Technical Sciences

UDC 004.056.53

Tykhonov Konstiantyn
Student of the Faculty of Informatics
and Computer Science of the
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"

BLUEBORNE VULNERABILITIES IN BLUETOOTH IMPLEMENTATIONS IN DIFFERENT OPERATION SYSTEMS

Summary. *Ubiquitous adaptation of protocols and technologies for implementations of old solutions in new platform make it more unsecured. That leads to constant change and adaptation. Many solutions aren't revised and insufficiently tested, which is connected to spectrum of systems and devices. It isn't surprising that one of the main and most popular technology stacks - Bluetooth have serious vulnerabilities.*

Key words: *Bluetooth, BlueBorn, Information Security.*

Bluetooth is standard of wireless technology for data exchange at short distances that providing exchange of information between mobile phones, personal computers, printers, earphones etc. Annually world electronics market gets more than 3.6 billion devices supporting Bluetooth technology [1].

Realization of Bluetooth protocols stack can be conditionally divided in two groups:

- For general purpose. Realization are written with the emphasis on functionality and flexibility, more often, for desktop computers.
- For built-in systems. Realization are intended for use in peripheral Bluetooth devices where resources are limited, and requirements are lower.

Security parameters [2]:

1. Bluetooth Addresses;
2. Private Authentication Key;
3. Private decryption key;
4. RAND — pseudo random number generated by device.

This technology is tremendous and sufficiently protected. But the inability to test all implementations of such large technology led to serious problems.

BlueBorne is term uniting a number of vulnerabilities of safety in Bluetooth at Android, iOS, Linux and Windows systems. Vulnerabilities have been found for the first time by Armis, IoT firm of safety, on September 12, 2017. According to Armis, "the vector of BlueBorne attack can potentially affect all devices with Bluetooth opportunities estimated today more than on 8,2 billion devices [3].

A number of problems became a basis for this vector of the attack:

1. SMP (Security Manager Protocol) problem

In Bluetooth basics of communication is principle of association and binding devices by means of their unique identifiers. For gaining access to another device through Bluetooth it is necessary to be authenticated, and after to become authorized. But modern means of protection didn't provide additional check for device without interface (without an opportunity to confirm connection). These devices used default key which is consisted in device memory. And device without interface undergoes all security checks and their security access level is equal to level of device which has passed all protocols of protection with user interface. This vulnerability is partially solved by possibility from one of devices to request protection check against Men-In-the-middle attack, but this check isn't always requested by device, as leads to the vulnerability manifestation [4].

2. L2CAP stack overflow

During creation of new connection participants generate packages - request configuration and response configuration. These packages contain a basic information about future connection and are used for basic configuration.

When fuller connection is required, system uses Pending state. It is blocking until obtaining full answer from the device for making bound. Realization of this feature also became vulnerability as size of received answer isn't controlled, and it is become possible to set size of the buffer for the proceeding answer. This vulnerability allows the overflowing the buffer of 64 bytes in size that will lead to stack overflow exception.

3. Data leak from SDP (Service Discovery Protocol)

SDP allows you to access all services and applications that device supports. This service works with L2CAP. When connection has set, client will response by sending inquiry. If response consist information about MTU, then a part of the answer will be returned, and the subsequent answers will be added to available response. Then same inquiry will be sent again on the server. Main problem of this decision is that the answer isn't standardized and it isn't used by client directly. Due to lack of the uniform standard there was an opportunity to obtain information, outside the buffer of answers [5].

4. BNEP (Bluetooth network encapsulation protocol) stack overflow.

BNEP facilitates network encapsulation via Bluetooth. In most cases, this is used to allow an Internet sharing on Bluetooth [6]. The problem was noticed on last protocol realization in Android OS at the moment when system receiving several control messages in one L2CAP message. The error is hidden in an attempt to read information received in advance, which will result in buffer size being increased. This vulnerability allows overflowing of 8 bytes on the heap following a buffer of any chosen size.

But this isn't the only vulnerability in BNEP implementation. The problem was in the function that handles all control messages. The specification

allows ignoring unrecognized extension messages by receiving side and it tries to skip these messages using the extension length from the extension header.

There are similar actions for selection and configuration of the exploit for all vectors of attack on all operating systems (OS).

Stages of BlueBorn attack:

1. Malefactor finds active Bluetooth connections in visibility range. Activation of the visibility mode isn't obligatory for detection.
2. Malefactor receives MAC address of vulnerable device. One of ways for receiving MAC address - hcitool. This framework will allow obtaining necessary information by hcitool scan command.
3. Malefactor adjusts an exploit and specifying victim's device MAC address.
4. Further vulnerability in implementation of the Bluetooth protocol is used.
5. At this stage actions of hacker depends on the OS type as the vector of the attack changes depending on vulnerability type to which the system is subject use. Selection of an exploit depends on OS, but many actions and settings are similar for all systems that is due similarity of realization of Bluetooth.

As further stages of attack will differ for different vulnerabilities and systems it is necessary to pass to detailed description of these differences.

BlueBorne Attack on Android

1. In case victim uses Android OS, malefactor have four vectors of the attack. At the moment there is a mass of ready decisions which use the found vulnerabilities. Difference of decisions - a programming language. A part of presented exploits - Python scripts, a part realization on C. The original decision from Armis has been written on Python, but for obvious reasons it hasn't been published in open access. Available analogs are

developed on the basis of technical documentation and information provided by Armis and their principles of work is similar. For this analysis it is necessary to neglect insignificant differences in realization as generally all decisions follow the same algorithm, differing only in libraries for realization. Approach when developing of all analyzed exploits is identical and for this reason there is no difference what decisions will be analysis. For communication with Bluetooth L2CAP protocol is used. Further Maximum Transmission Unit is established (maximum volume of data which can be transferred by the protocol for one iteration) [7].

Then there is a connection to in advance defined MAC address. Following stage - sending request to the device. Victims device information will be response to this inquiry that will allow getting further full access over him.

2. Vulnerabilities of CVE-2017-0781 [8] and CVE-2017-0782 [9] are similar in mechanics of breaking and differ in that at what levels interact with service Bluetooth Network Encapsulation Protocol (BNEP). These vulnerabilities allow to get full access to device of the victim.
3. Man-in-The-Middle (MiTM) attack allows to intercept and change, obtain and sent data. Vulnerability exists in a PAN profile (Personal Area Network) Bluetooth stack that allows to create the network interface and redirect data through him.

BlueBorne Attack on Windows

Vulnerability in Windows allows malefactors to carry out Man-in-The-Middle attack. It is similar to vulnerability that was found in Android systems. Connection also happens by means of MAC address. Attack happens according to the similar scenario and allows to substitute obtain and get transferred

information. Identity of the attack is connected to similarities of implementations in different systems.

BlueBorne Attack on Linux

In Linux OS is two vectors of attack which allow malefactors to control completely infected devices.

1. First vulnerability secularly repeats CVE-2017-0785 [10] problem on Android devices and is also connected with SDP. On each inquiry information bit including the ciphered information will reveal.
2. Second — internal defect in L2CAP. Which leads to damage of memory and will allow carrying out a malicious code far off.

BlueBorne Attack on iOS

There is no detailed information on this vulnerability neither in documentation of Armis nor in open sources. Judging from the description vulnerability proves similarly above described. The main difference - a way of influence through the system of voice commands, more precisely her vulnerability.

The vulnerabilities described above are not so complex. And it points to difficulties with implementation of massive protocols as Bluetooth.

Bluetooth implementations have not received the same level of scrutiny and research like other outward-facing protocols. This might be result of Bluetooth's relative complexity.

The lack of testing and analysis led to the emergence of huge direction for attack. This analysis should raise the issue of vulnerability and help in its understanding.

References

1. Abiresearch research about Bluetooth devices market range https://www.abiresearch.com - Retrieved

from https://www.abiresearch.com/market-research/product/1023547-bluetooth/

2. Specification Volume 1: Specification of the Bluetooth System – Core, Version 1.1, February 22, 2001, [Bluetooth_1_1_vol1.pdf] – Retrieved from http://www.bluetooth.org
3. Armis research. Retrieved from - https://www.armis.com/blueborne/
4. Bluetooth Low Energy SMP Pairing. Retrieved from - https://community.nxp.com/thread/332191
5. An Offer/Answer Model with the Session Description Protocol (SDP) June 2002 – Retrieved from https://tools.ietf.org/html/rfc3264
6. Bluetooth Network Encapsulation Protocol (BNEP) Revision 0.95a Specification June 12, 2001, [BNEP.pdf] – Retrieved from http://grouper.ieee.org/groups/802/15/Bluetooth/BNEP.pdf
7. Maximum Transmission Unit (MTU). Мифы и рифы - Retrieved from https://habr.com/post/226807/
8. Complete Vulnerability Database & Security Scanner https://vulners.com Information about vulnerability CVE-2017-0781 - Retrieved from https://vulners.com/cve/CVE-2017-0781
9. Complete Vulnerability Database & Security Scanner https://vulners.com Information about vulnerability CVE-2017-0782 - Retrieved from https://vulners.com/cve/CVE-2017-0782
10. Complete Vulnerability Database & Security Scanner https://vulners.com Information about vulnerability CVE-2017-0782 - Retrieved from https://vulners.com/cve/CVE-2017-0785