International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cyber Security in Evil Twin Attack

Madugala Sowjanya*

GMR Institute of Technology Razam, Kinneravada, Thogiri, Saravakota, Srikakulam, Andhra Pradesh, PIN-532427, India.

ABSTRACT

An evil twin attack could be a hack attack within which a hacker sets up a fake Wi-Fi network that appears sort of a open entry area to steal victims' sensitive details. The fake Wi-Fi entry area be in work to listen in on users and steal their login credentials or other sensitive information. These are evil twin hotspots are public places, coffee shops, offices Instructions, organizations. In globally 549 million people are using public wifi networks. My Aim is detection the evil twin attact. A man-in-the-middle attack requires three players. There's the victim, the entity with which the victim is trying to speak, and also the " Man in the Middle," who's intercepting the victim's communications. Critical to the scenario is that the victim isn't alert to the person within the middle. A Denial-of-Service (DoS) attack is an attack meant to pack up a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In information security, KARMA is an attack that exploits a behaviour of some Wi-Fi devices, combined with the shortage of access point authentication in numerous wifi protocols. it's a variant of the evil twin attack. They are many methods to find an evil twin attacks Using python 3.8 evil twin detection, 802.11b/802.11g WIFI Devices with Evil Twin defender.

Keywords: MITM, KARMA, Fake AP, Detection Method, Evil twin, Wireless LAN, BSSID

1. Introduction

Cyber security is that the practice of protecting critical systems and sensitive information from digital attacks. Also called information technology (IT) security, cybersecurity measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of a corporation.Security system complexity, created by disparate technologies and an absence of in-house expertise, can amplify these costs. But organizations with a comprehensive cybersecurity strategy, governed by best practices and automatic using advanced analytics, AI (AI) and machine learning, can fight cyberthreats more effectively and reduce the lifecycle and impact of breaches after they occur. In cybersecurity they are so many attacks are there. One of the attack is EvilTwinAttack. An evil twin attack is a rogue Wi-Fi access point (AP) that masquerades as a legalized one, enabling an striker to gain access to sensitive information without the end user's knowledge. An striker can easily create an evil twin with a smartphone or other internet-capable device and some easily available software.In this review we are going to do literature review and will know about each reference papers that we attached previously, we will discuss regarding methods such be used in the reference papers. These algorithms and classifiers mainly tells what is going to be do in these papers. In this review we are discussing about 5 reference papers which I have attached in the abstract review.

2. Literature Review

- [1] However, there's no proper solution to detect ETA in Wi-Fi personal networks. Latest Wi-Fi security algorithms, namely Wi-Fi Protected Access 3 (WPA3) and Opportunistic Wireless Encryption (OWE) also susceptible to ETA. This paper proposes a unique Proof of Existence (PoEx) scheme, bringing network lifetime to Access Point (AP). Wi-Fi client devices will detect and forestall ETA using associated AP lifetime
- [2]Wi-Fi is all most used at any places to gainthe internet access. In which to provide internet access in so many places like coffeeshops, Railway stations, University campuses, Restaurants and then on. Deselection methods are client side detection, in this ET-sporter tool is used. Machine , MACHINE LEARNING BASED DETECTION Alogorithms the Most of approaches perform in server side or in user side and few approaches need particular hardware such as Sensor, IDS and etc.
- [3]The ETA has been an unsettled problem for many years in WLANs. during this section, this paper introduce the wireless network background and analyse the essential observation. In a wireless network, wireless APs periodically broadcast their SSIDs so as to create users discover and connect with them. Yet the SSID of a LAP is straightforward to be spoofed by a malicious adversary.
- [4]This paper, introduced novel method whatever allows us to find with each other four cyber attacks in Wifi networks. In this procedure enables the identified of many cyber attacks in local wireless networks. The execution was write down in Python for a low-cost network system depend on Raspberry Pi 4. During our experiments, select any one of the most testing attack, i.e., the fake access place attack, and also the KARMA attack, the frequency congestion attack and the DE authentication attack. Proved the functionality of in the procedure and implementation at the experimental areas.

- [5]This article discusses about the Herein, rogue-AP detection techniques are reviewed. they'll be categorized as detection on guided and unguided media. This paper present two algorithms, TMM and HDT. We implement our prototype system and evaluate it in several real-world wireless networks, and our evaluation results proved its effectiveness and efficiency.

3. Methodology

Fake access point attack

A hacker chooses a public place that has many hotspots, like your local Starbucks or an airport. Such places usually have multiple Wi-Fi access points with the identical name. It's good if you're walking round the building and don't want to lose your connection, but it also makes the hacker's job much easier when it involves creating a fake hotspot with the identical Wi-Fi name Now the bad actor can use anything from a network card, tablet, or laptop to a transportable router or a Wi-Fi Pineapple (if they have more range) to build a hotspot. It's pretty easy! Just give some thought to the rear hour you used your phone as a hotspot to share a mention to your other devices or your friends. That's exactly what a hacker does; however, they use the identical Service Set Identifier (SSID) name, also referred to as simply the Wi-Fi name, because the legitimate one does Why does this matter? Because most devices aren't clever enough to tell apart between a legitimate and a fake access point if they need the identical SSID. (Some hackers can go as far as cloning the MAC address of the trusted network.) That's why it's called an evil twin!.

DE authentication Attack

DE authentication attack could be a disruptive technique against wireless connections. It belongs to the denial-of-service family, abruptly rendering networks temporarily inactive. These tactics are usually low-key as they are performance no needed unique skills or elaborate equipment. For some, DE authentication attacks are innocent pranks on co-workers, friends, or neighbours. However, it are often a component of a much bigger ruse, like an evil twin attack. DE authentication attacks represent fraudulent requests that interfere with the communication between routers and devices. The strategy attacks 802.11-based wireless networks, as they require DE authentication frames whenever users terminate connections. Wi-Fi networks also don't have effective mechanisms for verifying MAC addresses. Perpetrators could spoof addresses and perform DE authentication attacks. Forged frames terminate connections. If attackers still send requests, users won't be ready to reconnect. While the attack could specialise in one target, all clients could lose connection to the access point.

Log File

log file is computer-generated file that have facts regarding usage patterns, activities, and operations within an software, application, server or another device. IT organizations can implement security event monitoring (SEM), security information management (SIM), security information and event management (SIEM), or another analytics tool to aggregate and analyze log.

Wireless Interface

A wireless network interface controller (WNIC) may be a network interface executer which attaches to a radio-based network instead of a wire-based network. If you've got a land line in your apartment you'll be ready to setup wireless internet with a wireless router which an ISP will introduced you to after you subscribe them.

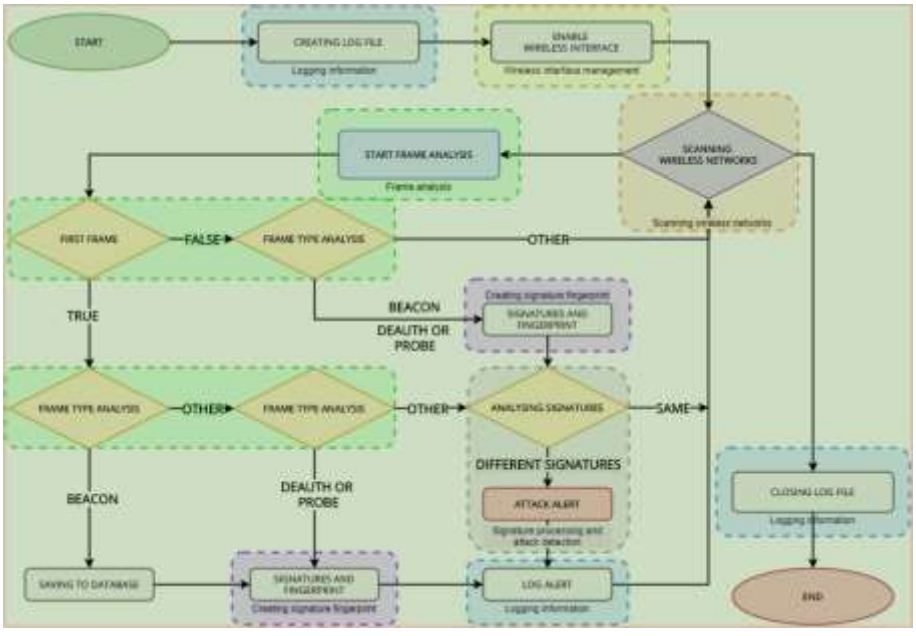

Fig 1 from [1]

Frame analysis

Frame analysis (also called framing analysis) is a multi-disciplinary science research method accustomed analyse how users knows circumstances and analysis.

Signatures And Fingerprint

The fingerprint is that the hash of a key. A digital signature is tied to some message, and is often a one-way encrypted hash of the message When bearing on computers and security, a fingerprint or digital fingerprint refers to any trace of data left by someone. Often, if somepeson has accessed unknown user gain to a computer or network, an administrator or security agent may seek for any digital "fingerprints" left by the attacker. This identifying evidence may include IP addresses, hostname, MAC address, etc. A digital signature could be a mathematical technique which validates the authenticity and integrity of a message, software or digital documents. It allows us to verify the author's name, date and time of signatures, and authenticate the message contents. The digital signature offers way more inherent security and intended to resolve the matter of tampering and impersonation (Intentionally copy another person's characteristics) in digital communications.

Application of Digital Signature

- Authentication
- Non-repudiation
- Integrity

Beacon

Beaconing is when the malware communicates with a C2 server soliciting for instructions or to exfiltrate collected data on some predetermined asynchronous interval. The C2 server hosts instructions for the malware, which are then executed on the infected machine after the malware checks in. How frequently the malware checks in, and what methods it uses for this communication are typically configured by the attacker Malware beaconing is one amongst the primary network-related indications of a net or a peer-to-peer (P2P) malware infection. A botnet could be a network of system injected with poisonous software that's being controlled by a foreign malicious party without the owner's knowledge P2P infections indicate malware that's laterally moving to infect one system after another. After malware infects a vulnerable host, it quickly scans the host environment and initiates a command and control (C2) channel with its creator (i.e., the intruder). The compromised host then initiates regular interval malware beaconing calls resolute the C2 infrastructure to await further installation begin data exfiltration.

4. Results

Table-1 use the distance measurement algorithm we can arrange the 4 experiments. And in every one can be split int for times take output is average of each experiment. Observe the table it gives the lowest accuracy values and highest accuracy values. 74.64% is lowest accuracy value and as well as the is 90.95% highest accuracy.

S.NO	ACTUAL VALUE	1	2	3	4	AVERAGE-ERROR	ACCURACY
1	8.10	8.97	6.01	8.59	8.13	0.87	89.26%
2	9.72	7.08	8.97	10.03	12.05	1.50	84.57%
3	12.15	12.93	11.57	10.83	10.42	1.10	90.95%
4	14.58	16.10	11.69	11.99	20.76	3.29	76.97%
5	16.20	18.01	17.38	11.58	21.64	3.26	79.88%
6	17.82	23.31	21.85	25.87	18.36	4.52	74.64%
7	20.25	26.97	24.48	24.21	21.64	4.07	79.91%
8	21.87	15.87	22.15	20.37	26.66	3.14	85.65%
9	24.30	21.84	26.65	19.01	28.72	3.63	85.07%
10	28.35	31.06	34.83	21.86	26.12	4.47	84.24%

5. Discussions

There are the three references points. The first references points are placed fixed with coordinates can't changes the places. The second references points are very flexible you can change any time at any place. They are introduced my distance measurement algorithm and can and fix the refences points are experiments al group. consisted the three compare the values group 2 reference are the less error. In every row compare flexible references points are produced less error compare group1 and experimental group.

s.no		a	b	c	d	measurments	Actual value	error
1	Comparsion group 1	(4,05,-3.24)	(4.05,5.67)	(-3.24,5.67)	(-3.24,-4.24)	(-2.54,1.70)	(0,0)	(2.54,1.70)
	Comparsion group 2	(2.43,-2.43)	(2.43,2.43)	(-2.43,2.43)	(-2.43,2.43)	(-0.46,-0.49)	(0,0)	(0.64,0.03)
	Experiment group	(2.43,-2.43)	(2.43,3.09)	(-2.25,3.09)	(-2.25,-3.35)	(-1.41,0.27)	(0,0)	(1.41,0.27)
2	Comparsion group 1	(4.05,-3.24)	(4.05,5.67)	(-3.24,5.67)	(-3.24,-4.24)	(-3.57,2.35)	(-1.62,0.81)	(0.04,1.31)
	Comparsion group 2	(1.62,-1.62)	(1.62,3.24)	(-3.24,3.24)	(-3.24,3.24)	(-1.66,2.12)	(-1.62,0.81)	(0.86,0.85)
	Experiment group	(1.62,-1.62)	(1.62,4.46)	(-2.94,4.46)	(-2.94,-3.26)	(-2.48,1.66)	(-1.62,0.81)	(4.45,2.70)
3	Comparsion group 1	(4.05,-3.24)	(4.05,5.67)	(-3.24,5.67)	(-3.24,-4.24)	(-2.02,1.89)	(2.43,-0.81)	(0.91,0.38)
	Comparsion group 2	(4.05,-3.24)	(4.05,1.62)	(-0.81,1.62)	(-0.81,-3.24)	(1.52,-1.19)	(2.43,-0.81)	(1.41,0.31)
	Experiment group	(4.05,-3.24)	(4.05,2.28)	(-0.63,2.28)	(-0.63,-4.16)	(1.02,-1.12)	(2.43,-0.81)	(2.92,1.63)
4	Comparsion group 1	(4.05,-3.24)	(4.05,5.67)	(-3.24,5.67)	(-3.24,-4.24)	(-2.11,2.42)	(0.81,4.05)	(3.02,0.58)
	Comparsion group 2	(3,24,0)	(3.24,5.67)	(-2.43,5.67)	(-2.43,0)	(-2.21,4.63)	(0.81,4.05)	(3.84,0.14)
	Experiment group	(3,24,0)	(3.24,6.30)	(-3.15,6.30)	(-3.15,-1.56)	(-3.03,3.91)	(0.81,4.05)	(0.87,1.67)
5	Comparsion group 1	(4,05,-3.24)	(4.05,5.67)	(-3.24,5.67)	(-3.24,-4.24)	(-3.30,2.38)	(-2.43,4.05)	(0.71,0.48)
	Comparsion group 2	(2.43,0)	(2.43,5.67)	(-3.24,5.67)	(-3.24,0)	(-1.72,3.57)	(-2.43,4.05)	(0.92,1.67)
	Experiment group	(2.43,0)	(2.43,6.48)	(-3.94,6.48)	(-3.94,1.11)	(-2.99,4.00)	(-2.43,4.05)	(0.56,0.05)

6. Conclusion

They introduced and execution the Novel method its use is detect the four types of Wifi networks cyber attacks. They are KARMA attack, Beacon attack, DE authentication attack, Frequency congestion attack in Wifi networks. We confirm and performance for our using method and our execution at the process. The detector strongly finds the all attacks and throughout the structure understand the experiment.

References

1. K. Murugesan K. k. Tangaroa and V. N. Muralitharan," PoEx: Proof of existence for Evil Twin Attack Prevention in WIFI personal Networks," 2021 8th International Confrence on Future Internet of Things and Cloud (Ficloud), pp. 92-98, doi:10.1109/FICloud 49777.2021.00021.
2. S. A. A. Ahadi, N. rakesh and S. varshney," overview on Public WiFi-Security Threat Evil Twin Attact Detection",2020 IEEE International Journal on Advent Trends in Multidisciplinary Research and Innovation (ICATMIRI) ,2020, pp.1-6, dio:10.1109/ICTMI51801.9398377.
3. M. A. C. Aung and K. P. Thant, "Detection and mitigation of wireless link layer attacks," 2017 IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA) pp. 173–178, 2017. DOI: 10. 1109 / SERA. 2017. 7965725. [Online]. Available: http: / / IEEExplore. IEEE. org/document/7965725/.
4. L. Oliveira, D. Schneider, J. De Souza, and W. Shen, "Mobile device detection through WiFi probe request analysis," IEEE Access, vol. 7, pp. 98 579–98 588, 2019.

5. S.-L. Wang, J. Wang, C. Feng, Z.-P. Pan, T. Gong, T. Yang, and J. Xu, "Wireless network penetration testing and security auditing," ITM Web of Conferences, vol. 7, 2016, ISSN: 2271-2097. DOI: 10.1051/itmconf/ 20160703001. [Online]. Available: http:// www. itm - conferences.org/10.1051/itmconf/20160703001.

6. S.-L. Wang, J. Wang, C. Feng, Z.-P. Pan, T. Gong, T. Yang, and J. Xu, "Wireless network penetration testing and security auditing," ITM Web of Conferences, vol. 7, 2016, ISSN: 2271-2097. DOI: 10.1051/itmconf/ 20160703001.

7. A. M. Alsahlany, A. R. Almusawy, and Z. H. Alfatlawy, "Risk analysis of a fake access point attack against wi-fi network," International Journal of Scientific & Engineering Research, vol. 9, pp. 322–326, 2018.

8. A. M. Alsahlany, A. R. Almusawy, and Z. H. Alfatlawy, "Risk analysis of a fake access point attack against wi-fi network," International Journal of Scientific & Engineering Research, vol. 9, pp. 322–326, 2018.

9. B. Xu, M. Peng, Q. F. Zhou, and X. Cheng, "Fake access point localization based on optimal reference points," 2018 IEEE 4th Interational Confrence on Computer and Communications (ICCC), pp. 784–788, 2018. DOI: 10.1109/CompComm.2018.8780768.

10. S.-D. Liu, Y.-l. Liu, and Z.-g. Jin, "Attack behavioural analysis and secure access for wireless access point (ap) in open system authentication," in Wireless Communications and Mobile Computing Conference (IWCMC), 2017 13th International. IEEE, 2017, pp. 741–746.

11. I. F. KILINC¸ ER, F. ERTAM, and A. S¸ENGUR, "Auto- mated fake access point attack detection and preventionsystem with iot devices," Balkan Journal of Electrical and Computer Engineering, ISSN: 2147-284X. DOI: 10.17694 / bajece. 634104. [Online]. Available: https:/ /dergipark.org.tr/tr/doi/10.17694/bajece.634104.

12. J. Martin, T. Mayberry, C. Donahue, L. Foppe, L. Brown, C. Riggins, E. C. Rye, and D. Brown, ''A study of MAC address randomization in mobile devices and when it fails,'' Proc. Privacy Enhancing Technol., vol. 2017, no. 4, pp. 365–383, 2017.

13. B. Soewito, I. Faahakhododo, and F. E. Gunawan, "Increasing the accuracy of distance measurement between access point and smartphone," in Knowledge, Information and Creativity Support Systems (KICSS), 2016 11th International Conference on. IEEE, 2016, pp. 1–6.

14. S. M. Hussain and G. R. Beigh, "Impact of ddos attack (udp flooding) on queuing models," in 2013 4th International Conference on Computer and Communication Technology (ICCCT), 2013, pp. 210–216.

15. Y.-W. Bai, C.-H. Yu, and S.-C. Wu, "Using a three-axis accelerometer and gps module in a smart phone to measure walking steps and distance," in Electrical and Computer Engineering (CCECE), 2014 IEEE 27th Canadian Conference on. IEEE, 2014, pp. 1–6.