COMP 815 – PROBLEM SET 1

PAVAN KUMAR DONDAPATI

SEPTEMBER 30, 2020

Research question: *[5 points]*

1) *[1 point]* We covered the classic CIA Triad for security professionals in class. Discuss what type of attack would violate each goal (i.e. talk about three different types of attacks, one per goal).

Word count: 578

According to the CIA Triad for security professionals, there are three major goals such as “confidentiality, integrity, and availability”. Each of these three goals is found to be prone to security breaches or vulnerable to cyber-attacks. These three goals can be violated by different types of attacks such as Direct-attacks, MitM (Man-in-the-Middle) attack, DOS (Denial-of-Service), Eavesdropping attack, Phishing and many others. In order to have in-depth understanding of what attack, each goal is vulnerable to, following is the overall description with evaluation for each goal, for instance:

Confidentiality: This goal refers to the degree of efforts that an organization puts for keeping their data secret and private.
This goal of CIA Triad for the security professionals can be violated in different manner, for instance, directs attack is a way to violate this goal. Direct-attacks are designed for gaining unauthorized access to the systems, databases, and applications with an objective of stealing or tampering with the data. This area is also vulnerable to the threat vectors, which direct the attackers capturing the network-traffic or stealing the passwords. Even a more-layered attack such as phishing and social engineering, a part of direct-attacks, violate “confidentiality”. Social-engineering is found to be the art of exploiting the human-psychology, instead of technical-hacking techniques for gaining access to systems, buildings or data. Social-engineer violates confidentiality by giving a call to an employee instead of trying for finding a software-vulnerability, and pose as an IT Support-executive, and finally trying for tricking the employee into divulging the employee’s password.

Integrity: Integrity is all about ensuring that the data is not tempered with, and thus, can further be trusted. Integrity ensures that the data is correct, authentic, and reliable enough. For instance, customers of a bank need to be able for trusting that their banking-information and a/c balances will never be tempered with.
This as one goal of Triad can also be violated through an attack-vector such as changing the system-logs for evading detection, tempering with intrusion detection-system or modifying the configuration files. This goal can be violated by “MitM”, for instance, this happens when the attacker intercepts communication between two different parties either for secretly eavesdropping or modifying the traffic travelling between the involved two parties. Attackers use MitM attacks for stealing the login credentials or personal-information, spying on the victim or sabotaging the communication or corrupting the data. For instance, the communication between a banker and its customers, here, MitM attackers steal customer’s login-credentials.

<u>Availability:</u> Applications, data and systems are found to be of least valuable to a firm and its consumers if the authorized users find these three inaccessible whenever the authorized users seek them. This means that applications, data, network and systems are well running, updated, and are available or give access to the authorized users.
DOS is the attack to which availability is vulnerable. DOS is found to be the most well-recognized attack, which threatens this goal, in this attack, the performance of the system, web-based application, website or web-based services, is maliciously and intentionally degraded, or even the system becomes entirely out of reach or unreachable. DOS attack is considered as the most brute force-act of cyber-aggression out there, the attackers do not alter the victim's data or even sneaking a peak at which the information, the attackers need not to have, they just overwhelm with traffic, thus, they cannot keep their website up. However, DOS attacks can be highly damaging, and hence, illustrates why this goal belongs to the CIA Triad.

2) *[1 point]* Choose two online systems (websites) you belong to and discuss their password policy. Talk about whether or not you feel each system's policy is secure enough and how you balance that with the type of risk it exposes you to.

Word count: 870

The two online-systems (websites) are "Facebook" and Amazon, however, the policy for creating password maintained by each of the websites is provided below:

<u>Facebook:</u> The password-policy used by Facebook seeks its users for creating that password, which needs to be unique to their Facebook ID and complex one to guess. Password to be used in securing Facebook account cannot be based on anything, which cannot be determined from the user's account. For protecting the security of FB A/c, Facebook asks its users for creating a password of minimum 6 characters of length, and that password needs to be composed by using a mix of lowercase (A-Z) and uppercase characters (a-z), symbols (special-characters and punctuations), and digits (0-9). If a user enters his/her password incorrectly for more than 20-times, then, their account will automatically be locked-out for temporary period. Thus, currently Facebook seeks for entering mobile-number, thus, a code could be sent on that number, and then password could be retrieved from there.

From own perspective, the ***password-policy of Facebook*** is found to be secured enough. It is due that Facebook invests time and amount both for securing every account at its best. Facebook offers security tips and features to its users, thus, the users can use Facebook security features such as login-alerts with approvals. In this way, the users can review and further update their security settings at any time. There are few FAQs (Frequently Asked Questions), which also lead Facebook users to be aware of any fraudulent activity, for instance, a few set of questions, a Facebook user can have on Facebook website such as what a user can do for protecting his/her account, how a user can start Facebook Security Checkup, and many others. Furthermore, Facebook at a constant rate seeks its users for updating their application, and gives notification to update their application, which keeps the users away from any cyber-attack.

Risks: There is a risk of being exposed to prying-eyes, unwanted marketers, and scammers. Privacy and security are at a greater risk of being violated, when a user log-into Facebook because of the security gaffes or the marketing efforts put by the global company. As Facebook ads sometimes contain malware, scammers are creating fake-profiles, real-friends sometimes unknowingly make the user vulnerable, and user's information can be shared with third-parties. Keeping own account secured and confidential is completely up-to the users, a key to be safe all the time is to keep a password of around 10-15 characters of length and every three-months, this password is to be updated. Users need to be wary of the banner ads being displayed on Faceboook, on Facebook. Although, if any malware contained website gets flashed over a user's profile, it will surely ask the user for downloading anti-virus, this message is hint of malware. Making friends on Facebook and trusting them is up-to a user, thus, it is in their hand to keep them safe, it is advised for not sharing any confidential information or data with that friend, who is somehow (in real-life) unknown to the users. Keeping own system/device secured by having a firewall defender or a strong anti-virus software, however, downloading anything from Facebook seeks a user special attention over it.

<u>Amazon:</u> The password-policy of Amazon asks the users to create their password of at least 6 characters (minimum) length to 16 characters (up-to) length. The users need to maintain three criteria while creating their password such as "UPPER-CASE, lower-case, or/and special characters ($, @, %, !, &, and, many others). There is a Two-Step Verification for the Amazon customers, whenever they need to connect with Amazon from an unknown device, then they need to enter a unique security code with respect to their password. Amazon customers can get a code on their registered mobile-number with which they can reset their password or enter with the last password. This two-step verification adds an additional layer of security to the Amazon account.

Considering own perception about the ***security-level maintained by Amazon***, it can be stated that customers can rely over the security-level that Amazon provides them. It is due to that Amazon provides the customers with every small instruction and indication about how to identify any spoofing and phishing, the customers also get an option for immediately reporting any phishing email. The customers can keep them safe by going through every single instruction provided by Amazon on its website.

Risks offered by using "Amazon" include over-payment, credit-card fraudulent, malware & adware, and identity theft. However, major risks, which the Amazon website makes its users getting exposed to, are identity-theft and credit-card fraud. Although, these risks can also be kept away from the user's accessibility to Amazon website, for instance, the customers of Amazon are well-instructed about not using a WebView for displaying Amazon-Pay web-pages within their application. It is important for the users for setting-up API-based transaction management and setting-up recurring payments. Furthermore, a few more instructions if followed can keep the risks away from the Amazon-user's reach, such as use of an approved browser-view mechanism for instance Safari-View Controller on the iOS or Chrome Custom-Tabs on Android and Amazon-Pay's recommendation is to thoroughly be followed, use of redirect authentication for the mobile-web for ensuring an optimal user-experience.

3) ***[1½ points]*** **Locate three sites on the internet that deal with web security. Use whatever means you want and give a brief 2 - 3 paragraph summary of each.**

Word count: 784

The three sites available on the internet, which deal with the security of the website with its description, are provided below:

Avast: Avast is among the pioneers in the business of computer-security, having its portfolio, which includes free anti-virus software for Mac, PC and Android, to the premium-services and suites for both the businesses and consumers. The CEO of this website security company is "Vincent Steckler", who privately holds this company, this has been founded in 1991, and currently the size of this company is 1K to 5K. Specialties of this company include the following:

- Application security
- Antivirus
- Recovery & Backup
- Network Security
- Data protection
- Data Security
- Email Security
- DLP
- Web Gateway Security or VPN
- IoT
- Secure communications
- Threat Management & Intelligence, and
- Web-application Security

This company has been educated towards creating such world, which provides privacy and safety for all, no matter who its users are, where they are or how they connect to the entire world or another device. Avast is recognized across the world as one of the largest security firms using the next-generation technologies for fighting against the cyber-attacks in the real-time world. This company differs from other next-gen firms in that manner that Avast has an immense machine-learning engine based on cloud receiving data-stream at a constant rate from their hundreds of millions of users. In addition, this rate of data-stream from a huge number of users facilitates learning at the unprecedented pace and makes their AI engine much faster and smarter as compared to anything else. This company has developed a scalable security-infrastructure based on cloud, which sees everything happened over the internet, currently, this firm prevents around 1.5 billion attacks on a monthly basis.

Cipher CIS: Cipher is such cyber-security firm, which provides white-gloves, holistic services for protecting the companies from attackers. This company as a part of the cyber-security division associated with "Prosegur", combines deep cyber-expertise with a deep understanding of the IoT and physical security. Its core services include the following:

- Cyber-technology Integration
- Governance Compliance and Risk
- Management of Security-services
- Cyber Intelligence-Services
- Red-Team Service, and
- Management of Detection with Response (MDR)

This Company being the leading cyber-security company across the world, has the right solution for its customers, for example, MDR end-to-end solution allows its customers for quickly adding 24*7 dedicated monitoring of threat, and many others. There are various reasons for which this company can be preferred as a website-security firm, for instance, its dedication towards reliability, this company is a part of group being huge traded by public, Cipher is a part of Prosegur, a MNC of security. This company has offices across 26 different countries across five continents; this company is offered as an integral part of Integra, which is the most comprehensive platform of security over the market, and this firm is also known as a "Pure-Player" having great specialization, their division has only one focus and that is on "Cyber-security". This company has been delivering from its local projects to the projects of global-scale to medium-sized firms to the large firms. Due to its reputation, approach towards innovation, capabilities, and certification that this company holds is of the highest-level, this company is highly preferred when it comes to website-security.

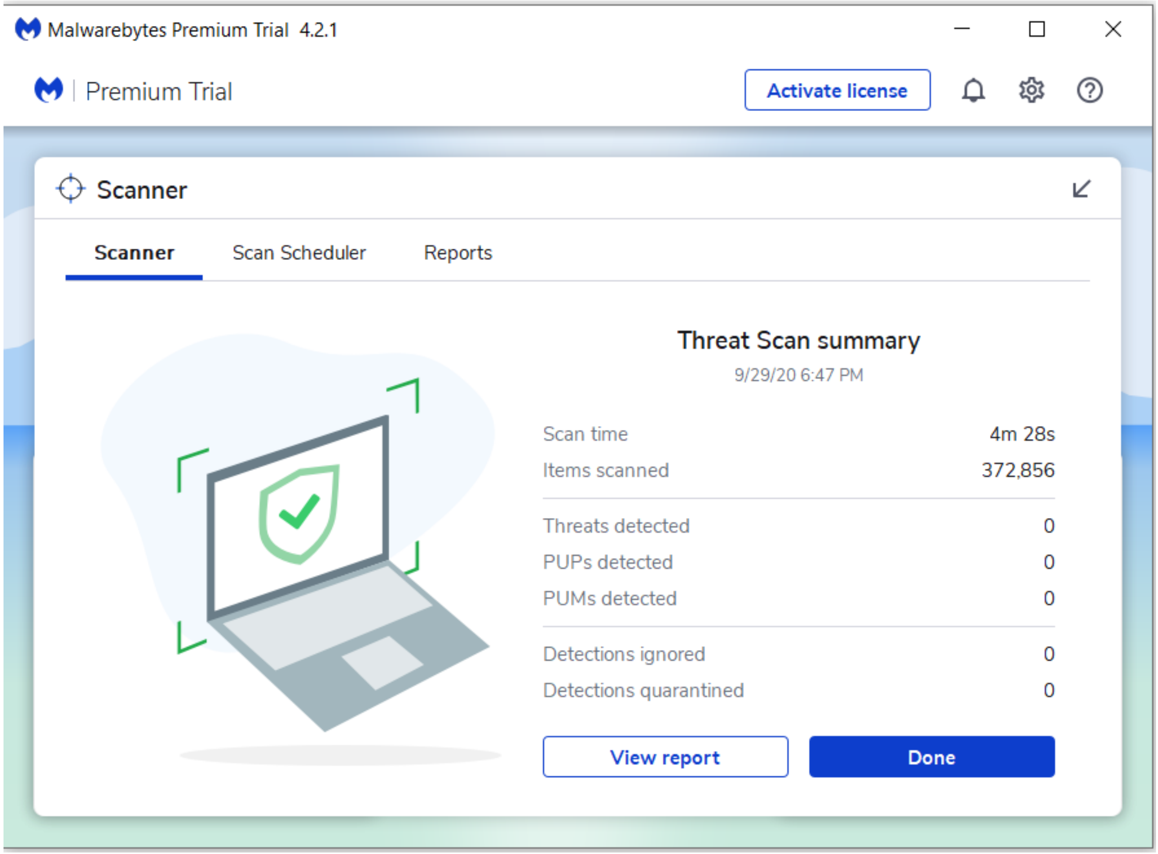
Cisco: Cisco provides a platform to its users for exploring the security solutions and using cases for their company. This company provides a solution for the IT, cyber-security, and networking, and its solutions are available for every single company irrespective of their size. Cisco has been founded in 1984 having revenues around 49 billion USD. The core security-services of this company include the following:

- Email-Security
- Malware Protection
- Firewall
- Endpoint Security
- Security services
- Multi-factor authentication, and
- Cloud-Security

This company maintains four major divisions such as Cisco Ransomware Defense, Cisco Secure Data Centre, Cisco Security & insurance, and, Cisco Trusted Access. According to Cisco's analytics, the businesses comparatively of smaller-size are usually hit by around 62% of all the cyber-attack, and the average investment needed of such compromise for the small-medium sized businesses was 1.24 million dollar last year. As per Cisco, around 58% of the SMBs state that their businesses were not having visibility into the practices and passwords of their employees. These insights, Cisco Company works on, for instance, this company's analysis reflects that around 19.7 billion threats are blocked by this company every day, around 600 billion emails are inspected by them every-day, and approximately 1.5 million samples are taken by this company every day. With the integrated approach of Cisco to security, its customers can have a simplified experience of security, security working as faster as its users do, and security growing with the user's business. Cisco strengthens its user's security-system and reduces risks by providing a reliable solution.

4) ***[1½ points]*** **For this task you need a Windows based PC. Use one of the lab's laptop if you do not have access to one. Install Malwarebytes' Anti-Malware (locate it on the internet) and run the "Perform quick scan" on your machine.**

Answer: show run



Threat Scan summary
9/29/20 6:47 PM

Scan time	4m 28s
Items scanned	372,856
Threats detected	0
PUPs detected	0
PUMs detected	0
Detections ignored	0
Detections quarantined	0

4-a) Did it find any questionable items?

No, I have not find any questionable items.

4-b) How many Objects did it scan and how much Time elapsed?

Items Scanned: 372,856

Scan Time: 4 minute 28s

5) *[-2 points]* Research and catalog some of the latest online security breaches that have occurred in the past year, starting June 2016. Then choose one specifically and give a detailed description of what happened and how it could have been prevented. We haven't defined yet what specific terms such as viruses, worms, etc, mean so I'm not asking you to classify them, just to talk about any breaches you can find *(COMP 815 students only)*

Word count: 748

In 2016, the firms have had their security solutions, which have increasingly been tested by the sophisticated cybercriminals. Data breaches since 2016 have gained enough attention with the increasing usage of companies and digital files, and users being hugely relied onto the digital data. Although, the data-breaches had happened before the trend of digitalization of information started to be followed, for example, looking at an individual's hard-copy regarding the medical-files without permission (authorization in digital world) could also be considered as an event of data-breach, however, the popularity of the digital platforms have brought the data-breach to another unique and new dimension as the importance and volume of the data getting exposed is getting increased. Across the world, stealing of identity is the most common-type of data-breach incident reflecting that approximately 59% of incidents based on data-breach across the globe in 2016.

The total number of data-breaches along with the number of exposed-records across the US reaches the highest-figures for dating in 2018; around 481 mn records had been exposed in U.S in the respective year. However, 2016 has been recognized as a challenging year for the celebrity longevity, politics and public-sanity, however, for the companies and individuals, this year was a testing-time in terms of online-security. For instance, Dyn DDoS attack is the most popular one being recognized as a cyber-attack, where, cybercriminals had launched major DDoS attacks through disrupting the host of the websites along with the likes of Netflix, Twitter, the PlayStation Network, Pinterest, Paypal, and a lot more. Although, the effects of this attack were found to be of short-term, however, method of attacking makes it significant and popular. Apart from this, there are a lot to go in this list of cyber-attack, for instance, the customers of Tesco Bank lost their real-money, around 40K accounts in the Tesco Bank had been compromised in this cyberattack, as a result, a thousand of customers lost their physical money from their

Tesco Bank Accounts. Yahoo suffered from different data-braches, however all of them were massive, voters of Philippine had also been triggered by anonymous. In addition to the U.S scenario of online-breaches, the fields, which have gone through online data-breaches, are Finance, Government, Entertainment, Education, and Medical. Furthermore, Trojans, viruses, worms, and malware are the basic types of cyber-attacks, which the American Companies have experienced since 2016.

SPECIFIC BREACH:

The most popular data-breach in US is the data breach in the field of the ***U.S Government, FEMA (Federal Emergency Management Agency***). The findings of this breach had been revealed by the Office of the Inspector General on March 15th, 2019. Around 2.3 million numbers of records had been exposed in this breach, where, information getting exposed was related to the street-addresses, transfer-number of electronic-funds, financial-institution names, along with the bank-transit numbers associated with the survivors of hurricanes, Maria, Harvey, and Irma, including the California wildfires. Every single data-breach is not the result of a hacker, sometimes the errors by the governmental-agencies' parts or the private companies could also expose the confidential and secured information of the people to the hackers. This case has the similar reason, where, 2.3 million of records, which had unnecessarily exposed by the FEMA. As per the General Inspector, the FEMA had released some sensitive, confidential and personally identifiable information regarding the natural-disaster's survivors such as Irma, Harvey, and Maria followed by the California wildfires. This information must not be released, as per the General Inspector; as a result the FEMA had violated the Privacy Act 1974 by doing so.

As per the Complaint of Office, this governmental body had released all the unnecessary information to the contractor, which regulates such program being designed for helping the survivors finding temporary staying at the hotels. Furthermore, this governing body had also provided the contract information by accessing more than 20 unessential data-sets along with the financial-institutions of the applicant-name, their transfer-no of online-fund, and their bank based transit numbers. More than two mn survivors related to the natural disaster in the U.S, as per the governing body, there would not be notifying affected individuals or providing such mechanism for the people for checking whether those people are affected. It is due to that FEMA does not consider this as an incident of data-breach. As per the spokesperson of FEMA, none of the information had been released or even compromised. Although, it is considered as a data-breach because unauthorized and unnecessary data-sharing is commonly found to be dangerous in both the government and corporate arenas.

Lab Question: *[3 points]*

1) *[1 points]* Describe your approach in detail of how you plan to convert a character string to a numeric value to seed the random number generator.

Word count: 200

Below are the approaches to convert a character string to a numeric value to seed the random generator:
To convert the string to a numeric value the first approach is to make use of the JavaScript function parseInt that will parse the string and return an enter, but it does not work with character values.
After trying couple of approaches, the suitable logic that I came up with to convert the entered set of character string to number is to iterate over the string of characters and finding out its char code value which is an integer value. The next thing I did was add up the char code value to get an integer number for the entered character string.
This function is called with the string value and it return and integer value for the string, this value is then used as seed value. The function is called in encryptStr and decryptStr functions to generate the string value based on the entered password string.

Pseudo Code

```
• Accept a string
• Declare total=0
• Start a loop to iterate over each character of the string
    o Get the char code value
    o Add the value to the total
• Return the total value
```

2) [*2 points]* Implement the approach in Java Script.

```
function stringToNumber(stringval)
                {
                        total=0;
                        for (index = 0; index < stringval.length; index++) {
                                total=total+stringval.charCodeAt(index);
                        }
                        return total;
                }
```

Used in encryptStr

```
  function encryptStr()
      {
       var msg = document.info.source.value;  // M
       var cyph = "";  // C
       var ascii;
       var shift;
       seed = stringToNumber(document.info.passwd.value);

       for (var i=0; i<msg.length; i++)
       {
         ascii = msg.charCodeAt(i);
         ascii = ascii - 32;  // normalize start to 0

         shift = getRandom() % 95;

         ascii = (ascii + shift) % 95;
         ascii = ascii + 32;  // unormalize back to 32

         cyph = cyph + String.fromCharCode(ascii);
       }

       document.info.dest.value = cyph;
      }
```

Used in decryptStr

```
function decryptStr()
      {
       var msg = "";  // M
       var cyph = document.info.dest.value;  // C
       var ascii;
       var shift;

       seed = stringToNumber(document.info.passwd.value);

       for (var i=0; i<cyph.length; i++)
       {
         ascii = cyph.charCodeAt(i);
         ascii = ascii - 32;  // normalize start to 0

         shift = getRandom() % 95;

         ascii = (ascii + (95 - shift)) % 95;
         ascii = ascii + 32;  // unormalize back to 32

         msg = msg + String.fromCharCode(ascii);
       }
```

```
  document.info.source.value = msg;
}
```