Encountering social engineering activities with a novel honeypot mechanism

Mwaffaq Abualhija[1], Nid'a Al-Shaf'i[2], Nidal M. Turab[2], Abdelrahman Hussein[2]
[1]Department of Computer Science, Faculty of Information Technology, Al-Ahliyya Amman University, Amman, Jordan
[2]Department of Networks and Cyber Security, Faculty of Information Technology, Al-Ahliyya Amman University, Amman, Jordan

Article Info

Article history:

Received Jan 8, 2023
Revised Jan 16, 2023
Accepted Feb 26, 2023

Keywords:

Artificial intelligence
Cyberattacks
Intrusion prevention system
Social engineering attacks
Honeypot

ABSTRACT

Communication and conducting businesses have eventually transformed to be performed through information and communication technology (ICT). While computer network security challenges have become increasingly significant, the world is facing a new era of crimes that can be conducted easily, quickly, and, on top of all, anonymously. Because system penetration is primarily dependent on human psychology and awareness, 80% of network cyberattacks use some form of social engineering tactics to deceive the target, exposing systems at risk, regardless of the security system's robustness. This study highlights the significance of technological solutions in making users more safe and secure. Throughout this paper, a novel approach to detecting and preventing social engineering attacks will be proposed, combining multiple security systems, and utilizing the concept of Honeypots to provide an automated prevention mechanism employing artificial intelligence (AI). This study aims to merge AI and honeypot with intrusion prevention system (IPS) to detect social engineering attacks, threaten the attacker, and restrict his session to keep users away from these manipulation tactics.

Corresponding Author:

Nidal M. Turab
Department of Networks and Cyber Security, Faculty of Information Technology, Al-Ahliyya Amman University
Amman, Jordan
Email: N.turab@ammanu.edu.jo

1. INTRODUCTION

Information and communication technology (ICT) simplified everything through virtual networks and allowed people to perform tasks that were previously impossible due to national boundaries. Literally, everything can be performed easily, quickly, and most importantly, anonymously if needed. The investigation of computer network security defensive mechanisms had become vital to make the users feel safer and more protected when using the network. ICT can be used to commit crime in a variety of ways [1], [2]. It can be a target for crime where the attackers attempt to compromise the confidentiality, integrity, and availability of data, a.k.a. the confidentiality, integrity, and availability (CIA) triads, or in some cases the attacker attempts to use ICT as a method of operation to enable the crime such as: harassment and bullying. or it may hold and share terrorism content within the ICT component. Whatever the used approach, the attacker will always try to cause harm or get a financial gain or to satisfy his malicious instinct [3].

Most of these attacks, particularly the harmful ones, are carried out from outside and frequently from countries that have not signed international cooperation agreements, so law enforcement agencies face a variety of challenges in responding to such attacks, due to the difficulty of subjecting countries to these agreements and the impact of these crimes on people's lives, which has led many people and children specially to commit or attempt suicide. In this period, the safest way is to strive to limit these attacks and raise user awareness about them [1], [4], [5].

Popular preventative mechanisms include system hardening measures, which include establishing several barriers to avoid future attacks and mitigate the severity of those that do occur. These measures, however, are less effective in preventing cybercrimes perpetrated through social engineering mechanisms, in which the attacker exploited weaknesses in victim personalities to carry out his crime, either by having personal information about the victim or simply targeting a large group of people and attempting to deceive them. In the year 2020, statistics indicated that 80% of cybercrimes started with social engineering, and because people's knowledge and age groups vary and hacking tactics are renewed, this approach remains the most difficult to control [6]–[8].

Compared to traditional crimes, perpetrators of cybercrimes feel safe in an environment of greater anonymity, where there is a perceived barrier between them and victims [9]. This study threatens the safety principle offered by cyberspace which facilitates the process of concealing the identity of the perpetrator by demonstrating to the attacker that you are no longer anonymous. Moreover, the victim can be kept safe and protected by blocking the malicious channels, through presenting a unique technique for dealing with social engineering attacks to fill a research gap in this field. The proposed architecture suggests a model for blocking the malicious sessions and adding them to the intrusion prevention system (IPS) blacklist policy to threaten internet users who seeks to conduct a cybercrime utilizing a social engineering approach. The research builds on the findings of previous studies in this field, which focus on the detection and response to hacking and malware threats.

The proposed architecture is based on the honeypot concept, where the honeypot feedback is used to build a dataset to learn both intrusion prevention systems (IPS) and firewalls (FWs). The proposed infrastructure has several tiers, allowing the connections to be conducted in a controlled environment with only restricted access. The paper begins by discussing the concept of honeypots and describing how it assists with cyber defense. Following that, a brief overview on social engineering approaches will be provided, along with some applied prevention techniques. Furthermore, the research will provide the proposed architecture for encountering these threats using a honeypot integrated system in the method section.

Honeypots principles origin just before internet became a hotbed of cybercrime, one astute American citizen saw its terrible potential. Armed with solid evidence of electronic espionage, he began on a deeply personal mission to unmask a hidden network of spies jeopardizing national security. Cliff Stoll discovered an intruder accessing United States computer networks to steal high-value assets related to critical military and security information by spying on the attacker, which resulted in the hacker's arrest and prosecution for crimes of betraying national security, making it the first case in which digital evidence was presented as proven criminal evidence. As a result, Stoll released "The cuckoo's egg: tracking a spy through the maze of computer espionage," which included a proposal for a honeypot [10], [11].

A honeypot is a cybersecurity approach that uses deception to divert the attacker's attention away from legitimate targets or to understand contemporary hacking processes and safeguard networks from them. It operates by presenting itself on the internet as a potential target for attackers, usually a server or other high-value asset, then collecting data and alerting defenders when an unauthorized person attempts to access the honeypot. Honeypots can be considered as a distinct from and alternative methods of defense that are frequently employed in the production environment as a preventative measure [10]–[13]. Honeypots operation consist of: computer (acts as s server full of vulnerabilities like opened ports), application (acts as common services like web, dynamic host configuration protocol) and data (spoofed high value assets and unencrypted data). All these characteristics mislead the attacker into targeting this network, which is simply a monitored entity. There is a lot of classifications for honeypots depending on the infrastructure of the honeypot [14], [15] as shown in Table 1.

Table 1. Honeypots infrastructures and features

Infrastructure	Features
Pure honeypot	Production systems that track the honeypot's network connection. They are the most complicated and difficult to maintain, but also the most convincing to attackers, replete with simulated confidential files and user information
High-interaction honeypots	These replicate the operations of production systems, hosting a range of services and collecting a big amount of data. The purpose of a high-interaction honeypot is to lure an attacker into gaining root access to the server and then monitor the attacker's actions.
Low-interaction honeypots	They simulate the most common network attack vectors, making them less hazardous and easier to manage. The disadvantage of this form of honeypot is that it is more likely to appear to an attacker as forgery.

In our proposed solution, we will adapt the high-interaction honeypot scheme for social honeypot, where it can be connected to production network and still appear legitimate for attackers. Honeypots are considered a beneficial security entity in providing the security experts with real data about the behaviors and techniques for attackers, in addition to preventing network exploitation by providing the network admin with sufficient time to counter the attack and stop it. Even though there is a great security efficiency for honeypots, honeypots can put the production system under risk. This is since honeypots are not isolated networks and there is a connection enabling the administrator to collect information. Moreover, the experienced attacker can detect the honeypot system and then use it as jumping hop instead of stopping stone. Hence, it professionals need extra security measures to prevent honeypot exploitation [11], [12].

Social engineering attacks emerged as a result of internet and social engineering wide spread, socialization has become more accessible and immediate since digital communication technologies had developed. Personal and sensitive information could be available online through social networks. Telecommunication systems are vulnerable and can be effortlessly breached by malicious actors using social engineering techniques [16]. These cyberattacks are designed to deceive individuals or businesses into doing actions that benefit the attackers or reveal sensitive data such as social security numbers, health records, and passwords. Social engineering is one of the most challenging difficulties in network security regardless the robustness of the security scheme, because it takes advantage of the inherent human desire to trust, as they are the weakest link in security domain [17], [18]. According to the cyber security hub mid-year market for year of 2022, it is reported that 75% of respondents defined social engineering/phishing tactics as the biggest danger to cyber security at their business [19]. Although there are several methods and targets for conducting this form of penetration, they all have a common framework for the stages to be performed, which is illustrated in the Figure 1.

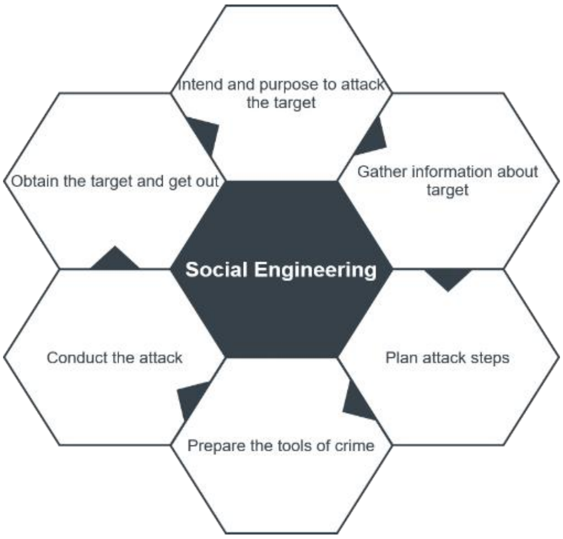
Intend and purpose to attack the target
Gather information about target
Plan attack steps
Prepare the tools of crime
Conduct the attack
Obtain the target and get out
Social Engineering

Figure 1. Social engineering attack stages

Depending on the perspective, social engineering assaults may be categorized into different types, and there many classification techniques depending on the categorized perspective. This research considered both direct and indirect approaches. Depending on the way the attacker follows to gather information about victim, whether through physical direct contact with him or using ICT networks where the existence of the attacker is not necessary, this operation may be carried out remotely using malicious software delivered via email attachments, short message services (SMS) or any form of online social engineering, and reverse social engineering [20]–[22]. The commonly used techniques are summarized in Table 2.

Prevention techniques are vital as social engineering attacks pose significant security threats. Hence, mitigating them should be a company's or institution's top priority, as well as being explicitly specified in their risk management plan. Companies should strive to foster safety awareness among their employees by properly training them and forcing them to sign the company policy, which contains all known techniques to mitigate social engineering attacks, as well as transfer responsibility for some attacks that occur due to unaware employees, keeping in mind that the highest level of awareness cannot mitigate this type of attack. Recently, much software is applied to avoid certain types of phishing attacks. Some proposed software used to ban blacklisted websites, because now the researcher is confident that a technological solution is needed. Combining multiple security systems together helps the network administrator to harden their security by reaching a proactive defense measure. There are some techniques accredited in defense in depth approach, such as intrusion detection system (IDS) and FWs, that are a proactive protective mechanism as they can notify the administrator of upcoming occurrences or respond to them in real time by restricting traffic access. Moreover, data encryption is essential to assure data confidentiality. Furthermore, other techniques are used to increase the cost of attack by adapting multi-layer security [23]–[25]. Yet, all the combined techniques cannot limit the extend of social engineering attacks [26], [27].

Table 2. Social engineering attacks

Social engineering attack	Description
Phishing attacks	Deceiving internet users (through fraudulent email messages or websites) into disclosing personal or private information. For example, in whale phishing, the attacker targets high-profile professionals to gain valuable company information, relying on psychological aspects of humans. These categories of people desire to succeed and accomplish achievement, and this is exactly what the notion adopts in social engineering, by analyzing each target's desire to make it easy to deceive them [28]–[30].
Pretexting attacks	Attempting to create bogus and convincing circumstances to obtain a victim's confidential information. These depend on false premises to convince the victim to believe and trust the perpetrator [20].
Baiting attacks	Type of phishing attempts that entice users to click on a link to receive free products, usually ending up with downloading malicious software [20].
Ransomware attacks	Disclose or restrict access to data or a computer system, often by encrypting it, unless the victim pays a ransom cost to the attacker [31]–[34].
Reverse social Engineering attacks	Takes an entirely different technique. It is a person-to-person operation in which the attacker makes direct contact with the victim to persuade them to provide sensitive information. In most situations, the hacker contacts the target via emails and social media platforms, employing numerous methods and masquerading as a benefactor or competent security staff to persuade them to grant access to their system/network [35].

2. PROPOSED SOLUTION AND METHOD

Currently there are four mitigating of social engineering attacks. These approaches depending on technology used widely to encounter some forms of social engineering attacks such as biometrics, sensors, artificial intelligence and social honeypots [26]. These approaches and their description are illustrated in Table 3.

This study proposed a novel approach to encountering social engineering attempts, in which social honeypot data is summarized in data sets and used to learn IPS to recognize this content and deny it. In addition, the attacker is notified and threatened by proving that they are no longer anonymous. Consequently, combining two mitigation techniques to ensure protection. This can be considered as automation for prevention mechanism. Honeypots acquire a significant interest from their potential to deceive lawbreakers by ability to attack legitimate network. As a result, the honeypots used in this research were more than simply basic internet sites that were established and posted online for to be view at arbitrary. A framework was built to guarantee that they were realistic in design and setup to provide users with a realistic exploration experience. We suggest adding social honeypots to track malicious behavior. Social honeypots are described as information system resources that monitor attackers' activities and log their data, while these logs can be classified in datasets in a predefined structure to be used as a source material to learn the IPS associated with this network. The outcome expected is having an automated security system encountering social engineering attacks.

Table 3. Social engineering mitigating approaches

Approach	Description
Biometrics	Aims to verify the identity of user, to avoid the physical attack, usually it is recommended to use more than one technique to verify the legitimate user.
Sensors	A way to verify the persons using sensor-based methods and might take benefit of inner body communication.
Artificial intelligence	Tries to improve and automate the security action, by adding new layer of security adapting the circumstances though adding, modifying, and updating some parameters.
Social honeypots	An information system resources that monitor malicious activities and log their information.

2.1. The proposed architecture

The proposed solution accomplishes the following tasks. Upon receiving malicious traffic from internet, traffic will be forwarded to firewall and then to IPS. Since they do not have the ability to detect social engineering behavior, traffic will be forwarded to internal network, but simultaneously a mirror for web traffic data forwarded to the honeypot. The Honeypot attempts to analyze the traffic by analyzing: the target of traffic, the content of messages (common message structure) used in phishing, and other configurable parameters. If a suspicious activity is observed, the honeypot immediately sends a threat message to the source and update the dataset information upon it the IPS will be updated to block the malicious connection. If the attacker's identity is hidden, the session traffic will be handled by a honeypot to provide enough time to uncover the attacker's identity. The flow of these steps is illustrated in Figure 2. Figure 3 provides a high-level architecture for the proposed solution. It also shows how the entities are connected to perform the requested task.

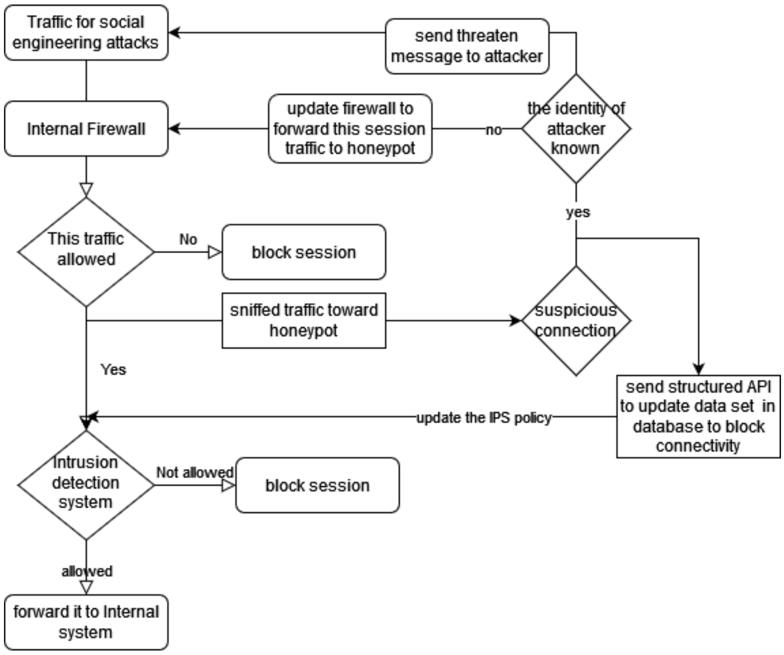
Traffic for social engineering attacks
send threaten message to attacker
Internal Firewall
update firewall to forward this session traffic to honeypot
no
the identity of attacker known
yes
This traffic allowed
No
block session
sniffed traffic toward honeypot
suspicious connection
Yes
send structured API to update data set in database to block connectivity
update the IPS policy
Intrusion detection system
Not allowed
block session
allowed
forward it to Internal system

Figure 2. The proposed solution data flow

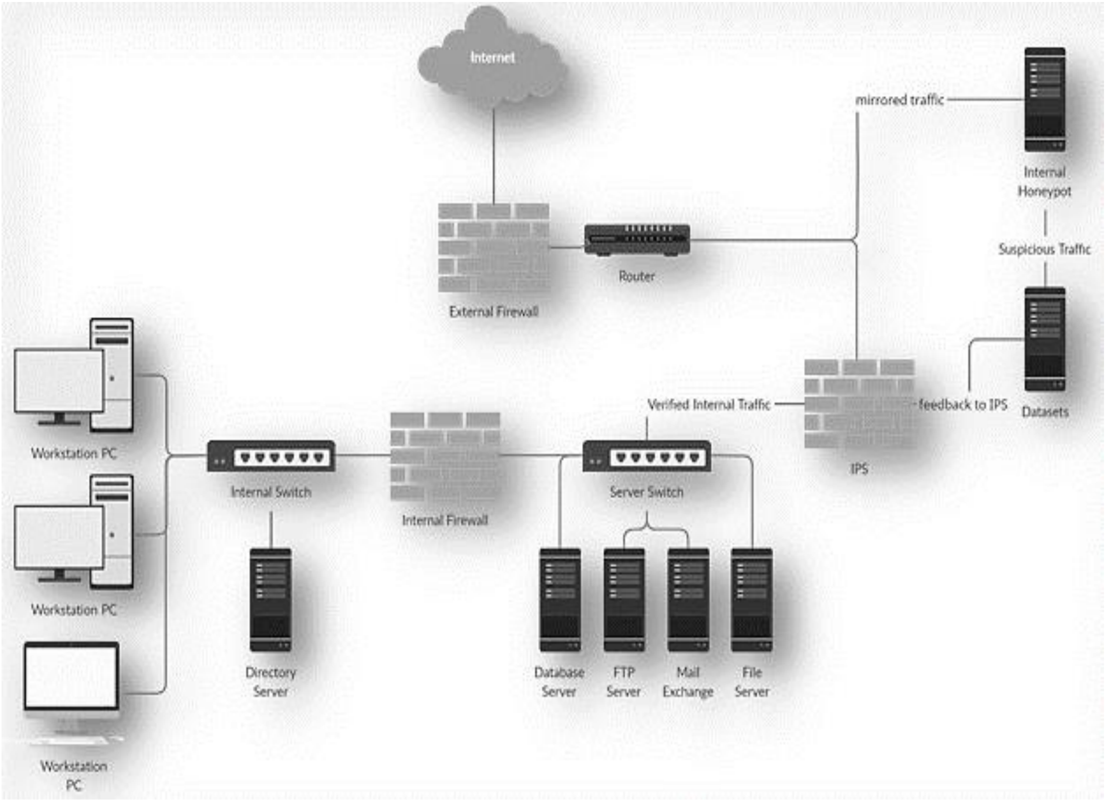

Figure 1. The architecture for the noble framework using integrated systems

3. RESULT AND DISCUSSION

Threatened attackers can minimize the amount of social engineering attacks, which is the ideal situation for risk management. However, risk avoidance cannot be guaranteed, that is why preventing attacks once they occur and mitigating the harm that may be done is a good aspect that we strive for. Through the above proposed architecture, the traffic will be passed as per the Figure 2.

Neither FW, IPS or IDS has the ability on its own to detect or capture social engineering attacks. A customized honeypot is configured to check pre-defined testing scenario, which is common between all phishing schemes, where it occurs on suspicious connection part of the above flow chart. A suspicious session is used to determine if this session is legitimate or fraudulent. Based on common indicators of phishing attempts defined by cybersecurity and infrastructure security agency (CISA), cybercriminal uses many forms to perform social engineering attacks such as: e-mail, short message service (SMS), instant chat and posts on social media, which typically looks to be from a reputable, well-known business, bank, or other organization. Furthermore, these suspicious forms usually include one or more recognized indicators of fraud [36]. Table 4 illustrates on the searching characteristics configured on honeypot for several indicators of fraud.

Table 4. Checking mechanism to determine suspicious traffic based on common characteristics

Testing	Indicators of fraud	Searching characteristics	Checking mechanism to determine suspicious traffic
1	Traffic contains suspicious link, hyperlinks, and websites	Identical to the original addresses (exist on DNS), with minor letter alterations	- Check if the address is like another address in DNS with 1 or 2 letter alternation maximum. - Check the reputation of the link or the site.
2	Suspicious sender’s address	Unknown sender, copying known e-mails with tiny differences in spelling	- Check if the address like anther known e-mail address with 1 or 2 letter alternation maximum.
3	Spelling and layout	Fraudulent e-mail translated via common tools and contained many mistakes	- Usually integrated with scenario 2, 3 and 6, in all these scenarios it is preferred to use misspelling as an indication
4	Suspicious attachments	Unknown sender email with an attachment	- Usually, this scam integrated with testing scenario 2, if there is suspicious sender the attachment is fraudulent indication
5	Generic greetings and signature	A generalized salutation, such as "Dear valued customer" or "Sir/Ma'am," and the absence of contact details in the signature	- This scam integrated with scenario 2 and 3, and mainly this message is broadcast, to deceive as many victims as possible.
6	Spread the need of immediate response	Attacker spread fear, threaten, panic, love and wealth in multiple form to induce victim response	- This scam integrated with scenario 2 and 3, and mainly this message is broadcast, to deceive as many victims as possible.

These testing procedures may be changed in response to the discovery of new social engineering techniques, allowing them to accommodate for any scenario. Upon receiving the traffic and performing the checking steps mentioned in Table 4 and detecting a suspicious traffic, honeypot will open a session to detect attacker location and threaten him by sending SMS to this entity that this action is illegal, and you will be prosecuted by law. Simultaneously, the honeypot will update the IPS, IDS, and FW to block the session. By this way, we are not relaying on user awareness 100%, still there is a system can perform this action based on artificial intelligence (AI) and machine learning (ML). The expected control from this proposed solution is very high in terms of common attacks such as whaling, cat phishing, and advanced fee scam. Nonetheless, it still needs attention to be compatible with new attacks [37], [38].

4. CONCLUSION

Organizations are investing money and effort into developing viable anti-social engineering measures. Nevertheless, present detection systems have fundamental limitations, and solutions are ineffectual in dealing with the rising number of social engineering attacks, approaches to innovation might also be limited since technical vulnerabilities can be exploited. Using this solution almost any type of social engineering attacks can be handled automatically, and incase new technique appeared simply we can update the honeypot configuration to monitor it. Detection systems have fundamental limitations, and solutions are ineffectual in dealing with the rising number of social engineering attacks, approaches to innovation might also be limited since technical vulnerabilities can be exploited.

Lack of researches on the use of automation security mechanisms to counter social engineering was also a big challenge in this study, because mostly all researchers are convinced that, regardless of the robustness of security systems, social engineering attacks can easily bypass them and that the only way to reduce harm is to raise user awareness. The researcher proposed a novel method in this study, however this solution should be tested, confirmed, and updated in a production network, therefore evaluating this technique in a production network is strongly encouraged for future work.

This research presents an overview of social engineering attacks, available detection technologies, and current countermeasure tactics in this study. Therefore, because of the nature of this attack, whatever the strength of system security is, it can be easily bypassed. Additionally, regardless of the amount of knowledge the users have, there is always a method to deceive them. That is why a new technical security model is required to overcome these vulnerabilities, which cost countries millions of dollars and contribute to the suicide of many people.

The research presents a novel technique in this study which merge AI and honeypot with IPS to detect these attacks, threaten the attacker, and restrict his session to keep users away from these manipulation tactics. This is the best technical approach that security experts can afford to counter attacks. However, this does not mean that user awareness is not crucial. User awareness comes first, particularly when considering that many social engineering attacks still begin by obtaining the information physically, which is outside of the security expert control area. As a result, users should be always aware to achieve the optimal security level.

REFERENCES

[1] S. Ibrahim, "Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals," *International Journal of Law, Crime and Justice*, vol. 47, pp. 44–57, Dec. 2016, doi: 10.1016/j.ijlcj.2016.07.002.

[2] D. Soylu, T. D. Medeni, R. Andekina, R. Rakhmetova, and R. Ismailova, "Identifying the cybercrime awareness of undergraduate and postgraduate students: example of Kazakhstan," in *2021 IEEE International Conference on Smart Information Systems and Technologies (SIST)*, Apr. 2021, pp. 1–7, doi: 10.1109/SIST50301.2021.9465995.

[3] AFP, "Cyber Crime," *Australian Federal Police*, https://www.afp.gov.au/crimes/cybercrime (accessed Mar 12, 2022).

[4] H. Almohannadi, I. Awan, J. Al Hamar, A. Cullen, J. P. Disso, and L. Armitage, "Cyber threat intelligence from honeypot data using elasticsearch," in *2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*, May 2018, pp. 900–906, doi: 10.1109/AINA.2018.00132.

[5] T. J. Holt, "Regulating cybercrime through law enforcement and industry mechanisms," *Annals of the American Academy of Political and Social Science*, vol. 679, no. 1, pp. 140–157, Aug. 2018, doi: 10.1177/0002716218783679.

[6] G. Costantino, A. La Marra, F. Martinelli, and I. Matteucci, "CANDY: a social engineering attack to leak information from infotainment system," in *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, Jun. 2018, pp. 1–5, doi: 10.1109/VTCSpring.2018.8417879.

[7] F. Breda, H. Barbosa, and T. Morais, "Social engineering and cyber security," in *INTED2017 Proceedings*, Mar. 2017, vol. 1, pp. 4204–4211, doi: 10.21125/inted.2017.1008.

[8] A. M. Aroyo, F. Rea, G. Sandini, and A. Sciutti, "Trust and social engineering in human robot interaction: will a robot make you disclose sensitive information, conform to its recommendations or gamble?," *IEEE Robotics and Automation Letters*, vol. 3, no. 4, pp. 3701–3708, Oct. 2018, doi: 10.1109/LRA.2018.2856272.

[9] S. Mazepa, L. Dostalek, V. Krivan, and S. Banakh, "Cybercrime in Ukraine and the cyber security game," in *2020 10th International Conference on Advanced Computer Information Technologies (ACIT)*, Sep. 2020, pp. 787–790, doi: 10.1109/ACIT49673.2020.9208942.

[10] L. Spitzner, *Honeypots: tracking hackers*. Addison-Wesley Professional, 2005.

[11] A. Mairh, D. Barik, K. Verma, and D. Jena, "Honeypot in network security," *Proceedings of the 2011 International Conference on Communication, Computing and Security*, 2011, doi: 10.1145/1947940.1948065.

[12] S. Touch and J.-N. Colin, "A comparison of an adaptive self-guarded honeypot with conventional honeypots," *Applied Sciences*, vol. 12, no. 10, May 2022, doi: 10.3390/app12105224.

[13] P. Radoglou-Grammatikis *et al.*, "Strategic honeypot deployment in ultra-dense beyond 5G networks: a reinforcement learning approach," *IEEE Transactions on Emerging Topics in Computing*, pp. 1–12, 2022, doi: 10.1109/TETC.2022.3184112.

[14] N. Eliot, D. Kendall, and M. Brockway, "A flexible laboratory environment supporting honeypot deployment for teaching real-world cybersecurity skills," *IEEE Access*, vol. 6, pp. 34884–34895, 2018, doi: 10.1109/ACCESS.2018.2850839.

[15] R. C. Perkins and C. J. Howell, "Honeypots for cybercrime research," in *Researching Cybercrimes*, Cham: Springer International Publishing, 2021, pp. 233–261.

[16] T. Mahmood and U. Afzal, "Security analytics: big data analytics for cybersecurity: a review of trends, techniques and tools," in *2013 2nd National Conference on Information Assurance (NCIA)*, Dec. 2013, pp. 129–134, doi: 10.1109/NCIA.2013.6725337.

[17] L. Xiangyu, L. Qiuyang, and S. Chandel, "Social engineering and insider threats," in *2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, Oct. 2017, pp. 25–34, doi: 10.1109/CyberC.2017.91.

[18] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," *Journal of Information Security and Applications*, vol. 22, pp. 113–122, Jun. 2015, doi: 10.1016/j.jisa.2014.09.005.

[19] CS Hub, "CS Hub Mid-Year Market Report 2022," Cyber Security Hub, 2022. Accessed: Apr 20, 2022. [Online]. Available: https://www.cshub.com/executive-decisions/reports/cs-hub-mid-year-market-report-2022.

[20] S. Gupta, A. Singhal, and A. Kapoor, "A literature survey on social engineering attacks: phishing attack," in *2016 International Conference on Computing, Communication and Automation (ICCCA)*, Apr. 2016, pp. 537–540, doi: 10.1109/CCAA.2016.7813778.

[21] H. Wilcox and M. Bhattacharya, "A framework to mitigate social engineering through social media within the enterprise," in *2016 IEEE 11th Conference on Industrial Electronics and Applications (ICIEA)*, Jun. 2016, pp. 1039–1044, doi: 10.1109/ICIEA.2016.7603735.

[22] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda, "Cutting the gordian knot: a look under the hood of ransomware

attacks," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9148, Springer International Publishing, 2015, pp. 3–24.

[23] A. Felt and D. Evans, "Privacy protection for social networking platforms," *Workshop on Web 2.0 Security and Privacy*. Oakland, CA. 22 May 2008.2008.

[24] P. Heymann, G. Koutrika, and H. Garcia-Molina, "Fighting spam on social web sites: a survey of approaches and future challenges," *IEEE Internet Computing*, vol. 11, no. 6, pp. 36–45, Nov. 2007, doi: 10.1109/MIC.2007.125.

[25] A. Alharbi, A. Alotaibi, L. Alghofaili, M. Alsalamah, N. Alwasil, and S. Elkhediri, "Security in social-media: awareness of phishing attacks techniques and countermeasures," in *2022 2nd International Conference on Computing and Information Technology (ICCIT)*, Jan. 2022, pp. 10–16, doi: 10.1109/ICCIT52419.2022.9711640.

[26] R. Vishwakarma and A. K. Jain, "A honeypot with machine learning based detection framework for defending IoT based botnet DDoS attacks," in *Proceedings of the International Conference on Trends in Electronics and Informatics*, Apr. 2019, pp. 1019–1024, doi: 10.1109/ICOEI.2019.8862720.

[27] M. Abu-Alhaija, "Cyber security: between challenges and prospects," *ICIC Express Letters, Part B: Applications*, vol. 11, no. 11, pp. 1019–1028, 2020, doi: 10.24507/icicelb.11.11.1019.

[28] J. Alqatawna, A. Madain, A. M. Al-Zoubi, and R. Al-Sayyed, "Online social networks security: threats, attacks, and future directions," in *Social Media Shaping e-Publishing and Academia*, Cham: Springer International Publishing, 2017, pp. 121–132.

[29] P. Patil and R. Devale, "A literature survey of phishing attack technique," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 5, no. 4, pp. 198–200, 2016.

[30] M. Masoud, Y. Jaradat, and A. Q. Ahmad, "On tackling social engineering web phishing attacks utilizing software defined networks (SDN) approach," in *2016 2nd International Conference on Open Source Software Computing (OSSCOM)*, Dec. 2016, pp. 1–6, doi: 10.1109/OSSCOM.2016.7863679.

[31] N. Andronio, S. Zanero, and F. Maggi, "HelDroid: dissecting and detecting mobile ransomware," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9404, Springer International Publishing, 2015, pp. 382–404.

[32] N. Scaife, H. Carter, P. Traynor, and K. R. B. Butler, "CryptoLock (and drop it): stopping ransomware attacks on user data," in *Proceedings - International Conference on Distributed Computing Systems*, Jun. 2016, vol. 2016-Augus, pp. 303–312, doi: 10.1109/ICDCS.2016.46.

[33] R. Brewer, "Ransomware attacks: detection, prevention and cure," *Network Security*, vol. 2016, no. 9, pp. 5–9, Sep. 2016, doi: 10.1016/S1353-4858(16)30086-1.

[34] E. Kirda, "UNVEIL: a large-scale, automated approach to detecting ransomware (keynote)," in *2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER)*, Feb. 2017, doi: 10.1109/SANER.2017.7884603.

[35] C. Lekati, "Complexities in investigating cases of social engineering: how reverse engineering and profiling can assist in the collection of evidence," in *2018 11th International Conference on IT Security Incident Management and IT Forensics (IMF)*, May 2018, pp. 107–109, doi: 10.1109/IMF.2018.00015.

[36] Y. Li, Z. Yang, X. Chen, H. Yuan, and W. Liu, "A stacking model using URL and HTML features for phishing webpage detection," *Future Generation Computer Systems*, vol. 94, pp. 27–39, May 2019, doi: 10.1016/j.future.2018.11.004.

[37] M. Abu-Alhaija, N. M. Turab, and A. R. Hamza, "Extensive study of cloud computing technologies, threats and solutions prospective," *Computer Systems Science and Engineering*, vol. 41, no. 1, pp. 225–240, 2022, doi: 10.32604/csse.2022.019547.

[38] M. Abu-Alhaija, "Crypto-steganographic LSB-based system for AES-encrypted data," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 10, pp. 55–60, 2019, doi: 10.14569/ijacsa.2019.0101009.

BIOGRAPHIES OF AUTHORS

Mwaffaq Abualhija Ph.D. in computing machines, system and networks, Associate Professor at the Computer Science, Al-Ahliyya Amman University, Jordan. His research interests operating system design, distributed computing systems, multimedia communication and networking, mobile and wireless networks, data and network security, wireless sensor networks, sorting and searching algorithms, parallel computing. He can be contacted by this email: m.abualhija@ammanu.edu.jo.

Nid'a Al-Shaf'i received her B.Sc. in Electronic and Telecommunication Engineering, graduated with Highest Honors from Philadelphia University in 2013. Currently, she is M.Sc. student at Cyber Security, Al-Ahliyya Amman University, Jordan. She can be contacted by email at nedaa.shafi@yahoo.com.

Nidal M. Turab Ph.D. in computer science Professor at the Networks and Cyber Security Department, Al-Ahliyya Amman University, Jordan. His research interests include WLAN security, computer networks security and cloud computing security, eLearning and internet of things. He can be contacted by this email: N.turab@ammanu.edu.jo.

AbdelRahman Hussein Ph.D. in computer science Assoicate Professor at the Networks and Cyber Security Department, Al-Ahliyya Amman University, Jordan. His research interests include mobile ad hoc networks, database management system, wireless networking. He can be contacted by this email: a.husein@ammanu.edu.jo.