Deceiving Attackers in Wireless Local Area Networks Using Decoys

A. Aswin Kumar*, Ashok Kumar Mohan and P. P. Amritha

TIFAC-CORE in Cyber Security, Amrita School of Engineering,
Coimbatore, Amrita Vishwa Vidyapeetham, India
E-mail: iamaswinkumar@outlook.com;
{m_ashokkumar, pp_amritha}@cb.amrita.edu
**Corresponding Author*

Received 11 January 2018; Accepted 25 April 2018;
Publication 12 June 2018

Abstract

Detecting a malicious activity like fingerprinting on wireless local area network is a challenging task. With cyber deception strategy, we can gather information about the malicious activity by placing honeypots that can act as a trap to lure the attacker. Cyber deception is a conventional method to cloak real-time environment into a virtual legitimate environment. Our analysis shows that deception is an existing strategy in a wired LAN environment. This paper provides a wider perspective of deception strategy on wireless LAN. We primarily focus on the evil twin access point which causes serious threat to the legitimate Wi-Fi access points. Here a novel approach has been suggested to detect and identify the malicious activity by deceiving the attackers in their evil twin access points using decoys which are honeypots. The paper also provides a reliable way to gather the attacker's activity information. We can also detect SSL stripping and DNS spoofing attack using this approach.

Keywords: Wi-Fi, Cyber deception, Evil twin, Decoys, SSL stripping.

Journal of Cyber Security and Mobility, Vol. 7_1, 201–214. *River Publishers*
doi: 10.13052/jcsm2245-1439.7114

1 Introduction

In the current world scenario, the need for the Internet is drastically high and Wi-Fi technology plays a major role in connecting people to the Internet. Nowadays, common places such as airports, coffee shops and hotels have Wireless access points (WAP) or in general Access Points (AP) that allows the people to connect to the Internet at ease. Access point supports security settings such as WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA2 (Wi-Fi Protected Access 2). An Access Point can also be configured with no security, which means any client can connect to the Access point without any authentication and it is called as open access point. According to the recent survey, 60% of access points are open, 30% of them are partially configured and remaining 10% are properly configured. Recently, Key Reinstallation Attack (KRACK) has been released that makes WPA2 configured access points vulnerable to exploit. Deauthentication, brute-forcing the pre-shared key, evil twin are the other common attacks which are possible. Among these attacks Evil Twin is stealthy and harder to detect. In this attack, the attacker will flood the legitimate access point by sending deauthentication packets to all the clients which are connected to the targeted access point. Once the access point is made inaccessible, the attacker will create a fake access point with the same SSID (service set identifier) and force the clients to connect to that attackers access point. If the client's mobile or computer is configured to connect automatically to the open networks, then it will try connect to the fake access point AP. When the client's mobile or computer is connected to the fake access point, the attacker can monitor and control the entire network traffic of the client which are flowing through the access point. Attacker can perform Man In the Middle (MITM) attack to impersonate the client's device traffic by stealing sensitive informations such as usernames, passwords, credit card details and session cookies.

In this paper, the cyber deception on wireless networks has been implemented. Cyber Deception is a traditional approach to lure the attackers to attack a sandbox environment. Using this approach, the fingerprint of the entire activity of an attacker's strategy can be found. Honeypots are the key elements of a deception environment. It is a device which acts as a bait or a trap to counteract the attacks. It contains some legitimate data which is used to lure the attacker to compromise the honeypot device. A deception environment contains several honeypots (decoys) which are configured to look like a normal machine. If an attacker tries to compromise the honeypot machine, his activity

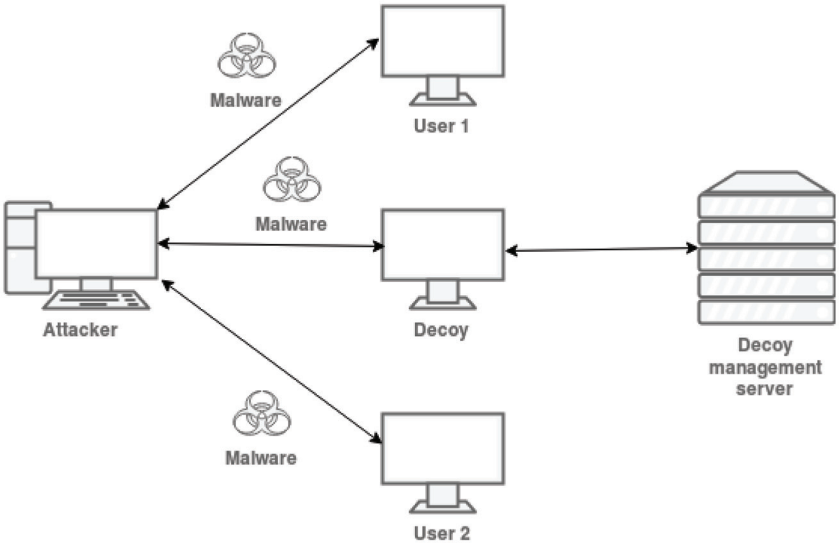


Figure 1 Cyber deception strategy environment.

will be logged and notified by the intrusion detection system (IDS) which is installed on the honeypot. Using this we can capture the attacker's activity on the honeypot device lively. Cyber deception strategy helps in identifying the 0-day vulnerabilities. Figure 1 illustrates the malicious activity of an intruder sending a malware to compromise the decoys. Once the decoys are infected with the malware, honeypot present in the decoys will capture the malware and send it to decoy management server for analysis. The whole set up mentioned here was implemented previously on the wired Local Area Network (LAN). We followed the same strategy in Wireless LAN environment (WLAN).

2 Literature Survey

Evil Twin is a stealthier attack which makes the attacker to perform Man In The Middle attack (MITM) to steal sensitive credentials. Media Access Control (MAC), noise checking, site survey and manual analysis are some of the ways to detect the Evil Twin AP but with the clever configuration of the Evil Twin AP may evade those detection techniques [1–3, 5]. So detection of evil twin access point requires lot of parameters to decide whether it is a legitimate AP or the Evil Twin. WiNX is an add-on firmare for a wireless router used to scan AP, to create custom captive portals or splash pages to capture usernames and passwords and acts as a honeypot to deceive attackers. Wi-Fi honeypot does not withstand against a flooding attack and hence deceiving the access point will not prevent the attacker [4]. Implementing the cyber deception in wired LAN fingerprints the malicious activity of an attacker with the greater efficiency and lesser false positives [6, 7]. Spreading malware, port scanning, backdoor installation and denial of service(DoS) are the malicious activities which can be monitored using the decoys. Decoys are properly configured and some amount of legitimate data will be stored in it to get the exposure of genuine device. All the decoys will be monitored and the generated logs will be send to the centralized decoy management server. The decoy management server stores all the decoy logs in a centralized fashion [17]. All the real time analysis will be done by the management server and also it performs automatic forensic investigation regarding the incident. So far all these deception strategies are implemented only on Wired LAN [8, 9]. The whole set up can be implemented in WLAN environment [12, 13]. Deception strategy will uncover the 0-day bugs. Our work focuses entirely on the Wireless LAN decoys which requires the understanding of Evil Twin and the cyber deception.

Wireless Intrusion Detection System (WIDS) is not a novel approach to detect and prevent intrusion inside the wireless LAN [10, 11]. Anyone, with even little knowledge about the penetration testing can scan the connected hosts in the particular access point. The attacker does not need to connect to the access point to perform the attacks. So WIDS is not a complete solution in detecting the Evil Twin attacks.

3 Proposed Work

In this paper, the concept of cyber deception strategy on wireless Local Area Network (LAN) is been implemented. The proposed method involves three stages. Deauthenticate the decoys, forcing the decoys to connect to evil twin AP and performing malicious activity on decoys. This paper will not focus on detection of evil twin AP, but on deceiving the attackers by connecting our decoys on evil twin to gather information about the attacker and his methods. All the activity of an attacker will be logged when he tries to attack any of the decoys. Analyzing the logs will reveal information about the attacker's strategy and it can be done either manually or automatically. The motivation behind this paper is to monitor the attacker's activity on his evil twin AP by connecting our decoys to it.

3.1 Experimental Setup

The experimental setup in the Figure 2 shows the basic wireless network in which our decoys are connected to the evil twin access point. 3 decoys are configured and connected to the evil twin AP. Decoys are monitored by the decoy server. Decoy server manages all the 3 decoys in a centralized fashion. The responsibility of the decoy server is to analyze the captured logs and report the incident to the Intrusion Detection System (IDS) if any malicious activity occurs on the evil twin AP. Network traffic in captured by all the decoys. If any attack pattern is detected on the wireless LAN, logs will be generated and that incident will be reported to the decoy server for further analysis.

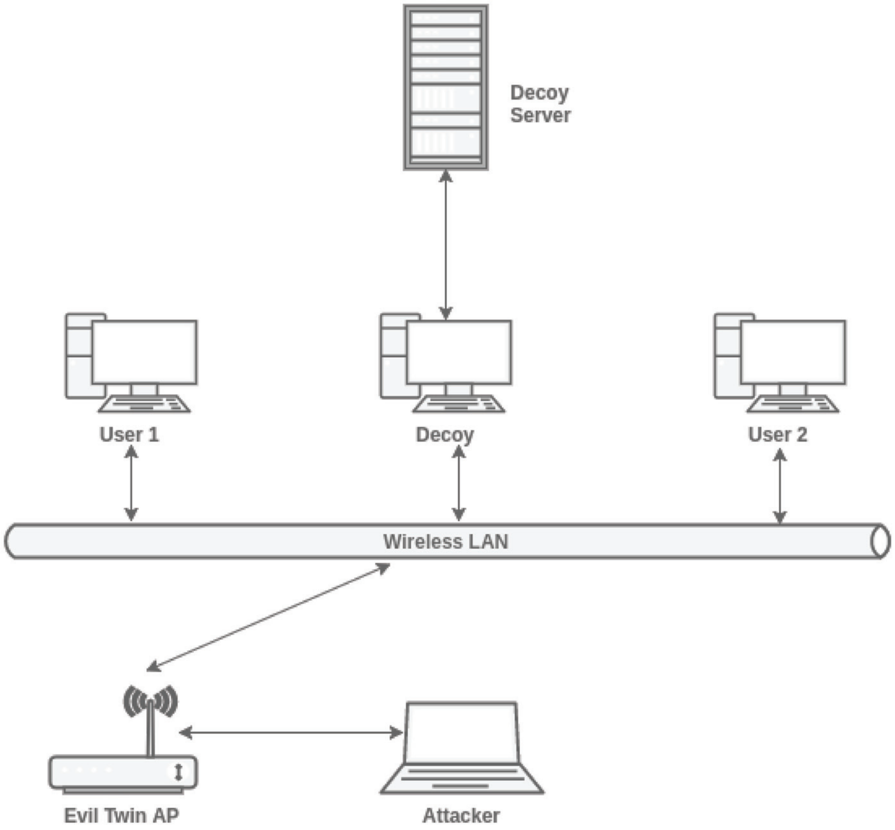


Figure 2 Experimental setup.

3.2 Decoys

Decoys are the honeypots which look like a legitimate device in the network. It contains some valuable information which lures the attackers to compromise the decoys. Here our decoys are configured to send fake network traffic over evil twin AP. Whenever the attacker tries to launch Man In The Middle (MITM) attack, the logs will be generated by the decoys and alerts the Intrusion Detection System (IDS) which is configured on the decoy server. We have configured low interaction honeypot that will randomly send some web traffic over the evil twin AP. These honeypots are easy to set up and configure. Random traffic will be generated by the decoy to find out any malicious activity that are performed on its request and response.

4 Attack Scenario

The attack scenario involves 3 phases as shown in Figure 3. In phase 1, the attacker machine will send numerous deauthentication packets to the decoys that are connected to the legitimate access point. In phase 2, evil twin AP will be set up by the attacker. Then the disconnected decoys are forced to connect to the evil twin. Attacker listens to the network traffic of the decoys. The phase 3 involves attacking the decoys. Both active and passive attack is possible since the evil twin AP is controlled by the attacker. Attacker will perform Man In The Middle (MITM) attack, DNS spoofing attack [14], packet injection, packet modification and SSL stripping attack to steal valuable information from the decoy machine [15]. Once the phase 3 starts, the decoys will collect logs about the attacker's activity and report it to the decoy server.

```
aireplay-ng -0 1 -a 00:19:55:34:99:72 mon0
```

Aireply-ng tool is used to inject frames over the wireless networks. The second command (airbase-ng) sends a deauthenication packet to all the clients that are connected to the access point with the MAC id 00:19:55:34:99:72.

```
airbase-ng -a 00:19:55:34:99:72 --essid Freenet -c 7 mon0
```

(-0) flag indicates the deauthentication packet, –essid flag indicates the access point name, -c flag indicates the channel and mon0 is the network interface which is in the monitor mode. Evil twin AP is switched on by executing the second command. Now the attacker will force the clients to connect to his evil twin access point with the same ESSID (Extended Service Set Identifier)

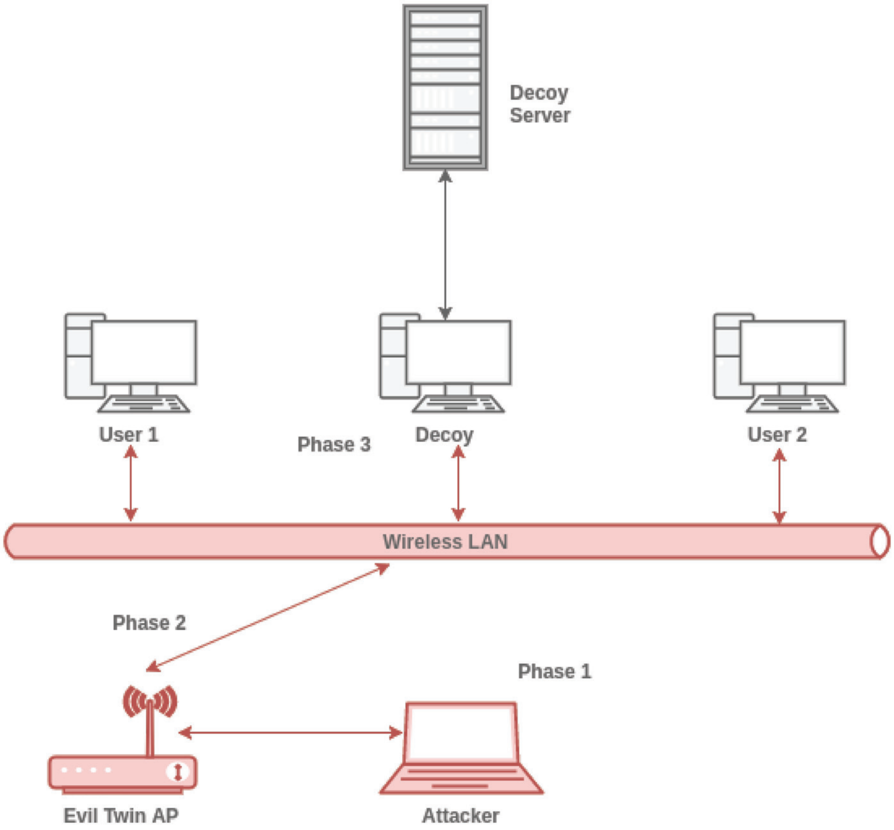
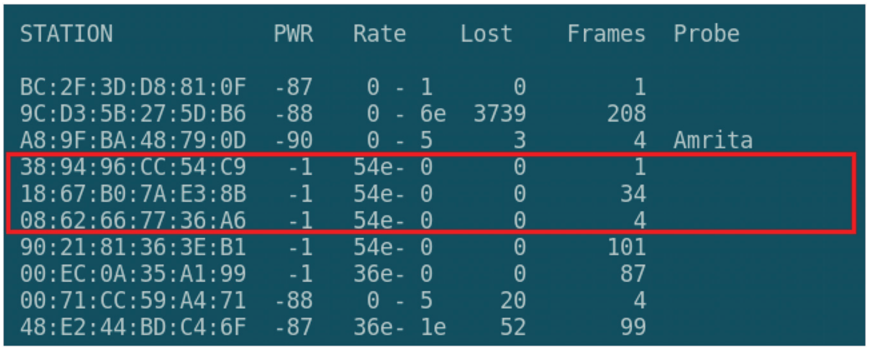


Figure 3 Attack scenario.

”Freenet”. DHCP server is configured and Internet access is provided to the evil twin AP. The red color box shows the MAC id of the 3 decoys that are connected to the evil twin as shown in Figure 4.

```
python sslstrip.pl l 1000
```

The attacker performs Man In The Middle attack to capture the network traffic of all the decoys and tries to decrypt the traffic by SSL stripping i.e downgrading the HTTPS to HTTP protocol [16]. The above command will perform the SSL stripping attack. Once the attack starts,the infected decoy will trigger an alert since it detects the downgrading attack and reports to the decoy management server.



```
STATION              PWR   Rate    Lost    Frames  Probe

BC:2F:3D:D8:81:0F   -87    0 - 1      0        1
9C:D3:5B:27:5D:B6   -88    0 - 6e  3739      208
A8:9F:BA:48:79:0D   -90    0 - 5      3        4  Amrita
38:94:96:CC:54:C9    -1   54e- 0      0        1
18:67:B0:7A:E3:8B    -1   54e- 0      0       34
08:62:66:77:36:A6    -1   54e- 0      0        4
90:21:81:36:3E:B1    -1   54e- 0      0      101
00:EC:0A:35:A1:99    -1   36e- 0      0       87
00:71:CC:59:A4:71   -88    0 - 5     20        4
48:E2:44:BD:C4:6F   -87   36e- 1e    52       99
```

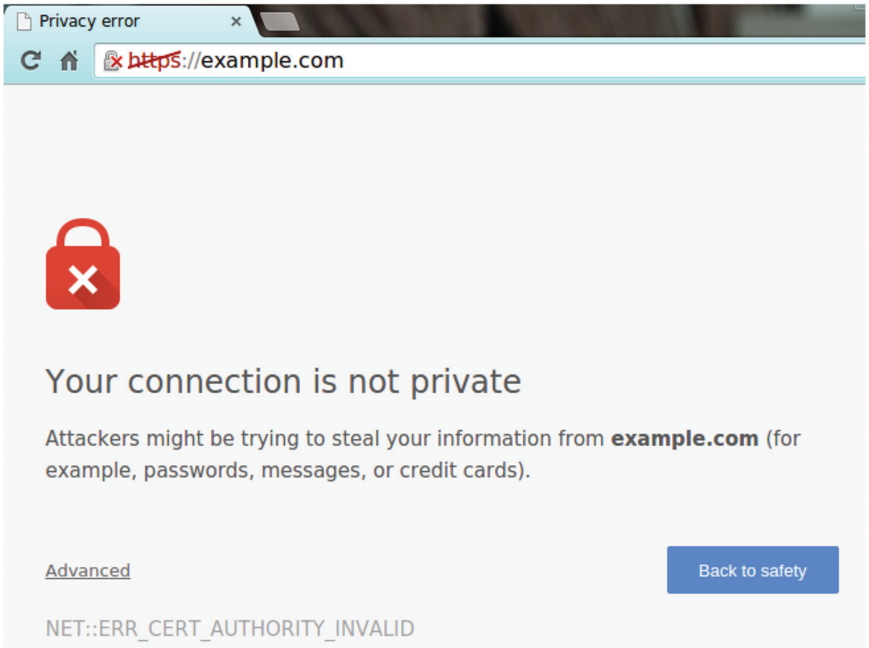
Figure 4 The red color box indicates 3 decoys are connected decoys to the evil twin AP.

5 Monitoring and Logging

All the network traffic pattern is monitored and logged in real-time. Log management is done by the decoy management server. We have not configure the decoy management server at this moment. Logs are collected in each decoys and analysis is performed manually. Example: Consider an attacker performing SSL striping attack in his evil twin. He can downgrade the HTTPS protocol to HTTP, making the network traffic of all the decoys unencrypted. Logs will be generated and alert will be raised by the decoy since HTTPS downgrade attack is detected on the decoy machines. This incident will be reported to the configured decoy server. Figure 5 shows the certificate error and Figure 6 shows the network traffic log after the SSL stripping attack on the decoy machine. The username and password field is decrypted after the downgrade attack. The attack is successfully performed on the decoy machines and logs are collected using the wireshark tool. The generated log is analyzed and the incident be reported as a SSL stripping attack.

6 Conclusion

Wi-Fi access point security plays a crucial role in securing the information of the connected users. In this paper, we have implemented the small-scale deception environment to fingerprint the information about the attacker's malicious behavior. The attacker's activity is efficiently captured by our decoys with the less false positives. With this proposed approach we can identify and detect the attacks like Man In The Middle, Packet injection, Packet modification and SSL stripping without affecting the legitimate clients on the wireless Local Area Network (WLAN) effectively.

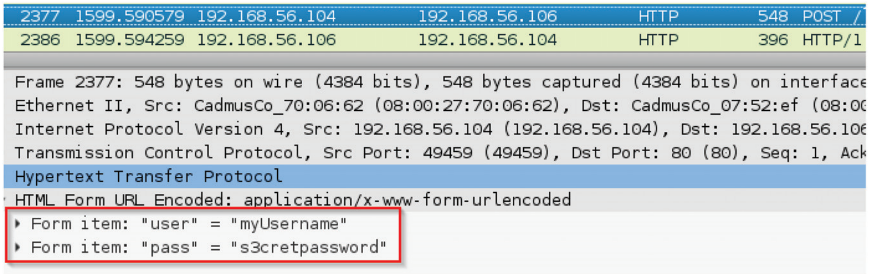


Your connection is not private

Attackers might be trying to steal your information from **example.com** (for example, passwords, messages, or credit cards).

NET::ERR_CERT_AUTHORITY_INVALID

Figure 5 Certificate error after the SSL Stripping attack.



```
 2377  1599.590579 192.168.56.104          192.168.56.106        HTTP          548  POST /
 2386  1599.594259 192.168.56.106          192.168.56.104        HTTP          396  HTTP/1

Frame 2377: 548 bytes on wire (4384 bits), 548 bytes captured (4384 bits) on interface
Ethernet II, Src: CadmusCo_70:06:62 (08:00:27:70:06:62), Dst: CadmusCo_07:52:ef (08:00
Internet Protocol Version 4, Src: 192.168.56.104 (192.168.56.104), Dst: 192.168.56.106
Transmission Control Protocol, Src Port: 49459 (49459), Dst Port: 80 (80), Seq: 1, Ack
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
 ▸ Form item: "user" = "myUsername"
 ▸ Form item: "pass" = "s3cretpassword"
```

Figure 6 Unencrypted network traffic after SSL stripping attack on the decoy machine.

7 Future Work

This entire paper focuses only on de-authentication attack and SSL Stripping attack. The low interaction decoys are configured to monitor these attacks. Advanced Persistent threats cannot be detected by these decoys as they are configured with minimal functionality and it requires high interaction decoys to fingerprint more information about the threat agents. Processing huge network traffic on the decoys is a trivial task and requires a manageable server to maintain logs. Further implementing this cyber deception strategy on large-scale wireless LAN environment will also enable the collecting of more information about the threat agents.

References

[1] Roth, V., Polak, W., Rieffel, E., and Turner, T. (2008). Simple and effective defense against evil twin access points. In *Proceedings of the first ACM conference on Wireless network security* (pp. 220–235). ACM.

[2] Bauer, K., Gonzales, H., and McCoy, D. (2008, December). Mitigating evil twin attacks in 802.11. In *IEEE International Performance, computing and communications conference, 2008. IPCCC 2008.* (pp. 513–516). IEEE.

[3] Lanze, F., Panchenko, A., Ponce-Alcaide, I., and Engel, T. (2014). Undesired relatives: protection mechanisms against the evil twin attack in IEEE 802.11. In *Proceedings of the 10th ACM symposium on QoS and security for wireless and mobile networks* (pp. 87–94). ACM.

[4] Modi, V., and Parekh, C. (2017). Detection & Analysis of Evil Twin Attack in Wireless Network. *International Journal of Advanced Research in Computer Science,* 8(5).

[5] Mohan, A. K., and Sethumadhavan, M. (2017). Wireless Security Auditing: Attack Vectors and Mitigation Strategies. *Procedia Computer Science,* 115, 674–682.

[6] Heckman, K. E., Stech, F. J., Schmoker, B. S., and Thomas, R. K. (2015). Denial and deception in cyber defense. *Computer,* 48(4), 36–44.

[7] Almeshekah, M. H., Spafford, E. H., and Atallah, M. J. (2013). Improving security using deception. *Center for Education and Research Information Assurance and Security, Purdue University, Tech. Rep. CERIAS Tech Report,* 13, 2013.

[8] Horák, K., Zhu, Q., and Bošanskı, B. (2017). Manipulating Adversary's Belief: A Dynamic Game Approach to Deception by Design for Proactive Network Security. In *International Conference on Decision and Game Theory for Security* (pp. 273–294). Springer, Cham.

[9] Heckman, K. E., Stech, F. J., Schmoker, B. S., and Thomas, R. K. (2015). Denial and deception in cyber defense. *Computer,* 48(4), 36–44.

[10] Wafi, H., Fiade, A., Hakiem, N., and Bahaweres, R. B. (2017). Implementation of a modern security systems honeypot Honey Network on wireless networks. In *2017 International Young Engineers Forum (YEF-ECE)*, (pp. 91–96). IEEE.

[11] Santoro, D., Escudero-Andreu, G., Kyriakopoulos, K. G., Aparicio-Navarro, F. J., Parish, D. J., and Vadursi, M. (2017). A hybrid intrusion detection system for virtual jamming attacks on wireless networks. *Measurement,* 109, 79–87.

[12] Rodrigues, M., and Shobayo, O. (2017). Design and Implementation of a Low-Cost Low Interaction IDS/IPS System Using Virtual Honeypot Approach. Covenant *Journal of Informatics & Communication Technology,* 5(1), 48–64.

[13] Agrawal, N., and Tapaswi, S. (2017). The Performance Analysis of Honeypot Based Intrusion Detection System for Wireless Network. *International Journal of Wireless Information Networks,* 24(1), 14–26.

[14] Maksutov, A. A., Cherepanov, I. A., and Alekseev, M. S. (2017). Detection and prevention of DNS spoofing attacks. In *Data Science and Engineering (SSDSE), 2017 Siberian Symposium on* (pp. 84–87). IEEE.

[15] Puangpronpitag, S., and Sriwiboon, N. (2012). Simple and lightweight HTTPS enforcement to protect against SSL striping attack. In *2012 Fourth International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN),* (pp. 229–234). IEEE.

[16] Clark, J., and van Oorschot, P. C. (2013). SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements. In *2013 IEEE Symposium on Security and Privacy (SP),* (pp. 511–525). IEEE.

[17] Nath, H. V. (2011). Vulnerability Assessment Methods–A Review. In *International Conference on Network Security and Applications* (pp. 1–10). Springer, Berlin, Heidelberg.

Biographies

A. Aswin Kumar is pursuing his M.Tech. in Cyber Security at TIFAC-CORE in Cyber Security from Amrita School of Engineering, Coimbtore and will graduate in 2018. He is currently working at Council of Scientific and Industrial Research – Fourth Paradigm (CSIR-4PI) as a part of the Students Programme for Advancement in Research Knowledge (SPARK) for his M.Tech. thesis. His area of research include Network Security and Reverse Engineering.

Ashok Kumar Mohan, M.Tech. specialized in Cyber Security, is a Research Associate at TIFAC-CORE in Cyber Security, Amrita Vishwa Vidyapeetham, Coimbatore, Tamil Nadu, India. He is currently a Ph.D. scholar doing his research in the area of Cyber Forensics funded by Ministry of Electronics & Information Technology (Government of India) under Visvesvaraya PhD scheme for Electronics and IT. He is currently pursuing his research over the cyber security core vicinity in Metadata Forensics, Wireless Security Auditing, Rumor Prediction in Social Media Networks and Slack Space Analysis of NTFS File Systems. He is also the Certified EC-Council Instructor (CEI) for ethical hacking and penetration testing certification courses at the research centre.

P. P. Amritha received her M.Tech. in Cyber Security from Amrita University. She is now a Ph.D. scholar at Amrita University. Her current research interests include: Steganography and Code Obfuscation.