Honeypot Security Efficiency versus Deception Solution

Sviatoslav Vasylyshyn[1], Ivan Opirskyy[1], and Svitlana Shevchenko[2]

[1] *Lviv Polytechnic National University, Stepana Bandery str., 12, Lviv, 79000, Ukraine*
[2] *Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*

Abstract

Deception technology has appeared on the market of information security systems relatively recently. However, some experts still consider Security Deception to be just a more advanced "honeypot." In this article, we will try to highlight both the similarities and fundamental differences between these two solutions. In the first part, we will tell you about honeypot, how this technology developed and what are its advantages and disadvantages. And in the second part, we will dwell on the principles of operation of platforms for creating a distributed infrastructure of false targets (DDP).

Keywords

Honeypots, baits, security, analysis, deception.

1. Introduction

Information security is a complex of technical and organizational measures and developed documents in the broadest sense of the word. The main goal is to protect and preserve information owned by the organization. However, information security remains an integral part of cybersecurity, a much broader category, and includes the protection of information and data, as well as the protection of systems, networks, etc. [1–3]. The main goals of information security also include the creation of a set of business processes that will protect information assets regardless of how information is formatted, whether it is in transit, processed, or is at rest, that is, stored in appropriate databases. According to experts, the value of an object is determined primarily by what information the company owns and how it is stored. Information security is a critical factor in ensuring the efficient conduct of business operations, as well as in maintaining and gaining the trust of customers, both future and existing [4]. And that is precisely why there is a problem of how to ensure the security of information during cyberattacks. One of these ways is the use of decoys and deception solutions. Honeypot is fundamentally different from all developments in the field of security. As a rule, all products in this market are designed to solve a strictly defined function (it doesn't matter whether hardware or software is involved): the firewall solves the tasks of restricting access from one network to another at different levels, the SSH service is designed for encrypted access to operating system resources, etc. Honeypot technology is not designed to solve a specific problem but represents a whole philosophy—flexible, customizable in accordance with the goal [5]. The basic principle underlying honeypots is to create traps for hackers. The very first Deception solutions were developed on the same principle. But, modern DDPs considerably surpass honeypots, both on the functionality, and on efficiency [6]. Deception platforms include: traps (decoys, traps), lures, applications, data, databases, Active Directory. Modern DDPs can provide ample opportunities for threat detection, attack analysis, and automation of responses. Thus, Deception are techniques to simulate the enterprise's IT infrastructure and mislead hackers. As a result, such platforms allow you to stop attacks before causing significant damage to the company's assets. Hoheypots, of course, do not have such a wide range of functionality and such a level of automation, so their use requires more skills from employees of IS departments.

CPITS-II-2021: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2021, Kyiv, Ukraine
EMAIL: swat2244@gmail.com (S. Vasylyshyn); iopirsky@gmail.com (I. Opirskyy); 0000-0002-9736-8623 (S. Shevchenko)
ORCID: 0000-0003-1944-2979 (S. Vasylyshyn); 0000-0002-8461-8996 (I. Opirskyy); s.shevchenko@kubg.edu.ua (S. Shevchenko)

2. Honeypot

For the first time, the term “honeypots” was used in 1989 in the book “The Cuckoo’s Egg” by Clifford Stoll, which describes the events of tracking a hacker at the Lawrence Berkeley National Laboratory (USA). This idea was put into practice in 1999 by Lance Spitzner, an information security specialist at Sun Microsystems, who founded the Honeynet Project. The first honeypots were very resource intensive, difficult to set up and maintain [7–10].

Let’s take a closer look at what honeypots and honeynets are. Honeypots are separate hosts, the purpose of which is to attract intruders to penetrate the company's network and try to steal valuable data, as well as expand the network coverage. A honeypot (literally translated as “a keg of honey”) is a special server with a set of different network services and protocols such as HTTP, FTP, etc. (Fig. 1).

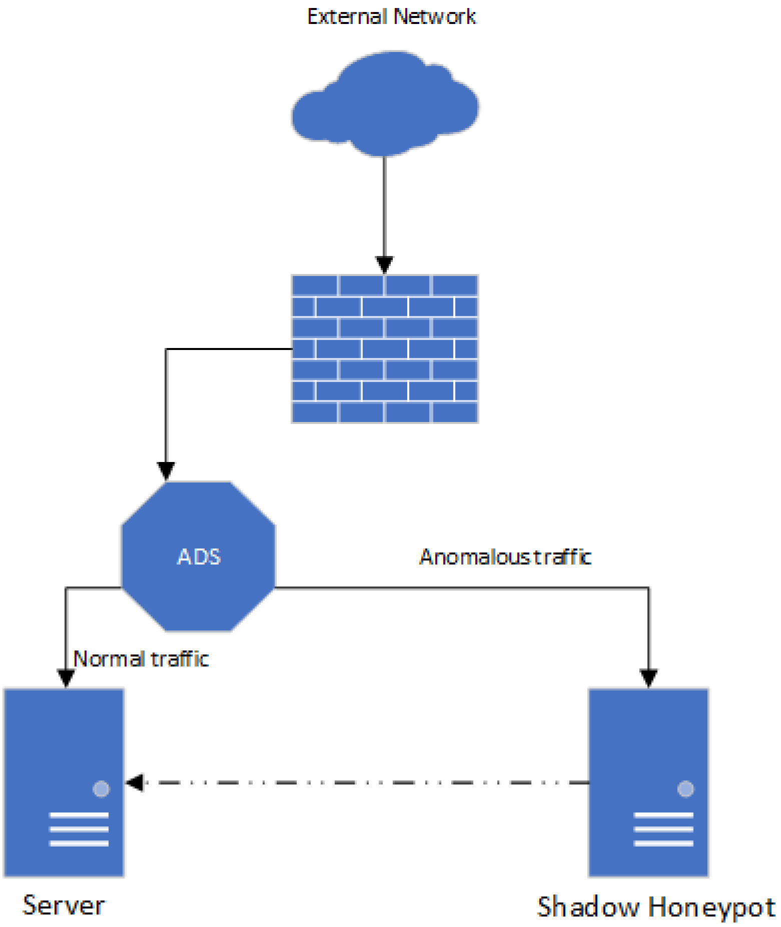

Figure 1: Honeypot placement scheme

If we combine several honeypots into a network, then we get a more efficient honeynet system, which is an emulation of the company's corporate network (web server, file server, and other network components). Such a solution allows us to understand the strategy of actions of the attackers and mislead them. A typical honeynet typically runs in parallel with, and completely independent of, a production network. Such a "network" can be published on the Internet via a separate channel, and a separate range of IP addresses can also be allocated for it [11].

The obvious benefit of honeynets is that they mislead intruders, wasting their energy, resources and time. As a result, instead of real targets, they attack false ones and can stop attacking the network without achieving anything. Most often, honeynets technologies are used in government agencies and large corporations, financial organizations, since these structures are the targets for large cyber attacks.

Why are honeypots and honeynets not the best solutions to counter attacks today? It should be noted that attacks are becoming more large-scale, technically complex and capable of causing serious damage to the IT infrastructure of an organization, while cybercrime has reached a completely different level and represents highly organized shadow business structures equipped with all the necessary resources. To this must be added the “human factor” (errors in the settings of software and hardware, actions of insiders, etc.), so the use of only technologies to prevent attacks is no longer enough at the moment.

Below are the main limitations and disadvantages of honeypots (honeynets):

- Honeypots were originally designed to identify threats that are outside the corporate network, are intended rather to analyze the behavior of intruders and are not designed to quickly respond to threats.
- Attackers have usually learned how to recognize emulated systems and avoid honeypots.
- Honeynets (honeypots) have an extremely low level of interactivity and interaction with other security systems, as a result of which, using honeypots, it is difficult to obtain detailed information about attacks and attackers, and therefore, to effectively and quickly respond to information security incidents. Moreover, information security specialists receive a large number of false alerts about threats.
- In some cases, hackers can use a compromised honeypot as a starting point to continue their attack on an organization's network.
- Problems often arise with the scalability of honeypots, high operational load and configuration of such systems (they require highly qualified specialists, do not have a convenient management interface, etc.). There are great difficulties in deploying honeypots in specialized environments such as IoT, POS, cloud systems, etc.

3. Deception Technology

Having studied all the advantages and disadvantages of honeypots, we come to the conclusion that a completely new approach to responding to information security incidents is needed in order to develop a quick and adequate response to the actions of attackers. And such a solution is Cyber deception (Security deception) technologies [12].

The terminology “Cyber deception,” “Security deception,” “Deception technology,” “Distributed Deception Platform” (DDP) is relatively new and appeared not so long ago. In fact, all of these terms mean the use of “deception technologies” or “techniques to imitate IT infrastructure and misinform attackers.” The simplest Deception solutions are the development of honeypots ideas, only at a more technologically advanced level, which involves more automation in detecting and responding to threats. However, there are already serious DDP-class solutions on the market, which imply ease of deployment and scalability, and also have a serious arsenal of “traps” and “baits” for attackers.

How does the “Distributed Deception Platform” work? After the deployment of DDP, the IT infrastructure of the organization will be built as if from two layers: the first layer is the real infrastructure of the company, and the second is an "emulated" environment consisting of decoys, traps and decoys. lures) that are located on real physical devices on the network (Fig. 2).

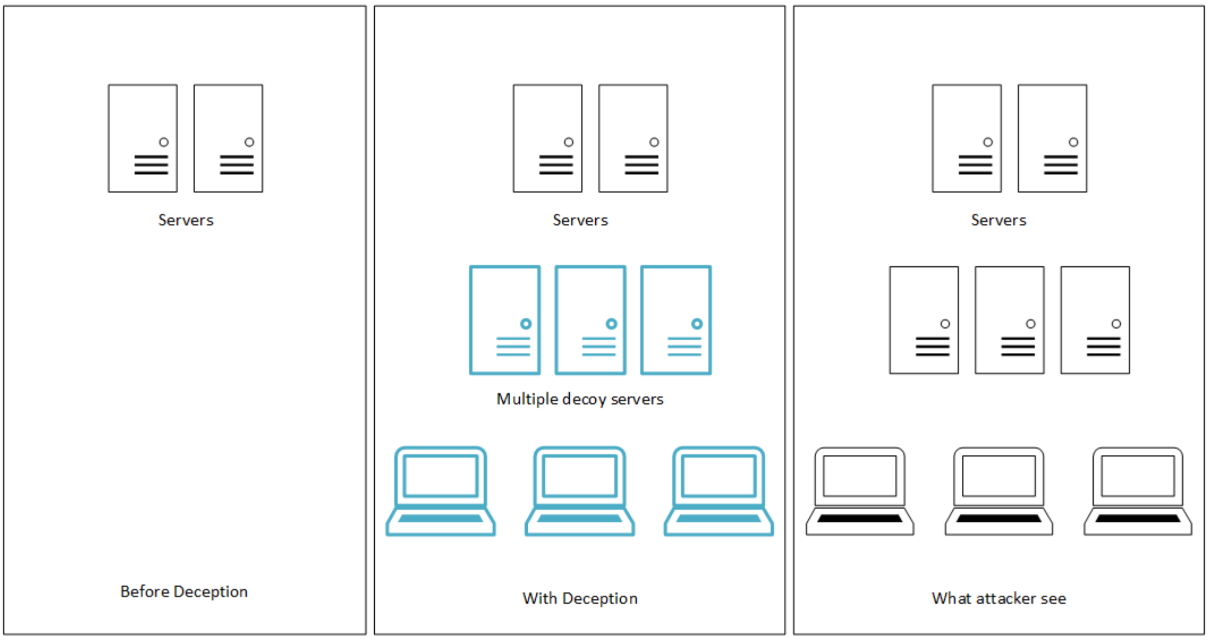

Figure 2: Deception system scheme

For example, an attacker can detect false databases with “confidential documents,” fake credentials of supposedly “privileged users”—all these are false targets, they can interest the attackers, thereby diverting their attention from the true information assets of the company.

DDP is a novelty in the market of information security products, these solutions are only a few years old and so far only the corporate sector can afford them. But small and medium businesses will soon be able to take advantage of Deception, leasing DDPs from specialized providers “as a service.” This option is even more convenient, since there is no need for your own highly qualified personnel.

The main benefits of Deception technology are shown below:

- Authenticity (authenticity). Deception technology is able to reproduce a completely authentic IT environment of a company, qualitatively emulating operating systems, IoT, POS, specialized systems (medical, industrial, etc.), services, applications, credentials, etc. Decoys are carefully mixed with the production environment, and an attacker would not be able to identify them as honeypots.
- Implementation. DDPs use machine learning (ML) in their work. ML provides simplicity, customization, and efficiency in implementing Deception. “Traps” and “decoys” are very quickly updated, involving the attacker in the “false” IT infrastructure of the company, and in the meantime, advanced analysis systems based on artificial intelligence can detect active hacker actions and prevent them (for example, an attempt to access Active Directory based on fraudulent accounts).
- Ease of operation. Modern “Distributed Deception Platforms” are easy to maintain and manage. Typically, they are managed through a local or cloud console, there is the possibility of integration with the corporate SOC (Security Operations Center) through the API and with many existing security controls. DDP service and operation does not require the services of highly qualified information security experts.
- Scalability. Security deception can be deployed in physical, virtual and cloud environments. DDPs successfully work with specialized environments such as IoT, ICS, POS, SWIFT, etc. Enhanced Deception platforms can project “trickery” technologies into remote offices, isolated environments, without the need for additional full platform deployment.
- Interaction. Using effective and attractive decoys that are based on real operating systems and cleverly placed among the real IT infrastructure, the Deception platform collects a wealth of information about the attacker. DDP then delivers threat alerts, generates reports, and automatically responds to information security incidents.
- The starting point of the attack. In modern Deceptions, traps and baits are placed within the range of the network, rather than outside of it (as is the case with honeypots). This model of

deploying traps prevents an attacker from using them as a launching point for an attack on a company's real IT infrastructure. In more advanced solutions of the Deception class, there are traffic routing capabilities, thus it is possible to direct all traffic of the attackers through a dedicated connection. This will allow you to analyze the activity of intruders without risking the company's valuable assets.

- The persuasiveness of "technology of deception". At the initial stage of an attack, cybercriminals collect and analyze data about the IT infrastructure, and then use it to move horizontally across the corporate network. With the help of "technologies of deception" the attacker will surely fall into "traps" that will lead him away from the real assets of the organization. DDP will analyze potential paths to access credentials on the corporate network and provide the attacker with "decoys" instead of the real credentials. These capabilities have been sorely lacking in honeypot technology.

4. Honeypot and Deception Comparison

We come to the most interesting point of our research. Let’s try to highlight the main differences between Deception and Honeypot technologies. Despite some similarities, these two technologies are still very different, ranging from the fundamental idea to the efficiency of work [13,14].

- Different basic ideas. As we wrote above, honeypots are installed as “decoys” around valuable company assets (outside the corporate network), thus trying to distract intruders. While honeypots are based on an understanding of an organization’s infrastructure, honeypots can be a pivotal point to launch an attack on a company’s network. Deception technology is designed with an attacker's point of view in mind and allows you to identify an attack at an early stage, thus, information security specialists get a significant advantage over attackers and gain time.
- Attraction VS Obfuscation. When using honeypots, success depends on attracting the attention of attackers and further motivating them to navigate to the target in the honeypot. This means that the attacker still has to get to the honeypot before you can stop him. Thus, the presence of attackers on the network can last for several months or more, and this will lead to data leakage and damage. DDPs qualitatively imitate the real IT infrastructure of a company, the purpose of their implementation is not just to attract the attention of an attacker, but to confuse him so that he wasted time and resources, but did not gain access to the real assets of the company.
- “Limited scalability” VS “Automatic scalability.” As noted earlier, honeypots and honeynets have scaling issues. It is difficult and expensive, and in order to increase the number of honeypots in a corporate system, you will have to add new computers, operating systems, purchase licenses, and allocate IP. Moreover, it is also necessary to have qualified personnel to manage such systems. Deception platforms are automatically deployed as the infrastructure scales, without significant overhead.
- “A large number of false positives” VS “no false positives.” The essence of the problem is that even a simple user may encounter a honeypot, therefore the “flip side” of this technology is a large number of false positives, which distracts information security specialists from their work. "Decoys" and "traps" in DDP are carefully hidden from the common user and are designed only for the attacker, so each signal from such a system is a notification of a real threat, and not a false alarm.

As an example of Honeypot and Deception technology comparison, please check Table 1. Please note that this is rough comparison chart made by looking over the standard possibilities provided by each platform and don’t includes unique solutions provided by private companies. Also this chart uses format from the previous tables that can be seen. It is done for the sake of formatting and for the purpose to create a standard for this kind of comparison between similar but different technologies. This way we will have a basic chart using all actual and use-case technologies in one place.

Table 1
Deception technology versus Honeypot comparison chart

Specifications	Honeypot technology	Deception technology
Fake OS platforms	—	Linux/ Windows
Phased attack detection	—	Intelligence: Active
C&C Detection	+	+
MITM Detection	+	+
Emulated traps	+	+
Industry Lures	+	+
NAC Integration	+	+
Full OS traps	+	+
SIEM Integration	+	+
EP Integration	+	+
EDR	+	+
AD	—	+
Correlation	—	+
Sandbox Integration	—	+
Database	—	+
POS	+	+
ATM	+	+
SCADA	unknown	+
IoT	+	+
Clouds	+	AWS/Azure
UCI	—	+
Open API	—	+
Botnet	—	+
Automatic code analysis	—	+
Trap constructor	+	+
API state passing	+	+
Forensics collection	—	+
Lures to real hosts	—	+
The mechanism for creating lures in AD	— —	+
IwC orchestration systems	—	+

For a scientific point of view we conducted a simple test by facing both out-of-the-box systems before written detection bot. As far as we can see form the Fig. 3, the Deception system has lower percentage in comparison to Honeypot to be detected. This tendentious fracture is secured on every try of the test. On average Honeypot is by 7% more detectable. The comparison you can see from the Fig. 4.

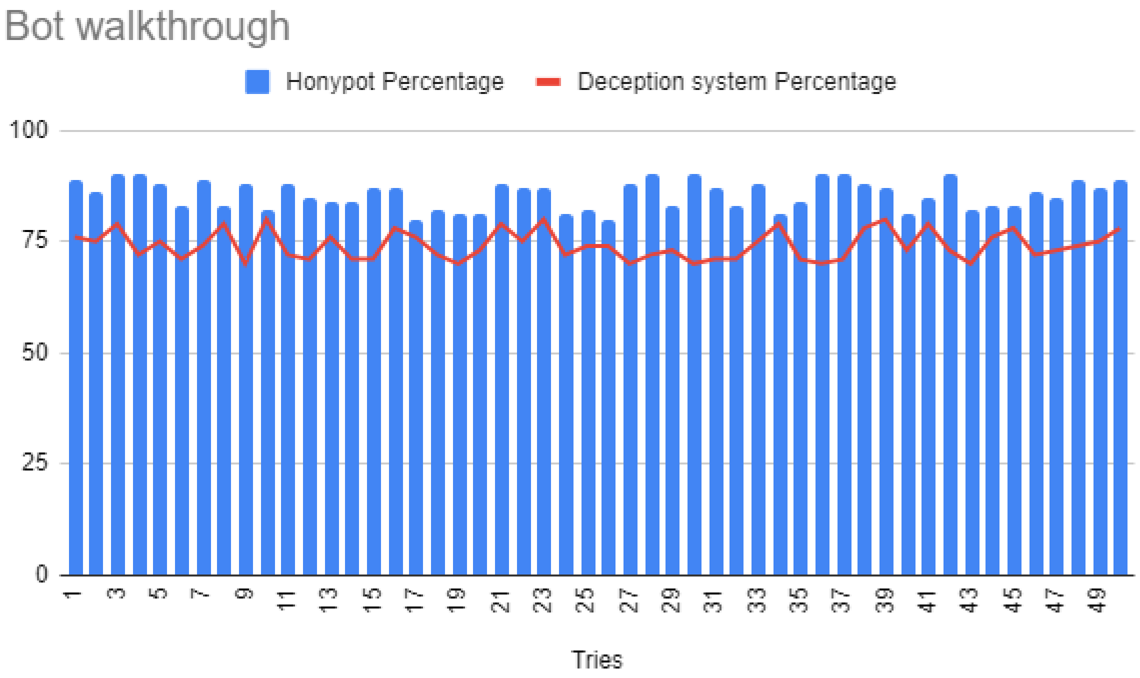

Figure 3: Systems pentest

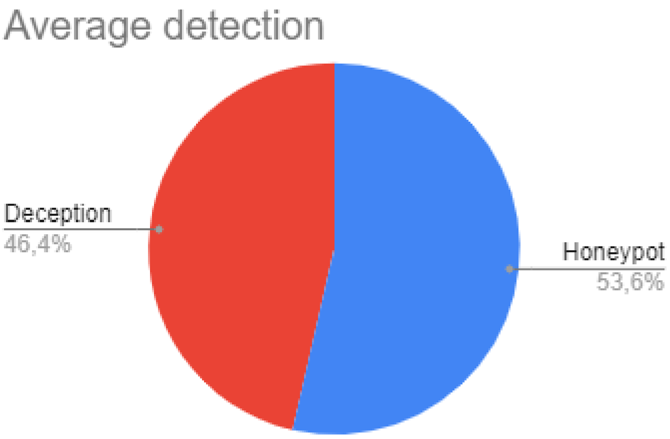

Figure 4: Average detection result

5. Conclusions

Deception technology is a huge improvement over the older Honeypots technology. In essence, DDP has become a comprehensive security platform that is easy to deploy and manage.

Modern platforms of this class play an important role in accurate detection and effective response to network threats, and their integration with other components of the security stack increases the level of automation, increases the efficiency and effectiveness of incident response. Deception platforms are based on authenticity, scalability, ease of management and integration with other systems. All this gives a significant advantage in the speed of response to information security incidents.

Also, based on observations of pentests of companies where the system was implemented, it can be concluded that even experienced pentesters often cannot recognize the baits in the corporate network and are defeated, falling for the set traps. This fact once again confirms the effectiveness of Deception and the great prospects that open up for this technology in the future.

6. References

[1] V. Lakhno, et al., Management of information protection based on the integrated implementation of decision support systems, Eastern-european journal of enterprise technologies. Information and controlling system, vol. 5, no. 9(89), 36-41, 2017. https://doi.org/ 10.15587/1729-4061.2017.111081.

[2] V. Dudykevych, et al., A multicriterial analysis of the efficiency of conservative information security systems, Eastern-european journal of enterprise technologies. Information and controlling system, vol 3, no 9(99), 6-13, 2019. https://doi.org/10.15587/1729-4061.2019.166349

[3] M.-D. McLaughlin, G. Janis, Challenges and best practices in information security management, MIS Quarterly Executive 17.3 (2018): 237-262.

[4] V. Susukailo, Cybercrimes investigation via honeypots in cloud environments, CEUR Workshop Proceedings, pp. 91, 2021.

[5] R. C. Joshi, A. Sardana, Honeypots: A new paradigm to information security, in Honeypots: A New Paradigm to Information Security, 1-323, 2011.

[6] D. Zhuravchak, Creation of a system for preventing the spread of extractor viruses using the python programming language and auditd utility based on operational system. Electronic professional scientific publication “Cybersecurity: Education, Science, Technology,” 4 (12), 108-116, 2021. https://doi.org/10.28925/2663-4023.2021.12.108116

[7] S. Udhani, A. Withers, M. Bashir, Human vs bots: Detecting human attacks in a honeypot environment. in A Varol, M Karabatak, C Varol & S Teke (eds), 7th International Symposium on Digital Forensics and Security, ISDFS 2019., 8757534, 7th International Symposium on Digital Forensics and Security, ISDFS 2019, Institute of Electrical and Electronics Engineers Inc., 7th International Symposium on Digital Forensics and Security, ISDFS 2019, Barcelos, Portugal, 6/10/19. https://doi.org/10.1109/ISDFS.2019.8757534

[8] C. Moore, Detecting ransomware with honeypot techniques, Proceedings 2016 Cybersecurity and Cyberforensics Conference, CCC 2016, 77.

[9] S. Litchfield, et al., Rethinking the Honeypot for Cyber-Physical Systems, IEEE Internet Computing, vol. 20, no. 5, 9-17, 2016.

[10] Z. A. Khan, U. Abbasi, Reputation Management Using Honeypots for Intrusion Detection in the Internet of Things, Electronics, 9, 2020.

[11] M. Akiyama, et al., HoneyCirculator: distributing credential honeytoken for introspection of web-based attack cycle. International Journal of Information Security, 2017. https://doi.org/10.1007/s10207-017-0361-5

[12] V. Gandotra, A. Singhal, P. Bedi, Threat-Oriented Security Framework: A Proactive Approach in Threat Management. Procedia Technology, 4, 487-494, 2012. https://doi.org/10.1016/ j.protcy.2012.05.078

[13] V. Buriachok, V. Sokolov, P. Skladannyi, Security rating metrics for distributed wireless systems, in: Workshop of the 8th International Conference on “Mathematics. Information Technologies. Education,” Modern Machine Learning Technologies and Data Science (MoMLeT and DS), vol. 2386, 222–233, 2019.

[14] J. Onaolapo, E. Mariconti, G. Stringhini, What Happens After You Are Pwnd: Understanding The Use Of Leaked Account Credentials In The Wild. Proceedings of the 2016 ACM on Internet Measurement Conference, IMC 16, 2016. https://doi.org/10.1145/2987443.2987475