

---

**Bluetooth Networks: Risks & Defenses**

## Bluetooth Networks: Risks & Defenses

*The objective of this white paper is to provide an overall understanding of Bluetooth networks; to examine the inherent security features and limitations that are available in Bluetooth; and to make recommendations for enhanced Bluetooth security.*

### 1. Understanding Bluetooth Networks

Bluetooth technology is a cutting-edge open standard and specification that enables short-range wireless connections between a multitude of wireless devices, including desktop and notebook computers, handhelds, PDAs, mobile phones, camera phones, printers, digital cameras, headsets, keyboards, and even a computer mouse. More than 250 million Bluetooth devices are in operation worldwide and are expected to grow to more than one billion in the next two years.

Bluetooth was originally architected by Ericsson Mobile Communications, which named the technology after the 10th century Danish Viking, King Harald Blatand, also called Bluetooth. In addition to Ericsson, Bluetooth is supported by all major companies, including IBM, Intel, Nokia, and Toshiba.

#### ***A Personal Area Network***

Bluetooth is Personal Area Network (PAN) technology. It uses a globally available short-range digital radio band frequency for worldwide compatibility, to provide a mechanism for creating small wireless networks on an ad hoc basis. Bluetooth enables fast & reliable transmission for both voice & data. Bluetooth-enabled devices allow users to eliminate cables from their digital peripherals, making cable clutter a thing of the past and can also provide a bridge to existing networks.

The goal of Bluetooth is to connect different devices together, wirelessly, in a small environment, such as an office or home. Bluetooth can be used to connect almost any device to any other device, for example, to connect a PDA and a mobile phone.

According to its proponents, Bluetooth is inexpensive, takes little power to operate, and maintains a low profile. The standard effectively does the following:

- Eliminates wires and cables between stationary and mobile devices.
- Facilitates data and voice communications.
- Offers the possibility of ad hoc networks and delivers synchronicity between personal devices.

#### ***Operating Band***

Bluetooth transceivers operate in the unlicensed 2.45 GHz ISM band that is reserved for industrial, scientific, and medical applications. This band is available in most parts of the world (varies in some locations). In the United States and Europe, the frequency range is 2,400 to 2,483.5 MHz, with 79 1-MHz radio frequency (RF) channels. In practice, the range is 2,402 MHz to 2,480 MHz. In Japan, the frequency

range is 2,472 to 2,497 MHz with 23 1-MHz RF channels. The band is similar to the band WLAN devices and other IEEE 802.11-compliant devices occupy. **Table 1** summarizes the characteristics of Bluetooth.

**Table 1.** Key Characteristics of Bluetooth Technology

Characteristics	Description
Physical Layer	Frequency Hopping Spread Spectrum (FHSS).
Frequency Band	2.4 GHz – 2.45 GHz (ISM band).
Hop Frequency	1,600 hops/sec.
Data Rate	1 Mbps (raw). Higher bit rates are anticipated.
Operating Range	About 30 feet; can be extended to 330 feet.

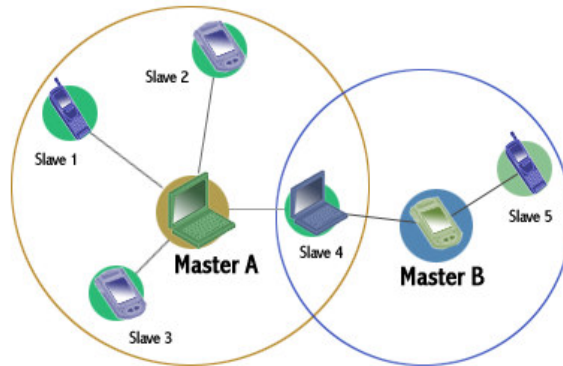
### ***How Bluetooth Devices Network***

Bluetooth networks are comprised of wireless stations or clients only, unlike a WLAN, which is comprised of both wireless user stations and access points. A Bluetooth client may be any Bluetooth-enabled device. There are currently more Bluetooth devices than WLAN devices in use.

Bluetooth-enabled devices automatically locate each other and form networks. As with all ad hoc networks, Bluetooth network topologies establish themselves on a temporary, random basis.

Bluetooth networks maintain a “master-slave” relationship between devices. This relationship forms a *piconet*. Up to eight Bluetooth devices may be networked together in a piconet, in which one device is designated as the master of the network with up to seven slaves connected directly to that network. The master device controls and sets up the network (including defining the network’s hopping scheme).

Devices in a Bluetooth piconet operate on the same channel and follow the same frequency hopping sequence. Although only one device can act as the master for each network, a slave in one network can act as the master for other networks, thus creating a chain of networks. This series of piconets, called *scatternets*, allows several devices to inter-network over an extended distance. This relationship also allows for a dynamic topology that may change during any given session: as a device moves toward and away from the master device in the network, the relationships of the devices in the immediate network change with the topology. **Figure 1** illustrates a typical piconet and scatternet.



**Figure 1.** A Typical Bluetooth Piconet & Scatternet.

### ***Range of Bluetooth Devices***

The operating range of a Bluetooth-enabled device depends on its Class, which in turn depends on the power level of the device.

**Table 2.** Device Classes of Power Management

Type	Power Level	Operating Range
Class 3 Devices	100 mW	Up to 330 feet.
Class 2 Devices	10 mW	Up to 30 feet.
Class 1 Devices	1 mW	Less than 30 feet.

At a 330-foot range, Bluetooth can compete with other WLAN technologies and applications. Additionally, as with the data rates, it is anticipated that even greater distances will be achieved in the future.

### ***Benefits of Using Bluetooth***

Bluetooth offers five primary benefits to users. These benefits make Bluetooth a very attractive, currently available technology that can result in increased efficiency and reduced costs. The efficiencies and cost savings are attractive for the home user and enterprise business user alike.

- **Cable replacement**  
Bluetooth technology replaces cables for most device and peripheral interconnections.
- **Ease of file sharing**  
Bluetooth enables file sharing between Bluetooth-enabled devices, for example, a Bluetooth-compatible mobile phone can act as a wireless modem for laptops.

- **Wireless synchronization**

Bluetooth provides automatic wireless synchronization with other Bluetooth-enabled devices, without user input.

- **Automated wireless applications**

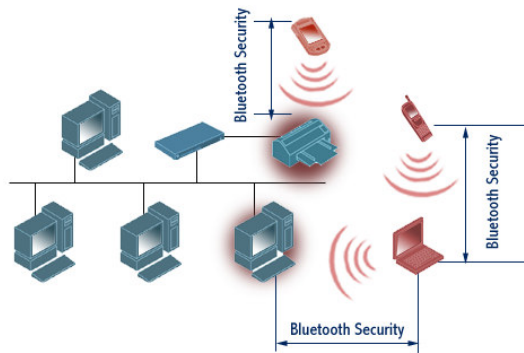
Bluetooth supports automatic wireless application functions for interface with the LAN and Internet.

- **Internet connectivity**

Bluetooth is supported by a wide variety of devices and applications.

## 2. Bluetooth Security Features

As a wireless technology, Bluetooth has some inherent, but limited security features that users can optionally implement.



**Figure 2.** Bluetooth Air-Interface Security

As shown in **Figure 2**, security for Bluetooth is provided on the various wireless links – on the radio paths only. Link encryption and authentication may be provided, but true end-to-end security is not possible. In the figure, security services are provided between the PDA and the printer, between the cell phone and laptop, and between the laptop and the desktop. The Bluetooth specification defines three basic services:

- **Confidentiality (privacy)**

Bluetooth confidentiality attempts to prevent information compromise from eavesdropping (passive attack). This service addresses, “Are only authorized persons allowed to view my data?”

- **Authentication**

Bluetooth authentication provides an abort mechanism if a device cannot authenticate properly. This service addresses, “Do I know with whom I am communicating?”

- **Authorization**

Bluetooth authorization allows the control of resources. This service addresses, “Has this device been authorized to use this service?”

It is important to note that, like the 802.11 standard, Bluetooth does not address other security services, such as audit and non-repudiation.

Bluetooth provides a 1,600 hops-per-second frequency-hopping scheme with radio link power control to limit transmit range. These characteristics provide Bluetooth with some additional, albeit small, protection from eavesdropping and malicious access. The frequency-hopping scheme, primarily a technique to avoid interference, makes it slightly more difficult for an attacker to locate the Bluetooth transmission. Using the power control feature appropriately forces any potential adversary to be in relatively close proximity to pose a threat to the Bluetooth network.

### 3. Security Risks

How secure are Bluetooth devices that use only Bluetooth standard security? Bluetooth devices have inherent security vulnerabilities, which provide a motivation for using enhanced security. Some Bluetooth devices have serious flaws in their authentication and data transfer mechanisms (see table 3.)

*“Though Bluetooth devices have security features built in, most devices ship with unsecured default configurations that create gaping security holes.”*

**InStat/MicroDesign Resources**

Security Issue / Vulnerability	Comments
Shared master key.	The Bluetooth SIG needs to develop a better broadcast keying scheme.
No user authentication.	Bluetooth only provides device authentication. Application-level security and user authentication is optional.
Eavesdropping, resulting from device key sharing.	A corrupt user may be able to compromise the security, i.e., gain unauthorized access to, between two other users.
Compromise of privacy if the Bluetooth device address (BD_ADDR) is captured and associated with a particular user.	Once the BD_ADDR is associated with a particular user, that user’s activities could be logged, resulting in a loss of privacy.
Device authentication is simple shared-key challenge-response.	One-way only challenge-response authentication is subject to <i>man-in-the-middle</i> attacks. Mutual authentication is required to provide verification that users and the network are legitimate.
End-to-end security is not performed.	Only individual links re encrypted and authenticated. Data is decrypted at intermediate points. Applications software above the Bluetooth software can be developed.
Limited security services.	Audit, non-repudiation, and other services do not exist. If needed, these can be developed at particular points in a Bluetooth network.
Viruses and DoS attacks, via the Internet and Email.	Data is vulnerable to third-party providers.

**Table 3.** Security Issues.

Source: NIST

## ***Bluetooth Security Vulnerabilities***

Bluetooth devices are subject to a number of attacks.

### ***Eavesdropping Attacks***

Malicious users can use wireless microphones as bugging devices. There have been recorded incidents of successful attacks on PCs using programs such as Back Orifice and Netbus. If a malicious user has a program such as Back Orifice installed on a device in the Bluetooth network, that user could access other Bluetooth devices and networks that have limited or no security. These same programs could be used against Bluetooth devices and networks. Bluetooth devices are further vulnerable because the system authenticates the devices, not the users. As a result, a compromised device can gain access to the network and compromise both the network and the devices on the network.

*“Like wireless LAN devices, Bluetooth devices are being rapidly deployed with little or no security, however because of the pervasiveness of these unsecured devices left in default settings, they stand to be an attractive target for exploitation.”*

**Pete Lindstrom, research director, Spire Security**

### ***Authorized Remote User Attacks***

Authorized remote users pose a threat to Bluetooth networks. Remote users are not always subject to the same security requirements as users onsite. They frequently use nonsecure links, whether at home or on travel. In the process of connecting, they transmit user IDs and passwords, which a malicious user can capture using a network sniffer. Without the secure perimeter typically provided in an office environment, the need to be in close proximity to the user to intercept traffic becomes less. Once the device or link is compromised, all devices in that Bluetooth network are vulnerable to attacks. For example, a compromised link allows a malicious user to monitor data traffic, while a compromised device allows the malicious user to request and receive sensitive data. In addition, remote users often delegate authority (rights) to a host machine (e.g., a shared server) to execute programs. If the remote device is compromised and the authorized user had granted rights to the machine, the malicious user could then use those rights to compromise the network.

An example of this is a PDA automatically requesting a laptop to send and download emails. If the user had enabled (i.e., had delegated authority to) the PDA to download email from the laptop, a malicious user could use the compromised PDA to obtain the email.

### ***Signal Jamming Attacks***

Besides the typical DoS attacks directed against LANs and Internet services, Bluetooth devices are also susceptible to signal jamming. Bluetooth devices share bandwidth with microwave ovens, cordless phones, and other wireless networks and are thus vulnerable to interference. Malicious users can interfere with the flow of information (i.e., disrupt the routing protocol by feeding the network inaccurate information) by using devices that transmit in the 2.4GHz ISM band.

## ***SNARF Attacks***

Confidential and even restricted data can be obtained, anonymously, and without the owner's knowledge or consent, from some Bluetooth-enabled phones. This data can include the entire phonebook and calendar, and the phone's International Mobile Equipment Identity (IMEI), which remotely identifies the phone to the mobile network. The IMEI is used in illegal phone cloning.

## ***Backdoor Attacks***

The complete memory contents of some mobile phones can be accessed when an attacker establishes a trust relationship through the Bluetooth pairing mechanism, while ensuring that it no longer appears in the target's register of paired devices. This data includes not only the phonebook and calendar, but also media files, such as pictures and text messages. In essence, the entire device can be backed up to the attacker's own system. Not only can the attacker acquire data from the phone, but the attacker can also access other services, such as modems or Internet, and WAP or GPRS gateways.

## ***Bluejacking***

Bluejacking is a technique that involves abusing the Bluetooth pairing protocol. This protocol is a mechanism by which Bluetooth devices authenticate each other, to pass a message during the initial handshake phase. Abuse is possible because the name of the initiating Bluetooth device displays on the target device as part of the handshake exchange, and, as the protocol allows a large user defined name field (up to 248 characters), the field itself can be used to pass the message. This presents a potential security problem. The pairing protocol is the driving force behind Bluetooth, as the protocol is designed for information exchange. It is this protocol that gives Bluetooth its ability to interface with other devices and exchange, update, and synchronize data. The Bluejacking technique uses the first part of a process that allows that information exchange to take place, and is therefore open to further abuse if the handshake completes and the Bluejacker successfully pairs with the target device. If this occurs, all data on the target device becomes available to the attacker, including phone books, calendars, pictures, and text messages. Bluejacking can provide the means for an attacker to hijack valuable data from corporations, government bodies, and the like. Bluejacking can succeed because of the number of users who are often duped by a constant barrage of unsolicited messages, such as SPAM email or SMS text messages.

## **4. Mitigating Security Risks**

Countermeasures are now available to help secure Bluetooth Networks. There are countermeasures that enterprise management can take to establish security policies; there are limited software solutions inherent in Bluetooth; and now there is the industry's first commercial-grade Bluetooth monitoring system, AirDefense BlueWatch™.

## ***Management Countermeasures***

Enterprises that use Bluetooth technology can reduce risks by establishing and documenting security policies that address the use of Bluetooth-enabled devices and user responsibilities. Security policies should include a list of approved uses for Bluetooth networks, the type of information that may be transferred in the network, and disciplinary actions resulting from misuse. Security policies should also specify a set scheme for password use.

## ***Inherent Software Solutions***

Software solutions inherent in Bluetooth technology include the PIN and private authentication. Bluetooth enforces PIN codes at the link level. Because the PIN codes are necessary for authentication and link security, administrators should ensure that Bluetooth devices use PIN codes other than the default (or lowest) setting.

Passwords are fundamental measures that add an extra layer of security. As Bluetooth devices can store and automatically access link-level PIN codes from memory, a Bluetooth device should employ device authentication as an extra layer of security. Enterprises should incorporate application-level software that requires password authentication in Bluetooth devices.

## ***The AirDefense Solution—BlueWatch™***

**AirDefense BlueWatch™** is the industry's first solution that reaches beyond 802.11 monitoring and discovers the next generation of threats to the network, Bluetooth. By identifying all Bluetooth-enabled devices and their communications within a given air space, companies can identify misconfigured devices. AirDefense BlueWatch enables companies to take proactive steps to close any security holes or back doors mitigating the risk of security breaches.

*“Monitoring tools like AirDefense BlueWatch can play a critical role in providing visibility of unsanctioned or insecure Bluetooth devices and the security vulnerabilities they introduce.”*

**Pete Lindstrom, research director, Spire Security**

BlueWatch enables organizations to understand what Bluetooth devices are present in their airwaves and how and to whom the devices communicate. By monitoring the Bluetooth traffic, organizations can understand Bluetooth-related security threats, can take a proactive approach to prevent intrusion into their network, and can better protect their informational assets.

AirDefense BlueWatch runs on any computer or PDA installed with Windows 2000, XP, or CE and a Bluetooth adapter. AirDefense BlueWatch monitors the airwaves to:

### **Identify Devices**

BlueWatch can identify different types of Bluetooth devices, including laptops, PDAs, keyboards and cell phones.

### **Provide Key Attributes**

BlueWatch can provide key attributes, including device class, manufacturer, and signal strength.

## Provide Connection Information

BlueWatch illustrates and tabulates communication or connectivity among various devices.

## Identify Available Services

BlueWatch can identify services that are available on each device, including network access, fax, and audio gateway.

## Conclusion

More than 250 million Bluetooth devices are in operation worldwide and are expected to grow to 1 billion by 2006. Yet without a monitoring solution, organizations have no visibility into these devices or know whether the devices are pairing with and communicating with intruders.

AirDefense BlueWatch allows organizations to quickly scan the air space and detect Bluetooth devices as far away as 300 feet. A general misunderstanding exists that Bluetooth devices connect with another Bluetooth device within a range of 10-20 feet. Therefore the risk of a stranger in the parking lot picking up the signal for malicious purposes is disregarded. However as nearly every laptop, keyboard, pocket PC and cell phone shipped are Bluetooth-enabled, companies will come to depend on AirDefense.

*"Many of our new company-issued devices are Bluetooth enabled. Although this is a convenience for many of our associates, there is a risk that sensitive data may be compromised. AirDefense BlueWatch provides a monitoring solution that we can use to identify and track how and with whom these devices communicate."*

**Michael Ciarochi, senior security engineer, HomeBanc Mortgage**

By identifying security holes and back doors created by innocent users or intruders using Bluetooth, AirDefense BlueWatch enables corporations to lock down the environment making it secure. By monitoring and securing the devices, organizations can then enjoy all the benefits of Bluetooth without compromising security.

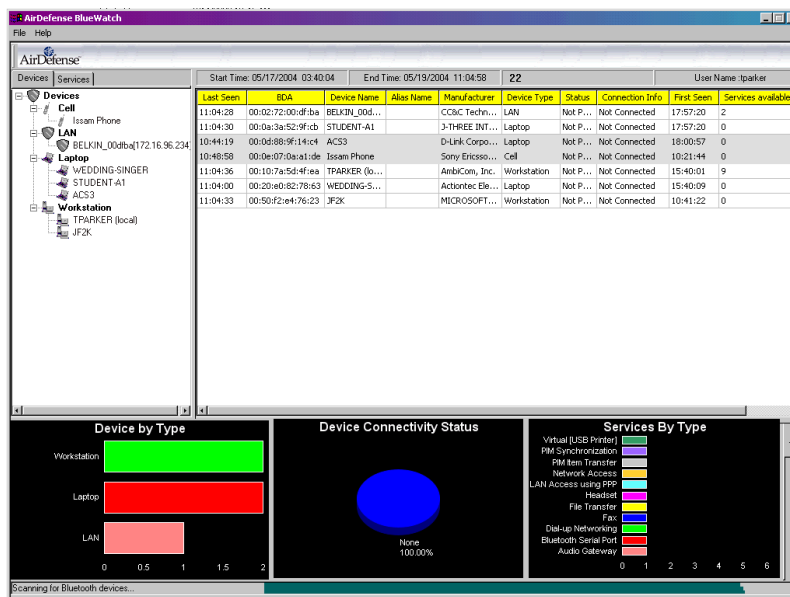


Figure 3. AirDefense BlueWatch Dash

**AirDefense**, the market leader in anywhere, anytime wireless security and monitoring, is trusted by more Fortune 500 companies, healthcare organizations and high-security government agencies for enterprise wireless protection than any other wireless security provider. Ranked among *Red Herring's* Top 100 Private Companies in North America, AirDefense products provide the most advanced solutions for rogue wireless detection, policy enforcement and intrusion prevention, both inside and outside an organization's physical locations and wired networks. Common Criteria-certified, AirDefense enterprise-class products scale to support single offices as well as organizations with hundreds of locations around the globe.

**AirDefense Enterprise**, the flagship product, is a wireless intrusion prevention system that monitors the airwaves 24x7 and provides the most advanced solution for rogue detection and mitigation, intrusion detection, policy monitoring and compliance, automated protection, forensic and incident analysis and remote troubleshooting. As a key layer of security, AirDefense Enterprise complements wireless VPNs, encryption and authentication. Using a monitoring architecture of distributed smart sensors and a secure server appliance, the AirDefense Enterprise system provides the most comprehensive detection of all threats and intrusions. Unlike any other solution on the market, AirDefense Enterprise analyzes existing and day zero threats in real time against historical data to more accurately detect threats and anomalous behavior originating inside or outside the organization. The system automatically responds to threats according to appropriate business process and compliance requirements on both wireless and wired networks, making AirDefense Enterprise the industry's most secure and cost-effective wireless intrusion prevention and troubleshooting solution.

**AirDefense Personal**, the industry's first end-point security solution, provides uninterrupted protection for all mobile employees and their enterprise wireless assets, regardless of location – at work, home, airports or other wireless hotspots. Policy profiles are defined centrally on AirDefense Enterprise and automatically downloaded to each mobile user. If threats are discovered, AirDefense Personal notifies the user and sends the alerts to AirDefense Enterprise for central reporting and notification. This unique solution allows the network administrator to enforce corporate policies and provide complete protection for the mobile workforce, regardless of location.

The **AirDefense InSite Suite** is a collection of powerful tools available today for network architects to design, install, maintain and troubleshoot wireless networks. Tools included in the suite are: **AirDefense Mobile**, complementary to AirDefense Enterprise allows administrators to perform wireless assessments, security audits, locate and manage rogues. **AirDefense Architect** provides complete design and 3D RF simulation of wireless LANs based on building-specific environments. **AirDefense Survey** provides real-time, in-the-field measurements of Wi-Fi RF environments for site-specific surveys.

For more information or feedback on this white paper, please contact [info@airdefense.net](mailto:info@airdefense.net) or call us at 770.663.8115. **All trademarks are the property of their respective owners.**