From Cyber-Security Deception To Manipulation and Gratification Through Gamification

Xavier Bellekens
Gayan Jayasekara
Hanan Hindy
Miroslav Bures
David Brosset
Christos Tachtatzis
Robert Atkinson

This is the accepted version of a paper presented at the 21st International Conference on Human-Computer Interaction (HCII 2019), held in Orlando, on 26th- 31st July 2019.The final publication is available at Springer via https://doi.org/10.1007/978-3-030-22351-9_7 .

From Cyber-Security Deception To Manipulation and Gratification Through Gamification

Xavier Bellekens, Gayan Jayasekara, Hanan Hindy, Miroslav Bures, David Brosset, Christos Tachtatzis and Robert Atkinson

[1] Abertay University, Division of Cyber-Security
[2] Naval Academy Research Institute, France
[3] Czech Technical University, Prague
[4] University of Strathclyde

1 Abstract

Over the last two decades the field of cyber-security has experienced numerous changes associated with the evolution of other fields, such as networking, mobile communications, and recently the Internet of Things (IoT) [3]. Changes in mindsets have also been witnessed, a couple of years ago the cyber-security industry only blamed users for their mistakes often depicted as the number one reason behind security breaches. Nowadays, companies are empowering users, modifying their perception of being the weak link, into being the center-piece of the network design [4]. Users are by definition "in control" and therefore a cyber-security asset. Researchers have focused on the gamification of cyber-security elements, helping users to learn and understand the concepts of attacks and threats, allowing them to become the first line of defense to report anomalies [5]. However, over the past years numerous infrastructures have suffered from malicious intent, data breaches, and crypto-ransomeware, clearly showing the technical "know-how" of hackers and their ability to bypass any security in place, demonstrating that no infrastructure, software or device can be considered secure. Researchers concentrated on the gamification, learning and teaching theory of cyber-security to end-users in numerous fields through various techniques and scenarios to raise cyber-situational awareness [2][1]. However, they overlooked the users' ability to gather information on these attacks. In this paper, we argue that there is an endemic issue in the the understanding of hacking practices leading to vulnerable devices, software and architectures. We therefore propose a transparent gamification platform for hackers. The platform is designed with hacker user-interaction and deception in mind enabling researchers to gather data on the techniques and practices of hackers. To this end, we developed a fully extendable gamification architecture allowing researchers to deploy virtualised hosts on the internet. Each virtualised hosts contains a specific vulnerability (i.e. web application, software, etc). Each vulnerability is connected to a game engine, an interaction engine and a scoring engine.

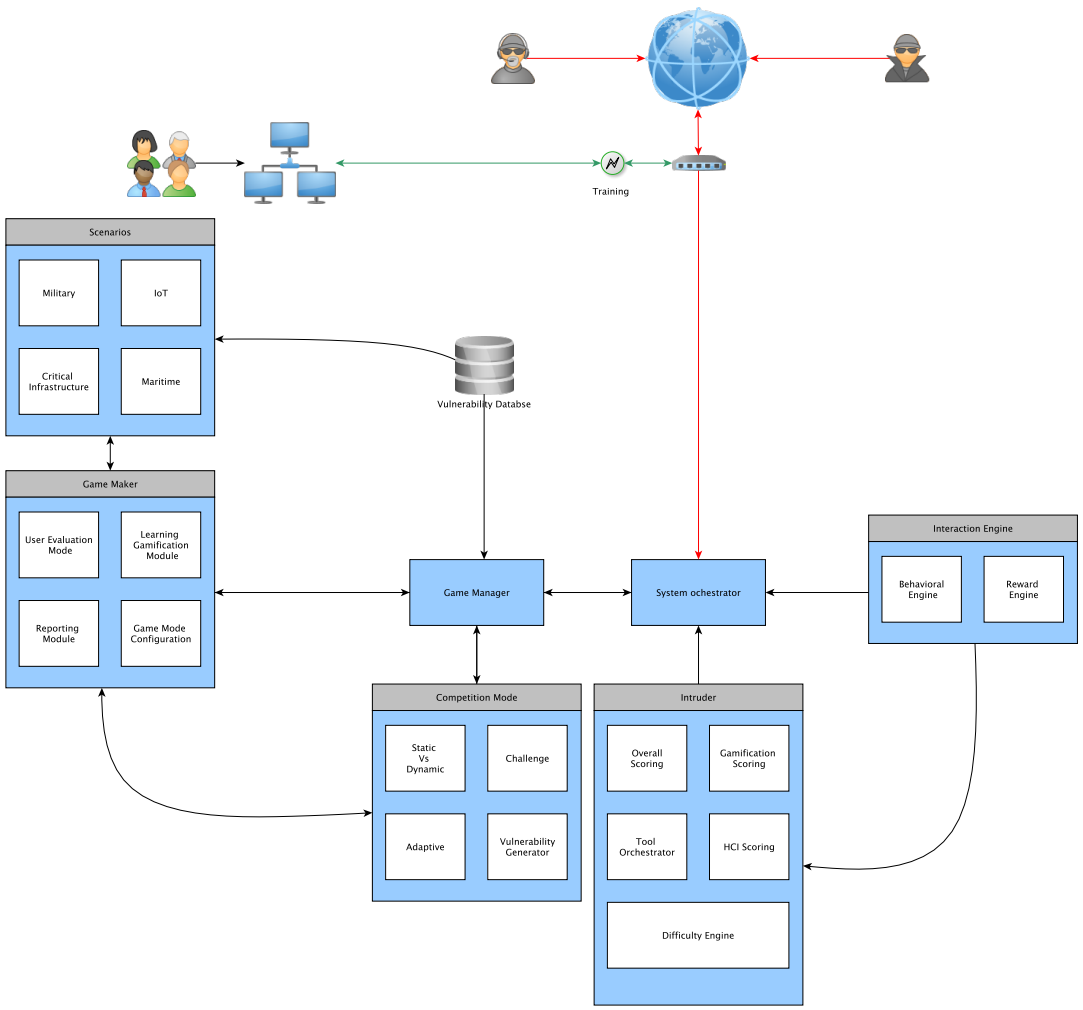

Fig. 1. Deceptive Platform Architecture

Figure 1 depicts the architecture of the platform. When a hacker connects to one or more virtual hosts, he is unable to differentiate it from a real-world computer (i.e. running a windows operating system), this is achieved by using port-scanning deception enabling to camouflage the signature of the operating system. Al interactions with the host(s) including time, behavioral (i.e. Keystroke dynamics, activity tracking, etc.), and engagement are further recorded and processed by the game and the scoring engines. allowing the hacker to be served with polymorphic vulnerabilities which, in turn, can increase or decrease their difficulties over time using, keeping the hacker engaged with the platform. Furthermore, Figure 1 shows that the interaction information gathered through the host(s) is fed to the scoring engine, which provides the hacker with rewards based on pre-defined scenarios. Using a threshold measures, the hacker's interest is further analysed. If his interest scores below threshold, subtle clues are provided to the hacker. The clues are inbuilt in each scenario. The clues vary from wireshark captures, to misleading network scans and vulnerability scans. The clues enable the hacker to seamlessly continue his malicious activity on the the network by following a pre-defined path, without suspecting interacting with a virtual environment. The path leads to data being gathered on the attacks, techniques, and tools used by hackers to solve each challenges thrown at him. All the gathered information are further analyzed using a circular methodology, enabling the operators to enhance the game engine and the variability of the difficulties. These information are further reported to build defence systems to protect against attacks. The vitalized hosts acts as a periscope for cyber-security operators but most importantly the information can be used to train end-users on the latest approaches a hacker employs to breach a network and potentially create hackers profiles through the data behavioral data obtained. In summary, this paper combines human-computer-interaction, behavioral analytics, gamification and deception to lure hackers into selected traps while peaking their interest to gather information that can further be used to enhance cyber-security training of end-users.

References

1. Almeshekah, M.H., Spafford, E.H.: Planning and integrating deception into computer security defenses. In: Proceedings of the 2014 New Security Paradigms Workshop. pp. 127–138. ACM (2014)
2. Almeshekah, M.H., Spafford, E.H.: Cyber security deception. In: Cyber deception, pp. 23–50. Springer (2016)
3. Desolda, G., Ardito, C., Matera, M., Piccinno, A.: Mashing-up smart things: a meta-design approach. In: Proceedings of workshop on end user development in the internet of things era–CHI15 EA. pp. 33–36 (2015)
4. Faily, S., Faily, S.: Why designing for usability and security is hard. Designing Usable and Secure Software with IRIS and CAIRIS pp. 3–8 (2018)
5. Zhan, X., Nah, F.F.H., Cheng, M.X.: An assessment of users cyber security risk tolerance in reward-based exchange. In: International Conference on HCI in Business, Government, and Organizations. pp. 431–441. Springer (2018)