THE INFORMATION SECURITY OF A

BLUETOOTH-ENABLED HANDHELD DEVICE

Frankie Tvrz[1] and Marijke Coetzee[2]

[1]Department of Business Information Technology
[2]Academy for Information Technology
University of Johannesburg

[1]frankie.tvrz@sita.co.za
[2]marijkec@uj.ac.za

ABSTRACT

Bluetooth connectivity allows workers to access information anywhere, including both personal and corporate information. Software and applications have been specifically developed for handheld devices such as PDAs, giving users a high level of usability and functionality. The goal of this paper is to present an information security evaluation of a Bluetooth enabled handheld device, such as a PDA. The use of Bluetooth wireless technology and functionality provides added benefits, but also brings new information security threats to organisation's information assets. The research attempts to understand the implications of using a Bluetooth enabled handheld device in both public and private environments. Five high-level layers are defined for this discussion. Security risks are evaluated based on current research into vulnerabilities, attacks and tools that exist to compromise a Bluetooth enabled handheld device. Possible recommendations to mitigate identified security risks are also suggested.

KEY WORDS:
Bluetooth, information security, layered approach, vulnerabilities, attacks

THE INFORMATION SECURITY OF A BLUETOOTH-ENABLED HANDHELD DEVICE

1 INTRODUCTION

Wireless technologies are deployed in both public and private networks, and may even be preferred over traditional wired networks [STAN02]. Bluetooth [GEHR04] gives mobile workers the ability to create ad-hoc connections with mobile devices, corporate networks, and Internet hotspots.

This offers mobility and convenience of use for Bluetooth enabled handheld devices such as PDAs (Personal Digital Assistant) and smart phones [GALL04]. Market research has indicated that Bluetooth-enabled devices will experience a 60% compound annual growth rate between 2003 and 2008. Bluetooth usage continues to increase especially in Bluetooth enabled handheld devices [BRIT07]. It was predicted that Bluetooth enabled devices would increase from 316 million units in 2005 to 866 million in 2009 [SDAA07]. The proliferation of Bluetooth enabled PDAs, smart phones and laptops bring Bluetooth past the enterprise door into the corporate network environment, usually without the knowledge of the corporation [HICK06].

Information security risks are introduced as people are utilising an easy to use technology such as Bluetooth, not really designed for information security, on handheld devices that are becoming more sophisticated in informal and corporate environments.

The aim of this paper is to provide an information security evaluation of a Bluetooth enabled handheld device, such as a PDA. Section 2 gives a basic background to the environment in which Bluetooth is used. Section 3 describes a layered approach to evaluating the Bluetooth handheld device. Section 4 describes the risks of using a Bluetooth enabled handheld device, and section 5 evaluates how information security services are implemented. Section 6 concludes the paper.

2 BACKGROUND

An IT consultant John uses his PDA for both corporate and private use, as shown in figure 1. He stores confidential client information on his PDA such as technical documents, minutes of meetings, calendar items and e-mails. His Bluetooth enable handheld device is a PDA that is a highly functional pocket sized computing device consisting of a small liquid crystal display, an operating system, a processor and memory. The PDAs utilises the Windows Mobile [PRIC03] operating system. John may unknowingly bring malicious software from the wireless public environment into the wired corporate network environment. To be able to comprehensively discuss the information security risks presented by the Bluetooth enabled handheld device of John, a layered approach is defined next.

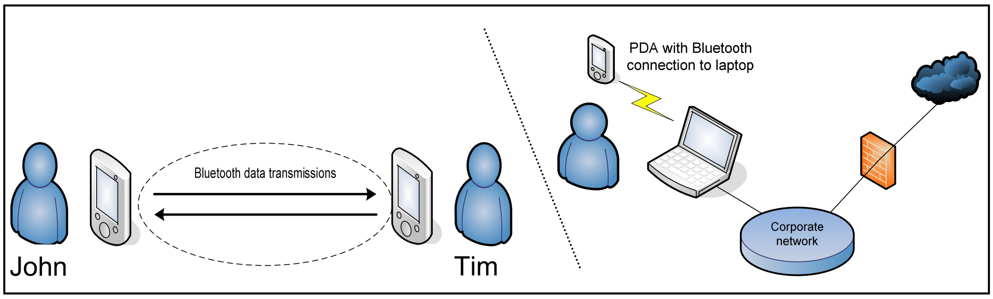

PDA with Bluetooth connection to laptop
Bluetooth data transmissions
Corporate network
John
Tim

Figure 1 – Bluetooth use in public and corporate networks

3 THE BLUETOOTH HANDHELD DEVICE

Layering is a method of combining different information security components to provide layers of protection. This assists in creating a defensive barrier. Layered information security improves the information security mechanism and increases the difficulty of compromising the handheld device. In contrast, a vulnerability or poor information security configuration in a layer could allow an attacker with a possible unauthorised access point.

In order to organise and structure the discussion on the information security of the Bluetooth enabled handheld device of John, the following layers are defined, as shown in figure 2:

- *Physical (Bluetooth)* – the implementation of Bluetooth in hardware;

- *Bluetooth(software)* – software implemented in, and defined over the physical device to allow wireless interconnectivity between devices;
- *Operating System* - the main control program of the handheld device that enables hardware and loaded applications, including Bluetooth configurations and services, to function correctly;
- *Applications* – programs dependent on the operating system such as e-mail, word processing, and calendar items;
- *User* – considered the administrator of the handheld device as it is under his/her full control. He/she configures features on the handheld device such as its information security, operating system and applications.

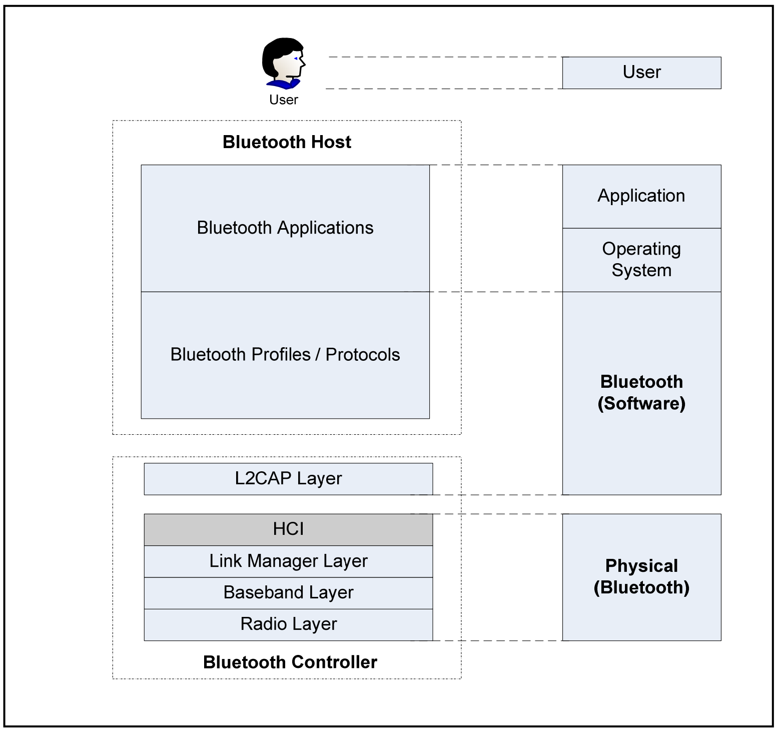


Figure 2 – Layers of the Bluetooth enabled handheld device

It is also important to further define the six layers of the Bluetooth architecture, shown in figure 2 [MCDE05] [ANAN01] [INSI06]:

- *Radio Layer* – the Bluetooth transceiver that defines the transmission and receiving of packets over the physical channel;

- *Baseband Layer* – enables devices search for and connect to other devices by enabling the physical radio link between the devices compromising the piconet;
- *Link Manager Layer* – manages the properties of the air-interface link between devices such as bandwidth allocation for data, bandwidth reservation for audio traffic, authentication by means of challenge response, trust relationships between devices, encryption of data and control of power usage;
- *Host Controller Interface (HCI)* – provides a standard interface for upper level applications to access the lower;
- *Logical Link Control and Adaptation Protocol (L2CAP)* – allows multiple protocols and application to share the air-interface;
- *Profiles* – profiles describe how the technology is used in different scenarios;

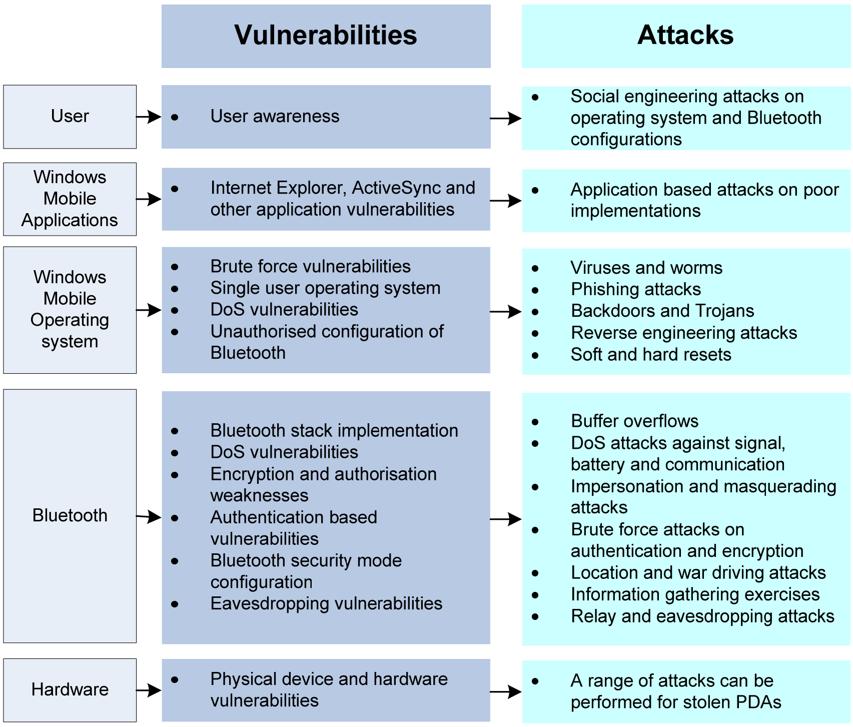
Possible information security risks, presented by each of theses layers are discussed next.

4 INFORMATION SECURITY RISK OF THE BLUETOOTH ENABLED HANDHELD DEVICE

An information security risk is the likelihood that an accidental or intentional threat will compromise vulnerabilities within the Bluetooth enabled handheld device. [SANS07], and bring new information security threats to organisation's information assets. Many vulnerabilities and attacks exist on a Bluetooth enabled handheld device that can be used to compromise its information security. In order to gain perspective on the risks that a Bluetooth enabled handheld device presents, Figure 3 gives high-level view of theses aspects. This may assist users to understand and be aware of the inherent risks in using a handheld device within a Bluetooth communication environment.

- *The physical layer* is inherently vulnerable to physical based attacks and manipulation of the Bluetooth enabled handheld device. The frequency hopping technique employed by *Bluetooth hardware* to prevent eavesdropping can be circumvented. Interference from other applications and implementation of the Bluetooth stack on different operating systems pose risks. At the *Baseband* layer inquiry scans can be used to discover

Bluetooth devices which could allow anonymous information gathering to be performed providing the Bluetooth device address, manufacturer and Link Manager protocol version information. Devices can be set to being discoverable or non-discoverable which can have an influence on Bluetooth based attacks. At the *Link Manager layer,* weaknesses exist within Bluetooth authentication, as input parameters are the Bluetooth device address and the user PIN, sent in clear text. This makes Bluetooth authentication vulnerable to eavesdropping and brute force attacks. Encryption provided by Bluetooth only encrypts the packet payload but the packet header and access code are not encrypted, allowing eavesdropping to be performed.



	Vulnerabilities	Attacks
User	• User awareness	• Social engineering attacks on operating system and Bluetooth configurations
Windows Mobile Applications	• Internet Explorer, ActiveSync and other application vulnerabilities	• Application based attacks on poor implementations
Windows Mobile Operating system	• Brute force vulnerabilities • Single user operating system • DoS vulnerabilities • Unauthorised configuration of Bluetooth	• Viruses and worms • Phishing attacks • Backdoors and Trojans • Reverse engineering attacks • Soft and hard resets
Bluetooth	• Bluetooth stack implementation • DoS vulnerabilities • Encryption and authorisation weaknesses • Authentication based vulnerabilities • Bluetooth security mode configuration • Eavesdropping vulnerabilities	• Buffer overflows • DoS attacks against signal, battery and communication • Impersonation and masquerading attacks • Brute force attacks on authentication and encryption • Location and war driving attacks • Information gathering exercises • Relay and eavesdropping attacks
Hardware	• Physical device and hardware vulnerabilities	• A range of attacks can be performed for stolen PDAs

Figure 3: Overview of attacks and vulnerabilities of the Bluetooth enabled handheld device

- *The Bluetooth layer:* The *L2CAP* layer is responsible for maintaining connections between communicating devices and is vulnerable to denial of service (DoS) attacks. Multiple vulnerabilities exist which allowing a number of attacks, with the complexity of the attack ranging from difficult to effortless execution. Attacks ranging from simple Denial of Service (DoS) attacks against the Bluetooth signal to detailed brute force attacks against the authentication mechanisms can be successfully performed due to inherent vulnerabilities within Bluetooth and its implementation. *Bluetooth profiles* are dependent on the manufacturers of the Bluetooth enabled handheld device and the information security of the protocols used outside of the Bluetooth Specification for the secure operation of the Bluetooth profile.

- *The operating system layer* can be targeted as another method of gaining access to or through the Bluetooth configuration. Vulnerabilities exist because of the single user operating system allowing brute force attacks. The increased threat of malicious software such as viruses and worms can be exploited by attackers. User identification and authentication is not performed, although a power on password is required when using the PDA. Bluetooth configurations are stored in the registry of the operating system and are dependent on operating system controls to protect the Bluetooth information security settings. If the operating system were to be compromised then Bluetooth configurations could be changed through the Windows Mobile operating system.
- *The application layer* has implementation vulnerabilities due to poor application programming, allowing application based attacks which can be used to gain unauthorised remote access to the operating system, and then to Bluetooth.
- *The user layer* is dependent on the user's actions, which would affect the information security of all the layers of the Bluetooth enabled handheld device. The user could be unaware of information security practices to ensure a secure operating environment for the Bluetooth enabled handheld device.

Next, Bluetooth information security services are evaluated that can be used to mitigate theses risks.

5 INFORMATION SECURITY SERVICES OF A BLUETOOTH ENABLED HANDHELD DEVICE

Information security services are the measures that are employed to prevent the unauthorised use, misuse, modification or denial of the use of assets [BRAU00]. Bluetooth information security is designed so that the end user is able to configure and manage the information security options for communication [GEHR04]. Table 1 shows how each layer implements identification, authentication, authorisation and confidentiality. It also indicates how each layer supports the next and whether information security mechanisms provided by one layer possibly supports the controls in the next layer of the Bluetooth enabled handheld device.

Each of the information security services is now evaluated. The integrated implementation of the four information security services is discussed, as it applies across all the layers of the Bluetooth enabled handheld device, and main concerns are highlighted.

Identification *is the act of identifying an entity such as a user, application or device to the Bluetooth enabled handheld device and its applications, so that it can recognise the entity and distinguish it from others.* The main concern is that when a handheld device is accessed via Bluetooth, the user is not identified, but rather the device making the connection. The Bluetooth device address is not used by the operating system or by any application. At the user layer, a concern is that the owner of the device may not be aware that the other user is not identified. Identification is thus not implemented in an integrated manner across the layers of the handheld device and does not comply with the definition given above. Only device based identification is performed. It would be very important to ensure that a user is fully aware of this, and must understand how Bluetooth identification takes place when another entity makes a Bluetooth connection to access services that are provided.

Authentication *verifies the identity of the user, process or Bluetooth enabled handheld device, as a prerequisite to allowing access to resources offered on the device.* The physical, Bluetooth, operating system and application layer of the Bluetooth enabled handheld device are responsible for their own authentication mechanisms. Bluetooth authentication is inherently weak and can be compromised. Furthermore, the operating system does not use the authentication performed by Bluetooth, neither do

Table 1: Information security services

Information Security Service	Physical	Bluetooth	Operating System	Applications	User
Identification	MAC address Bluetooth device address (BD_ADDR)	Bluetooth device address (BD_ADDR)	None, unless third party software is used or integration to the corporate network	Username unless third party software is used, or integration to corporate network	Awareness that device, not user is identified
Authentication	None	Windows Mobile information security policies Initialisation key and Link key based on random number, pin and Bluetooth device address	Windows Mobile information security policies Power-on password	Password integration to server based applications Application execution authentication	Awareness of power-on password or strength of pin number
Authorisation	Windows Mobile information security policies Remote and local storage card wipe	Windows Mobile information security policies Bluetooth security manager consisting of trust relationships, device and service database	Windows Mobile information security policies Application permissions Certificates	Windows Mobile information security policies Application permissions Certificates	Awareness of Windows Mobile information security policies and Bluetooth security mode configuration
Confidentiality	Windows Mobile information security policies Encryption for storage cards	Windows Mobile information security policies Bluetooth encryption algorithms Encryption key	Windows Mobile information security policies Stream based encryption Block cipher encryption One-way hashing algorithm Digital signatures	Windows Mobile information security policies Application based encryption SSL encryption	Awareness of Windows Mobile information security policies, Bluetooth security mode configuration and use of encryption programs

the applications. At the user layer, the user might not be aware that he is not authenticated at the Bluetooth or operating system layer. Bluetooth authenticates the handheld device and the operating system authenticates via a power-on password. He also needs to understand that authentication is based on the link key and not the pin entered by the user when performing Bluetooth authentication. Only device based authentication is performed for the Bluetooth and operating system layers which does not fully comply with the definition given above. The user needs to understand how Bluetooth authentication is performed when gaining access to Bluetooth services, especially since the information security risk is increased when Bluetooth authentication is performed in public environments.

Authorisation *is the process of determining whether the user or Bluetooth enabled handheld device can be granted access to services offered by the host device.* Authorisation mechanisms provided by information security policies can be used on the physical, Bluetooth, operating system and application layers. However, these authorisation mechanisms are not integrated across the layers of the Bluetooth enabled handheld device. The main concern is that detailed authorisation controls are not provided for services offered by Bluetooth, access is based on the first two layers of the Bluetooth enabled handheld device. If devices have paired, they may trust each other, and may be granted access to any service exposed by Bluetooth. Authorisation is not implemented in an integrated manner across the layers of the Bluetooth enabled handheld device, but only partially complies with the definition above. It is important for the user to be aware that Bluetooth device based authorisation is used and when other entities make a Bluetooth connection to access services provided by the Bluetooth enabled handheld device.

Confidentiality *is the property that guarantees that Bluetooth communicated information or information stored on the handheld device is not made available to unauthorised individuals, entities or processes.* Confidentiality can be enforced across all the layers through the use of information security policies, if handheld devices are managed centrally by the organisation. From when a Bluetooth connection is made, the information security policy could enforce that all services offered through Bluetooth use encryption. However the confidentiality mechanisms provided by each layer for the Bluetooth enabled handheld device are independently enforced. The main concern is that inherent information security risks exist within the Bluetooth specification which are present when using Bluetooth on the handheld device. Confidentiality is not adequately enforced by the Bluetooth specification allowing a number of attacks to be performed. The operating system does not use the encryption provided by Bluetooth when making a Bluetooth connection, neither does the application. At the user layer, he may not be aware that each layer of the Bluetooth enabled handheld device uses their own confidentiality mechanisms which each require to be configured to ensure that data transmitted and stored is encrypted. Confidentiality is not implemented in an integrated manner across the layers of the Bluetooth enabled handheld device and partially complies with the definition given above. It is important that the user understands how Bluetooth encryption is performed, when Bluetooth devices make connections to services offered.

From this evaluation, it is clear that Bluetooth negatively affects the information security of a handheld device such as PDA, as it provides wireless connectivity that is not integrated into the different layers of the Bluetooth enabled handheld device. Fundamental weaknesses exist within the identification and authentication information security weaknesses, impacting on the authorisation information security mechanism. Inherent weaknesses exist within the Bluetooth specification and implementation of Bluetooth on the handheld device, this has led to vulnerabilities and attacks that can be performed successfully to compromise the information security services of the Bluetooth enabled handheld device.

6 CONCLUSION

It is clear that the Bluetooth enabled handheld device presents a new risk within the information security realm. New threats have been created when introducing the handheld device to Bluetooth connectivity within the public and private environments.

Information security risks have been identified on all layers forming part of the Bluetooth enabled handheld device, which have led to the compromise of a number of information security services. The identified vulnerabilities and attacks could be used by to bypass information security mechanisms of all the layers of a Bluetooth enabled handheld device such as a PDA.

Information security services are not adequately addressed, and cannot sufficiently protect assets stored on the device. A compromised device may also be used to gain entry to a corporate network and the information that it stores. The information security risk of using a Bluetooth enabled handheld device should thus be clearly understood by the organisation before introducing it into the corporate network. The user also needs to understand the actions that can be performed to ensure that information security risks are mitigated against, to operate the handheld device in a secure Bluetooth environment.

7 REFERENCES

ANAN01 ANAND N. 2001. An Overview of Bluetooth Information security. SANS Institute 2003.

BRAU00 BAUKNECHT K. 2000. 5 Information Security Services ISO 7498/2. Website. http://www.ifi.unizh.ch/ikm/Vorlesungen/sec/02.pdf. 25 February 2004

BRIT07 Study Says Bluetooth Entering the Mainstream, http://www.brighthand.com/default.asp?newsID=10643, accessed 25 March 2008

GALL04 GALLEGOS F, Auditing Wireless Telecommunications: An Issue of Standards, Information Systems Control Journal, Volume 3 of 2004

GEHR04 GEHRMANN C, PERSSON J, SMEETS B. 2004. Bluetooth Information security, Norwood: Artech House computing library

HICK06 Mobile Computing News, http://searchmobilecomputing.techtarget.com/news/article/0,289142,sid40_gci1179892,00.html , accessed 25 March 2008

INSI06 INSIGHT CONSULTING. 2006. How can Bluetooth services and devices be effectively secured? Computer Fraud & Information security Journal. January 2006

MCDE05 McDERMOTT-WELLS P. 2005. What is Bluetooth? , Potentials, IEEE, Volume 23, Issue 5, of December.

PRIC03 PRICE R. 2003. PDA as a Threat Vector. SANS Institute 2003

SANS07 Glossary of Terms Used in Information security and Intrusion Detection. http://www.sans.org/resources/glossary.php?portal=c43474178943e08ef4a460dfb96fb20f#i . SANS institute. Accessed 25 July 2007

SDAA07 Mobile Phone Market Pushes Growth of Bluetooth Chip Market, http://searchmobilecomputing.techtarget.com/news/article/0,289142,sid40_gci1179892,00.html, accessed 25 March 2008

STAN02 STANLEY R.A. 2002. Wireless LAN Risks and Vulnerabilities. Information Systems Audit and Control Foundation (ISACA).