Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Bluetooth Command and Control channel

Heloise Pieterse [a,*], Martin S. Olivier [b]

[a] Defence, Peace, Safety and Security Unit, Council of Scientific and Industrial Research, PO Box 395, Pretoria 0001, South Africa
[b] Department of Computer Science, University of Pretoria, Private Bag X20, Hatfield 0028, South Africa

ARTICLE INFO

Article history:
Received 8 November 2013
Received in revised form
10 April 2014
Accepted 25 May 2014
Available online 6 June 2014

Keywords:
Mobile
Applications
Command and Control
Bluetooth
Android
Malware

ABSTRACT

Bluetooth is popular technology for short-range communications and is incorporated in mobile devices such as smartphones, tablet computers and laptops. Vulnerabilities associated with Bluetooth technology led to improved security measures surrounding Bluetooth connections. Besides the improvement in security features, Bluetooth technology is still plagued by vulnerability exploits. This paper explores the development of a physical Bluetooth C&C channel, moving beyond previous research that mostly relied on simulations. In order to develop a physical channel, certain requirements must be fulfilled and specific aspects regarding Bluetooth technology must be taken into consideration. To measure performance, the newly designed Bluetooth C&C channel is executed in a controlled environment using the Android operating system as a development platform. The results show that a physical Bluetooth C&C channel is indeed possible and the paper concludes by identifying potential strengths and weaknesses of the new channel.

1. Introduction

Bluetooth is a radio frequency technology using the unlicensed 2.5 GHz industrial, scientific and medical (ISM) band (Sairam et al., 2002) It is an open standard for wireless connectivity, mostly found in mobile devices (smartphones, tablet computers, laptops) to enable short-range communications and replaces proprietary cables. The aim and purpose of Bluetooth technology is to offer universal low cost and user friendly communication. Since the earlier developments of Bluetooth technology, vulnerability exploits have plagued this technology. Well-known vulnerabilities include eavesdropping and impersonation, both which led to various attacks such as Denial of Service (DoS), relay attacks and the creation of Backdoors (Potter, 2004). These vulnerabilities led to the need to improve Bluetooth security by including techniques such as authorisation, authentication and encryption (Sun et al., 2001). Besides the security improvements, Bluetooth technology is still being exploited.

Vulnerabilities in Bluetooth technology allow for the development of Bluetooth Command and Control (C&C) channels. A Bluetooth C&C channel is a communication channel responsible for delivery data across a Bluetooth connection between two Bluetooth-enabled devices. Such a channel can allow for faster communication by automating the authentication and authorisation process. Thus, when two devices come within range, a bond will be created between the devices and data transfer can begin without requiring any user involvement. This is ideal for devices that must quickly share information when coming within range, such as mobile botnets. Previous research by Singh et al. (2010)

* *Corresponding author*. Tel.: +27 12 841 2110.
E-mail addresses: hpieterse@csir.co.za (H. Pieterse), molivier@cs.up.ac.za (M.S. Olivier).

http://dx.doi.org/10.1016/j.cose.2014.05.007
0167-4048/© 2014 Elsevier Ltd. All rights reserved.

and Hua and Sakurai (2012) explored the potential of Bluetooth C&C channels but relied on simulations when constructing the C&C channels. This paper explores the development of a physical Bluetooth C&C channel, moving beyond previous research that relied on simulations.

In order to develop a physical Bluetooth C&C channel certain requirements must be fulfilled and specific aspects regarding Bluetooth technology must be taken into consideration. There will be a focus on eliminating user involvement and automating authentication processes such as the pairing process. To measure performance of the newly designed C&C channel, execution takes place in a controlled environment by using the Android operating system (OS) as the development platform. To verify that communication is indeed taking place across the Bluetooth C&C channel, the Bluetooth packets are captured by using the Ubertooth One tool and are viewed in Wireshark. The results show that a physical Bluetooth C&C channel is constructed and capable of supporting communication.

The rest of the paper is structured as follows. Section 2 gives an overview of research relating to the development of Bluetooth C&C channels. Section 3 provides a brief introduction of Bluetooth technology, focussing on the history, pairing process and vulnerabilities of Bluetooth. Section 4 describes the requirements necessary for the development of a physical Bluetooth C&C channel. Section 5 provides a description of the development and initialisation of the Bluetooth C&C channel while Section 6 focuses on the communication and execution of the channel. Section 7 provides a discussion on the potential strengths and weaknesses, and Section 8 concludes the paper.

2. Related research

Few articles describe the development of Bluetooth C&C channels. Singh et al. (2010) evaluated the suitability of Bluetooth as a possible C&C channel in the design of a mobile botnet. With the Bluetooth C&C structure, each mobile bot acts as a peer in the mobile botnet, listening for new commands and forwarding the commands to the other discovered bots. During the initial infection, the mobile bots registers a Universal Unique Identifier (UUID) in the service register present in the mobile device. This allows the mobile bot to be discovered by the other bots as they come within range. The mobile bot then waits for new incoming connections and when such a connection arrives the mobile bot establishes a two-way Bluetooth connection to allow communication to occur. An advantage of this Bluetooth C&C is that it prevents a defender from easily taking down the mobile botnet since the defender needs to be in range of the mobile bots when communication takes place. This may not always be possible due to the changing topology of the network (Singh et al., 2010).

Hua and Sakurai (2012) focused on designing two separate mobile botnets using Short Message Service (SMS) messages and Bluetooth technology for command propagation. The SMS-based mobile botnet uses SMS messages to propagate the C&C messages by using a simple flooding algorithm. The proximity-based mobile botnet uses Bluetooth to forward the C&C messages and form the communication channel around seed nodes, which are selected based on their contact frequency with other infected nodes. When the number of contacted nodes within a specific time period exceeds a threshold, the device will recommend itself for the seed role. These nodes encounter other devices more frequently, allowing for quicker dissemination of commands. After multiple simulations, the authors proved that a uniform random graph is the most efficient topology for the SMS-based mobile botnet and that human mobility features can improve the command propagation of proximity-based mobile botnets (Hua and Sakurai, 2012).

The proposed Bluetooth C&C channels by Singh et al. (2010) and Hua and Sakurai (2012) only used simulations and neither constructed a physical Bluetooth C&C channel to determine the feasibility of such a channel. Simulations were used due to the multiple technical difficulties and overhead associated with the construction of a physical Bluetooth C&C channel. Firstly, direct interaction with the Bluetooth adapter build into the device has been severely limited by previous technology. Secondly, the security features used by the Bluetooth technology cause research relating to the development of a Bluetooth C&C channel to be cumbersome and time-consuming. Lastly, acquiring an adequate number of mobile devices can be problematic due to the cost associated with these devices.

The arrival of smartphones early in the 21st century provides new opportunities to explore the development of Bluetooth C&C channels.

3. Bluetooth technology

Bluetooth technology was invented in 1994 by L.M. Ericsson (Sairam et al., 2002). During the winter of 1998 Ericsson, Nokia, Intel, IBM and Toshiba further evolved the Bluetooth standard by establishing the Bluetooth Special Industry Group (SIG) (Bisdikian, 2001). The last few years saw 3COM, Microsoft, Lucent and Motorola also started participating in SIG (Sairam et al., 2002). The goal behind SIG is to further improve Bluetooth technology as short-range, low cost and user-friendly connection among portable devices, allowing for ad-hoc connectivity (Bisdikian, 2001). These capabilities are possible due to the architectural design of the Bluetooth technology.

The Bluetooth architecture consists of a protocol stack that is divided, by the Bluetooth specification, into three distinct groups: transport protocol group, middleware protocol group and the application group (McDermott-Wells, 2004). The transport protocol group consists of the following layers: radio, baseband, link manager and the Logical Link Control and Adaptation Protocol (L2CAP) (McDermott-Wells, 2004). These layers allow Bluetooth devices to locate each other while managing the physical and logical links (McDermott-Wells, 2004). The middleware protocol group includes third-party, industry-standard and Bluetooth-SIG protocols, allowing existing and new applications to operate over Bluetooth links (McDermott-Wells, 2004). Some of the protocols found in the middleware protocol group are the Internet Protocol (IP), Transmission Control Protocol (TCP) and serial port emulator (RFCOMM). The application group consists of the actual applications that use the Bluetooth links (McDermott-Wells,