Bluetooth vulnerability analysis

Samoilova Yana-Mariia

Odessa National Polytechnic University, Shevchenko Ave 1, Odessa UA-65063, Ukraine, yanamariyas1999@gmail.com

Annotation. *Attacks on personal data everyday become popular among hackers. Bluetooth is a kind of wireless network for file sharing between two devices, characterized by low cost, power, complexity and reliability, is a vulnerability to security protocols as well as user privacy. The purpose of the article is to analyze the shortcomings of Bluetooth security.*

Keywords: *information interception, vulnerability, hacking, Bluetooth, KNOB.*

I. Introduction And Problem Statement

In today's technical world, devices with Bluetooth technology are becoming increasingly popular. Users of gadgets and home appliances transmit a large flow of information every day. The more important and more confidential data, the greater threat of being intercepted by criminals.

Since the establishment of Bluetooth technology, many versions and bug fixes have been improved, but at the same time virus programs too. Bluetooth was developed as a cable replacement technology. This is a short-range radio intended for connecting portable electronic devices. There is a three-tier security control when transmitting data [1], but each system has its disadvantages. There are many applications, subroutines to control connection, such as[2]: MAC spoofing, Cabir Worm, BlueJacking, BlueSmack, BlueSnarfing, BlueBugging, Blueprinting, Blueover, BlueBorne, Fuzzing Attacks, Reflection attack, Backdoor attack, Denial of Service, Man-in-the-Middle/Impersonation Attack, War Nibbling, as well as distributions such as, Kali Linux, or a flash drive – MultiBlue Dongle. But one of the most active attacks that affect basically all devices - KNOB Attacks - is the topic of this article.

II. Problem Solution And Results

KNOB – Key Negotiation of Bluetooth[3]. The attack is possible due to the shortcomings in the Bluetooth specification that acts on the BR / EDR encryption key negotiation protocol. The attack allows a third party, without knowing the communication key or encryption keys, to force victims to match the encryption key only in 8 bits. The attack is hidden because the matching of the encryption key is transparent to Bluetooth users. As a result, the attacker completely breaches the security of Bluetooth BR / EDR by having access to personal data without being detected. Potential consequences may include charges for expensive calls, theft of sensitive information or malware downloads, full control of a connected "smart home" and tracking of user actions in online banking, keystrokes when transferring data between the wireless keyboard and the computer [4].

It was first discovered in 2018 by researchers at Singapore University of Technology and Design, as well as Oxford University's Computer Science Department, as a potential threat to users of any OS. Leading Bluetooth technology researchers was eliminating architectural vulnerabilities throughout the year. "We conducted KNOB attacks on more than 17 unique Bluetooth chips (attacking 24 different devices). … We were able to test the chips from Broadcom, Qualcomm, Apple, Intel and Chicony", says D. Antonioli (Singaporean University of Technology and Design) [5]. The study implemented the decryption of a file that is transmitted through an authenticated and encrypted Bluetooth connection at the link layer. A key with 1 byte of entropy leads to low costs, allowing the attacker to decrypt all encrypted text and enter other encrypted text even in real time. So, as a result, additional logic was plugged into the script to iterate over different CLK values (packets & clock metrics) and offset the E0 key stream. This basic logic only goes through the space of the encryption keys - 256 iterations [3]. Updated version Bluetooth 5.1 was introduced at the end of 2019, and all devices after 2018 that support this extension are safe.

III. Conclusions

The article deals with the dangers of Bluetooth encryption key negotiation protocol, which at first glance cannot pose such a threat, for example, when using headphones. This vulnerability has been skillfully identified and explored.

Developing upgraded versions of wireless communications has overcome data encryption gaps and security of use. The needs to analyze the technology, constantly study it, test it and improve it, are important factors for maintaining the privacy of users and, most importantly, their data.

References

[1] N. Be-Nazir Ibn Minar and M. Tarique, "Bluetooth Security Threats and Solution" A Survey. In International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012.

[2] V. Tsira, G. Nandi, "Bluetooth Technology: Security Issues and Its Prevention" A Survey. In International Journal of Computer Technology and Applications (IJCTA) Vol.5, No.5, October 2014.

[3] D. Antonioli, N. Ole Tippenhauer, K. Rasmussen, "KNOB Attack. Key Negotiation of Bluetooth Attack: Breaking Bluetooth Security.", 28th USENIX Security Symposium, August 2019.

[4] M. Dinney, "McKenzie interchange Project – Travel Time Monitoring System: Technology Review", February 2016.

[5] D. Goodin "New Attack exploiting serious Bluetooth weakness can intercept sensitive data", August 2019.