Information & Security

S. Mechev, E. Staneva & M. Rachev
vol. 47, no. 3 (2020): 300-305
https://doi.org/10.11610/isij.4721

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Cybersecurity Problems and Solutions in Operating Systems of Mobile Communications Devices

Stoyan Mechev (✉), ***Elisaveta Staneva***, ***Mariyan Rachev***

Nikola Vaptsarov Naval Academy, Varna, Bulgaria, http://www.naval-acad.bg/en

ABSTRACT:

Mobile communications devices use a variety of communication modes some of which can put those devices at great risks. This article explores weaknesses in some protocols exploited by simple Denial-of-Service attacks. The authors present also a solution to one of them, where the attack is executed using an ESP8266 microchip.

ARTICLE INFO:

RECEIVED: 28 JUNE 2020
REVISED: 07 SEP 2020
ONLINE: 22 SEP 2020

KEYWORDS:

ESP8266, Deauth attacks, DOS attacks

Introduction

According to statista.com,[1] in 2020 alone, nearly 1.560 billion mobile phones will be sold. This makes the issue of security of mobile operating systems particularly relevant. In this paper, we will look at attacks in which the attacker does not have physical access to the device.

The Most Common Vulnerabilities of Mobile Devices

The seven most dangerous mobile security threats in 2020, according to Kaspersky's Lab [2] are data leakage, unsecured Wi-Fi, network spoofing, phishing attacks, spyware, corrupted cryptography and improper session management.

✉ Corresponding Author: Tel.: +359886520725; E-mail: st.mechev@naval-acad.bg

- Data leakage

Data leakage most often occurs after users grant mobile applications too many permissions during installation. These are usually free apps that can be downloaded from official app stores (Google Play Store, App Store, etc.) that perform their functionality as outlined in the app description, but also send personal - and potentially corporate - data on a remote server, where it is obtained from advertisers and sometimes from cybercriminals.

- Unsecured Wi-Fi

Users typically avoid using mobile data traffic when wireless hotspots are available. Unfortunately, free Wi-Fi networks are usually not secure, as a result of which mobile devices can be easily attacked. In some cases, attackers require users to create an "account" to access these free services, supplemented by a password. Because many users use the same combination of email and password for multiple services, hackers are then able to compromise email, e-commerce, and other sensitive user information.

- Network Spoofing

In Network Spoofing attack, hackers create fake access points that look like Wi-Fi networks, but are actually traps. This most often happens in public places with high internet traffic, such as cafes, libraries and airports. Cybercriminals give access points misleading names, such as “Free Wi-Fi from the airport” or “Café” to encourage users to connect.

- Phishing attacks

Because mobile devices are always on, they are usually the first to fall under most phishing attacks. Mobile users are more vulnerable because they often monitor their communications in real time, opening and reading emails as soon as they receive them. Mobile users are also more susceptible to such attacks, as e-mail applications show less information about the sender of the message due to the smaller screen sizes of mobile phones. For example, even when open, an email can only show the sender's name unless you expand the header information bar.

- Spyware

In many cases, users do not have to worry about malware from unknown attackers, but rather spyware installed by spouses, colleagues or employers to track their whereabouts and activities. Also known as stalkerware, many of these applications are designed to be loaded on victims' devices without their consent or knowledge.

- Poor quality encryption

Poor quality encryption can occur when application developers use weak encryption algorithms or incorrectly apply strong encryption. In the first case, developers can use known encryption algorithms, despite their known vulnerabilities, to speed up the application development process. As a result, any moti-

vated attacker can use the vulnerabilities to crack the password and gain access. In the second example, the developers use strong encryption, but leave open other "back doors" that limit its effectiveness. For example, if developers leave flaws in the code that allow attackers to change high-level application features — such as sending or receiving text messages — they may not need passwords to cause problems.

- Improper session management

To facilitate access for mobile transactions, many applications use tokens, which allow users to perform multiple actions without being forced to authenticate. Like user passwords, tokens are generated by device identification and validation applications. Secure applications generate new tokens each time they try to access or "session" and must remain confidential. Session handling occurs incorrectly when applications inadvertently share tokens per session, for example with malicious participants, allowing them to impersonate legitimate users. This is often the result of a session that remains open after the user has left the application or website. For example, if you are logged in to a company intranet website.

Using the specialized chip ESP8266 for wireless network attacks

One way to attack wireless networks is by using the shortcomings of the 802.11 wireless standard.

Attacks that can be implemented using the specialized chip ESP8266: de-authentication, flood beacon.

- Flood beacon

Definition and mechanism of action

Flood beacon is an attack in which, the attacker transmits countless fake beacon frames. After a while, the available wireless networks are so many that the user is totally confused and lost in a large list of networks.

- De-authentication

Definition and mechanism of action

De-authentication is a type of attack in which a malicious person (hacker) causes a breakdown in the connection between a workstation (such as a laptop or smartphone) and a wireless access point (access point) that meets IEEE 802.11 specifications.

Mechanism of action: the attack is possible as a result of combining two factors: 1) The 802.11 standard provides for the possibility for each client in the network to request explicit de-authentication from the access point. 2) Standard 802.11 networks do not include a mechanism for verifying the correctness of the self-reported identity. As a result, a malicious person can clone the MAC address of a legitimate network client and apply for de-authentication on their behalf. The same actions are applied to the client from the access point, as a result of which the connection between the two stations breaks down.[3] Application: this type of attack can be used simply to disconnect customers from the

network, but also as a basis for another type of attack, for example in the form of social engineering.

The solution: this shortcoming was eliminated in 2009 with the adoption of the 802.11w standard and in particular with the introduction of secure management frames. The modern access points support the 802.11w standard, but in practice it is not enabled by default, so it has to be explicitly turned on. For example, for Cisco devices WAP150, WAP361 and WAP371 those settings can be set trough web interface.[4]

Specific Characteristics of ESP8266

ESP8266 is a highly integrated microchip with microcontroller capabilities manufactured by Espressif Systems. It is designed to provide a full internet connection in a small volume device.[5]

The ESP8266 can be used as an external Wifi module, using the standard firmware for the AT Command set, by connecting it to any microcontroller using the serial UART. It can also directly serve as a Wifi-enabled microcontroller by programming new firmware using the provided SDK.

For the experimental part a specialized device ESP8266 Deauther,[6] was used, with the help of which scanning of wireless networks and their attack can be performed.

The device supports microcontroller interface via Arduino SDK (Figure 1) and web interface with which its functionality can be used (Figure 2).

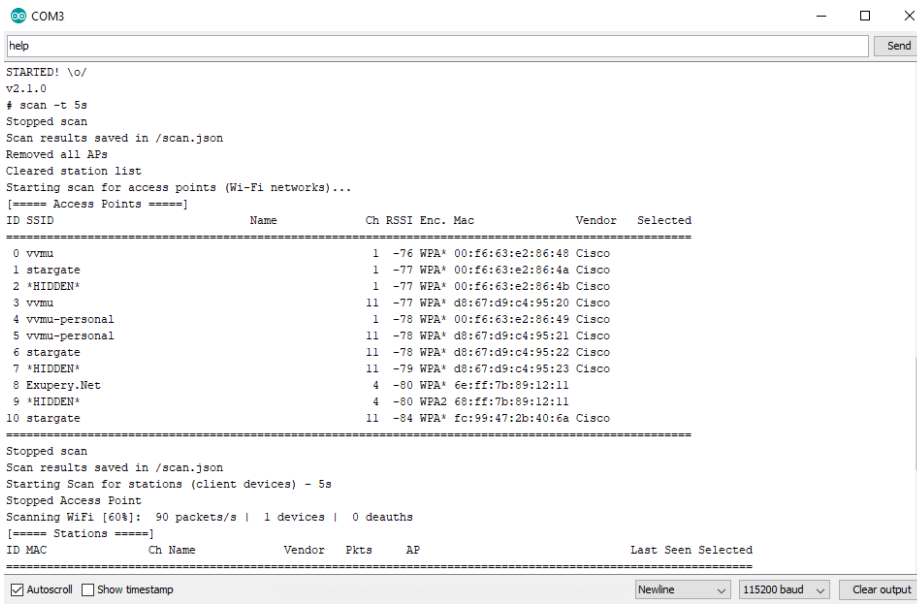

Figure 1: Connection to ESP8266 Deauther trough Arduino SDK.

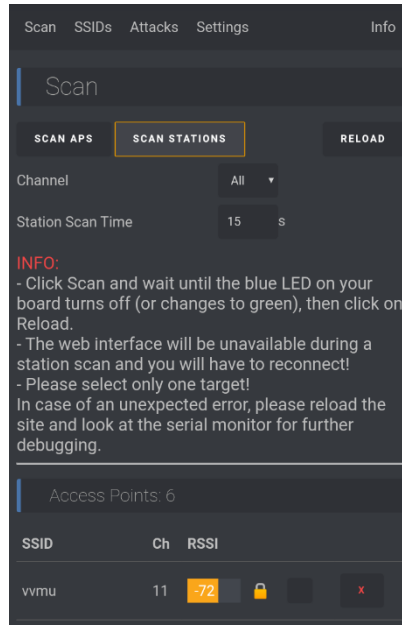

Figure 2: Example of wi-fi network scanning with ESP8266 Deauther trough web interface.

Principle of operation during the attack

1) Scan for wireless access points
2) Choose the target and type of attack
3) The attack itself begins.

These steps can be performed through the interface of the device, through the web interface (maybe using a mobile phone) or through the interface of the Arduino SDK.

Results

During the experiments, various hotspot devices were attacked. As a result of the attack, all workstations using the respective hotspot were left without wi-fi connection.

The experimental attacks were carried out directly via the buttons on the ESP8266 Deauther device. This avoided the use of additional equipment such as a computer or mobile phone.

Conclusions

It was experimentally confirmed that although the shortcomings of the 802.11 protocol were eliminated in 2009, in 2020 in practice, there are still devices that are vulnerable to de-authentication attack.

References

[1] Number of smartphones sold to end users worldwide from 2007 to 2020, https://www.statista.com/statistics/263437/global-smartphone-sales-to-end-users-since-2007/, accessed June 25, 2020.

[2] Top 7 Mobile Security Threats in 2020, https://www.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store, accessed June 20, 2020.

[3] John Bellardo and Stefan Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions", Department of Computer Science and Engineering, University of California at San Diego, https://cseweb.ucsd.edu/~savage/papers/UsenixSec03.pdf, accessed June 15, 2020.

[4] https://www.cisco.com/c/en/us/support/docs/smb/wireless/cisco-small-business-100-series-wireless-access-points/smb5302-configure-management-frame-protection-mfp-on-a-wireless-acce.html, accessed September 7, 2020.

[5] ESP8266 Introduction, http://fabacademy.org/archives/2015/doc/networking-esp8266.html, accessed June 9, 2020.

[6] esp8266_deauther, http://deauther.com, accessed June 6, 2020.

About the Authors

Stoyan **Mechev**, Researcher in the cyber security. Nikola Vaptsarov Naval Academy: Varna, BG, PhD student (Faculty of Engineering).

Elisaveta **Staneva**, Researcher in the cyber security. Active in publications and academic teaching. Nikola Vaptsarov Naval Academy: Varna, BG, PhD student (Faculty of Engineering).

Mariyan **Rachev**, Researcher in the cyber security. Nikola Vaptsarov Naval Academy: Varna, BG, PhD student (Faculty of Engineering).