International Journal of Advances in Scientific Research
ISSN: 2395-3616 (Online)
Journal DOI: 10.7439/ijasr
Short Communication

Bluetooth SIG oversees development of the specification and prediction of program that protects Bluetooth pin

Jyoti Dadwal and Bhubneshwar Sharma*

Department of Electronics and Communication Engineering, S.S.C.E.T, under Punjab Technical University, India

***Correspondence Info:**
Er. Bhubneshwar Sharma
Assistant Professor,
Department of Electronics and Communication Engineering,
S.S.C.E.T, under Punjab technical university, India
E-mail: bhubnesh86@gmail.com

Abstract

Bluetooth implements confidentiality, authentication and key derivation with custom algorithms based on the SAFER+ block cipher. Bluetooth key generation is generally based on a Bluetooth PIN, which must be entered into both devices. This procedure might be modified if one of the devices has a fixed PIN (e.g., for headsets or similar devices with a restricted user interface). During pairing, an initialization key or master key is generated, using the E22 algorithm. The E0 stream cipher is used for encrypting packets, granting confidentiality, and is based on a shared cryptographic secret, namely a previously generated link key or master key. Those keys, used for subsequent encryption of data sent via the air interface, rely on the Bluetooth PIN, which has been entered into one or both devices.

Keywords: Bluetooth PIN, fixed PIN.

1. Introduction

BlueZ is the Bluetooth stack for Linux kernel-based family of operating systems. Its goal is to program an implementation of the Bluetooth wireless standards specifications for Linux. As of 2006, the BlueZ stack supports all core Bluetooth protocols and layers. It was initially developed by Qualcomm, and is available for Linux kernel versions 2.4.6 and up. In addition to the basic stack, the bluez-utils and bluez-firmware packages contain low level utilities such as dfutool which can interrogate the Bluetooth adapter chipset to determine whether its firmware can be upgraded. The People's Liberation Army of China has ordered soldiers not to use personal wearable electronics because of concerns about cyber-security loopholes. Security researchers have documented some Bluetooth LE devices transmitting a unique device identifier that can be used to track people carrying the device without their knowledge. Many devices don't implement encryption or authentication that is provided for the protocol, despite this creating privacy risks.

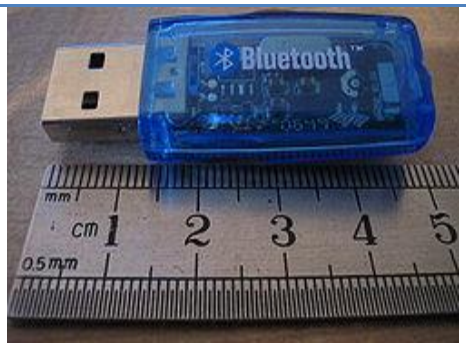

Figure 1: Bluetooth device development

An overview of Bluetooth vulnerabilities exploits was published in 2007 by Andreas Becker. In September 2008, the National Institute of Standards and Technology (NIST) published a Guide to Bluetooth Security as a reference for organizations. It describes Bluetooth security capabilities and how to secure Bluetooth technologies effectively. While Bluetooth has its benefits, it is susceptible to denial-of-service attacks, eavesdropping, man-in-the-middle attacks, message modification, and resource misappropriation.

Users and organizations must evaluate their acceptable level of risk and incorporate security into the lifecycle of Bluetooth devices. To help mitigate risks, included in the NIST document are security checklists with guidelines and recommendations for creating and maintaining secure Bluetooth piconets, headsets, and smart card readers. Bluetooth v2.1 – finalized in 2007 with consumer devices first appearing in 2009 – makes significant changes to Bluetooth's security, including pairing. See the pairing section for more about these changes.

Stream ciphers are vulnerable to attack if the same key is used twice (depth of two) or more. Say we send messages A and B of the same length, both encrypted using same key, K. The stream cipher produces a string of bits C (K) the same length as the messages.

The encrypted versions of the messages then are:

E (A) = A xor C

E (B) = B xor C

Where xor is performed bit by bit.

Say an adversary has intercepted E (A) and E (B). He can easily compute:

E (A) xor E (B)

However, xor is commutative and has the property that X xor X = 0 (self-inverse) so:

E (A) xor E (B) = (A xor C) xor (B xor C) = A xor B xor C xor C = A xor B

2. Bluetooth V4.2

Bluetooth v4.2 was released on December 2, 2014. It introduces some key features for IoT. Some features, such as Data Length Extension, require a hardware update. But some older Bluetooth hardware may receive some Bluetooth v4.2 features, such as privacy updates via firmware.

The major areas of improvement are:

LE Data Packet Length Extension

LE Secure Connections

Link Layer Privacy

Link Layer Extended Scanner Filter Policies

IP connectivity for Bluetooth Smart devices to become available soon after the introduction of BT v4.2 via the new Internet Protocol Support Profile (IPSP).

IPSP adds an IPv6 connection option for Bluetooth Smart, to support connected home and other IoT implementations.

3. Conclusions

Bluetooth is managed by the Bluetooth Special Interest Group (SIG), which has more than 25,000 member companies in the areas of telecommunication, computing, networking, and consumer electronics. The IEEE standardized Bluetooth as IEEE 802.15.1, but no longer maintains the standard. The Bluetooth SIG oversees development of the specification, manages the qualification program, and protects the trademarks. A manufacturer must make a device meet Bluetooth SIG standards to market it as a Bluetooth device. Networks of patents apply to the technology, which are licensed to individual qualifying devices.

References

[1] Marsh, Jennifer. "Bluetooth Hacking – Understanding Risks". Retrieved 26 April 2015.

[2] Elaina Chai, Ben Deardorff, and Cathy Wu. "Hacking Bluetooth" (PDF). Retrieved 26 April 2015.

[3] M. Hietanen, T. Alanko (October 2005). "Occupational Exposure Related to Radiofrequency Fields from Wireless Communication Systems" (PDF). XXVIIIth General Assembly of URSI – Proceedings. Union Radio-Scientifique International. Archived from the original (PDF) on 6 October 2006. Retrieved 19 April 2007.

[4] USB 3.0* Radio Frequency Interference Impact on 2.4 GHz Wireless Devices (PDF)

[5] A guide to resolving Bluetooth and USB 3.0 interference issues

[6] "Bluetooth Innovation World Cup". Bluetooth.com. Retrieved 4 September 2010.