Recent Developments in Electronics and Communication Systems
KVS Ramachandra Murthy et al. (Eds.)

doi:10.3233/ATDE221292

Practical Cybersecurity Learning with Usable Security

Binay Prakash Rout[a,1] and Dr. Vishal Bharti[b]
[a] *Chandigarh university*
[b] *Chandigarh university*

Abstract. In the digital era people are dependent on the web for the day-to-day needs. We human Beings use digital devices in every sector like from the chip of automobiles to the highly sophisticated medical equipment. From the road safety architecture to the home appliances all are connected to the internet. Having each and every device connected to the internet makes it easy for the bad actor to get into the system or the network and disrupt the intended use of the device even lead to many serious cybercrime issues. So, securing the network is the first priority of the software architecture. With this paper we are trying to explain the use of day-to-day software with the secure way which is useable by the user without any convenience. Also explain the different mitigation process at the time of and cybercrime incident and the walkthrough of the reach high level attacks and explaining the different software interface related to the security of the browser. The paper also mentioned some common tools used by bad actors. The method used by an attacker to intrude into a system is also explained in this paper which may help cybersecurity enthusiast to track down the infected device.

Keywords. Cyber kill chain, Usability Security, Phishing, implementation

1. Introduction

In this research paper we will focus on how a bad actor intrude into a system and conducts the attack and what are the basic or the first line of defense which is targeted by the attacker. As we all know humans are the first line of defense so the staff must have an awareness about the basic security concerns. Also, how well we're communicating with people about the risks of sharing their information and how they can protect it. The same difficulties exist in terms of privacy and security constraints. They're just not meant to be used by humans. People have trouble finding out how to make use of them. And the same solutions may be found in HCI for security and HCI for privacy. As a result, we'll go through the principles of human-computer interaction in this research paper. What is the most effective method for determining a person's cognitive and psychological abilities? How do we gain a better understanding of their professions and what they're trying to accomplish, and then seek for methods to incorporate that knowledge into systems and assess how effectively they're working?

Cyber kill chain basically how an intruder got into the system and violated the company policies. It's the process of understanding the mentality of an attacker how he approaches the system and carry the attack as the bad actors can be very much creative

[1] Corresponding author.

in conducting the attack so the cyber kill chain proposed by Lockheed Martin help the cyber security experts identify and block the attack at each of the respected stages.
Usability lives in the core of usable software. It's the method to calculate how convenient a system is for the user.

1.1. Swiftness

It is to say how fast a user can complete the task. Excluding the mistakes. For example, we'll take a survey to see if it's faster to unlock to an iPhone, using the finger print reader or a pin to authenticate. So the result is it took 1 second to login using the finger print authentication, but 4.8 seconds to unlock with the pin. Therefore, the finger print reader wins.

1.2. Effectiveness

It is to measure how effective a system is to the user for completing the task. Someone can complete the task quickly but can make a lot of mistakes. For example, it can type slow and correct but if you type fast then there can be higher chance of error.

If we want to measure the effectiveness of an IPhone authentication system like when the covid situation started the iPhone was unable to unlock using the face detection as people were using mask where as some android devices were able to unlock even if people were using mask. The IOS devices have also excluded the finger print feature in favors of Face ID Apple's iPhone 11 to iPhone 13 pro max have all out. This is where the iPhone effectiveness decreased. Similarly for the pin we will see how many times does the user makes a mistake or face a typing issue in the pin.

1.3. Learning

It's a eco system that's a system provides to the user that make's sure how easy the system is to access for the first time and the instructions provided by the system is very clear and visible to the user with the perfect clarity to continue working with the system and all the direction to the specific features needed by the user with little clustered information.

Like in iPhone after you turn on the screen it shows an option to slide the screen to unlock and similar in android it shows slide in the specific direction to unlock. This makes easy for a user to learn the method and when the pin pops up the user knows that he/she need to enter the pin to login. However, for the fingerprint and the face recognition it doesn't show any sign. Whereas in android it displays the finger print so that the user can use the finger print and login to the device.

1.4. Memorability

At the point when the client figured out how to utilize a system, memorability lets us know how simple it is for the client to remember the system. Regardless of whether they left the system for some time and return later, it is sure that they will recollect how to utilize the system. For example, the copy and paste keyboard shortcut in windows is easy to learn and use.

1.5. Personal Preference

This is the most important part of the remaining. In the field of usability security, personal preferences are quite important. Where the system may have all the factors sorted and secured but at last it really comes up to the personal preference, what a user likes about the system and how effective it is for the user to use the system, with little to no instructions needed. This has the worst usability of all other factors.
For example, the very popular discussion where the people are still confused whether to go with the IOS or the android Operating system. Lot of people argue that he IOS is the best optimized platform and way secure than android but android provide the significant or equal security compared to IOS.
The IOS is a very user-friendly platform where the user needs minimum instruction to perform the task as their focus is to provide the less but the best features, where as in android the user need to dig a little to find some features and functionality as it provides the freedom of customization and personal privacy policies override.
Its solely the User's preference what he likes as both the platform are stable and optimized and are reliable for the user.

1.6. Phishing

Phishing is a technique where the webpages or website pretend to be a legitimate webpage which tricks the user to enter the personal information or the financial information to the webpage. Here we are taking an example of Firefox browser which detects the phishing page and warns the user with a pop up showing that the page in fake and reported for web forgery and can lead to steal your personal and financial information.
Let's talk about security website and the issues in it. As we know there are number of phishing webpages flooded throughout the internet which makes the user life very hectic to decide and recognize the difference between the real and the fake web pages.
There are different types of browsers which help narrow out the legitimate webpages by displaying or flagging out the phishing webpages. But the way of warning a user plays a crucial role as the user may not be aware of the technical terms provided by the browser.
Talking about the active warning in the internet explorer warning it blocks the webpage from opening and displays the recommendation to close the webpage or continue with the webpage, the user not aware of the situation validates the page as authentic and continues as the warning are not that proper.
The passive warning in the internet explorer loads the page in the background and shows a popup window telling the user that the website may have been reported for web forgery which may or may not be understood by the user and may end up in filling the personal details in the web page.
The best example of the better detection of the phishing page is done by the Firefox browser which loads the page but popup a warning explains the user about the forgery page that the website is reported for stealing account credentials and you may lose your privacy and face a financial concern.
A flow chart of Cyber threat intelligence has been shown in Fig.1.

Figure 1. Cyber threat intelligence.

2. Problem Formulation

- The existing platform is complex and very difficult for a novice level enthusiast to learn and implement the tools and techniques.
- The installing of any ctf challenge is complex.
- The ctf zones face a constant issue of technical failure.
- Systems were leggy and the instruction to the challenges are difficult to understand.
- The paper provides an entry level learner to brush up with all the InfoSec terms to protect himself against any cybercrime and act as a first level of defence (human wall) as many organizations were not able to focus.
- Many organizations over build their cyber defence perimeter and miss out the basic level of defence making their employee self-awareness about the cybercrime scenario making the life easy for a bad actor to penetrate into the organization's system

3. Objective of Work

Creating a self-awareness among all the sectors of the company as it may decrease the load and focus area of the IT sector. Analysing the post exploit scenario, creation of proper documentation for future prevention. Implementation of proper chain of custody and usage of proper data recovery techniques in the time of a cyber-attack. Prepare the students for the future cybercrimes as the increase in cyber-attacks are increasing day by day. Unlike most specialized certifications, CTF challenges are 100% practical. The student must have a strong knowledge of the basic fundamentals of information security to pass the challenges successfully. This platform provides a practical way of learning the concept with practice providing the student with the basic white hat knowledge. The research paper focus on the real-life attacks and the case study of the walkthrough of high-profile attacks. Aims to simplify the learning of cyber security tools and techniques and mitigation of well-known attacks looking forward to software and human defence awareness using a virtual environment to learn and challenge the human mind using the ctf challenges and implement some real-life scenario like digital forensics, reverse engineering, binary exploits, web application vulnerability.

The flow chart of solutions has been shown in Figs 2, 3, 4 and 5.

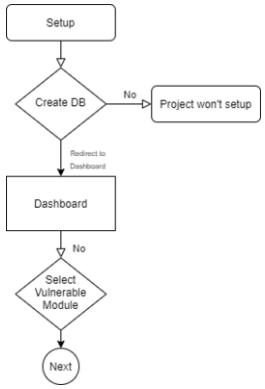

Figure 2. Flow chart of solution

Figure 3. Flow chart of solution (Contd.)

Figure 4: Flow Chart of Solution (Contd)

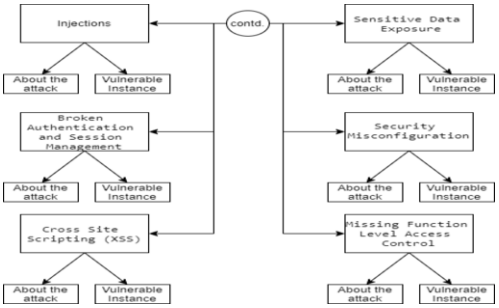

Figure 5: Flow Chart of Solution

4. Conclusion

In this digital era the cyber-attacks and the cybercrimes are increasing day by day. The bad actors are getting creative on each and every step. No matter how secure our network or devices are the cyber attackers will find a way to intrude into the system. In this fast-changing business environment, Shadow IT and cloud usage creep, 92% of the data breach are caused due to the human error and the average time to detect a data breach or a system compromise is 207 days in 2020 and the number of days is increasing per year. The number of files an average employee has access to be 11 million files. Hackers have many creative ways to tricks the victims and steal their personal information or financial credentials. In this paper we will discuss the techniques used by hackers to intrude and trick users. The software used by the user must also concentrate the security-based aspects because if the security is not compatible with the user experience, then it may ruin the overall security of the system as the user tries to override the security sector.

References

[1] NICK MAVIS, The art and science of detecting Cobalt Strike, TALOS, Cisco Security Researcher.
[2] Ioannis Lazaridis, Theodoros Arampatzis, Sotirios Pouros , Evaluation of Digital Forensics Tools on Data Recovery and Analysis, AMC Metropolitan College 14th El. Venizelou Str., 54624, Thessaloniki, Greece
[3] Paul Cucu , All about Rootkits, (https://heimdalsecurity.com/blog/author/paul/),SECURITY EVANGELIST
[4] Eldad Eilam, Reversing: Secrets of Reverse Engineering Published by Wiley Publishing, Inc. 10475 Crosspoint Boulevard Indianapolis, IN 46256
[5] Peter Mackenzie, What to expect when you've been hit with Avaddon ransomware, Ransomware as a Service {RaaS}(2021), https://news.sophos.com/en-us/2021/05/24/what-to-expect-when-youve-been-hit-with-avaddon-ransomware/
[6] OWASP Top 10 - 2017, The Ten Most Critical Web Application Security Risks, https://owasp.org/www-project-top-ten/2017/Top_10
[7] OWASP Web Application Penetration Checklist, OWASP, Version 1.1(2021)
[8] X-Force Threat Intelligence Index, IBM Security X-Force, IBM Security(2021)
[9] Dr. Allen Harper, Daniel Regalado, Ryan Linn, Stephen Sims, Branko Spasojevic, Linda Martinez, Michael Baucom, Chris Eagle, Shon Harris, Gray Hat Hacking The Ethical Hacker Handbook Fifth Edition, Copyright © 2018 by McGraw-Hill Education
[10] Dafydd Stuttard Marcus Pinto, The Web Application Hacker's Handbook Second Edition Finding and Exploiting Security Flaws, Published by John Wiley & Sons, Inc. 10475 Crosspoint Boulevard Indianapolis, IN 46256
[11] Numaan Huq , PoS RAM Scraper Malware Past, Present, and Future, Forward-Looking Threat Research Team
[12] INFOSEC Skills, https://app.infosecinstitute.com/portal/skills/home
[13] Kumar, Rohit. "DOS Attacks on Cloud Platform: Their Solutions and Implications." Critical Research on Scalability and Security Issues in Virtual Cloud Environments. IGI Global, (2018). 167-184.
[14] Georgia Weidman, "Penetration Testing- A hands-on Introduction to Hacking", Metasploit Framework, No Starch Press, (2018). 87-109
[15] Georgia Weidman, "Penetration Testing- A hands-on Introduction to Hacking", Password Attacks, No Starch Press, (2018). 197-214.
[16] Georgia Weidman, "Penetration Testing- A hands-on Introduction to Hacking", Wireless Attacks, No Starch Press, (2018). 339-357.
[17] Pandove, Kunal, Amandeep Jindal, and Rajinder Kumar. "Email spoofing." International Journal of Computer Applications 5.1 (2010): 27-30.
[18] G. McGraw, "Software Security", IEEE Security & Privacy, vol. 2, no. 2, pp. 80-83, 2004.
[19] OWASP, "Top-10 Application Risks - 2017" https://www.owasp.org/index.php/Top_10-2017_Top_10
[20] Penetration Testing – Wikipedia , (2017) https://en.wikipedia.org/wiki/Penetration_test
[21] https://CTFd.io & https://wiki.bi0s.in/