INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 08, August 2023, pp : 66-71

e-ISSN : 2583-1062

Impact Factor : 5.725

REVIEW PAPER ON WIRELESS NETWORK PENETRATION TESTING

Abid Salam[1], Dr. Nitin Kumar[2]

[1]M. Tech Scholar, Ganga Institute Of Tech. & Management, Jhajjar, India.

[2]Assistant Professor, Ganga Institute Of Tech. & Management, Jhajjar, India.

ABSTRACT

Wireless networks have become an integral part of our daily lives, providing convenient and ubiquitous connectivity. However, the widespread adoption of wireless technologies has also introduced new security risks and vulnerabilities. Wireless penetration testing is a critical process that aims to assess the security posture of wireless networks by simulating real-world attacks. This abstract explores the concept of wireless penetration testing, its objectives, methodologies, and tools used in the process. It emphasizes the importance of identifying and mitigating potential security vulnerabilities in wireless networks to protect sensitive data and ensure the integrity and availability of network resources. The abstract discusses various wireless penetration testing techniques, such as passive and active reconnaissance, wireless network scanning, encryption cracking, and exploiting weak authentication mechanisms. It also highlights the significance of understanding the specific security protocols and standards employed in wireless networks, such as Wi-Fi Protected Access (WPA) and WPA2, and the implications of vulnerabilities in these protocols. Furthermore, the abstract addresses the legal and ethical considerations associated with wireless penetration testing, emphasizing the importance of obtaining proper authorization and ensuring compliance with relevant laws and regulations. It also highlights the need for ongoing monitoring and periodic re-assessment to address emerging threats and evolving security landscape. By conducting wireless penetration testing, organizations can proactively identify and address vulnerabilities in their wireless networks, enhance their security posture, and prevent unauthorized access, data breaches, and other malicious activities. The abstract concludes by emphasizing the critical role of wireless penetration testing in maintaining a robust and secure wireless network infrastructure in today's interconnected world.

1. INTRODUCTION

The first Wi-Fi 802.11 wireless standard was created in 1997. In less than 20years, the data transfer speed increased from 1 Mb/s to an incredible speed of 6.75 Gb/s. Over time, Wi-Fi has penetrated a large number of companies, schools and households. Based on research from 2011, every fourth household has its own Wi-Fi network. More developed countries such as Germany and France reach over 70% household coverage.[1]According to predictions, there will be over 20 billion devices connected to the Internet by 2020, most of which will be connected wirelessly.[2]Wireless technologies, including Wi-Fi, are therefore still in development and their popularity is increasing every year. However, in addition to the benefits of Wi-Fi networks, their negative aspects must also be taken into account. One of these negative aspects is security. With classic cable networks, data travels only through the given medium-the cable. This data transfer is relatively safe, since the only way to steal it is through a direct physical connection to the network. However, in the case of Wi-Fi networks, the transmission medium is air. Data is flying all over the place, so anyone within signal range can theoretically capture and read it. Due to this fact, a number of security issues arise that must be addressed when using Wi-Fi networks. The aforementioned growing popularity of Wi-Fi networks and various security threats became the motivation for developing this work. Countless researches prove every year that ordinary users do not care much about their protection on the Internet. We therefore researched what threats users are really exposed to and what they are at risk of on Wi-Fi networks. However, we looked at security issues from a slightly different perspective. Instead of securing networks, we tried to disrupt their security. In the following document, we therefore describe different types of cyber attacks against Wi-Fi networks. We are not only dealing with attacks on a theoretical level, but all types of described attacks have also been carried out practically. We used the same tools used by professional security analysts and hackers to carry out the attacks. After carrying out these attacks, we subsequently proposed measures that would prevent similar attacks in the future.

2. LITERATURE REVIEW

2.1 **Security of wireless networks-** Already at the initial draft of the Wi-Fi standard, it was clear that data must be secured in some way. For this reason, the WEP protocol was developed, the task of which was to maintain the confidentiality of transmitted data. Using the RC4 algorithm, he encrypted the transmitted communication on the network, so that the attacker could not decrypt the captured data and thus read the communication. However, the first theoretical attack on the WEP protocol was invented already in 2001. Since then, new and new vulnerabilities have been found and the number of attacks has increased. Finally, WEP was declared insufficiently secure in 2004 and its development was suspended. To immediately solve the insufficient security of the WEP protocol, the WPA protocol was released, which tried to correct the errors found in its predecessor. WPA implemented a new, dynamic way of managing encryption keys called TKIP. This method creates a unique encryption key for each message sent. This was a huge change from WEP, which uses a 40 or 104 bit static encryption key throughout the communication. Another major change in the WPA protocol was related to authentication. The new method of authentication takes place using a method called the 4-way handshake. This method makes it possible to verify knowledge of the access password even without revealing it directly. However, WPA was only designed as a temporary solution to solve the problems with WEP. The main implementation of the new security protocol was released in 2004 as a set of 802.11i standards under the name WPA2. The latest WPA2 security protocol takes over some features from the WPA protocol land also adds other improvements to maximize security. Instead of TKIP, it uses another type of encryption called CCMP (AES type encryption family standard). The encryption change as well as other minor changes make WPA2 a very secure choice.

2.2 **Distribution of attacks on Wi-Fi networks-** Wireless communication has always been and always will be vulnerable to various types of attacks. The earliest attacks on WEP used discovered flaws in the encryption protocol. Since serious flaws have yet been discovered in the encryption used by WPA2, today's attacks on systems of this type are more focused on trying to break a weak password. Man-in-the-middle attacks and various phishing are also quite popular pg. 3 and social engineering procedures that rely on users lack of education or overconfidence. This work mainly deals with attacks with technical aspects, therefore we will not come across a description of phishing and social engineering procedures.

2.3 **WEP protocol vulnerabilities -** As we mentioned earlier, the WEP security protocol uses an outdated type ofencryption-theRC4algorithm.Thisalgorithmusesastatickey chosen by the user and a 24- bit random value called an initialization vector (IV). After processing these two data, an encryption key is created in the RC4 algorithm, which is used to encrypt thefollowingmessageusingtheXORfunction. ThisprocessisdemonstratedinFigure no.1

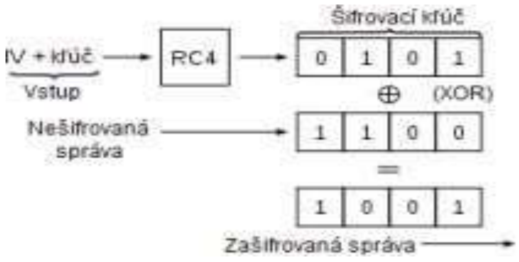

fig.No.1-RC4principleofencryption

Aninitializationvectorisappendedtoeach WEP frame, sending itunencrypted.

In this case, the question arises, what if the same initialization vector is generated twice.This condition would be a huge problem because the same encryption key would be usedtwice.Various analysis and calculations could then beusedtodeterminewhattheoriginalinputtotheRC4algorithmconsistedof.Thusitwouldbepossibletofindoutthepasswordusedonthe-network.Ontheprobabilityofgeneratingthe sameinitializationvectorat2^{12}

$$\bar{p}(2^{12}) = 1 * \left(1 - \frac{1}{2^{24}}\right) * \left(1 - \frac{2}{2^{24}}\right) ... \left(1 - \frac{2^{12} - 1}{2^{24}}\right) = \frac{2^{24} * (2^{24} - 1) ... (2^{24} - 2^{12} + 1)}{(2^{24})^{2^{12}}}$$

$$= \frac{(2^{24})!}{(2^{24})^{4096} * (2^{24} - 2^{12})!} = 0{,}60658$$

$$p(2^{12}) = 1 - 0{,}60658 = 0{,}39342$$

From the calculations, we found that there is a 39% chance of the same IVoccurring on the $2nd^{12}$wireless messages. This problem was followed by the first attackon WEP encryptionfrom 2001.Theat tack was base dontheassumptionthatanattackerwho passively monitors communication on the network can collect a sufficient number of initialization vectors. By using various mathematicalcal culations and analyses, itcanrecover the password used on the network with the number of severalmillioninterceptedmessages. This typeof attack takesseveral hoursto execute. Another significant decryption method was introduced in 2004 by the hackerKoreK, who minimized the number of necessary intercepted packets to approx. 700thousand. The latest attack from 2007, called PTW, uses other discovered bugs in RC4encryption, which gives us a 50% chance of success with 35,000 intercepted messages.At 45,000, there is even an 85% chance of a successful attack, which makes a PTWattackon aWEPnetwork possibleinlessthan aminute.[4]

2.4 **The principle of brute for ceattackon WPA/WPA2systems-** SincetheWPAandWPA2protocols do not use a static encryption key, a dynamickey is generated every time the client connects to the network and has a lifetime for then tiredurationofthesession. Iftheclients disconnected andreconnected, anewencryptionkeyisgeneratedagain.

Duetothisfact, attacksusingstatisticalanalysislikeinthe case of WEP are impossible. The process of authentication and dynamic encryptionkey generation is called 4-way handshake. It is therefore a kind of 4-step exchange ofmessagesbetween theaccesspoint andtheclient. The dynamic key generation process starts with connecting the device to thenetwork. After attempting association and authentication, devices must generate a Pre-SharedKey(PSK).Thisprocesstakesplaceonthebasisoftheentereduserpasswordandthe ESSID (name) of the network, which are processed in a special hash function. Theresult of the operation is a 256-bit string - PSK, also called PMK (Pair wise Master Key).After the PSK is generated, the access point itself initiates the 4-stageexchange, whichgenerates a pseudo-random value (ANounce) and sends it to the client. After receiving amessagewiththisvalue, the clien twill generat eitsownpresudo-randomvalue(SNounce). With the help of MAC addresses of devices, presudo-random values and PMK, a PTK value issu bse quently generated, which will beuse din future communication forthe purpose of encryptingmessages. ThisprocessisshowninFigureno.2.

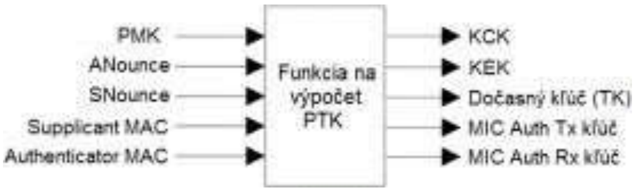

Fig.no.2-Processfunction tocalculatePTKvalue

After the client's PTK is generated, the MIC checksum is calculated from this value, which is subsequently included in report no.2 sent along with the client's prerandom value. After receiving the second message, the access point generates its own PTK value and derives its own MIC from it. The checksum is then compared with the result received from the client. If the MIC values match, the client has confirmed knowledge of the access key and the process is completed via message 3 and 4. If the MIC values do not match, the access point sends a de authentication packet, which causes the client to be kicked out of the network. Through this process, the client verifies knowledge of the access key and a new dynamic encryption key is also established. All this is handled in a secure way that attackers cannot exploit directly. Butlet's think about what things a potential attacker can read from the intercepted messages of the 4-way handshake process. ANounce and SNouce are sent unencrypted and the MAC addresses of the devices are also found in the message header. So the only thing that prevents the attacker from getting the PTK is the PMK key. Recall that the PMK is generated by a special hash function using the access Password and the ESSID. The only element that the attacker does not know is the afore mentioned access password. There is currently no way to crack this hash function, so the only option is to get the access password somehow. Once one of the possibilities is, for example, guessing it. A brute-force attack is based on this principle, which tries to replace the password with various strings, generate the PTK value and then compare the checksums. If the checksum matches, the PTK also matches and thus the password has been guessed successfully. Based on the password testing method, brute-force attacks can be divided into two types. A brute-force attack from and to z tries all possible variations of characters to form words. This type of attack always theoretically has a 100% success rate. However, due to the time-consuming nature of the billions of tested words, this attack may never end, so it may be impractical in practice due to time constraints. The second type of attack is dictionary brute-force, which is based on trying frequently used terms from an available word database.

2.5 Theoretical concepts of WPA protocol attacks- The WPA protocol was designed as an immediate solution to weak WEP security. Forth is reason, the same encryption algorithm (RC4) was used for the purpose of maximum hardware compatibility on less powerful devices of the time. The encryption protocol used represents a potential security risk, which is why various forms of attacks have begun to develop on this protocol over time. WPA TKIP attacks from 2008 and 2013 do not allow to obtain the access password from the network, but they allow to decrypt the transmitted packet and then push a certain number of packets to the network without knowing the access password. Pushing packets can trigger other attacks such as ARP spoofing, DNS poisoning and others. The intention of this attack is not to obtain an access password from the network, a successful attack only allows a few packets to be pushed onto the network without the need to know the password. However, these attacks are only in theoretical form, and there is no automated tool to enable this attack yet. Users of WPA networks are therefore relatively safe.

2.6 Online and offline WPS brute-force attacks- WPS (Wi-Fi Protected Setup) is a wireless standard that was originally created to facilitate access to a Wi-Fi network. Its intention is to provide very simple access to the network for ordinary users who do not have knowledge about the security protocols used on Wi-Fi. The use of the WPS service is possible either by pressing a button on the device or by entering an 8-digit WPS PIN code. The concept itself - to make it easier for the user to access the network sounds interesting, but based on the bad design of the protocol, access for attackers was greatly facilitated. Let's think about the situation if an unauthorized person came into physical contact with the router and subsequently read the PIN or simply pressed a button. In the case of good AP placement, this problem does not occur, but in WPS, a much more trivial error occurs. Since the WPS PIN code contains 8 digits, theoretically there are 108 different numerical combinations. Inexplicably, however, the PIN code is divided into 2 parts, which the router checks independently. Therefore, when entering the PIN, the router announces whether we have the first half of the code, the second half of the code, or the entire code. In the latter case, we will gain access to the network. By successively checking the code, the number is reduced to 104 + 104 options. However, the last digit in the PIN only serves as a checksum, so you don't need to know it, but the program can easily add it up. After these adjustments, we get 104 + 103 = 11,000 different PIN code variations. pg. 7 With such a small number, it is no longer a problem to try each option in order and wait until we guess the right one. The attack takes place online, which means that constant access to the network is required throughout the entire duration of the attack. This attack can be carried out within hours depending on signalstrength and other factors. The result of the attack is obtaining the WPA/WPA2 access password, and thus also obtaining unauthorized access to the network. The second method of WPS attack is the so-called an offline attack that goes by the name Pixie Dust. Since this is an offline type of attack, it is not necessary to be indirect range of the network all the time to carry it out. The concept is based on the insufficient entropy of pseudo-random values (nounce). The attack is based on the fact that when using the WPS service, messages are exchanged between the client and the access point. These messages contain a hash string that was created using the noun values and the WPS PIN code. In case of interception of such messages, we will have the mentioned hash value at our disposal. Since the random number generation is predictable or insufficient in some cases, the attacker can detect these numbers and thus will know half of the content of the WPS hash. The next stages of the attack are already similar to WPA/WPA2 breaking. The program inserts various PIN codes into the algorithm, creates hash strings from them, and then compares them with the original string it obtained from the intercepted message. If the strings match, the PIN code has been successfully reset. The offline variant takes much less time than the online attack, usually 2 to 3 minutes. This fact is due to the fact that the client does not have to transmit any messages over the network and also does not have to wait for the response of the WPS device. However, the Pixie Dust attack is only applicable to certain kinds of devices that are known to lack entropy in generating random numbers.

2.7 Interception of wireless communication

As mentioned in the previous sections, the biggest danger in wireless communication is the threat of interception and misuse of data by third parties. For this reason, individual security protocols implement message encryption. In this way, messages traveling in the wireless spectrum are protected against attackers outside the network. The WEP protocol uses a static key to encrypt all messages, so knowing the access key is enough and an attacker can immediately decrypt all messages transmitted on a wireless network. However, the WPA and WPA2 protocol uses a dynamic pg. 8 encryption key, so knowing the access password from the network is not enough. As we know, the whole process of provision of the dynamic key takes place unencrypted, therefore the attacker can capture pseudo-random values, MAC addresses and generate the same PTK key as is used in communication between the client and the access point. Under this assumption, the attacker must capture the currently ongoing 4-step exchange of messages from the beginning, otherwise he will not be able to decrypt the messages between the client and the AP. This process can be achieved either by waiting until the client arbitrarily joins the network, or by forcefully deauthenticating, forcing the 4-way handshake process and the desired messages are exchanged again. Using the described procedures, it is possible to decrypt all wireless communication if the key is known on WEP, but also on WPA and WPA2 networks. Decrypting wireless communication alone may not be enough, however, because data can also be encrypted at higher layers. Encryption at the L2 (link) and L3 (network) layers of the OSI model can be done using a VPN service. However, data is most often encrypted at the application level.

This kind of encryption is handled by many protocols, in the case of encryption of web content it is HTTPS. This protocol automatically encrypts the communication between the web server and the client during the entire session. If a message encrypted by one of these methods is intercepted, the attacker will not be able to read its content, even though he has successfully decrypted the security protocol of the Wi-Fi network. However, the process of intercepting wireless communication is still quite dangerous, as not all communication is encrypted. The attacker can find out from the intercepted messages which page the user is currently browsing, and if the user is not paying attention, the attacker can also intercept login data from sites that do not use encryption.

3 CONCLUSION

In this work, we have successfully demonstrated penetration into networks using different security standards. We were able to crack the WEP protocol within minutes. T hesetests confirmed the previously known facts about the vulne rability of Wi-Finetworks with support for WEP encryption and further strengthened our belief that the WEP security protocol should no longer be present in today's networks. Further tests on networks using WPA and WPA2 protocols confirmed that, if a strong password is used, network soft his type are almost in vulnerable. However, the only threat to these networks can be the WPS system, which is implemented on most devices from the factory. The WPS protocol can be easily abused by a classic brute-force attack, and therefore were commend disabling it. Most of the attacks exploiting WPA TKIP encryption are still only in theoretical or experimental form, but we, through the hackforums.net community, have joined a project to develop a tool that would allow such an attack. The tool is currently in the alpha version, but one of our D-link type routers succumbed to this attack and we were able to successfully push 4 packets onto the network via QoS channels. This type of attack is very time-consuming and the network must meet several conditions to carry it out, so the attack is inapplicable in some cases. Based on these facts, we do not expect this type of attack to succeed. For these reasons, WPA networks are still relatively secure.

4 REFERENCES

[1] M. Ghavami, L. Michael, and R. Kohno, “Ultra- Wideband Signals and Systems in Communication Engineering,” 2nd ed., John Wiley & Sons, pp. 166-174, 2007.

[2] G. Kumar, and K.P. Ray, “Broadband Microstrip Antennas”, Artech House, Inc. Boston, London, 2003.

[3] C. A. Balanis, “Advanced Engineering Electromagnetics,” 2nd ed., John Wiley and Sons, New York, 1989.

[4] R. Garg, P. Bhartia, I. Bahl and A. Ittipiboon, “Microstrip Antenna Design Handbook,” Dedham MA, Artech House, Inc. Canton Street, Norwood, 2001.

[5] N. Ida, “Engineering Electromagnetics,” New York, NY, USA: Springer, 2015.

[6] D. G. Fang, “Antenna Theory and Microstrip Antennas,” CRC Press, Boca Raton, 2006.

[7] I. J. Bahl, and P. Bhartia, “Microstrip Antennas,” Artech House, Inc. Boston, London, 1980.

[8] C. R. Johnson and H. Jasik, “Antenna Engineering Handbook,” 3rd ed., McGraw-Hill, New York, 1984.

[9] K.C. Gupta, R. Garg, I. Bahl, and P. Bhartia, “Microstrip Lines and Slot lines,” 2nd ed., Artech House, Boston, London, pp. 122-132, 1996.

[10] Y. Huang, and K. Boyle, “Antennas: From Theory to Practice,” John Wiley and Sons, New York, 2008.

[11] G. A. Deschamps, Microstrip Microwave Antennas, 1953, presented at Proc. 3rd USAF Symposium on Antennas.

[12] R. Munson, \Conformal microstrip antennas and microstrip phased arrays," IEEE Transactions on Antennas and Propagation, vol. 22, no. 1, pp. 74{78, 1974.

[13] J. Q. Howell, \Microstrip antennas," IEEE Transactions on Antennas and Propagation, vol. 23, no. 1, pp. 90{93, 1975.

[14] R. Garg, P. Bhartia, I. Bahl, and A. Ittipiboon, Microstrip Antenna Design Handbook, ser. Antennas and Propagation Library. Artech House, 2001, ISBN:9780890065136.

[15] J. W. Wallace, M. A. Jensen, A. L. Swindlehurst, and B. D. Je_s, \Experimentalcharacterization of the mimo wireless channel: Data acquisition and analysis,"IEEE Transactions on Wireless Communications, vol. 2, no. 2, pp. 335{343, 2003.

[16] X. Wang, Z. Feng, and K. Luk, \Pattern and polarization diversity antenna withhigh isolation for portable wireless devices," IEEE Antennas and Wireless Propagation Letters, vol. 8, pp. 209{211, 2009.

[17] N. Cohen, Tuning fractal antennas and fractal resonators," U.S. Patent 6 104 349A, 8 15, 2000.

[18] M. Kumar and V. Nath, "Microstrip-line-fed Elliptical Wide-slot Antenna with Similar Parasitic Patch for Multiband Applications," IET-Microwaves, Antennas & Propagation, vol. 12, no. 14, pp. 2172-2178, 2018.

[19] K. L. Lau, Q. Xue, C. H. Chan and Y. F. Liu, "Experimental Studies of Printed Wide-Slot Antenna for Wide-Band Applications," IEEE Antenna and Wireless Propagation Letters, vol. 3, pp. 273-275, 2004.

[20] A. Imani, M. N. Moghaddasi and A. Dastranj, "Printed Wide-slot Antenna for Wideband Applications," IEEE Transactions on Antennas and Propagation, vol. 56, no. 10, pp. 3097-3102, 2008.

[21] Y. Z. Yin, Y. Q. Wei, B. W. Liu, A. F. Sun and Y. Yang, "A Circular Wide-slot Antenna with Dual Band-Notched Characteristics for UWB Applications," Progrees in Electromagnetics Research Letters, vol. 23, pp. 137-145, 2011.

[22] B. K. Kanaujia, S. Dwari, S. Kumar, A. K. Gautam and M. K. Khandelwal, "Analysis and design of wide band Microstrip-line-fed antenna with defected ground structure for Ku band applications," International Journal of Electronics and Communications, vol. 68, pp. 951-957, 2014.

[23] R. Bayderkhani, G. Dadashzadeh, B. S. Virdee and M. N. Moghadasi, "Printed Wide-slot Antenna with High Polarization Purity for Wideband Applications," Microwave and Optical Technology Letters, vol. 52, no. 5, pp. 1001-1006, 2010.

[24] C. C. Tsai, C. Y. Huang and W. F. Chen, "Compact Wide-slot Antenna for Ultra-wideband Communications," Electronics Letters, vol. 44, no. 15, pp. 892-893, 2008.

[25] A. Nezhad, H. R. Hassani, A. Foudazi and S. Mohammad, "A Dual-band WLAN/UWB Printed Wide-slot Antenna for MIMO/Diversity Applications," Microwave and Optical Technology Letters, vol. 55, no. 3, pp. 461-465, 2013.

[26] H. Eskandari and M. N. Azarmanesh, "Bandwidth Enhancement of a Printed Wide-slot Antenna with Small Slots," Internaitonal Journal of Electronics and Communications, vol. 63, no. 10, pp. 896-900, 2009.