

## Securing Bluetooth™ Wireless Technology – The Next Step

a report by

**Mike McCamon**

*Chairman and Executive Director, Bluetooth Special Interest Group, Inc. (SIG)*

Bluetooth™ wireless technology is poised to change the way in which people live and work by offering short-range wireless connectivity between electronic devices. As Bluetooth becomes more widely used, it is increasingly important that security mechanisms be activated to ensure the integrity and security of the data flowing between devices.

The Bluetooth specification defines link level security but, in order to offer application developers the most flexibility, the creators of Bluetooth decided to allow developers to add their own additional security safeguards for their specific applications. This is because some applications will need very little or no security, while others may require high levels of security.

Rather than waiting to respond to security problems, the Bluetooth Special Interest Group, Inc. (SIG) moved to block security issues before they occur by proactively developing security architecture models as guidelines for application developers. As the technology and its applications evolve, the Bluetooth SIG is dedicated to ensuring security for Bluetooth connectivity.

Countless types of Bluetooth links will ultimately be available to consumers. The following four models for four common Bluetooth connections serve as a representative sample of tight security measures:

1. Headset – microphone/earpiece connection to a mobile phone, personal computer (PC) or CD player.
2. Dial-up networking – connection of a PC or personal digital assistant (PDA) to a modem or mobile phone.
3. Local area network (LAN) access point roaming – accessing a LAN via a Bluetooth link.
4. Synchronisation – keeping the same data on all of the user's devices.

In addition to these models, the Bluetooth SIG recommends some general policies designed to prevent potential security breaches.

### General Guidelines

The process of gaining trust between two communicating devices is called 'pairing' or 'bonding'. These terms refer to a secure exchange of preliminary information to set up the mechanisms of secure communication. It involves the establishment of encoding to protect the most fundamental level of Bluetooth communications – the link.

In general, the code used to ensure security – the key – must be protected to the highest degree that is feasible. The key need not be the same value over a period of time. A device that uses the same key at all times is said to use a unit key, which it shares with all devices it trusts. Combination keys, the preferred alternative, designate a unique key for each combination of Bluetooth™ device and therefore offer more robust security.

Establishing combination keys is an iterative process. When devices first interact, authorising each other as a trusted partner, they follow a number of steps, each reliant on the successful completion of the preceding step. The calculation of keys in each step has a low complexity but the cumulative effect is a very secure link. To initiate the process, the user must input a passkey. Long passkeys are recommended, which make it challenging for a hacker to break in on the authorisation process.

In addition, an intruder cannot steal the correct link key without being in the vicinity of the devices. As a result, the initial pairing of Bluetooth devices should not to be conducted in a public place.

With these basic security procedures in place, the following examples demonstrate how additional security architectures can secure the most common Bluetooth connections:

### Headset

Mobile phone, CD player and PC users can connect those devices to a headset, via a Bluetooth wireless link. When a user purchases a new headset intended

Mike McCamon is the Chairman and Executive Director of the Bluetooth Special Interest Group, Inc. (SIG), also serving on its board of directors. Prior to his work with Bluetooth, he was employed by Intel as Manager of Wireless Standards Evangelism and, prior to this, he built a successful 15-year career in various executive management, sales and product marketing roles at Informix, Apple Computer, Sybase and Iomega in the US and in Europe. He received his Bachelor's degree in History from the University of Kansas in 1985.

for use with a mobile phone, the following procedure for pairing and connection is performed:

1. The customer presses the pairing button on the headset then prepares the mobile phone for recognition of the new Bluetooth headset device.
2. This causes the phone to perform an enquiry over the Bluetooth link. It then receives a response from the headset.
3. The headset demands authentication from the phone, which detects that it does not have a previous link key with the headset. The phone then requests a Bluetooth pairing.
4. The pairing request causes the phone to prompt the user to enter the passkey – preset by the manufacturer and known to the customer – for the headset.
5. A key exchange is performed and a link key is derived that is shared between the devices. It is then possible for the user to specify a new, non-default key. This is highly recommended as an additional security measure. The updated link key is stored in non-volatile memory in both the phone and the headset after the pairing is complete.
6. Once the devices authenticate each other, they perform an encryption key exchange.
7. The headset and the phone encrypt all data they exchange from that point forward. No outsiders can eavesdrop on the conversation held over the Bluetooth link.
8. As a last step, the user switches the headset out of pairing mode so it will not accept new enquiries or pairing requests.

### Dial-up Networking

Laptop and PC users can connect to a modem or a mobile phone via a Bluetooth link. If, for example, a laptop owner wants to use Bluetooth to connect once only to a mobile phone for Internet access, as it is a one-time use, the key created for the connection will be deleted after the session:

1. The user manually switches the mobile phone and the laptop to one-time secure connection mode.
2. The user instructs the laptop to discover nearby Bluetooth devices. The laptop finds the phone.
3. The laptop and mobile phone are temporarily bonded and both devices ask the user to enter the

same Bluetooth passkey into each device. The user creates the passkey using a dedicated Bluetooth passkey generation application on the laptop or on the phone.

4. A common Bluetooth combination key is calculated and this common link key is stored in the phone and laptop for the duration of the link.
5. Authentication is performed and the devices exchange a temporary encryption key.
6. Once the secure link is established, a serial port emulation is established between the phone and the laptop, which makes both devices behave as if there is a non-tamperable 'wire' between them.
7. When the call is complete, the Bluetooth wireless connection is released and the phone and laptop delete their encryption keys.

### LAN Access Point Roaming

Laptop users can connect to a LAN via a Bluetooth link to a LAN access point. A common LAN connectivity scenario will be in 'hot spots', where users connect to a series of associated LAN access points in a public, non-secure area. The process of seamlessly moving between access points is called 'roaming'. Users should follow a unique set of security precautions in this environment.

The Bluetooth SIG has released an enhanced method of accessing a LAN – the personal area network (PAN) profile. It is likely to eventually replace the LAN profile, but the architecture described here is applicable to PANs as well.

The security architecture for LAN roaming is based on group keys, a solution based on an extension of the Bluetooth security mechanism. In group keys, link keys are not unique for each link but are used by one unit for one particular service for all of the associated LAN access points. This service-based key makes group keys different than other keys defined in the Bluetooth specification. Group keys are necessary because combination keys would be too cumbersome for roaming LAN connectivity. Each LAN access point would have to share a combination key for each laptop that uses the service.

In this example, a new laptop user signs up for LAN access. At sign-up time the user will receive a unique identification (ID) (e.g. a number) that identifies the service provider, a secret Bluetooth passkey and the ID unique to every Bluetooth laptop or other device. The LAN access provider stores the Bluetooth passkey and corresponding

laptop ID in a central secure database. All LAN access points in the network must have secure access to the database.

The user first accesses the service by following this pairing procedure:

1. The laptop connects to the LAN access point using the ordinary pairing method.
2. The laptop and the LAN access point exchange service IDs.
3. The key established at this point becomes the 'group key' that is valid for accessing all LAN access points in the associated network for that unit, for that service.
4. When the roaming device goes outside the range of the original LAN access point and encounters another LAN access point in the same network it presents its unique ID and the service ID of the previous LAN access point.
5. If the LAN access point recognises the service ID of the previous LAN access point, it asks the internal service database for the Bluetooth passkey corresponding to the unique ID of the laptop.
6. The LAN access point obtains the Bluetooth passkey corresponding to the laptop's ID from the network directory server and thus is able to communicate securely with a minimum of overhead.

In addition to the Bluetooth keys, the LAN service provider might also use Point-to-Point Protocol (PPP) passwords or keys to authenticate the user. Storing and retrieving of the PPP user name, password and keys can be performed using industry standard methods. Administrators must implement a solution to handle the users and subscriptions – typically a Remote Authentication Dial-in User Service (RADIUS) client at the access point can connect to a server that accesses the subscription database.

### Synchronisation

Synchronisation occurs using a client-server

architecture and is based on the Bluetooth version of the Infrared Data Association's (IrDA's) Infrared Object Exchange (IrOBEX). The client, typically the laptop or PC, initiates an object exchange (OBEX) session with the server, a PDA or mobile phone. The laptop uses OBEX to place and receive requests to drive and extract personal information management data to and from the server.

Bluetooth authentication and encryption protect the baseband. The IrOBEX includes an authentication mechanism. Users can also be required to input access codes to initiate the synchronisation process, which follows these steps:

1. The user performs bonding of the devices and may register the server device in the trusted devices database of the client device and vice versa.
2. The server must be in connectable mode. If not, the user must activate this mode on the device.
3. The user activates an application for synchronisation.
4. A list of devices in the radio frequency proximity of the infrared mobile communication client is displayed to the user.
5. The user selects a device to be connected and synchronised.
6. The synchronisation is processed.

If the client device is not trusted, the user is alerted to the fact that synchronisation must be performed and the user can authorise synchronisation.

### Conclusion

The combination of inherent Bluetooth security plus measures built by application developers will make Bluetooth a highly secure and reliable way to connect devices. The Bluetooth SIG continues to develop architectures and recommended practices to ensure that data can safely be exchanged between devices while maintaining flexibility for implementers. ■