devices. Bluejacking does not involve the removal or alteration of any data from the receiving device.
- Bluebugging allows hackers to access a target mobile phone's commands without the phone owner's knowledge. This allows the hacker to initiate phone calls, send and read text (SMS) messages, read and enter address book contacts, eavesdrop on phone conversations, and connect to the Internet.
- Bluesnarfing allows hackers to gain access to data stored on a Bluetooth phone without alerting the phone owner of the connection made to the device. The hacker can access the address book and associated images, calendar, and IMEI (International Mobile Equipment Identity).

The best practices described later in this paper including keeping the device nondiscoverable, requiring explicit user permission to accept data, and using long, nonstandard passwords, help prevent hacking methods such as these.

Security features inherent in Bluetooth technology

Product developers that use Bluetooth wireless technology in their products have several options for implementing security. Devices and services have various security levels. For devices, there are two levels, "trusted device" and "untrusted device." With regard to services, three security levels are defined: services that require authorization and authentication, services that require authentication only, and services that are open to all devices.

The Bluetooth protocol includes features that protect Bluetooth communications against hacking and data interception:

- A frequency-hopping algorithm. Bluetooth technology transmits signals using short bursts on a pseudo-random sequence of various frequencies. Thus, a receiver cannot simply be tuned to a given frequency to intercept Bluetooth traffic; it must use the same frequency-hopping pattern as the transmitter.
- Encryption algorithm based on SAFER+. The E1 encryption algorithm used by Bluetooth technology is based on SAFER+, an algorithm that has been in the public domain since 1998 and was a thoroughly reviewed AES candidate.
- New encryption key for each session. Bluetooth transmissions use separate keys for authentication and encryption. The encryption key is regenerated for every session, further limiting damage that can be done through man-in-the-middle attacks.
- Spread-spectrum frequency hopping. Bluetooth transmissions regularly switch among 79 individual random frequencies. The switch happens 1,600 times per second, so it's improbable that two Bluetooth devices will use the same frequency at the same time.

Additional security solutions can be used with Bluetooth technology to achieve excellent security. For example, many virtual private network (VPN) clients can run over a Bluetooth connection. Also, certain solutions such as the Trust Digital 2005 Enterprise software and the CREDANT®

Mobile Guardian product described later in this paper can be used to completely disable Bluetooth functionality on a device, thus eliminating any security risks.

Security features of the pairing process

Bluetooth pairing happens when two Bluetooth-enabled devices agree to communicate with each other. To begin pairing, one Bluetooth-enabled device searches for other devices within range.

To prevent hacking during the pairing process, many Bluetooth devices, including all Palm Bluetooth devices, use a passkey as an authentication tool. A passkey is a code entered on both devices that lets the sending device authenticate automatically without requiring the user to enter the passkey every time the sending device attempts to communicate with the other device. This is known as a "trusted pair." Depending on the device, you may set up a passkey on the fly (as long as you enter the same code on both devices), or on simpler devices like headsets, the passkey is preset and you can't change it.

Entering a pre-set passkey for a headset.

Security features implemented in Palm Bluetooth products

In addition to the inherent security features listed above, Palm Bluetooth devices such as smartphones and handhelds use the following security measures. These best practices for configuring Bluetooth devices help maintain the security of Bluetooth transactions among users:

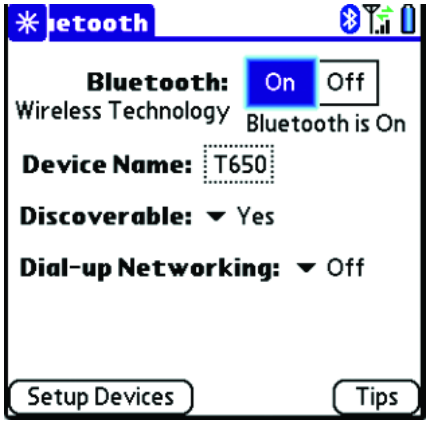
- All Bluetooth devices use link-level security with 128-bit encryption to protect privacy and prevent over-the-air hacking.
- All devices use Security Mode 2, in which security is enforced per service. In other words, individual services/profiles may require different security mechanisms. For example, for the dial-up networking (DUN) and headset/hands-free profiles, Treo™ 650 smartphones enforce security in the following way: Only paired devices can use the Treo 650 smartphone as a wireless modem, and a hands-free device must be paired before it can be used with the Treo 650 smartphone. If a trusted pair has not been formed between the smartphone and the other device, the DUN and headset/hands-free profiles cannot be accessed.
- Treo 650 smartphones require user authorization for data transmission. That is, smartphones require user permission before transmitting or receiving data.
- Treo 650 smartphones also do not allow any data to be pulled from the smartphone over a Bluetooth connection; data may be only pushed (sent) to other devices. This creates a situation in which someone cannot request information from the device and steal information from a device.
- On Treo 650 smartphones, the user must explicitly accept any data being sent to the device, even if the sending device is a trusted device. No data can be automatically pushed to the smartphone. This secures devices from proximity attacks and other attacks where a virus is distributed over a Bluetooth connection by sending Trojan horse applications to various devices.
- The default Discoverable setting on all devices is set to No/Off.
- Devices are set up to allow users to enter up to 16-digit passkeys. The longer the passkey, the more secure the communication.
- Devices use a mode in which users enter the passkey only once during initial pairing. After this, the manual key exchange is not requested per transaction between the paired devices. This reduces the probability of someone listening to the passkey exchange.

Best practices for maximizing security: Individual users

For individuals, the following best practices supplement the device security features and protect data on the device during Bluetooth transactions:

- Keep your Discoverable setting to "No/Off" when not actively in the pairing process. This is the default setting for all Palm Bluetooth devices. When a Bluetooth device is discoverable, it broadcasts its existence to other Bluetooth devices and announces that it is available for Bluetooth communications. When you turn off discoverability, your device will not appear when other Bluetooth devices search for available devices. This enables you to avoid detection of your device in environments such as public locations where there is a risk of

hacking. After your device has made a connection with a new device, return to the settings screen to make sure that the Discoverable setting is turned to No/Off.



Bluetooth setting.

- Do not accept data or pairing requests from unknown devices. Palm Bluetooth devices always prompt the user by asking whether to accept a pairing request from another device.
- Do not pair your device with your computer or hands-free device at a public place where a man-in-the-middle attack is possible. Try to pair it in a more controlled space.
- Always use nonstandard and long passkeys for pairing. For example, when given the option, don't use 0000 or 1234.

Third-party tools for maintaining IT policies

The following third-party solutions are available to maintain security in IT policies.

iAnywhere

www.ianywhere.com/afaria

Created with frontline worker success in mind, Afaria is an enterprise-class, scalable solution with a web-based console that allows you to centrally manage a host of key functions from a browser. Afaria enables customers to secure devices, automate processes, and manage wireless software, content and data regardless of the bandwidth available.

Credant

www.credant.com

The CREDANT® Mobile Guardian product secures notebooks, tablet PCs, PDAs, and smartphones from a single management interface, and integrates with enterprise directories for centralized security policy management. It offers intelligence-based encryption and automated smartphone/PDA detection and control.

Avocent

www.avocent.com

Avocent SonicSentinel password enforcement ensures that sensitive information on a mobile device does not get into the wrong hands. SonicSentinel allows IT administrators to view device details including device type, operating system, battery levels, connectivity patterns, installed software, wireless carrier info, and other important information, to help identify and troubleshoot device problems. This information is delivered over the air for collection on the SonicSentinel server, allowing administrators to track device status and uptime.

Trust Digital

www.trustdigital.com

Trust Digital 2005 Enterprise software protects corporate data from theft, loss, or corruption that results when unsecured devices in an organization expose private data to the outside world. Trust Digital's enterprise software solution transparently secures corporate data across all reaches of the enterprise network-on any mobile device, across any synchronization conduit.

Pointsec

www.pointsec.com

Pointsec® software for Palm OS® enables enforceable and manageable security without compromising the user experience. Pointsec for Palm OS combines sophisticated access control and the Picture PIN® user authentication method to protect confidential information stored within the PDA. Pointsec´s mandatory access control complies with new security regulations and ensures that only authorized users can access applications and data.

Compatible Bluetooth devices for the Treo™ 650 smartphone

Certain Bluetooth devices have been demonstrated to be compatible for all carriers of the Treo 650 smartphone. Individual carriers may have other compatible devices. For complete and up-to-date lists, see http://www.palm.com/us/support/bluetooth/bluetooth_compatibility.html.

Palm, Inc.
950 W Maude Ave
Sunnyvale, CA 94085-2801
www.palm.com

P 477 05