Excel Journal of Engineering Technology and Management Science
(An International Multidisciplinary Journal) (Impact Factor 2.119) IIFS
Vol. I No. 15 December – January 2019 - 20 (Online) ISSN 2277-3339

CYBER SECURITY AND ITS ELEMENTS

** Ms. Afshan Kausar, Lecturer,* *Jazan University, Dept. of Computer Science and Information Technology, Saudi Arabia.*
*** Wajid Ali Siddiqui, Lecturer,* *Jazan University, Dept. of Computer Science and Information Technology, Saudi Arabia.*

INTRODUCTION:

Today man is able to send and receive any form of data may be an e-mail or an audio or video just by the click of a button but did he ever think how securely his data id being transmitted or sent to the other person safely without any leakage of information? The answer lies in cyber security. Today Internet is the fastest growing infrastructure in everyday life. In today's technical environment many latest technologies are changing the face of the mankind. But due to these emerging technologies we are unable to safeguard our private information in a very effective way and hence these days cyber-crimes are increasing day by day. Today more than 60 percent of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions. Hence cyber security has become a latest issue. The scope of cyber security is not just limited to securing the information in IT industry but also to various other fields like cyber space etc. Even the latest technologies like cloud computing, mobile computing, E-commerce, net banking etc also needs high level of security. Since these technologies hold some important information regarding a person their security has become a must thing. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic wellbeing. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy. The fight against cyber-crime needs a comprehensive and a safer approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cyber-crime effectively. Today many nations and governments are imposing strict laws on cyber securities in order to prevent the loss of some important information. Every individual must also be trained on this cyber security and save themselves from these increasing cyber-crimes.

COMMON TYPES OF CYBER ATTACK:

- **Malware**

  If you've ever seen an antivirus alert pop up on your screen, or if you've mistakenly clicked a malicious email attachment, then you've had a close call with malware. Attackers love to use malware to gain a foothold in users' computers—and, consequently, the offices they work in—because it can be so effective.

"Malware" refers to various forms of harmful software, such as viruses and ransomware. Once malware is in your computer, it can wreak all sorts of havoc, from taking control of your machine, to monitoring your actions and keystrokes, to silently sending all sorts of confidential data from your computer or network to the attacker's home base. Attackers will use a variety of methods to get malware into your computer, but at some stage it often requires the user to take an action to install the malware. This can include clicking a link to download a file, or opening an attachment that may look harmless (like a Word document or PDF attachment), but actually has a malware installer hidden within.

- **Phishing**

Of course, chances are you wouldn't just open a random attachment or click on a link in any email that comes your way—there has to be a compelling reason for you to take action. Attackers know this, too. When an attacker wants you to install malware or divulge sensitive information, they often turn to phishing tactics, or pretending to be someone or something else to get you to take an action you normally wouldn't. Since they rely on human curiosity and impulses, phishing attacks can be difficult to stop. In a phishing attack, an attacker may send you an email that appears to be from someone you trust, like your boss or a company you do business with. The email will seem legitimate, and it will have some urgency to it (e.g. fraudulent activity has been detected on your account). In the email, there will be an attachment to open or a link to click. Upon opening the malicious attachment, you'll thereby install malware in your computer. If you click the link, it may send you to a legitimate-looking website that asks for you to log in to access an important file—except the website is actually a trap used to capture your credentials when you try to log in. In order to combat phishing attempts, understanding the importance of verifying email senders and attachments/links is essential.

- **SQL Injection Attack**

SQL (pronounced "sequel") stands for structured query language; it's a programming language used to communicate with databases. Many of the servers that store critical data for websites and services use SQL to manage the data in their databases. A SQL

injection attack specifically targets this kind of server, using malicious code to get the server to divulge information it normally wouldn't. This is especially problematic if the server stores private customer information from the website, such as credit card numbers, usernames and passwords (credentials), or other personally identifiable information, which are tempting and lucrative targets for an attacker. An SQL injection attack works by exploiting any one of the known SQL vulnerabilities that allow the SQL server to run malicious code. For example, if a SQL server is vulnerable to an injection attack, it may be possible for an attacker to go to a website's search box and type in code that would force the site's SQL server to dump all of its stored usernames and passwords for the site.

- **Cross-Site Scripting (XSS)**

In an SQL injection attack, an attacker goes after a vulnerable website to target its stored data, such as user credentials or sensitive financial data. But if the attacker would rather directly target a website's users, they may opt for a cross-site scripting attack. Similar to an SQL injection attack, this attack also involves injecting malicious code into a website, but in this case the website itself is not being attacked. Instead, the malicious code the attacker has injected only runs in the user's browser when they visit the attacked website, and it goes after the visitor directly, not the website. One of the most common ways an attacker can deploy a cross-site scripting attack is by injecting malicious code into a comment or a script that could automatically run. For example, they could embed a link to a malicious JavaScript in a comment on a blog. Cross-site scripting attacks can significantly damage a website's reputation by placing the users' information at risk without any indication that anything malicious even occurred. Any sensitive information a user sends to the site—such as their credentials, credit card information, or other private data—can be hijacked via cross-site scripting without the website owners realizing there was even a problem in the first place.

- **Denial-of-Service (DoS)**

Imagine you're sitting in traffic on a one-lane country road, with cars backed up as far as the eye can see. Normally this road never sees more than a car or two, but a county

fair and a major sporting event have ended around the same time, and this road is the only way for visitors to leave town. The road can't handle the massive amount of traffic, and as a result it gets so backed up that pretty much no one can leave.

That's essentially what happens to a website during a denial-of-service (DoS) attack. If you flood a website with more traffic than it was built to handle, you'll overload the website's server and it'll be nigh-impossible for the website to serve up its content to visitors who are trying to access it. This can happen for innocuous reasons of course, say if a massive news story breaks and a newspaper's website gets overloaded with traffic from people trying to find out more. But often, this kind of traffic overload is malicious, as an attacker floods a website with an overwhelming amount of traffic to essentially shut it down for all users. In some instances, these DoS attacks are performed by many computers at the same time. This scenario of attack is known as a Distributed Denial-of-Service Attack (DDoS). This type of attack can be even more difficult to overcome due to the attacker appearing from many different IP addresses around the world simultaneously, making determining the source of the attack even more difficult for network administrators.

- **Session Hijacking and Man-in-the-Middle Attacks**

When you're on the internet, your computer has a lot of small back-and-forth transactions with servers around the world letting them know who you are and requesting specific websites or services. In return, if everything goes as it should, the web servers should respond to your request by giving you the information you're accessing. This process, or session, happens whether you are simply browsing or when you are logging into a website with your username and password. The session between your computer and the remote web server is given a unique session ID, which should stay private between the two parties; however, an attacker can hijack the session by capturing the session ID and posing as the computer making a request, allowing them to log in as an unsuspecting user and gain access to unauthorized information on the web server. There are a number of methods an attacker can use to steal the session ID, such as a cross-site scripting attack used to hijack session IDs.

An attacker can also opt to hijack the session to insert themselves between the requesting computer and the remote server, pretending to be the other party in the session. This allows them to intercept information in both directions and is commonly called a man-in-the-middle attack.

- **Credential Reuse**

Users today have so many logins and passwords to remember that it's tempting to reuse credentials here or there to make life a little easier. Even though security best practices universally recommend that you have unique passwords for all your applications and websites, many people still reuse their passwords—a fact attackers rely on. Once attackers have a collection of usernames and passwords from a breached website or service (easily acquired on any number of black-market websites on the internet), they know that if they use these same credentials on other websites there's a chance they'll be able to log in. No matter how tempting it may be to reuse credentials for your email, bank account, and your favorite sports forum, it's possible that one day the forum will get hacked, giving an attacker easy access to your email and bank account. When it comes to credentials, variety is essential. Password managers are available and can be helpful when it comes to managing the various credentials you use.

CYBER SECURITY:

Privacy and security of the data will always be top security measures that any organization takes care. We are presently living in a world where all the information is maintained in a digital or a cyber form. Social networking sites provide a space where users feel safe as they interact with friends and family. In the case of home users, cyber-criminals would continue to target social media sites to steal personal data. Not only social networking but also during bank transactions a person must take all the required security measures.

Number of Cases Registered, Solved and Person Arrested by Cyber Crime Cells of Delhi Police (2017 and 2018-upto-30.06.2018)

Year	No. of Cases Registered	No. of Cases Solved	No. of Persons Arrested
2017	106	22	43
2018*	61	20	33

Note : * : Upto 30.06.2018.
Source : Rajya Sabha Unstarred Question No. 1675, dated on 01.08.2018.

State-wise Number of Cases Reported/Charge sheeted/Convicted and Persons Arrested/Charge sheeted/Convicted under Cyber Crimes (Section 67 and 67A of Information Technology Act) in India (2016)						
States/UTs	Cases Reported	Persons Arrested	Cases Charge Sheeted	Persons Charge Sheeted	Cases Convicted	Persons Convicted
Assam	114	119	9	9	0	0
Haryana	29	17	12	13	0	0
Punjab	26	47	17	21	1	2
Rajasthan	43	16	11	16	0	0
Tamil Nadu	27	29	16	20	1	1
Telangana	20	8	7	4	0	0
Uttar Pradesh	287	284	162	192	5	6
Uttarakhand	14	11	7	8	0	0
West Bengal	NR	NR	NR	NR	NR	NR

Abbr. : NR : Not Received.
Note : Data is Provisional as data is under Clarification.
Source : Lok Sabha Unstarred Question No. 453, dated on 1-.07.2017

TRENDS CHANGING CYBER SECURITY :

Here mentioned below are some of the trends that are having a huge impact on cyber security.

- **Web servers:**

  The threat of attacks on web applications to extract data or to distribute malicious code persists. Cyber criminals distribute their malicious code via legitimate web servers they've compromised. But data-stealing attacks, many of which get the attention of media, are also a big threat. Now, we need a greater emphasis on protecting web servers and web applications. Web servers are especially the best platform for these cyber criminals to steal the data. Hence one must always use a safer browser especially during important transactions in order not to fall as a prey for these crimes.

- **Cloud computing and its services**

  These days all small, medium and large companies are slowly adopting cloud services. In other words the world is slowly moving towards the clouds. This latest trend presents a big challenge for cyber security, as traffic can go around traditional points of inspection. Additionally, as the number of applications available in the cloud grows, policy controls for web applications and cloud services will also need to evolve in order to prevent the loss of valuable information. Though cloud services are developing their own models still a lot of issues are being brought up about their security. Cloud may provide immense opportunities but it should always be noted that as the cloud evolves so as its security concerns increase.

- **APT's and targeted attacks**

  APT (Advanced Persistent Threat) is a whole new level of cyber crime ware. For years network security capabilities such as web filtering or IPS have played a key part in identifying such targeted attacks (mostly after the initial compromise). As attackers grow bolder and employ more vague techniques, network security must integrate with other security services in order to detect attacks. Hence one must improve our security techniques in order to prevent more threats coming in the future.

- **Mobile Networks**

  Today we are able to connect to anyone in any part of the world. But for these mobile networks security is a very big concern. These days firewalls and other security measures are becoming porous as people are using devices such as tablets, phones, PC's etc all of which again require extra securities apart from those present in the applications used. We must always think about the security issues of these mobile networks. Further mobile networks are highly prone to these cyber crimes a lot of care must be taken in case of their security issues.

- **IPv6: New internet protocol:**

  IPv6 is the new Internet protocol which is replacing IPv4 (the older version), which has been a backbone of our networks in general and the Internet at large. Protecting IPv6 is not just a question of porting IPv4 capabilities. While IPv6 is a wholesale replacement in making more IP addresses available, there are some very fundamental changes to the protocol which need to be considered in security policy. Hence it is always better to switch to IPv6 as soon as possible in order to reduce the risks regarding cyber crime.

- **Encryption of the code:**

  Encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it.. In an encryption scheme, the message or information is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Encryption at a very beginning level protects data privacy and its integrity. But more use of encryption brings more challenges in cyber security.

Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, ecommerce), mobile telephones, wireless microphones, wireless intercoms etc. Hence by encrypting the code one can know if there is any leakage of information.

CYBER SECURITY PARAMETERS

The parameters for Cyber security are as follows:

1. Identify threats
2. Identify vulnerabilities
3. Access risk explore
4. Establish contingency plan
5. Respond to cyber security accident
6. Establish contingency plan

SHOWS THE PARAMETERS OF CYBER SECURITY

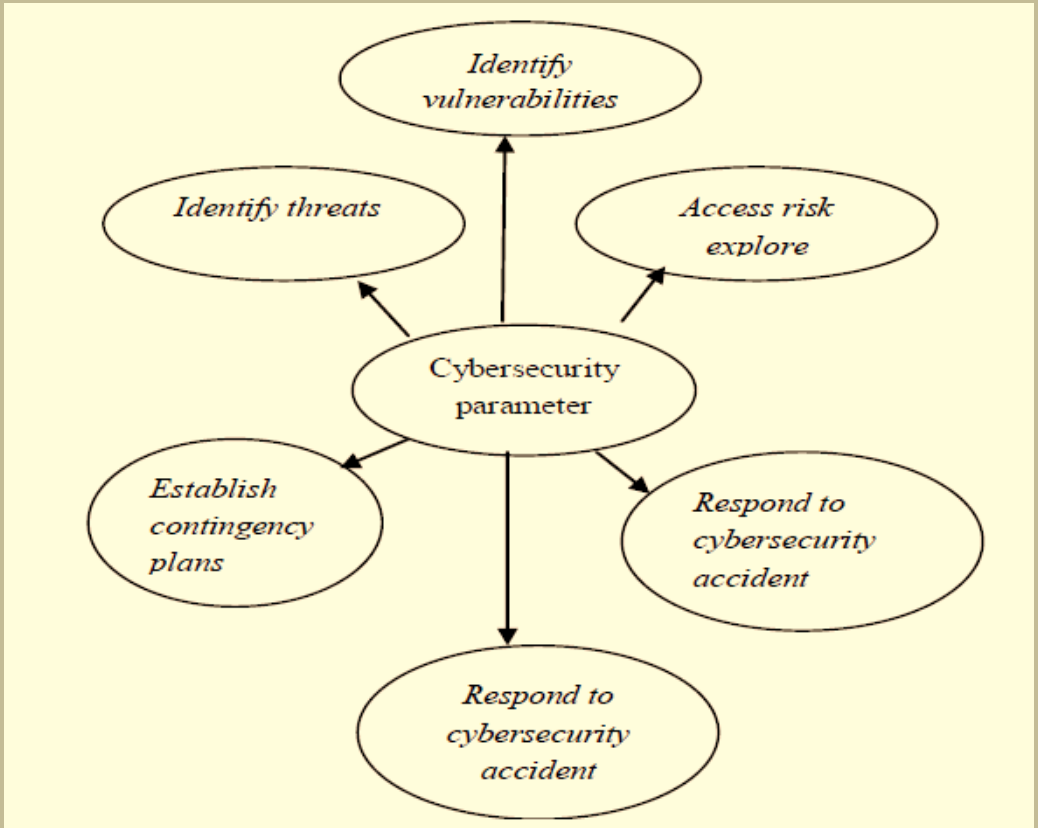

Figure 1 Parameters of Cyber Security

CYBER ETHICS:

Cyber ethics are nothing but the code of the internet. When we practice these cyber ethics there are good chances of us using the internet in a proper and safer way. The below are a few of them:

- ✓ DO use the Internet to communicate and interact with other people. Email and instant messaging make it easy to stay in touch with friends and family members, communicate with work colleagues, and share ideas and information with people across town or halfway around the world.
- ✓ Don't be a bully on the Internet. Do not call people names, lie about them, send embarrassing pictures of them, or do anything else to try to hurt them.
- ✓ Internet is considered as world's largest library with information on any topic in any subject area, so using this information in a correct and legal way is always essential.
- ✓ Do not operate others accounts using their passwords.
- ✓ Never try to send any kind of malware to other's systems and make them corrupt.
- ✓ Never share your personal information to anyone as there is a good chance of others misusing it and finally you would end up in a trouble.
- ✓ When you're online never pretend to the other person, and never try to create fake accounts on someone else as it would land you as well as the other person into trouble.
- ✓ Always adhere to copyrighted information and download games or videos only if they are permissible.
- ✓ The above are a few cyber ethics one must follow while using the internet. We are always thought proper rules from out very early stages the same here we apply in cyber space.

CONCLUSION:

Computer security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. Cyber crime continues to diverge down different paths with each New Year that passes and so does the security of the information. The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. There is no perfect solution for cyber crimes but we should try our level best to minimize them in order to have a safe and secure future in cyber space.

REFERENCES

1. Data Warehousing and Data Mining Techniques for Cyber Security by Anoop Singhal.
2. Preeti Aggarwal "Application of Data Mining Techniques for Information Security in a Cloud: A Survey" in International Journal of Computer Applications (0975 – 8887) Volume 80 No 13, October 2013.
3. Kartikey Agarwal & Dr. Sanjay Kumar Dubey "Network Security: Attacks and Defense" in International Journal of Advance Foundation and Research in Science & Engineering (IJAFRSE) Volume 1, Issue 3, August 2014.
4. Shikha Agrawal, Jitendra Agrawal "Survey on Anomaly Detection using Data Mining Techniques" in 19th International Conference on Knowledge Based and Intelligent Information and Engineering Systems Available online at www.sciencedirect.comProcedia Computer Science 60 (2015) 708 – 713 2015
5. APRA "Cyber Security Survey Results" in Australian Prudential Regulation Authority (APRA) 2016.
6. Farhad Alam1, Sanjay Pachauri2 "Usage of data Mining Techniques for combating cyber security" in International Journal Of Engineering And Computer Science ISSN: 2319-7242 Volume 6 Issue 1 Jan. 2017, Page No. 20011-20016 Index Copernicus Value (2015): 58.10, DOI: 10.18535/ijecs