ADVANCES IN CYBER-PHYSICAL SYSTEMS

Vol. 4, No. 1, 2019

THE METHODS OF PROTECTION AND HACKING OF MODERN WI-FI NETWORKS

Taras Boretskyy

Lviv Polytechnic National University, 12, Bandera Str., Lviv, 79013, Ukraine.
Author's e-mail: *Taras.R.Boretskyi@lpnu.ua*

Submitted on 24.06.2019

***Abstract*: In this paper, we discuss the most popular attacks on personal Wi-Fi networks, offer some improvements to the hacking process and possible methods of protection.**

Index Terms: Wi-Fi security, WPA2-PSK, dictionary attack, hacking, 4-way handshake, PBKDF2 authentication protocol.

I. INTRODUCTION

To ensure the security of authentication and data transmission in wireless access points (AP), two main protocols are currently available – WEP and WPA. Due to the large number of weaknesses and imperfection of the protocol, Wired Equivalent Privacy (WEP) technology does not provide data transmission security [1]. Since WEP is practically not used (except for compatibility with older devices), it is not considered here. In turn, there are two versions of the Wi-Fi Protected Access protocol currently in use (WPA and WPA2, Fig. 1), which are quite similar to each other, and only the encryption and hashing technologies in the authentication algorithm differ.

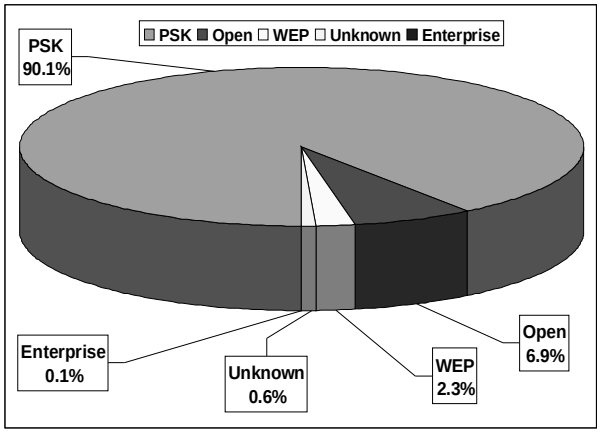


Fig. 1. Wi-Fi encryption market share

Also, in 2018, the Wi-Fi Alliance released a next-generation wireless security protocol WPA3, which should eventually replace WPA2, but it takes time for its full implementation and large-scale use. The WPA3 standard replaces the pre-shared key exchange with new Simultaneous Authentication of Equals (SAE) password-authenticated key agreement providing forward secrecy and protection against offline dictionary attacks. However, even in this new protocol, several security vulnerabilities have already been found (so-called Dragonblood attacks [2]).

Most wireless access points now use WPA/WPA2 with a pre-shared key (PSK, Fig. 2) for wireless security, known as WPA-Personal. This mode was designed for small home and office wireless networks. The methods presented in this work can be applied to both versions of the WPA protocol which use a pre-shared key. In contrast to the WPA-Personal, WPA-Enterprise mode (802.1X) requires using a separate RADIUS authentication server and provides a much higher level of security. But statistically, WPA-Personal authentication is more common.

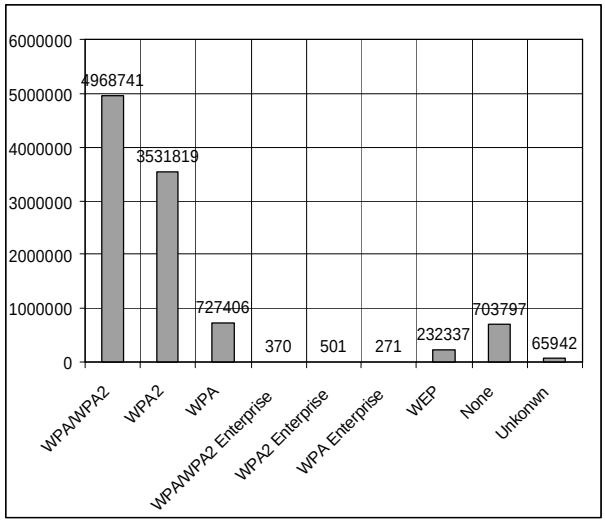


Fig. 2. Statistical sample of 10 million AP's

Since all data in the current version of the standard WPA2-PSK is protected using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) and Advanced Encryption Standard (AES) [5, 6] cipher, protocol security (data privacy, integrity, and authentication) depends mainly on the reliability of this encryption standard and the authentication process known as PBKDF2 (Password-Based Key Derivation Function 2, Fig. 3). This algorithm is used to construct a 256-bit PSK based on

the password phrase and Wi-Fi network identifier (SSID) by repeatedly applying a hash function.

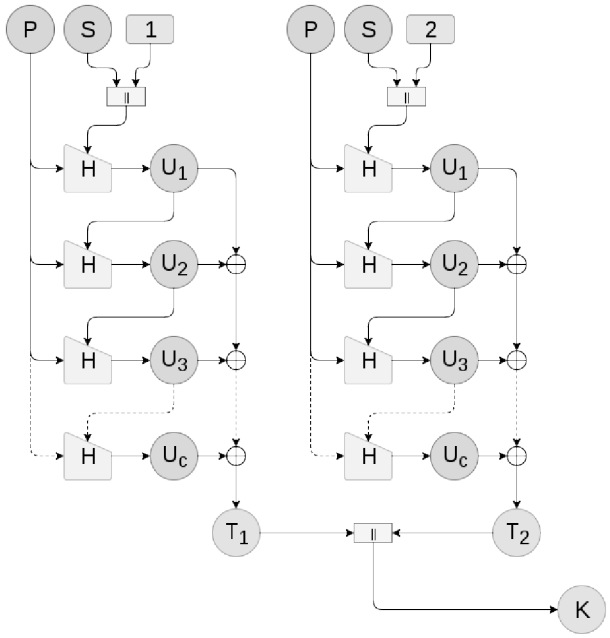


Fig. 3. Password-Based Key Derivation Function 2

II. WEAKNESSES OF THE PROTOCOL

Next, we consider the methods of increasing the level of security of the Wi-Fi networks that use PSK and, on the other hand, methods of improving the hacking techniques. There are a number of shortcomings in both firmware access points and protocols developed; among the most commonly used technologies there are WPS / QSS, which allow the attacking side to penetrate a secure wireless network. Of course, after disclosure of the vulnerability of the protocol or firmware used at the access point, the vulnerability (in most cases) is closed by the equipment manufacturer. However, not all models of access points receive appropriate updates to the software. The reasons may be either morally obsolete equipment or the elimination of the manufacturer's companies, or the obvious economy of resources by the manufacturer. Thus, network equipment of known manufacturers on the same equal terms is more potentially protected, at least from the point of view that such a manufacturer will try to preserve the reputation and to close the future vulnerability of their facilities. Although it is fair to note that even the largest companies are rarely interested in the proportion of their products by placing them in a legacy category. Usually in such cases, the situation can be corrected by replacing the original software with one of the alternative access points firmware, like XX-WRT. However, such a replacement is not always possible due to the hardware features of the platform, and in what it becomes, in essence, similar to the outdated access points, which have only WEP encryption available. Thus, although the wireless network is protected, but there is a guaranteed possibility to circumvent this protection for a short period of time. Such methods, although highly effective, are nevertheless highly specialized and suitable only when the equipment or program part contains one or more known bugs. After all, users rarely replace the software even in the event of critical defects or errors due to low awareness, incompetence, irresponsibility or obvious shortage of time. However, in the opposite case, with the correct configuration, modern access points still represent a relatively inaccessible fortress, since the absolute level of protection for today, unfortunately, is not available.

With regard to effective ways of hacking modern access points, such methods are well-known and widely described in information sources. The strength of such approaches as intercepting the “4-way handshake” phase is the fact that the access key to a wireless network may be known to the attacker, but this fact is by no means recorded by the end-of-life equipment, and the entire attack can take place both in passive mode and using the resources of the remote network equipment located in the zone of attack of the access point and completely in automatic mode. The most common and universal attack on access points with WPA2-PSK protection is the interception of “4-way handshakes” procedure. This process consists of exchanging between the access point and the client with four packages, of which the first two of which are intended to match the private key, and the next two – the exchange of the group key (Fig. 5). Also, the third “handshake” package contains a confirmation of a private key signature and a repeat of a random number (ANonce) sent in the first packet.

To perform an attack, the third and fourth packets are not required, and in the case of a false key they are not sent, but their presence allows to verify the correctness received during a key attack. However, most Wi-Fi monitoring software avoids logging of group handshakes and organizes their attack on the first two packages, which reduces the effectiveness of the attack.

The basic difficulty of calculating PBKDF2 functions is the demand of calculation SHA1 hash function for WPA2 or MD5 for WPA1 2^{15} times. Quite easily, this number can be reduced to $2^{14} + 8$ times, but the results of the calculations of the previous stage are fed to the input of the next, which hinders the parallelization of this process. Both hash functions are similar in structure to the SHA2 algorithm, which is the basis of the block chain used for Bitcoin cryptography valuation. So it is possible to make a comparison between the speed of equipment for cabinet exchange and switching keys using the PBKDF2 algorithm by scaling the already well-known results of a large number of hardware at a factor of 2^{14} and without paying attention to a larger bus size of the SHA2 algorithm, which compared with SHA1 uses eight instead of five 32-bit registers and 64 instead of 80 rounds. However, one type of equipment still falls out of the overall comparison of the process of landing and calculating the PBKDF2 function – these are specialized ASIC systems

that are widely used in block chain, but are not serially released for other algorithms, although it is easy to set such an opportunity in the system data, given the slight difference between hashing algorithms and lower computational complexity SHA1. Such an approach would allow to use the specialized ASIC equipment in other areas, such as attacks on the PBKDF2 algorithm after it became irrelevant for the cryptology exchange, which becomes irrelevant, usually due to poor performance and power consumption. In addition to ASIC systems, there are four more common types of attack platforms that are sorted in descending order – GPU, FPGA, CPU (x86) and various embedded systems. The fastest in this regard are video cards, the top models of which provide a speed of about 100–500 thousand keys per second with the hardware-built algorithm for calculating hash functions. FPGAs that occupy a niche between the GPU and the CPU have somewhat lower performance. The main parameter that provides high performance is the number of logical elements. This in turn allows you to organize several independent conveyors to calculate hash functions without using additional chip blocks, memory, or other elements embedded in the FPGA. The experiments on the Altera Cyclone III FPGAs allow us to assert that the algorithm can work at about 230 MHz, depending on the number of independent pipes and with one round of the SHA1 algorithm per cycle. Replacing an FPGA with more elements can achieve faster performance. In this case, the limiting factor begins to be heat dissipation from the FPGA, which can reach hundreds of watts, depending on the frequency of the chip.

The speed of a modern CPU ranges from a few hundred to several thousand PBKDF2 calculations, and the performance of multi-core systems also rests in heat dissipation. The best performance is boosted by x86 processors that include SSE and AVX extensions, which provides parallel computation of functions with 416 independent threads for each of the cores. It should be noted here that specialized extensions from Intel (including AMD and VIA), such as Intel SHA Extension, will not be effective for the attack, because although they can quickly (with low latency) compute the hash function, they are not able to calculate several hash functions in parallel. This is, to a certain extent, related to such algorithms as FastPBKDF2, which use all 15 (without RSP stack registers) 64-bit integer CPU registers, but provide the same performance as SSE commands only at few AMD processors. On Intel processors, this algorithm significantly loses the performance to media expansion block. The ratio of performance and power to energy-efficient processors such as Intel Atom CPU is maintained within the same range as the FPGA and GPU, about 500 keys per watt. As for high-speed multi-core i7 processors, this ratio is an order of magnitude lower for them.

The lowest performance has built-in systems, which, although they have the worst show both in terms of performance and efficiency, can be used massively to carry out an attack during an idle time, when they are free from the main system tasks. Among such devices, smartphones should be allocated during charging, as well as most of routers and other network equipment with permanent Internet access.

III. POSSIBLE ATTACKS ON THE PBKDF2 PROTOCOL

The proposed method is an improved method of standard “hacking” of WPA-PSK network, which is based on intercepting the authentication process followed by brute forcing possible keys and comparing the result with the signature of the packet (MIC – Message Integrity Check) sent by the client. To speed up the attack, we can use a list of the most popular Wi-Fi passwords (dictionary attack). This packet is taken from the insecure WPA-PSK four-way handshake. A hacker can use for this the cracking software such as aircrack-ng [3].

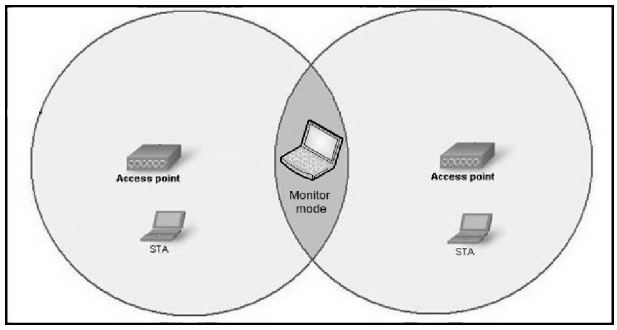


Fig. 4. Monitor mode interference phenomenon with sensitive receiving antenna

The successful implementation of the attack is hampered by such a physical phenomenon as interference (Fig. 4), which makes it difficult to verify the correctness of the data obtained in the process of radio communication. The source of such “interferences” can be APs in which the signal transmission level is higher than their sensitivity. The Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) standard assumes that only one client-server pair can work on the air at any time at a selected frequency. However, it is directly proportional to the sensitivity of the attacking device equipment and the number of the network segments, where it intersects with adjacent AP.

In packets intercepted in such places, there are a number of bits of characters compared to the package that was sent to the AP. The damaged sequences do not necessarily spoil the caught handshakes, especially if they are placed in the second part of the EAPOL frame (Fig. 6), which is not taken into account when hashing the switch from PMK to PTK.

Thus, depending on the specific conditions, on average only 30–70 % of packets are suitable for further analysis. Moreover, in some cases, damaged packets may also be suitable for further decryption.

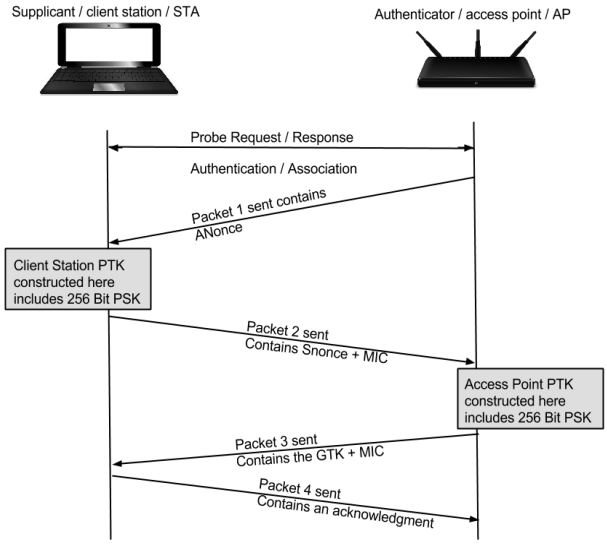


Fig. 5. 4-way handshake protocol

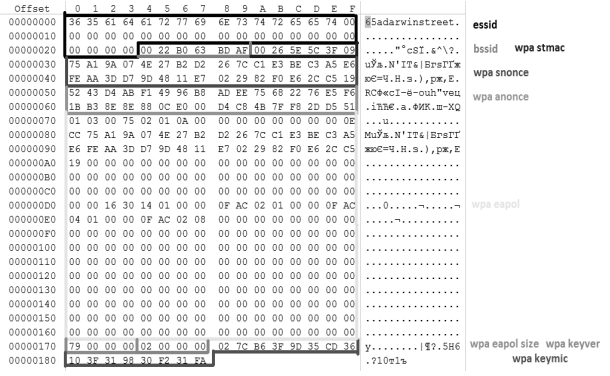


Fig. 6. Example of the captured .ivs frame

That is why most programs intercept packets from a given access point after the authenticated pair received stops the further traffic analysis. This also applies to the AP name analysis. Because after determining the relation between the MAC address and the network SSID, the sniffing software stops analyzing further possible name changes that may occur, for example, during the initial configuration or reconfiguration of the AP. This limitation is partly due to the imperfect format of storing initialization vectors (.ivs), which does not provide for a change in the SSID, as well as the generally accepted opinion that in order to repeat the attack for a new session, the entire process must be repeated. This opinion is partly correct, because by intercepting the clearly correct "handshake", it is possible to uniquely determine (although it is not always technically possible) which key was used. However, even in case of successful key selection, only the password entered by the client (for example, mistakenly) becomes clear, and not the one at the access point. Also, this effect can be seen, if someone (or something) tries to guess the password. Therefore, the increase in attack capabilities can be achieved by forming the base of the large number of "handshakes" with the subsequent brute forcing for each of them. Here, in contrast to the popular belief that the number of "handshakes" is directly proportional to the time of the keys selection, this is ambiguous.

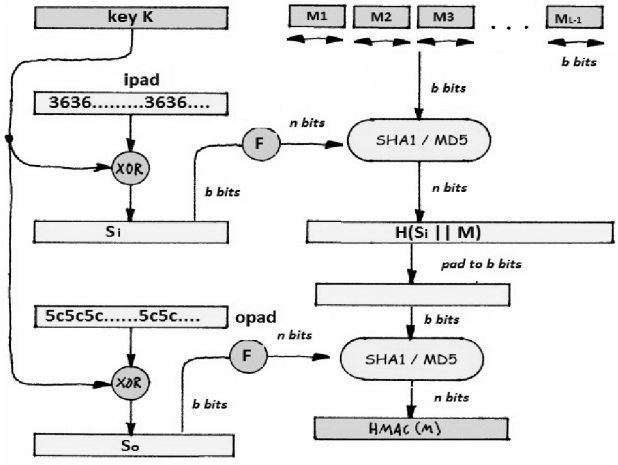


Fig. 7. One round of HMAC, the part of PBKDF2 4096 iteration process

So, if we look into the PBKDF2 authentication process, we can see that it consists of two parts (Fig. 7). The first stage is used to complicate the brute force procedure by 2^{12} repetitions of the SHA1 hashing algorithm for WPA2 (in case of WPA1, MD5 is used). At the same time, there is the SSID of the AP. It is used like a "salt", for the rainbow tables counter attacks complication. The implementation of such attacks is possible only in the case of using standard network identifiers offered by the manufacturer of Wi-Fi routers, such as Asus, D-Link, Netis, or simply non-unique identifiers: home, wireless, Wi-Fi, etc. If the SSID contains information about the model of the router, attackers can use this information to compromise the Wi-Fi network. The PSK obtained at this stage (also known as PMK – Pairwise Master Key) can be used for storage on the client and server parts, without the risk of reproducing the password. This procedure takes the main part (more than 99.9 %) of the computing resources of the PBKDF2 authentication algorithm, for completing it is enough to make four hash function calls using the "random" numbers given in the handshake (Anonce and Snonce). Thus, the obtained 256-bit general master key (PMK) is converted into a 128-bit unique temporal key (PTK – Pairwise Transient Key) used to encrypt data for each connected client. This asymmetry of the resource intensity allows you to verify the correctness of the previously received "handshakes" by applying the PMK to PTK conversion with different nonce values for various handshakes. Thus, in terms of the resource consumption, the calculation of two possible keys using the PBKDF2 authentication method is equal to checking a thousand "handshakes"; and the more of them should be verified, the greater will be the efficiency of the method. However, in practice, 5–10 distinct "handshakes" taken from unique clients at different times is enough for an effective attack.

IV. METHODS OF PROTECTION AGAINST ATTACKS STRUCTURE OF THE ARTICLE

Let us consider the methods of protecting Wi-Fi networks. Although the simplest attacks, such as dictionary search of common passwords, are easily implemented in practice, for example, in the form of common mobile applications. They are ineffective due to the low bandwidth of communication channels and computing resources of the attacking platform. In theory, the maximum speed is limited by the rate of "beacon" generation, which is at least 100 kbps, and, as a rule, is 100 ms between attempts. In practice, the real time between brute force attempts can be several seconds, which makes such an attack effective only if the password to the AP is very poor. However, there are practically no publicly available filters (built into the firmware by the manufacturer) to implement the restrictions on the number of attempts. We can say that, in general, it is possible to guess a password from a public database if it has already been used by more than a thousand of another wireless APs. PCI Data Security Standard [4] recommends using in the WPA-Personal mode 13-character or more (maximum 63 characters) truly random passphrases that are highly unlikely to be cracked. Another possible way to protect against this attack is by hiding the name of the AP. In this case, the attack will be much more difficult. It should be noted here that this approach only helps if connections to the access point are rarely made, since according to the standard APs reveal their SSIDs in clear text at each handshake. Therefore, a more advanced method of protection will be to improve the client part of the protocol in which the client connects to the AP without announcing its SSID. Then even in the case of a known password, connecting to a wireless station becomes almost impossible due to the lack of information about its SSID in case if both values are unknown. Although this method is able to increase the level of security, it should be said that it is not suitable for mass use, since in this case, it will become difficult to determine the correct AP to connect if its MAC address is not known. Besides, the user will also have to remember the SSID of the access point in addition to the key. However, this approach requires modifying only slight part of the protocol and, with limited use, is highly effective and fully justified. Following the recommendations for trusted password rules, it must contain 12 ASCII characters, 17 lower case letters or 24 digits. These requirements are appropriate for the case if only one round of hashing function is used for password phrase. However, using the PBKDF2 hashed password requirements of similar stability can be reduced to 10 ASCII characters or 14 Latin letters or 19–20 digits. There are also a number of techniques that can reduce the possibility of intercepting a "shake hands". For example, increasing the data rate increases the connection security between the parties. The higher sensitivity of the antenna as a client and access point can also reduce the radius of "handshake" interception. It is also desirable to arrange the possibility of backup power of the access point, since any short-term power outages are forced to refresh the pseudorandom generator with a lack of entropy, and to re-enforce the authorization process, which the attacking party hopes. Regarding the software, the possibility of upgrading the firmware up to the latest version, or install alternative versions of the software, such as XX-WRT. It is also obligatory to check your chosen password using an online database with already known passwords or phrases that are found on the Internet. It should not be forgotten that a large number of rainbow tables have been created for standard access point names. Therefore, for the sake of security, you should choose a unique AP name with its validation in existing databases [7, 8]. Even the fact that manufacturers try to give the AP unique ESSID including the part of the MAC address in the title, it does not prevent from creating the appropriate number of rainbow tables. Therefore, it is not superfluous to hide the ESSID, if possible, and to avoid its coverage using the method described above. And, of course, to disconnect authentication using threatening technologies such as WPS / QSS, the IE Robust Secure Network, or WEP / WPA1. The same effect that the client side of the software may be threatened, for example, as detected KRACK vulnerability in wpa_supplicant.

V. CONCLUSIONS

In conclusion, it should be noted that with the correct configuration of the AP with a unique SSID and a complex password, it is practically impossible to bypass the protection based on the WPA2-PSK protocol. However, there are also "pitfalls" here. So, when using FPGAs and specialized hardware systems for cracking WPA/WPA2 keys, the speed of a single possible "brute force method" is within a few hundred thousand values per second. And, for example, it will take at best up to ten years to bust a password of ten small Latin letters, which is quite acceptable for ensuring the sufficient level of security. It should be noted that generally accepted requirements for passwords are not suitable here since they provide only one stage of hashing, and keys based on the PBKDF2 algorithm are four thousand times more secure. That is why it is recommended to choose simpler randomized associative passwords, which are easier to keep in memory or use password manager software for longer passwords.

REFERENCES

[1] S. Fluhrer, I. Mantin, and A. Shamir. "Weaknesses in the key scheduling algorithm of RC4", International Workshop on Selected Areas in Cryptography, Springer, Berlin, Heidelberg, 2001, p. 1–24.

[2] M. Vanhoef and E. Ronen. "Dragonblood: A Security Analysis of WPA3's SAE Handshake", p. 1–16.

[3] Aircrack-ng. [Online]. Available: http://www.aircrack-ng.org/ [Accessed: Nov. 25, 2018].

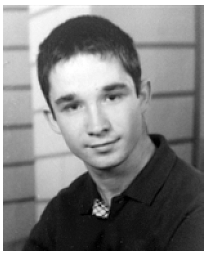
[4] IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. (2016 revision). IEEE-SA. 14 December 2016. doi:10.1109/IEEESTD.2016. 7786995. ISBN 978-1-5044-3645-8.

[5] Federal Information Processing Standards (FIPS) Publication 197. Announcing the Advanced Encryption Standard (AES). November 26, 2001. Available at http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf [Accessed:Nov.25, 2018]

[6] NIST Special Publication 800-38C. Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality. May 2004.

[7] Have I been pwned? Biggest free online e-mail and password database. (Almost 8 billion leak accounts) [Online]. Available: http://www.haveibeenpwned.com/ [Accessed: Nov. 25, 2018].

[8] Online Wi-Fi password database collected by Router scan software (Almost 10 million AP names and passwords) [Online]. Available: http://www.3wifi.stascorp.com/ [Accessed: Nov. 25, 2018].



Taras Boretskyy is an assistant of the Department of Information Technology Security at Lviv Polytechnic National University, Ukraine. He was awarded with the academic Doctor of Philosophy degree in 2019 at Lviv Polytechnic National University. He has scientific, academic and hands-on experience in the field of computer systems research and design, proven contribution into FPGA and high-performance algorithms for computer systems design methodology. He is experienced in computer data protection, including cryptographic algorithms, its implementation, wireless and network security.