EasyChair Preprint

№ 4550

Searching for a Potential Criminal Using Wireless Internet Networks as One of the Targets of State Security

Serhii Buchyk and Yaroslav Andrushchenko

November 11, 2020

Serhii Buchyk
Doctor of Technical Sciences, Professor at the Department of Cyber Security and Information Protection, Faculty of Information Technologies, the Kyiv Taras Shevchenko National University
Yaroslav Andrushchenko
Student
Taras Shevchenko National University of Kyev

SEARCHING FOR A POTENTIAL CRIMINAL USING WIRELESS INTERNET NETWORKS AS ONE OF THE TARGETS OF STATE SECURITY

One possible way of finding potential criminals through using the wireless Internet to ensure the security of the country and critical facilities. It also highlighted the use of modern digital and networked technologies for development an integrated system searching and manipulating the offender's cell phone.

Keywords: wireless network security, 'man-in-the-middle', cybercriminals, cyber special service, data interception, deauthers.

In the context of the hybrid war, in which Ukraine is currently engaged, the question of ensuring security and integrity of the country is beyond doubt. Many countries, for their territorial integrity, are investing not only in the armed forces, in the traditional sense of this term, but also in cyber-weapons. The advent of cyber-weapons also makes it necessary to develop means of countering these weapons. That is why governments fund and support projects that protect the country in cyberspace.

Detection and prevention are the main objectives of the country's special services. That is why they must use modern equipment and technology, by means of which, they can monitor and, if necessary, influence the work of information systems or individual devices. But how to set up this solution? And what would that take? It's impossible to track every single person in the country. People generate a lot of information, and there are physically not enough specialists to process that information. And furthermore, the Constitution protects the human rights of privacy. Special services have the right to interfere in the life of a person only if suspicion has been made and a court order has been executed. And only after that you can legally interfere with a certain person's life.

You can't defend yourself if you can't attack. That is why it is not uncommon for special services to use the help of cybercriminals to solve cybercrime. They also train their specialists, the so-called "white hackers" who work for the country. However, such specialists are not of much use without special tools. The authorities seek help from developers who create tools to search for and deanonymize criminals.

One of those tools that could help special services is a tool that can scan mobile phones with an enabled Wi-Fi adapter. This type of solution should consist of two parts. The first part is a server that processes, stores and transmits information, and the second part is an access point that emits the work of a Wi-Fi router. Such Wi-Fi points are placed in strategically important and lively places such as airports, bus stations, train stations and

so on. They're also placed in shopping and entertainment centers - all the places where there are a lot of people. In such public places, there is usually free Wi-Fi that people gladly use. Also, these places are visited by criminals, as they can be "invisible" among the crowd. And it is this solution that would allow us to detect the presence of such attackers.

As mentioned earlier, the solution should consist of a server and an access point. However, there should be two access points, so that a person can be found by x and y coordinates. Each point runs at frequencies of 2.4 Ghz and 5.0 Ghz. These are the open frequencies on which the Wi-Fi protocol works according to IEEE 802.11[1] standard. These points are different from others because they have a much higher power, their signal power reaches several kilometers. The points cover 360 degrees around, but their antennas have a clear direction, which is why they have to be positioned in the direction of these antennas. Otherwise, their efficiency will be reduced. These antennas must be reprogrammed with special software that is based on the Linux kernel with long-term support distributions such as Debian, or its descendant - Ubuntu. However, the specific user (operator) "shell" should be developed which is oriented to the Cisco command-line interface (CLI). These access points should be connected to the Internet and directly to the mini-server on which the scanned information will be stored and the database will be supplemented.

Next up is the server. There should be two types of server. The first one is a cell phone - a small computer that will be connected directly to the point which stores, processes and transmits the information to the data center, where a more powerful server, operated by the information security administrator will already be. The mobile server will also update and configure the access point.

For easy operation, a graphical interface (GUI), operated by a cybersecurity specialist, should be developed. With this interface, the operator should be able to process all incoming information. Scanning information should be displayed on his/her monitor and have certain filters to make the work easier. He/she should also be able to control, configure and reconfigure the version of the access point. In case of sensor problems, the operator should be able to connect to it directly, and with debugging commands that are specially designed to test the work of the sensor, reconfigure it or gather information which will be forwarded to the developers for further software correction and updating.
The question then is: What is this all about? With such a solution, the operator will monitor and, if necessary, conduct an attack on the mobile phone in order to capture the attacker's phone. In that case, two phases of intervention would be carried out. The first one is known as the Man-in-the-Middle attack[2]. The essence of the attack is that it interferes with the transmission of information in such a way, that from the target victim the information passes through the attacker and then to the router and vice versa. When the victim requests the information, the router first directs it to the attacker because it considers him to be the end-user and then the attacker redirects it to the user.

This is a description of the classical method, but the solution will use a more effective method. The information, that is most often transmitted, is encrypted and cannot

be retrieved. In case of using this solution, the public router, which is located in the mall, will be replaced by the router of the cybersecurity operator. This all will be done thanks to these sensors. That is why these access points will work exclusively with the cell phone of the criminal and not with the cell phone of ordinary citizens. The operator chooses his target; the system first calculates the frequency at which it operates - 2.4Ghz or 5.0Ghz, then finds the exact channel using the phone. The sensor then sends deauthers[4]. Deauthers are images that are sent to the target's phone and report that it has been disabled. At this time, the point is fixed to a specific channel at a certain frequency and creates an access point with an exact copy of the SSID[3]. When the criminal's phone tries to reconnect the Wi-Fi, the access point is no longer public, but artificially created by the system. The victim won't notice any change in work, because it happens pretty quickly. And once the target is caught, we can analyze and alter the traffic. That's how phase one ends. Next, phase number two - infection of the target's phone and retrieval of information from the device - begins. The solution starts sending packets and switching the phone so that it can "tell" about itself. This enables the installation of malicious software for spying purposes, the ability to redirect the phone to phishing sites in order to obtain confidential data or download programs.

All actions described above are illegal and can be carried out exclusively by special services, the ones that have the permission of the court. The operator's target won't be random. The MAC address of the target's phone must be approved by the court, and permission for obtaining the information from the target phone must be granted. Otherwise, all obtained information in the course of an investigation cannot be considered in court, because it has been obtained illegally.

The theoretical material discussed above is all about improving cybercrime investigations and the work of the special services of the country.

References:

1. IEEE 802.11-2012 - IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
2. Man in the middle (MITM) attack. - https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/
3. What Is an SSID, or Service Set Identifier? - https://www.howtogeek.com/334935/what-is-an-ssid-or-service-set-identifier/
4. Wi-Fi deauthentication attack. - https://en.wikipedia.org/wiki/Wi-Fi_deauthentication_attack