Security in Bluetooth, WLAN and IrDA: a comparison

Keijo M.J. Haataja

Report A/2006/1

ISBN 951-781-271-X
ISSN 1795-9195

UNIVERSITY OF KUOPIO
Department of Computer Science

P.O.Box 1627, FI-70211 Kuopio, FINLAND

Security in Bluetooth, WLAN and IrDA: a comparison

Keijo M.J. Haataja
Department of Computer Science
University of Kuopio
P.O.Box 1627
FI-70211 Kuopio, Finland
E-mail: haataja@cs.uku.fi

Abstract

Excluding mobile phone related data transfer, there are three popular wireless data transfer technologies: Bluetooth, WLAN and IrDA. In this report we compare the security of these three technologies.

Contents

1 Introduction

Bluetooth [1] is a technology for short range wireless data and realtime two-way voice transfer providing data rates up to 3 Mb/s. WLAN (Wireless Local Area Network) [2] is a technology for wireless data transfer providing data rates up to 54 Mb/s. IrDA (Infrared Data Association) [3] is a technology for very short range wireless data transfer providing data rates up to 16 Mb/s. Bluetooth and WLAN are wireless RF (Radio Frequency) communication systems, while IrDA is wireless infrared communication system.

Bluetooth, WLAN and IrDA are wireless communications technologies, which differ in terms of their features and data security solutions. These three wireless communication technologies have been chosen for comparison, because they are widely used all over the world. Bluetooth and WLAN represent the new and promising generation of wireless communication, while IrDA can be considered as old and impractical technology.

The rest of the report is organized as follows. Section 2 briefly describes Bluetooth technology and its security. An overview of WLAN technology and its security is given in Section 3. Section 4 gives a brief description of IrDA technology and its security. The comparison between Bluetooth security, WLAN security, and IrDA security is provided in Section 5. Finally, Section 6 concludes the report.

2 Bluetooth

Section 2.1 gives a brief description of Bluetooth technology. An overview of Bluetooth security is provided in Section 2.2. A more detailed description of Bluetooth technology and its security can be found in [1, 4, 5, 6, 7, 8].

2.1 Overview of Bluetooth technology

Bluetooth SIG (Bluetooth Special Interest Group) [9] was founded in 1998. It develops Bluetooth technology and brings new devices to the market. Bluetooth 1.0 specification was released in 1999. The latest specification, Bluetooth 2.0+EDR (Enhanced Data Rate), was released in 2004. Bluetooth SIG has currently over 6000 members.

Bluetooth is a technology for short range wireless data and realtime two-way voice transfer providing data rates up to 3 Mb/s. It operates at 2.4 GHz frequency in the free ISM-band (Industrial, Scientific, and Medical) using frequency hopping. Bluetooth can be used to connect almost any kind of device to another device. Typical range of Bluetooth communication varies from 10 to 100 meters indoors.

Bluetooth devices that communicate with each other form a *piconet*. The device that initiates a connection is the piconet master. One piconet can have maximum of seven active slave devices and one master device. All communication within a piconet goes through the piconet master. Two or more piconets together form a *scatternet*, which can be used to eliminate Bluetooth range restrictions as Figure 1 illustrates. Scatternet environment requires, that different piconets must have a common device (so-called *scatternet member*) to relay data between the piconets.

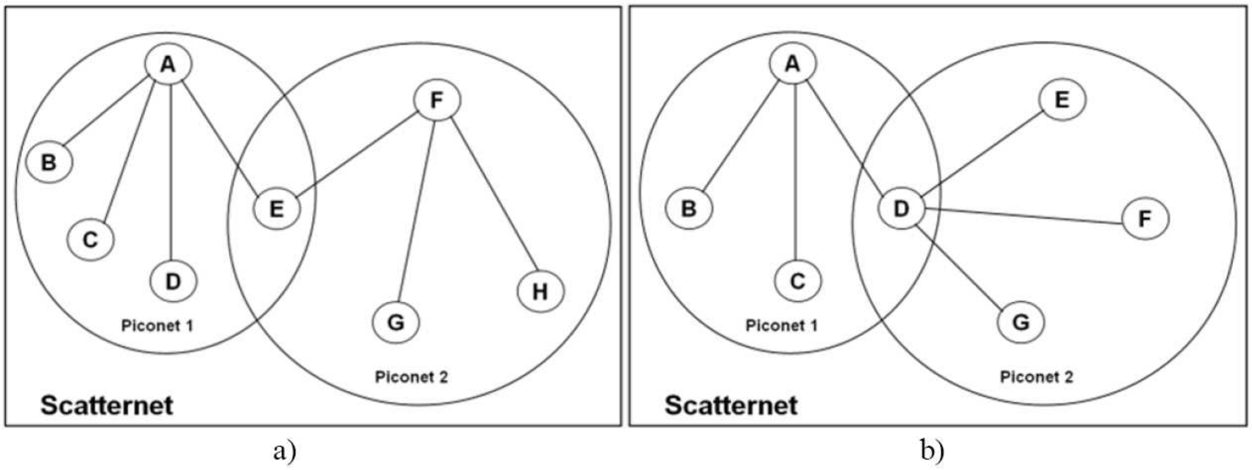

Figure 1: a) Bluetooth topology when data links are used. b) Bluetooth topology when realtime two-way voice links are used.

When data links are used (Figure 1a), the scatternet member is the slave for both piconets. Device A is the master for piconet 1, and devices B, C, D and E are equal slaves for that piconet. Device F is master for piconet 2, and devices E, G and H are equal slaves for that piconet. Piconets 1 and 2 together form a scatternet. Piconets 1 and 2 are not synchronized with each other and the scatternet member must multiplex between these two piconets.

When realtime two-way voice links are used (Figure 1b), the scatternet member must be slave for piconet 1 and master for piconet 2. If, for example, master A's clock runs at slightly slower rate than the clock of the common device D, master A's timeslots are drifting slowly to the right. To avoid an eventual overlap of timeslots, the common device D must periodically delay the exchange of voice packets by a pair of timeslots. Device A is the master for piconet 1, and devices B, C and D are equal slaves for that piconet. Device D is master for piconet 2, and devices E, F and G are equal slaves for that piconet. Piconets 1 and 2 together form a scatternet.

2.2 Overview of Bluetooth security

Security begins when a user decides how a Bluetooth device will implement its connectability and discoverability options. The different combinations of connectability and discoverability capabilities can be divided into three categories, or *security levels*:

- *Silent*: The device will never accept any connections. It simply monitors Bluetooth traffic.

- *Private*: The device can not be discovered (so-called *non-discoverable device*). Connections will be accepted only if the device's *BD_ADDR (Bluetooth Device Address)* is known to the prospective master.

- *Public*: The device can be both discovered and connected to (so-called *discoverable device*).

There are also three different *security modes* that a device can implement. A device can be only in one security mode at a time:

1. *Nonsecure*: Bluetooth device does not initiate any security measures.

2. *Service-level enforced* security mode: Two Bluetooth devices can establish a nonsecure Asynchronous Connection-Less (ACL) link. Security procedures, namely authentication, authorization and optional encryption, are initiated when a L2CAP (Logical Link Control and Adaptation Protocol) Connection-Oriented or Connection-Less channel request is made.

3. *Link-level enforced* security mode: Security procedures are initiated when an ACL link is established.

Security within Bluetooth technology covers three major areas: authentication, authorization and encryption. *Authentication* is used for proving the identity of one piconet member to another. The results of authentication are used for determining the client's *authorization level. Encryption* is used for encoding the information being exchanged between Bluetooth devices in the way that eavesdroppers can not read its contents. Bluetooth security is based on building a chain of events, none of which provides meaningful information to an eavesdropper, and all events must occur in a specific sequence for security to be set up successfully. Two Bluetooth devices begin their communication with the same PIN (Personal Identification Number) code that is used for generating several 128-bit keys as illustrated in Figure 2. Each master-slave pair can have a different PIN code for providing trusted relationship between the devices.

An *initialization key* is generated when Bluetooth devices meet for the first time, and is used for securing the generation of other more secure 128-bit keys which are generated during the next phases of the security chain of events. An initialization key is derived from an unencrypted 128-bit random number IN_RAND, an L-byte ($1 \leq L \leq 16$) PIN code, and a BD_ADDR. If one device has a fixed PIN code, the BD_ADDR of the another device is used. If both devices can support a variable PIN code, the BD_ADDR of the device that received IN_RAND is used. The initialization key is used for encrypting a 128-bit random number LK_RAND exchanged in the next phase when a link, or a combination key, is generated.

A *combination key* is always dependent on two devices and therefore derived from information of both devices (BD_ADDR$_A$, LK_RAND$_A$, BD_ADDR$_B$, LK_RAND$_B$). It is used in the next phase for challenge-response authentication in which a claimant's knowledge of a secret link key is checked. During each authentication, a new 128-bit unencrypted random number AU_RAND is exchanged. The claimant returns a 32-bit result (*SRES, Signed Response*) to the verifier. The verifier also calculates the same SRES value and compares it to the received SRES. If the SRES values match, the authentication is completed successfully and a 96-bit result (*ACO, Authenticated Ciphering Offset*) is computed in both devices. An ACO, a link key and an unencrypted 128-bit random number EN_RAND are used for

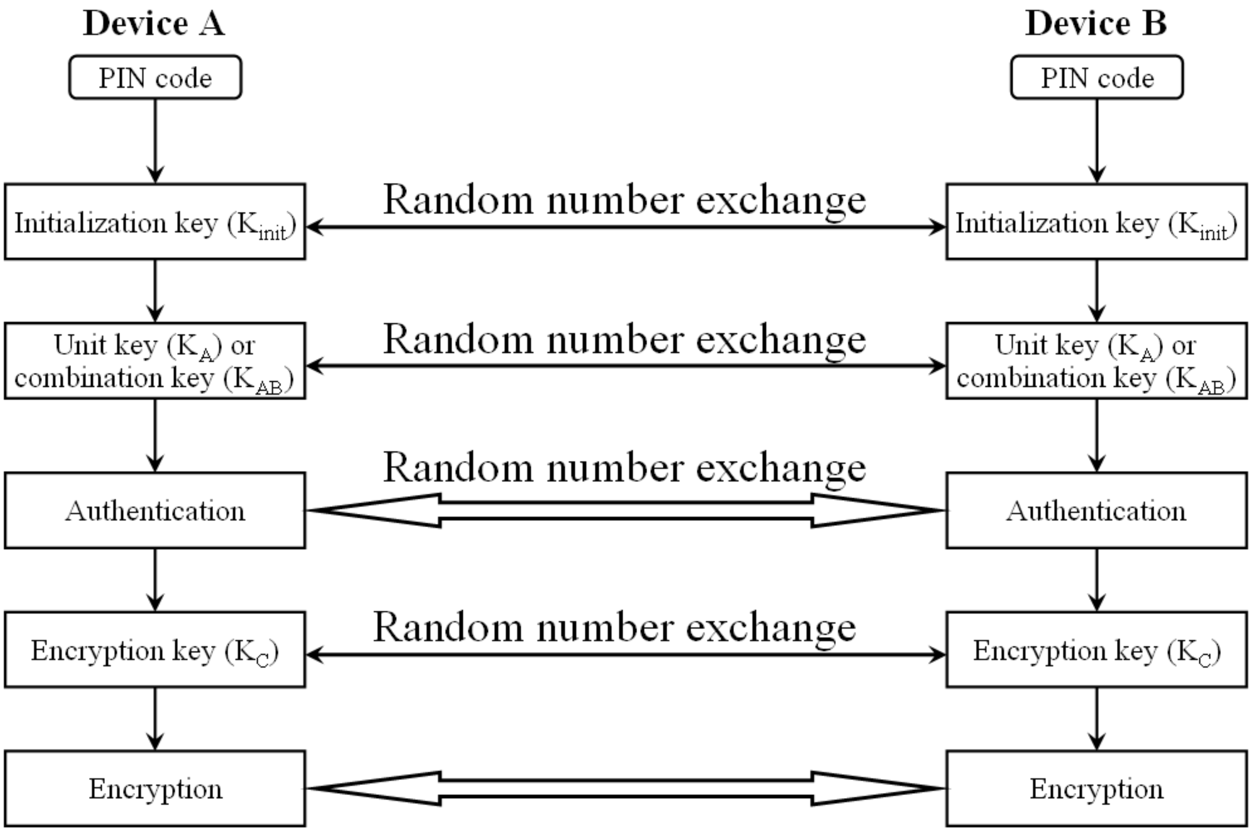

Figure 2: Summary of Bluetooth security operations [1, 5]

generating *an encryption key*, which is one input to the keystream generator that generates the keystream and makes symmetric encryption possible. Other inputs to the keystream generator are master's BD_ADDR and 26 bits of the master's real-time clock.

Application layer key exchange and encryption methods can also be used to secure communication on top of the existing Bluetooth security measures.

Bluetooth security has remained almost unchanged since the first Bluetooth 1.0 specification was released 1999. Next major security improvements are roadmapped to two upcoming Bluetooth specifications, which are expected to be released by Bluetooth SIG in 2007 and in 2008.

3 WLAN

Section 3.1 gives a brief description of WLAN technology. An overview of WLAN security is provided in Section 3.2. A more detailed description of WLAN technology and its security can be found in [2].

3.1 Overview of WLAN technology

IEEE (Institute of Electrical and Electronics Engineers) [10] is a non-profit, technical professional association of more than 365000 individual members in over 150 countries. IEEE has released several significant standards for wired and wireless local area networks such as Ethernet (IEEE 802.3) [11] and WLAN (IEEE 802.11).

WLAN is a technology for wireless data transfer providing data rates up to 54 Mb/s. It operates at 2.4 GHz (IEEE 802.11b and IEEE 802.11g) or 5 GHz (IEEE 802.11a) frequency in the free ISM-band and needs APs (Access Points) for collecting and relaying data between network segments. WLAN is intended to replace or complement traditional wired local area networks. Typical range of WLAN communication varies from 20 to 100 meters indoors.

A WLAN network can operate in *ad-hoc mode* (so-called *station-to-station mode*) or in *infrastructure mode* (so-called *station-to-AP mode*). An area where WLAN stations of ad-hoc type network can directly communicate with each other without AP, is called *BSS (Basic Service Set)*. Figure 3 illustrates an example of a typical BSS. WLAN station A can communicate with B, and vice versa. B can also communicate with C and D. A can not communicate with C and D, and vice versa. A and B can communicate with each other, because they form BSS1 (i.e. they are in each other's range). B, C and D can also communicate with each other in BSS2. All four WLAN stations (A, B, C and D) can not communicate with each other, because they are not in the same BSS.

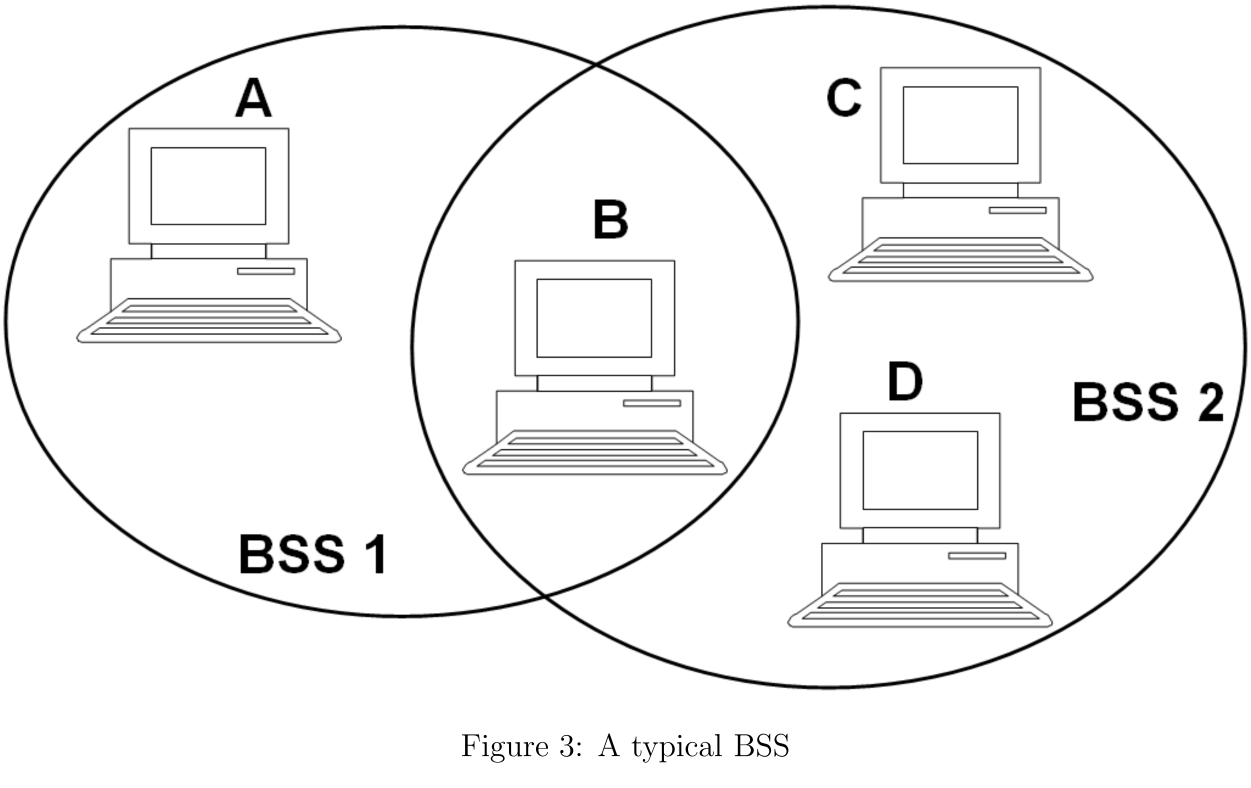

Figure 3: A typical BSS

An AP can combine several BSSs by creating a *DS (Distribution System)*. A BSS that has not been connected to a DS, is called an *IBSS (Independent BSS)*. An AP can also combine wired LANs (Local Area Networks) to a DS by using a feature called *portal*. A portal is a logical point in which data goes from a wired LAN to a WLAN and vice versa. Figure 4 illustrates how several BSSs and a wired LAN can be combined together by using an AP. This combining process is called a *DSS (Distribution System Service)*. When an AP is used to combine one or more BSSs via a DS, and one or more wired LAN, the resulting network is called an *ESS (Extended Service Set)*.

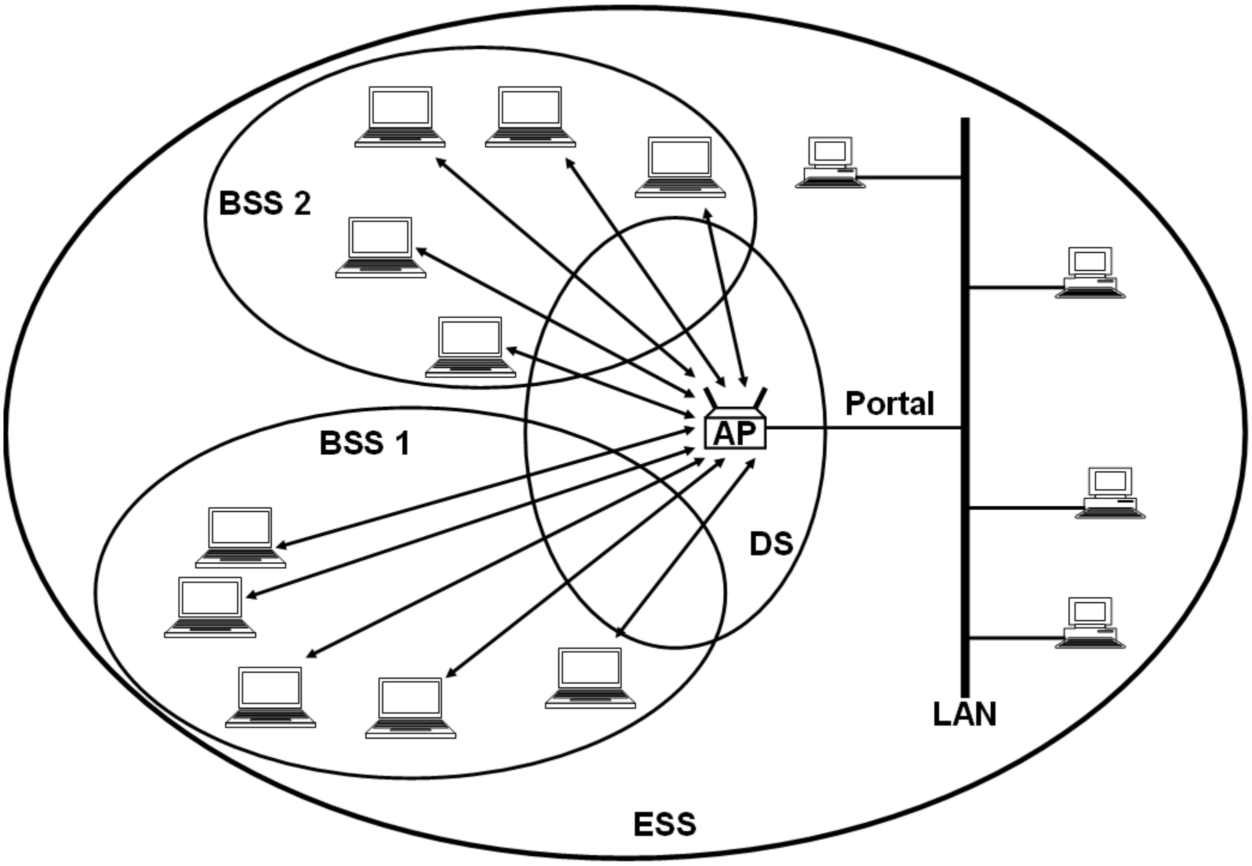

Figure 4: A typical ESS

3.2 Overview of WLAN security

Old versions of WLAN (IEEE 802.11 and IEEE 802.11b) introduced WEP (Wired Equivalent Privacy) for encrypting information being exchanged via air. MAC (Medium Access Control) filtering can also be used to prevent unauthorized WLAN devices from accessing the WLAN network. Unfortunately both of these security features can be quite easily bypassed by an attacker. First, WEP encryption leaks information little by little. An average of two hours eavesdropping on WEP encrypted WLAN communication is enough to crack the cipher [12]. Second, WLAN network adapter's physical MAC address is quite easy to clone, so MAC filtering provides only a primitive protection against attackers.

New versions of WLAN (IEEE 802.11a and IEEE 802.11g) introduced WPA (Wi-Fi Protected Access) [13] for correcting all known WEP weaknesses. WPA offers an *Enterprise mode* and a *PSK (Pre-Shared Key) mode*, so it is suitable for homes, small companies and large enterprises. The Enterprise mode requires an authentication server (RADIUS, Remote Authentication Dial-In User Service), which is used for authentication and key delivery. The PSK mode does not require an authentication server. A shared secret key is used for connecting to an AP when authentication is also performed.

WPA is a part of IEEE 802.11i standard [2], and it is supported in almost all new WLAN devices on the market. WPA2 (Wi-Fi Protected Access 2) [13] is the latest version of WPA, which is also a part of IEEE 802.11i standard. WPA2 provides stronger encryption than WPA by using the AES (Advanced Encryption Standard) algorithm. On the other hand, it requires more processing power than WPA. Almost all new WLAN devices on the market also support WPA2. Both the Enterprise mode and the PSK mode are supported in WPA2, so the main difference between WPA and WPA2 is in the encryption: WPA2 uses AES with 128-bit encryption keys, while WPA uses a modified RC4 (Ron's Code 4) algorithm in which the RC4 encryption engine is divided into four new algorithms.

Although WPA and WPA2 correct all known WEP weaknesses, they are vulnerable to DoS (Denial-of-Service) attacks. This is due to the way WPA and WPA2 recover from an attack. When WPA/WPA2 discovers an attack, it shuts down the whole WLAN segment for a minute, so the legitimate WLAN users of that segment are also without network connection and services! This kind of DoS vulnerability is very serious, because an attacker can perform such an attack by sending only a few packets every two minutes. Moreover, it is very difficult to trace such an attacker who is sending only few packets seldom.

A main principle for protecting a wired LAN against attackers that are abusing a WLAN is to treat a WLAN as a separate network from a wired LAN, i.e. a WLAN should function in a role of WDMZ (Wireless Demilitarized Zone). A WDMZ must provide strong security between a wired LAN and the rest of the world. The easiest way for building a WDMZ is to connect all WLAN APs together and after that placing a NAS (Network Access Server) between a WDMZ and a wired LAN as Figure 5 illustrates. Every WDMZ should have its own DHCP (Dynamic Host Configuration Protocol) server for allocating IP (Internet Protocol) addresses to connecting users. If there are a very large number of WLAN workstations, there can be several WDMZs.

4 IrDA

Section 4.1 gives a brief description of IrDA technology. An overview of IrDA security is provided in Section 4.2.

4.1 Overview of IrDA technology

The Infrared Data Association (IrDA) is a nonprofit organization whose goal is to develop specifications for infrared wireless communication. IrDA was founded in 1993 and it has

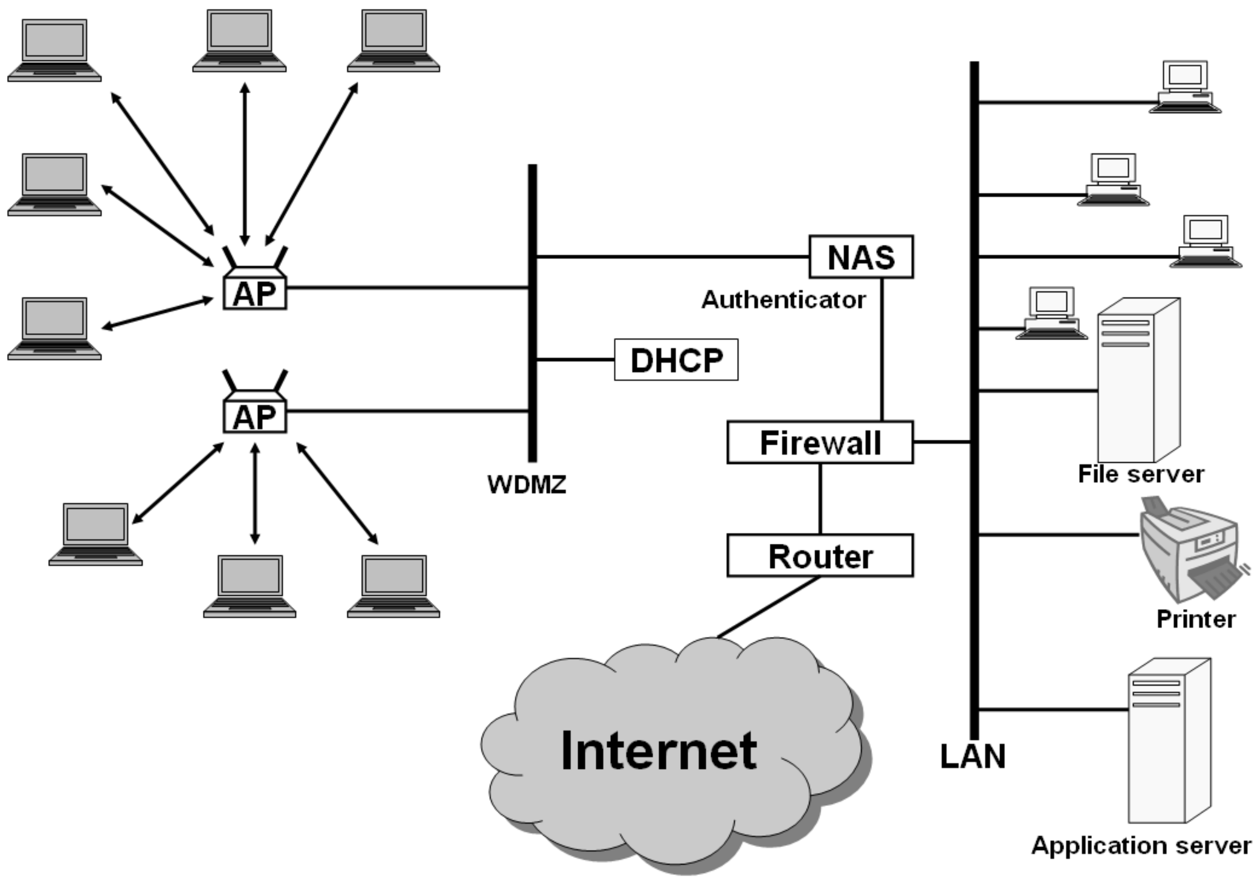

Figure 5: A typical WDMZ configuration

currently over 200 members.

The IrDA 1.0 specification was released in 1994. It was designed for cheap and realiable short range wireless communication providing data rates up to 115.2 kb/s (so-called basic rate). IrDA 1.0 specification included SIR (Serial Infrared) link, IrLAP (Infrared Link Access Protocol), and IrLMP (Infrared Link Management Protocol). The SIR standard was updated to FIR (Fast Infrared) in 1995 for supporting data rates up to 4 Mb/s. IrOBEX (Infrared Object Exchange Protocol) was released in 1997 as a compact, efficient, binary protocol that enables a wide range of devices to exchange data in a simple and spontaneous manner. It has been adopted by other data transfer technologies such as Bluetooth.

IrDA released the IrTran-P (Infrared Picture Transfer) standard in 1997 for image exchange used in digital image capture devices and cameras. IrMC (Infrared Mobile Communications), a new standard for interoperability between mobile communication devices, was also released in 1997. IrDA released IrDA Control, a new standard for cordless human input devices such as mice, keyboards, joysticks and gamepads, in 1998. AIrMAC (Advanced Infrared Medium Access Control) standard was released in 1999 for supporting Advanced Infrared Wireless Office. VFIR (Very Fast Infrared), a 16 Mb/s speed extension to the IrDA standard was also released in 1999. A 100 Mb/s version of IrDA is currently under development. A more detailed description of IrDA technology can be found in [3].

4.2 Overview of IrDA security

IrDA does not provide any link-level security, so there is no authentication or authorization, and all information is sent unencrypted. If authentication/authorization/encryption is needed, it has to be implemented at software level.

IrDA supports only Point-to-Point connections, and requires direct line-of-sight between two IrDA devices as Figure 6 illustrates. In addition, typical range of IrDA communication is only up to 2 meters. So, in spite of lacking support for explicit security measures, IrDA can be considered as a relatively secure technology. On the other hand, IrDA lacks the convenience of wireless RF technologies such as Bluetooth and WLAN.

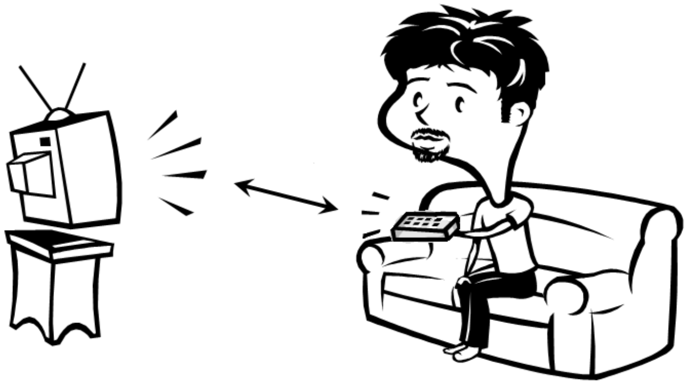

Figure 6: A typical IrDA Point-to-Point connection

In spite of IrDA's limited communication range, it is possible (at least in theory) to eavesdrop on a communication by detecting reflected infrared-light and filtering out the surrounding ambient noise. A more detailed description of IrDA security can be found in [3, 14, 15, 16, 17, 18, 19].

5 Comparison

Because Bluetooth and WLAN are wireless RF communication systems using mainly omnidirectional antennas, there is always a great possibility that their transmissions could be jammed, deliberately intercepted, or false/altered information would be passed to the network members. IrDA has no such security problems, because it requires direct line-of-sight between two IrDA devices and the typical range of IrDA communication is only up to 2 meters.

Old WLAN versions (IEEE 802.11 and IEEE 802.11b) using WEP are insecure compared to Bluetooth. New WLAN versions (IEEE 802.11a and IEEE 802.11g) using WPA/WPA2 provide as strong security as Bluetooth, if the DoS vulnerability of WPA/WPA2 is excluded.

Table 1 summarizes the main differences between Bluetooth, WLAN and IrDA technologies and their security.

Table 1: The main differences between Bluetooth, WLAN and IrDA technologies and their security

	Bluetooth:	**WLAN**:	**IrDA**:
Communications medium	RF waves	RF waves	Infrared light
Typical range (indoors)	10 - 100 meters	20 - 100 meters	0 - 2 meters
Size of network	2 - 8 devices	Dozens of devices	Two devices
Direct line-of-sight requirement	No	No	Yes
Maximum data rate	3 Mb/s	54 Mb/s	16 Mb/s
Realtime two-way voice links	Yes	No	No
Power consumption	Low	High	Very low
Component cost	Low ($\approx$ \$4)	High ($\approx$ \$15)	Very low ($\approx$ \$1)
Tolerance to third-party interference	Good	Bad	Excellent
Authentication, authorization and encryption	Yes	Yes	No
Shipments in 2005 (million units)	$\approx$ 300	$\approx$ 200	$\approx$ 500

6 Conclusion

A comparison between Bluetooth security, WLAN security, and IrDA security was described in the report. The purpose of this report is to connect security issues in a larger context by providing the comparison between three popular wireless communication technologies.

References

[1] Bluetooth SIG, *Bluetooth specifications 1.0, 1.1, 1.2 and 2.0+EDR.* Bluetooth SIG, technical specifications, 1999-2004. https://www.bluetooth.org

[2] IEEE Standards Association, *IEEE 802.11 specifications.* IEEE Standards Association, technical specifications, 1999-2004. http://standards.ieee.org/getieee802/802.11.html

[3] Infrared Data Association, *IrDA specifications.* Infrared Data Association, technical specifications, 1993-2005. http://www.irda.org

[4] Keijo M.J. Haataja, *Evaluation of the Current State of Bluetooth Security.* Licentiate Thesis, University of Kuopio, Department of Computer Science, Finland, January 2007.

[5] Keijo M.J. Haataja, *Bluetooth Security Threats and Possible Countermeasures.* Proceedings of the Annual Finnish Data Processing Week at the University of Petrozavodsk (FDPW'2004), Advances in Methods of Modern Information Technology, vol. 6, Petrozavodsk, 2005, pp. 116-150.

[6] Keijo M.J. Haataja, *Bluetooth Network Vulnerability to Disclosure, Integrity and Denial-of-Service Attacks.* Proceedings of the Annual Finnish Data Processing Week at the University of Petrozavodsk (FDPW'2005), Advances in Methods of Modern Information Technology, vol. 7, Petrozavodsk, 2006, pp. 63-103.

[7] Keijo M.J. Haataja, *Two Practical Attacks Against Bluetooth Security Using New Enhanced Implementations of Security Analysis Tools.* Proceedings of the IASTED International Conference on Communication, Network and Information Security (CNIS 2005), Phoenix, Arizona, USA, November 14-16, 2005, pp. 13-18.

[8] Keijo M.J. Haataja, *Detailed Descriptions of New Proof-of-concept Bluetooth Security Analysis Tools And New Security Attacks.* University of Kuopio, research report, 2005.

[9] Bluetooth SIG, *The Official Bluetooth Membership Site – About the SIG.* Bluetooth SIG, homepage, 2005. https://www.bluetooth.org/foundry/sitecontent/document/About_the_SIG

[10] IEEE, *The Official IEEE Website.* IEEE, homepage, 2005. http://www.ieee.org

[11] IEEE Standards Association, *IEEE 802.3 specifications.* IEEE Standards Association, technical specifications, 2000-2004. http://standards.ieee.org/getieee802/802.3.html

[12] Adam Stubblefield, John Ioannidis and Aviel D. Rubin, *A Key Recovery Attack on the 802.11b Wired Equivalent Privacy Protocol (WEP).* ACM Transactions on Information and System Security, Vol. 7, No. 2, May 2004, pp. 319-332.

[13] Wi-Fi Alliance, *WPA2 – Wi-Fi Protected Access 2.* Wi-Fi Alliance, homepage, 2005. http://www.weca.net/OpenSection/protected_access.asp

[14] William Ottaway, *Mobile Security: Cause for Concern?* QinetiQ Ltd., white paper, 2002. http://www.qinetiq.com/home_ep/insight/insight_archive_nov_2003/mobile_security_cause_for_concern.SupportingPar.0001.File.pdf

[15] Igor Sedov, Marc Haase, Clemens Cap and Dirk Timmermann, *Hardware Security Concept for Spontaneous Network Integration of Mobile Devices.* Proceedings of the International Workshop on Innovative Internet Computing Systems 2001 (IICS'01), 2001, pp. 175-182.

[16] Enrique Soriano Salvador, *SHAD: A Human Centered Security Architecture for Partitionable, Dynamic and Heterogeneous Distributed Systems.* Proceedings of the 1st international doctoral symposium on Middleware, 2004, pp. 294-298.

[17] Dave Piscitello, *IPComm2004 – Mobile user security.* MediaLive International & Core Competence Inc., Wellesley Information Services, 2004. http://hhi.corecom.com/IPcomm2004-MobileUserSecurity.pdf

[18] Dave Suvak, *IrDA and Bluetooth: A Complementary Comparison.* Extended Systems Inc., 2000. http://resolution.extendedsystems.com/NR/rdonlyres/edi2szgu55nmm6nixyjup2r2o543iftppisugjjfwd3bwowucygynpwzu5i43kvhkwo6xc2yaxhswvm4gavq4vkuodf/ir_bt_compare.pdf

[19] John Earley, *Infrared meets speed and security needs.* Reed Business Information Limited, newscopy, 2005. http://www.computerweekly.com/Articles/2005/05/26/210170/Infraredmeetsspeedandsecurityneeds.htm