WIRELESS Networking

Manual

Erik Bluethner
Patrick Conway
Rob Garfinkel
James Robinson
Kevin Walker

Topics Discussed

Basics

What is a wireless network?

- LAN – A local area network (LAN) is a computer network covering a small local area, like a home, office, or small group of buildings such as a college
- **Wireless LAN** – LAN that uses radio waves as its carrier to give a network connection to all users in the surrounding area.

Why build a wireless network?

- Flexibility and wireless
- Easy to use
- Setting of equipment
- Prices

Network Adapters

In order to connect your computer to a wireless network it will need a wireless network adapter. The adapter contains a built in radio transmitter in order to send and receive data over the network. As long as it is in within range of another adapter or an access point it will receive the transmission. It can transmit in either 2.4 GHz (802.11b, 802.11g) or 5 GHz (802.11a) bands. They come in a variety of formats; most new laptops will already have them installed by the factory, but otherwise they can be found to fit PCI, PCMCIA, and USB ports. With these compatibility options, wireless technology is available to almost anyone within antenna range. Shown below are Linksys© current offerings for wireless network adapters for the home (PCI) and laptop (PCMCIA).

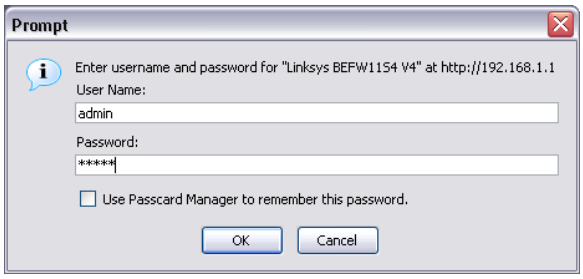
Wireless Standards

When configuring a wireless network there are certain wireless standards that must be used. The 802.11a, 802.11b, and the 802.11g are all standards at with you can choose from. The 802.11a is a device that only works with other 802.11a devices, which mean it is not compatible with any other devices. When working wireless standards a installer might want to consider the transmission speed. The 802.11a and the 802.11g devices have a transmission rate of up 54 Mbps, while the 802.11b only runs at 11 Mbps. There are also good and bad information that an installer should know about wireless standards. The 802.11a has a fast maximum speed, supports more simultaneous users, and regulates frequencies to prevent signal interference from other devices. The down side to using the 802.11a is the high cost and the short range signal and is easily obstructed. The 802.11b on the other hand has a lower cost and the best signal range and is not easily obstructed. The down side to using the 802.11b is slow maximum speed, the support of fewer simultaneous users, and appliances may interfere on the unregulated frequency band. The 802.11g has a fast maximum speed, it supports more simultaneous users, and its signal range is best and is not easily obstructed. The negative about using the 802.11g is the cost which is more than 802.11b, and appliances may interfere on the unregulated signal frequency. The 802.11a and 802.11g are very similar when look at its capabilities, but however 802.11b has a cheaper cost. When configuring a wireless network the user should know the capabilities and the limits of what wireless standards.

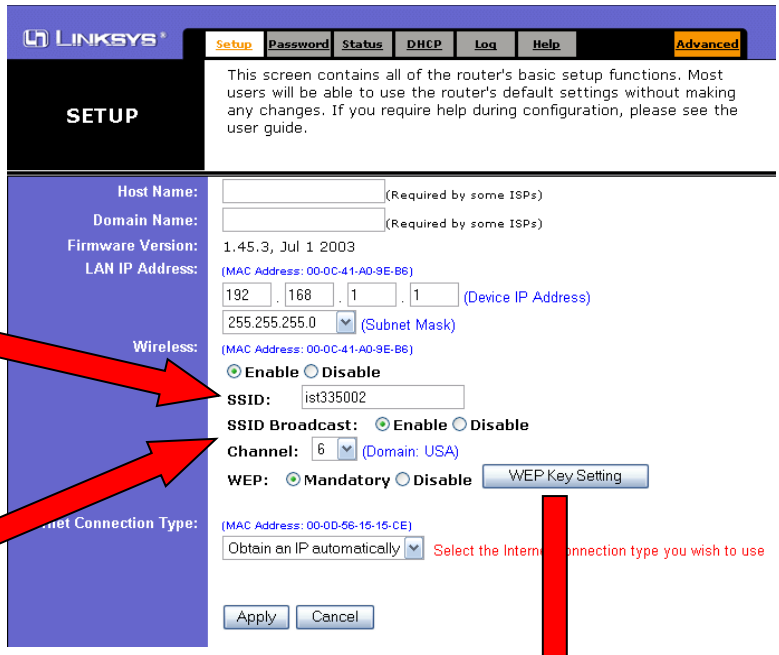
Setting Up and Configuring a Wireless Network

1. Plug in the Ethernet cable from the cable/DSL modem to the router, and another Ethernet cable from the router to the computer.

2. To configure the router, you must open a browser on the connected computer—the interface usually works the best in Internet Explorer. In the location bar, enter the numbers, 192, 168, 1, and 1, with periods between each set of numbers ("192.168.1.1"), then press enter. You will get a login prompt similar to the one on the right, asking for a User Name and a Password. If this is your first time setting up the router, the User Name and Password fields are both set to the default login as "admin".



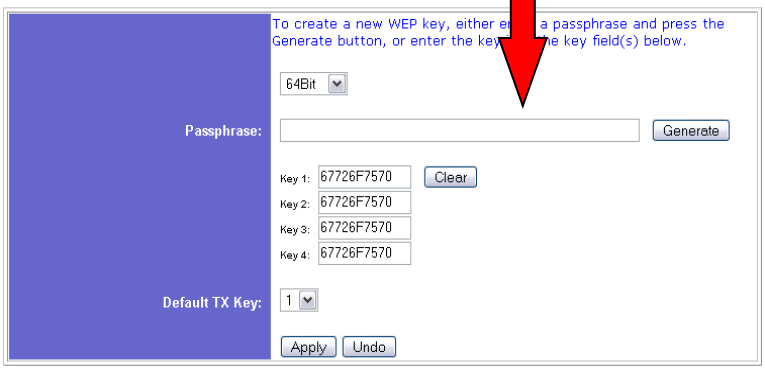
3. The first screen you will see will be similar to this; the most common settings for users are available, and customizable within this screen.



The SSID may have a default name set by the company; it does not necessarily need to be changed, but changing it will ensure that you connect to the correct network.

After configuring the computers, disabling the SSID broadcast will help to prevent unknown people from connecting to your network.

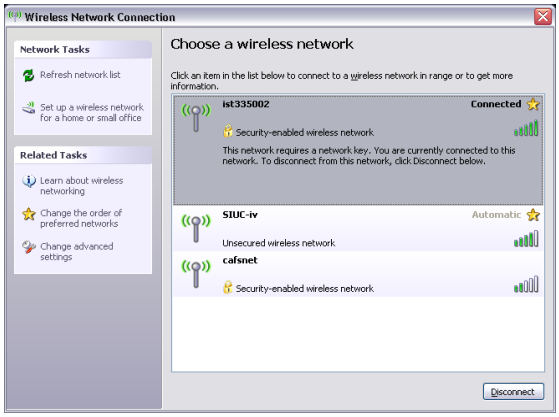
Wireless Encryption Protection (WEP) is recommended for security, to be sure that sensitive information will not be stolen from individuals. The screen on the right will appear by clicking on the "WEP Key Setting" on the first screen of configuring the router. Always apply the changes for the settings when configuring items further.



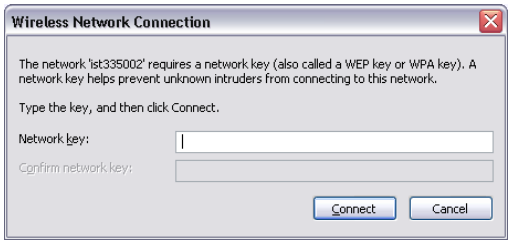
Connecting a Windows XP Computer To The Wireless Network

1. Windows XP contains several ways to access the area where you configure the wireless adaptor of your computer. In the Control Panel, if you see “Network and Internet Connections” within the screen on the left, click on this text, then click on “Network Connections.” If you do not see this text, double click on the icon that reads, “Network Connections.” Right click on the Wireless Network Connection icon, and select “View available networks.”

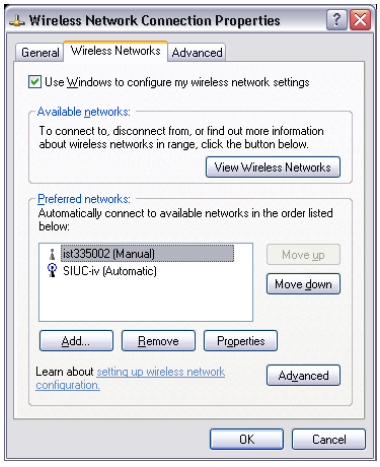
2. In order to connect to a wireless network, search for the broadcast identification name, which appears at the top left for each network name. In this example, ist335002, SIUC-iv, and cafsnet are the network names; the green bars on the right of the prompt display the strength of the signal to the receiver. Networks with the lock icon require a security key to connect to the router.



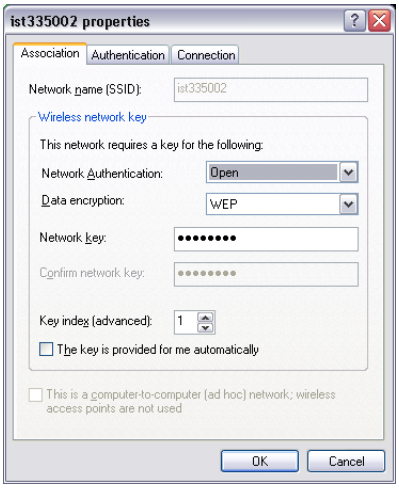
3. To connect to the network, double click on the network name that you have setup in the previous steps. If you are connecting to a network with the security icon, you will see this prompt, in which you type the network key that you had setup while configuring the router; you will need to do this twice, to confirm that you have keyed it in accurately. Press enter, or click “Connect,” and Windows will connect. Once you see, “Connected!,” the settings were correct, and you have access to the connection.



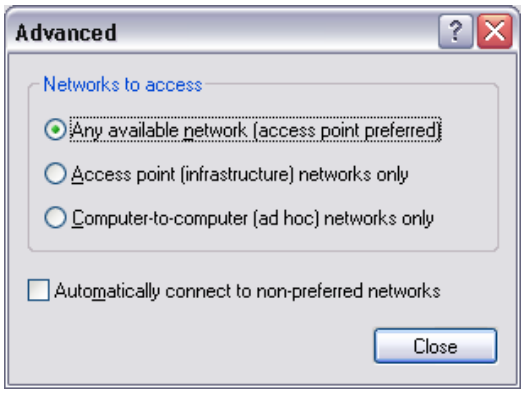
4. Further configuration of the wireless adapter may be necessary if you receive an error. In the same window as step one, click on the text on the left, “Change the order of preferred networks.” You will get the prompt on the left. Click on the network you are connecting to, and then click on, “Properties.”



5. The window that will appear will look similar to the picture on the right. You may have to log in to the wireless access point to confirm these settings; but most of the time, the Key index is the cause of the problem. If needed, this is where the Network key can be changed.

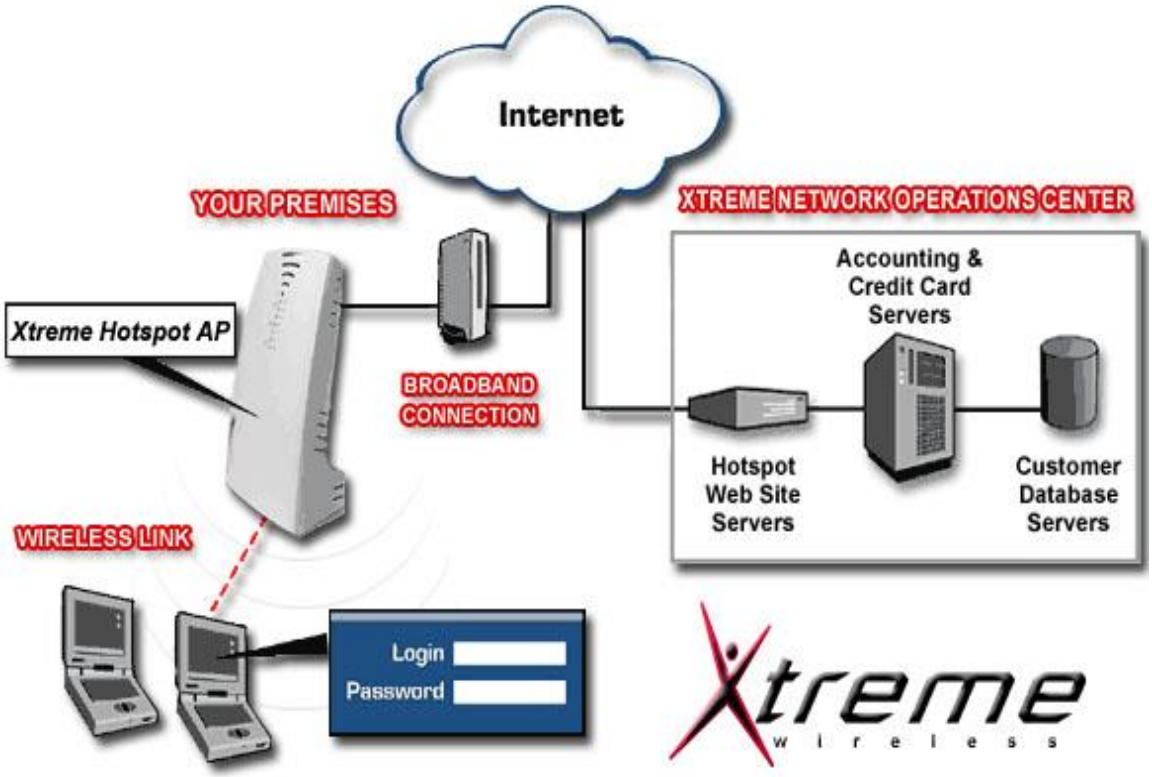


6. You may want a network where printers or files can be shared between computers. This is called an ad hoc network. This option does not permit a connection to the internet. To do so, in the prompt of step four, click on the Add button below the Network selection box. Type in a network name in the SSID box, and disable the Data Encryption by clicking on the drop-down menu. To configure the wireless card to only accept ad hoc networks only, using step four again, click on "Advanced" at the bottom of the prompt, and select the third option, "Computer-to-computer (ad hoc) networks only," then click on Close. Set up any other computers in this same way with the SSID remaining the same.



Wireless Hotspots

A Hotspot is a location that will provide wireless access to the internet for mobile devices such as a laptop or PDA. They can be found all over in places such as airports, train stations, restaurants, schools, libraries, and coffee shops. A wireless hotspot access point can be a little different than a regular access point, with some more business oriented features attached. For example when a user will log on the hotspot will re-direct the user to a payment prompt or require them to login first. In addition it will also likely be complaint to the 802.11b or 802.11g standards and offer security options to the user such as WEP or WPA. If you have trouble locating a hotspot near in your local town you can search for one on the internet using one of the many hotspot directories on the internet. Here is a good example of how a Hotspot works using a Wireless Hotspot Access point that is offered by Extreme Wireless©.



Wireless Security

Security is a huge side of the computer industry today, and in wireless technology it is no different. As the use of wireless technology keeps growing and growing, so do the risks involved with using one. One of the most important aspects of a wireless network is the level of security that is in place on it. There are several known security flaws that are currently associated using wireless technology. These all mainly stem from vulnerabilities in encryption methods, protocols, and ignorance of the user. It is often all too easy for a user with a little bit of knowledge to easily access an un-secured wireless network and have all the other users be at risk.

In order to protect yourself it is important to understand some things about the options that are out there today. A number of users use the Wired Equivalency Privacy, or WEP, for security encryption. It was the original encryption standard created for wireless and with 128 bit key encryption it became a little better but a user's key can still be easily cracked with tools available over the internet. While it is better than nothing, it is far from being secure making it the bare minimum level of security to have. A more secure alternative to WEP is using WPA or WPA2. It was created as a result of the serious weaknesses that were exploited in WEP, particularly in Key encryption. WPA inherits the majority of the 802.11i standard while WPA2 implements the full standard but might be incompatible with older hardware. WPA was started in April of 2003 and was meant as a quick solution to WEP while WPA2 (802.11i) was being finished. WPA was designed to use with an authentication server that distributes keys to each user. A major advantage it has over WEP is the Temporal Key Integrity Protocol, which dynamically changes a user's key, stopping most intrusions. An innovation to WPA2 is its Advanced Encryption Standard (AES) block stream encryption, superior to RC4 encryption of WEP and WPA. There is also an option for home and small networks to use the Pre-Shared Key mode, which requires the user to enter a pass-phrase every time they want to access the network. An Extensible Authentication Protocol (EAP) is a universal authentication mechanism that is most commonly used in wireless networks. There are over 40 different variations of the EAP method and the WPA and WPA2 standard has officially adopted 5 of them as its official authentication method.

In order to secure a network it is important for the user to make sure the right methods are used for their particular network environment. With this in mind a user should abide by these general guidelines:

- Not rely on WEP for Encryption
- Change Encryption Keys Often
- Change the default factory SSID name to something random
- Change default passwords set by the factory
- Broadcast your wireless signal only to the desired area you need it
- Select appropriate EAP protocols for your network environment
- Set the access point to 'Closed Network'
- Disable File and Print sharing
- Enable MAC Address Filtering

Bluetooth Technology

Basics

- *Bluetooth* is a specification for the use of low-power radio communications to wirelessly link phones, computers and other network devices over short distances
- *Bluetooth* technology has achieved global acceptance such that any *Bluetooth* enabled device, almost everywhere in the world, can connect to other *Bluetooth* enabled devices in proximity.

Core Specification Versions

- Version 2.0 + Enhanced Data Rate (EDR), adopted November, 2004
- Version 1.2, adopted November, 2003

Specification Make-Up

Unlike many other wireless standards, the *Bluetooth* wireless specification gives product developers both link layer and application layer definitions, which supports data and voice applications

Spectrum

Bluetooth technology operates in the unlicensed industrial, scientific and medical (ISM) band at 2.4 to 2.485 GHz, using a spread spectrum, frequency hopping, full-duplex signal at a nominal rate of 1600 hops/sec. The 2.4 GHz ISM band is available and unlicensed in most countries

Interference

Bluetooth technology's adaptive frequency hopping (AFH) capability was designed to reduce interference between wireless technologies sharing the 2.4 GHz spectrum. AFH works within the spectrum to take advantage of the available frequency. This is done by detecting other devices in the spectrum and avoiding the frequencies they are using. This adaptive hopping allows for more efficient transmission within the spectrum, providing users with greater performance even if using other technologies along with *Bluetooth* technology. The signal hops among 79 frequencies at 1 MHz intervals to give a high degree of interference immunity

The operating range depends on the device class:

- Class 3 radios – have a range of up to 1 meter or 3 feet
- Class 2 radios – most commonly found in mobile devices – have a range of 10 meters or 30 feet
- Class 1 radios – used primarily in industrial use cases – have a range of 100 meters or 300 feet

Power
The most commonly used radio is Class 2 and uses 2.5 mW of power. *Bluetooth* technology is designed to have very low power consumption. This is reinforced in the specification by allowing radios to be powered down when inactive

Data Rate
1 Mbps for Version 1.2; Up to 3 Mbps supported for Version 2.0 + EDR

Overview of Operation
The *Bluetooth* RF (physical layer) operates in the unlicensed ISM band at 2.4GHz. The system employs a frequency hop transceiver to combat interference and fading, and provides many FHSS carriers. RF operation uses a shaped, binary frequency modulation to minimize transceiver complexity. The symbol
rate is 1 Megasymbol per second (Msps) supporting the bit rate of 1 Megabit per second (Mbps) or, with Enhanced Data Rate, a gross air bit rate of 2 or 3Mb/s. These modes are known as Basic Rate and Enhanced Data Rate respectively.

During typical operation, a physical radio channel is shared by a group of devices that are synchronized to a common clock and frequency hopping pattern. One device provides the synchronization reference and is known as the master. All other devices are known as slaves. A group of devices synchronized in this fashion form a piconet. This is the fundamental form of communication for *Bluetooth* wireless technology.

Devices in a piconet use a specific frequency hopping pattern which is algorithmically determined by certain fields in the *Bluetooth* specification address and clock of the master. The basic hopping pattern is a pseudo-random ordering of the 79 frequencies in the ISM band. The hopping pattern may be adapted to exclude a portion of the frequencies that are used by interfering devices. The adaptive hopping technique improves *Bluetooth* technology co-existence with static (non-hopping) ISM systems when these are co-located.

The physical channel is sub-divided into time units known as slots. Data is transmitted between *Bluetooth* enabled devices in packets that are positioned in these slots. When circumstances permit, a number of consecutive slots may be allocated to a single packet. Frequency hopping takes place between the transmission or reception of packets. *Bluetooth* technology provides the effect of full duplex transmission through the use of a time-division duplex (TDD) scheme.

Above the physical channel there is a layering of links and channels and associated control protocols. The hierarchy of channels and links from the physical channel upwards is physical channel, physical link, logical transport, logical link and L2CAP channel.

Within a physical channel, a physical link is formed between any two devices that transmit packets in either direction between them. In a piconet physical channel there are restrictions on which devices may form a physical link. There is a physical link between each slave and the master. Physical links are not formed directly between the slaves in a piconet.

The physical link is used as a transport for one or more logical links that support unicast synchronous, asynchronous and isochronous traffic, and broadcast traffic. Traffic on logical links is multiplexed onto the physical link by occupying slots assigned by a scheduling function in the resource manager.

A control protocol for the baseband and physical layers is carried over logical links in addition to user data. This is the link manager protocol (LMP). Devices that are active in a piconet have a default asynchronous connection-oriented logical transport that is used to transport the LMP protocol signaling. For historical reasons this is known as the ACL logical transport. The default ACL logical transport is the one that is created whenever a device joins a piconet. Additional logical transports may be created to transport synchronous data streams when this is required.

The link manager function uses LMP to control the operation of devices in the piconet and provide services to manage the lower architectural layers (radio layer and baseband layer). The LMP protocol is only carried on the default ACL logical transport and the default broadcast logical transport.

Above the baseband layer the L2CAP layer provides a channel-based abstraction to applications and services. It carries out segmentation and reassembly of application data and multiplexing and de-multiplexing of multiple channels over a shared logical link. L2CAP has a protocol control channel that is carried over the default ACL logical transport. Application data submitted to the L2CAP protocol may be carried on any logical link that supports the L2CAP protocol.

Security

Product developers that use *Bluetooth* wireless technology in their products have several options for implementing security. There are three modes of security for *Bluetooth* access between two devices.

Security Mode 1: non-secure
Security Mode 2: service level enforced security
Security Mode 3: link level enforced security

The manufacturer of each product determines these security modes. Devices and services also have different security levels. For devices, there are two levels: "trusted device" and "untrusted device." A trusted device, having been paired with one's other device, has unrestricted access to all services.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.

What is bluejacking?

Bluejacking allows phone users to send business cards anonymously using *Bluetooth* wireless technology. Bluejacking does NOT involve the removal or alteration of any data from the device. These business cards often have a clever or flirtatious message rather than the typical name and phone number. Bluejackers often look for the receiving phone to ping or the user to react. They

then send another, more personal message to that device. Once again, in order to carry out a bluejacking, the sending and receiving devices must be within 10 meters of one another. Phone owners who receive bluejack messages should refuse to add the contacts to their address book. Devices that are set in non-discoverable mode are not susceptible to bluejacking.

What is bluebugging?
Bluebugging allows skilled individuals to access the mobile phone commands using *Bluetooth* wireless technology without notifying or alerting the phone's user. This vulnerability allows the hacker to initiate phone calls, send and receive text messages, read and write phonebook contacts, eavesdrop on phone conversations, and connect to the Internet. As with all the attacks, without specialized equipment, the hacker must be within a 10 meter range of the phone. This is a separate vulnerability from bluesnarfing and does not affect all of the same phones as bluesnarfing.

What is bluesnarfing?
Bluesnarfing allows hackers to gain access to data stored on a *Bluetooth* enabled phone using *Bluetooth* wireless technology without alerting the phone's user of the connection made to the device. The information that can be accessed in this manner includes the phonebook and associated images, calendar, and IMEI (international mobile equipment identity). By setting the device in non-discoverable, it becomes significantly more difficult to find and attack the device. Without specialized equipment the hacker must be within a 10 meter range of the device while running a device with specialized software. Only specific older *Bluetooth* enabled phones are susceptible to bluesnarfing.

What is Car Whisperer?
The car whisperer is a software tool developed by security researchers to connect to and send or receive audio to and from *Bluetooth* car-kits with a specific implementation. An individual using the tool could potentially remotely connect to and communicate with a car from an unauthorized remote device, sending audio to the speakers and receiving audio from the microphone in the remote device. Without specialized equipment, someone using the tool must be within a 10 meter range of the targeted car while running a laptop with the car whisperer tool. The security researchers' goal was to highlight an implementation weakness in a select number of *Bluetooth* enabled car-kits and pressure manufacturers to better secure *Bluetooth* enabled devices.

What is the cabir worm? Which devices does the cabir worm affect?
The cabir worm is malicious software, also known as malware. When installed on a phone, it uses *Bluetooth* technology to send itself to other similarly vulnerable devices. Due to this self-replicating behavior, it is classified as a worm. The cabir worm currently only affects mobile phones that use the Symbian series 60 user interface platform and feature *Bluetooth* wireless technology. Furthermore, the user has to manually accept the worm and install the malware in order to infect the phone. More information on the cabir worm is available from the software licensing company Symbian and on the websites of F-Secure, McAfee and Symantec.

How does a PIN affect security?
The personal identification number (PIN) is a four or more digit alphanumeric code that is temporarily associated with one's products for the purposes of a one time secure pairing. It is

recommended that users employ at minimum an eight character or more alphanumeric PIN when possible. Product owners must share that PIN number only with trusted individuals and trusted products for pairing. Without this PIN number, pairing cannot occur. It is always advisable to pair products in areas with relative privacy. Avoid pairing your *Bluetooth* enabled devices in public. If, for some reason, your devices become unpaired, wait until you are in a secure, private location before repairing your devices.

Why does pairing in a public location potentially introduce a security risk?
Theoretically a hacker can monitor and record activities in the frequency spectrum and then use a computer to regenerate the PIN codes being exchanged. This requires specially built hardware and thorough knowledge of *Bluetooth* systems. By using a PIN code with eight or more alphanumeric characters it would take the hacker years to discover the PIN. By using a four digit numeric PIN code, the hacker could discover the PIN in a matter of a few hours. Still advanced software is required.

What is denial of service (DoS)?
The well known denial of service (DoS) attack, which has been most popular for attacking internet web sites and networks, is now an option for hackers of *Bluetooth* wireless technology enabled devices. This nuisance is neither original nor ingenious and is, very simply, a constant request for response from a hacker's *Bluetooth* enabled computer (with specific software) to another *Bluetooth* enabled device such that it causes some temporary battery degradation in the receiving device. While occupying the *Bluetooth* link with invalid communication requests, the hacker can temporarily disable the product's *Bluetooth* services.

Can a hacker get access to my devices data or content with DoS?
The DoS attack only offers the hacker the satisfaction of temporary annoyance, but does not allow for access to the device's data or services – no information residing on the receiving device can be used or stolen by the attacker.

What devices are vulnerable to attacks, and what is the Bluetooth SIG doing about it?
DoS attacks can be performed on any discoverable *Bluetooth* enabled device but in some cases, advanced hackers can determine the address of a non-discoverable *Bluetooth* device. The *Bluetooth* SIG takes all security issues seriously, and we constantly work to make the specification more secure. Therefore, future *Bluetooth* core specifications are planned to include features that will make it impossible to penetrate non-discoverable devices. There are also ways for manufacturers to reduce the risk of DoS attacks at the implementation level of *Bluetooth* wireless technology.

What is the risk of being on the receiving end of a DoS attack?
To date, DoS attacks on *Bluetooth* devices have only been conducted in laboratory tests. The risk of an attempted DoS attack should be considered minimal given the requirements and the normally short range of *Bluetooth* wireless technology.