Trends in 2021 Major Cyber-Security Breaches

Molly Miller
Vanderbilt University
Nashville, TN
molly.h.miller@vanderbilt.edu

ABSTRACT

The goal of this project is to analyze the major security breaches of the present year 2021, and to identify trends from those breaches. Then, to map those identified trends to the CIA triad and other popular security topics.

Most major security breaches of the year 2021 were caused by attackers finding vulnerabilities in the companies' software systems. Fortune 500 Companies have been the victim to most of the breaches this year, even though these Fortune 500 companies pride themselves in acquiring secure software for their companies.

The worst data breaches of 2021 thus far include Parler, US Cellular, Kroger, Hobby Lobby, Facebook, and the famous Colonial Pipeline ransomware attack.

1. INTRODUCTION

Why do hackers and attackers like to hack into companies, mostly Fortune 500 Companies, and steal their personal data? Well, that's an easy answer, either to exploit company data, for money, or for both of those reasons. This just shows how and why Cyber-Security attacks will always be happening and will be a norm.

All the Cyber-Security breaches of 2021 can be mapped to popular security topics. The security topics that the attacks can be trended and mapped to include the CIA Triad, Principle of Least Privilege, Threat Modeling, Libraries/Dependencies, Cryptography, Phishing, and Two-Factor Authentication.

The CIA Triad is composed of confidentiality, integrity, and availability. These three standards of the triad are intended to be the foundation of a respectable security model/policy for a company. To understand the CIA triad, the three standards need to be explained. Confidentiality involves the efforts of an organization to make sure data is kept secret or private. Integrity involves making sure your data is trustworthy and free from tampering. Even if data is kept confidential and its integrity maintained, it is often useless unless it is available to those in the organization and the customers they serve. This means that systems, networks, and applications must be functioning as they should and when they should [4].

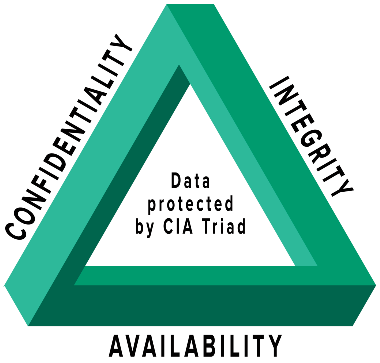

Figure 1: The CIA Triad

Principle of Least Privilege is a type of Role Based Access Control, which is where several users can be associated with different roles and those roles have different permissions and in turn, those permissions lead to different resources. Explaining Role Based Access Control, leads to defining Principle of Least Privilege, which is where each layer of the system for users should have a least set of privileges for the user to accomplish their job [15].

Threat Modeling works to identify, communicate, and understand threats and mitigations within the context of protecting something of value.

A Threat Model includes:

- Description of the subject to be modeled
- Assumptions that can be checked or challenged in the future as the threat landscape changes
- Potential threats to the system

- Actions that can be taken to mitigate each threat
- A way of validating the model and threats, and verification of success of actions taken [3]

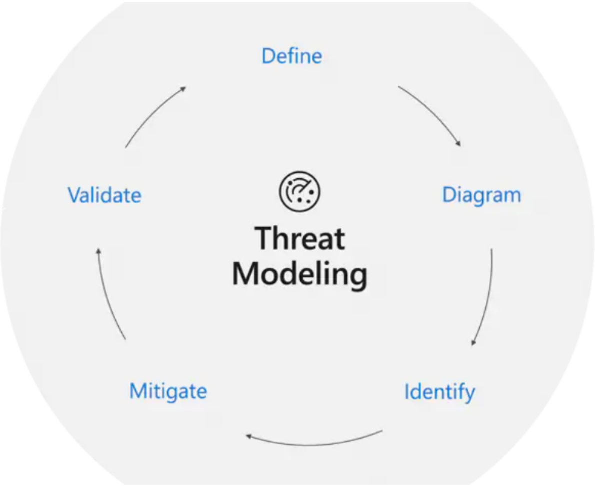

Figure 2: 5 Major Threat Modeling Steps

Libraries/Dependencies are utilized by software developers to plug into their codebase. This topic is a sense of why create the wheel, if it has already been created. Software developers will use libraries/dependencies to implement their code quickly, instead of having to write that portion of code themselves. When an open-source library is used in a software product (e.g. another library or an application), a dependency between the product and the library is created. This adds the task of managing these dependencies to the maintenance tasks of the product, and this task is not a trivial one. Open-source libraries can have security vulnerabilities that may affect the products that depend on these libraries [14].

Cryptography's aim is to construct schemes or protocols that can still accomplish certain tasks even in the presence of an adversary. A basic task in cryptography is to enable users to communicate securely over an insecure channel in a way that guarantees their transmissions' privacy and authenticity [1].

Phishing is a major security attack that can happen in a matter of seconds. This threat can lead to companies and individuals losing a great extent of personal identifiable information. A great deal of Phishing attacks happen through individuals giving up sensitive data in fraudulent emails.

Common Features of Phishing Emails:

- Too Good To Be True - Lucrative offers and eye-catching or attention-grabbing statements are designed to attract people's attention immediately.
- Sense of Urgency - A favorite tactic amongst cybercriminals is to ask you to act fast because the super deals are only for a limited time.
- Hyperlinks - A link may not be all it appears to be. Hovering over a link shows you the actual URL where you will be directed upon clicking on it.
- Attachments - If you see an attachment in an email you weren't expecting or that doesn't make sense, don't open it!
- Unusual Sender - Whether it looks like it's from someone you don't know or someone you do know, if anything seems out of the ordinary, unexpected, out of character or just suspicious in general don't click on it! [11]

Two-Factor Authentication is implemented in most software systems to validate authentication of the individual trying to access the system. Two-factor authentication (2FA) schemes aim at strengthening the security of login password-based authentication by deploying secondary authentication tokens. Two-factor authentication (2FA) promises a higher protection level by extending the single authentication factor, i.e., what the user knows, with other authentication factors such as what the user has (e.g., a hardware token or a smartphone), or what the user is (e.g., biometrics) [2].

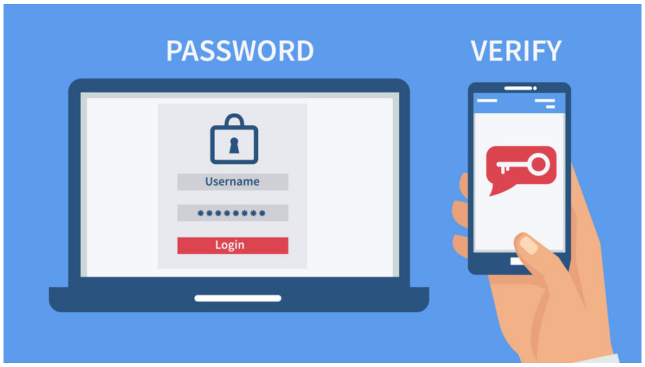

Figure 3: Two-Factor Authentication

2. 2021 CYBER-SECURITY BREACHES

All companies, including Fortune 500 companies, spend an abundance of funding on software security. Even though how prepared these companies are for cyber-attacks, the attacks will still happen. According to the Government Technology Magazine, the number of data breaches through September 30, 2021 has exceeded the total number of events in full year 2020 by 17 percent (1,291 breaches in 2021 compared to 1,108 breaches in 2020). Also, the total number of cyber-attack-related data compromises year-to-date (YTD) is up 27 percent compared to FY 2020 [9].

2.1 Parler: The Social Talking App Hack

Back in January of 2021, Parler, the app which is known as an outlet for free speech like Twitter, was hacked. During the election of 2020, many Trump supporters utilized this app to write about their republican views. Shortly after the election, Amazon cut off Parler from their web services due to a plan made on the application to invade the US Capitol Building. According to a security article about the breach written by Andy Greenberg, in the days and hours before

Amazon shutdown Parler, a group of hackers scrambled to download and archive the site, uploading dozens of terabytes of Parler data to the Internet Archive. The mass disemboweling of Parler's data had been carried out by exploiting a security vulnerability in the site's two-factor authentication that allowed hackers to create "millions of accounts" with administrator privileges. The truth was far simpler: Parler lacked the most basic security measures that would have prevented the automated scraping of the site's data [5].

The cyber-attack against Parler can clearly be mapped to the Principle of Least Privilege. If the Role Based Access Control had been correctly implemented in the social talking application codebase, attackers wouldn't have been able to create millions of administrative user accounts. Also, the Parler breach can be trended towards all the standards of the CIA Triad. The Confidentiality standard was broken in the breach since data was not kept private when the site's data was scraped. The concept of Integrity with the private, sensitive data fell apart, when the data was interfered with. The Availability standard was useless, after the Confidentiality and the Integrity standards collapsed. Two-Factor Authentication also plays a role, due to the fact that this major company didn't have the simple 2FA implemented into their system.

2.2 U.S. Cellular Scam

Another cyber-security breach happened in January 2021 and it affected the company U.S. Cellular, which is the fourth largest phone carrier brand in the United States. In a Forbe's article, the breach is explained that hackers reportedly gained access to protected systems by installing malware on a computer at a U.S. Cellular retail store. Hackers targeted a handful of U.S. Cellular store employees who had access to its customer relationship management (or CRM) software. The hackers were able to access customer names and addresses, cellular phone numbers, plan information and access PINs used when making changes to service. In some cases, the attackers used that information to port customers' phone numbers to other cellular carriers [10].

This breach can be gravitated towards the major security topic of Phishing. Attackers phished employees by sending them fraudulent emails and those employees fell victim to the scam. This led to the exploitation of U.S. Cellular customers' personal identifiable information. Also, it can be linked to the CIA Triad, since the Confidentiality standard was flawed when U.S. Cellular customers' private data was exploited, the Integrity standard was broken after the personal data was tampered with, and the Availability standard was ineffective because the system wasn't functioning as it was intended to function.

2.3 Kroger Accellion Incident

In early February of 2021, Kroger's third-party software Accellion, utilized for secure file transfers, was compromised. As stated by Kroger, Accellion notified Kroger that an unauthorized person gained access to certain Kroger files by exploiting a vulnerability in Accellion's file transfer service. The incident was isolated to Accellion's services and did not affect Kroger's own IT systems, including its grocery store systems. However, the Accellion software was used for secure file transfers of certain HR data and pharmacy and clinic customer information. Approximately 2% of our customers were impacted [8].

After analyzing this security breach, it's clear that it deals with the topic of Libraries/Dependencies. Kroger customers' personal identifiable information was exploited due to a library that Kroger utilized up until February of 2021. Kroger depended on this dependency, and it failed to remain secure. The topic of Cryptography is involved with this attack as well as the CIA Triad. The attacker stole Kroger customers' private information, but fortunately the data was encrypted. Unfortunately, the attacker was able to lay their hands on the decryption key to decrypt the customers' data. The Confidentiality standard of the CIA Triad was broken when the hacker exploited Kroger customers' personal, sensitive data. The Integrity standard was flawed when the encrypted customer private data was decrypted by the attacker. Lastly, the Availability standard failed when the hacker was able to steal data as the system wasn't functioning as it was inteneded to function.

2.4 Hobby Lobby Exposed

In late March of 2021, Hobby Lobby was involved in a cybersecurity breach. According to an article about the attack, Hobby Lobby has suffered a cloud-bucket misconfiguration, exposing a raft of customer information, including customer names, partial payment-card details, phone numbers, physical and email addresses, along with source code for the company's app. This attack totaled 138GB of data and impacted around 300,000 customers. It was housed in an Amazon Web Services (AWS) cloud database that was misconfigured to be publicly accessible [13].

This cyber-security breach trends with the Threat Modeling security topic. If Hobby Lobby followed this engineering technique of Threat Modeling, this Cloud misconfiguration to be accessible to the public would have been detected as a serious threat and vulnerability against their software system in the mitigation step. This breach can also be mapped to all the standards of the CIA Triad. This attack released 138GB of customers' private data to the world, so it broke the Confidentiality standard. The Integrity standard of the personal data was disregarded, and the Availability standard didn't matter since the system wasn't functioning correctly.

2.5 Facebook Data Breach

April of 2021, Facebook's site was scraped, and over 533 million users were affected. A user in a low-level hacking forum published the phone numbers and personal data of hundreds of millions of Facebook users for free. The exposed data includes the personal information of over 533 million Facebook users from 106 countries, including over 32 million records on users in the US, 11 million on users in the UK, and 6 million on users in India. It includes their phone numbers, Facebook IDs, full names, locations, birth dates, bios, and, in some cases, email addresses [6].

This major breach affects all the standards in the CIA Triad. The Confidentiality standard was violated as 533 million users' private data was published to the world. The Integrity of the user's private information had been tampered with by the attack. The Availability of the information was not in authorized hands, and that's how the Availability standard was compromised.

2.6 The Famous Colonial Pipeline

In May of 2021, the Colonial Pipeline was hacked, and this breach led to a gas shortage in the Southern United States. As explained in The New York Times, the hack underscored how vulnerable government and industry are to even basic assaults on computer networks. The attacker was not a terror group or a hostile state like Russia, China or Iran, as had been assumed in the simulations. It was a criminal extortion ring. The goal was not to disrupt the economy by taking a pipeline offline but to hold corporate data for ransom [12]. Colonial Pipeline Chief Executive Joseph Blount told a U.S. Senate committee that the attack occurred using a legacy Virtual Private Network (VPN) system that did not have multi-factor authentication in place [7].

Figure 4: The Famous Colonial Pipeline

As it is clearly seen, this famous ransomware attack is mapped to the topic of Two-Factor Authentication. Even if the password for the Colonial Pipeline's Virtual Private Network (VPN) had been complex, Two-Factor Authentication should have been implemented. Also, Threat Modeling should have been implemented for the Government's software and database systems. The engineering technique of Threat Modeling in the Mitigation step would have shown this vulnerability in the Government's system and possibly other threats and risks.

3. CONCLUSIONS

Cyber-Security Breaches are happening every day to Fortune 500 companies and even to Government Facilities. These attacks are happening often because hackers are finding security vulnerabilities in the companies' software systems. The major breaches of 2021 include Parler (the social talking app, similar to Twitter), U.S. Cellular (fourth largest mobile phone carrier in the United States), Kroger, Hobby Lobby, Facebook, and the Famous Colonial Pipeline ransomware attack. After analyzing these major cyber-attacks, the trends have been mapped to the security topics: the CIA Triad, Principle of Least Privilege, Threat Modeling, Libraries/Dependencies, Cryptography, Phishing, and Two-Factor Authentication.

4. REFERENCES

[1] J. S. Coron. What is cryptography? *IEEE Security Privacy*, 4(1):70–73, February 2006.

[2] A. Dmitrienko, C. Liebchen, C. Rossow, and A.-R. Sadeghi. On the (in)security of mobile two-factor authentication. In N. Christin and R. Safavi-Naini, editors, *Financial Cryptography and Data Security*, pages 365–383, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg.

[3] V. Drake. Threat modeling, 2020.

[4] Fortinet. What is the cia triad?, 2018.

[5] A. Greenberg. An absurdly basic bug let anyone grab all of parler's data, 2021.

[6] A. Holmes. 533 million facebook users' phone numbers and personal data have been leaked online, 2021.

[7] S. Kelly and J. Resnick-ault. One password allowed hackers to disrupt colonial pipeline, ceo tells senators, 2021.

[8] Kroger. Information about the accellion incident, 2021.

[9] D. Lohrmann. Data breach numbers, costs and impacts all rise in 2021, 2021.

[10] L. Matthews. Hackers breach u.s. cellular customer database after scamming employees, 2021.

[11] Phishing.org. What is phishing?, 2020.

[12] D. E. Sanger and N. Perlroth. Pipeline attack yields urgent lessons about u.s. cybersecurity, 2021.

[13] T. Seals. Hobby lobby exposes customer data in cloud misconfiguration, 2021.

[14] N. B. T'arrega and A. Oprescu. *Measuring the impact of library dependency on maintenance*. PhD thesis, University of Amsterdam, 2020.

[15] D. J. White. What least privilege means and why it matters.