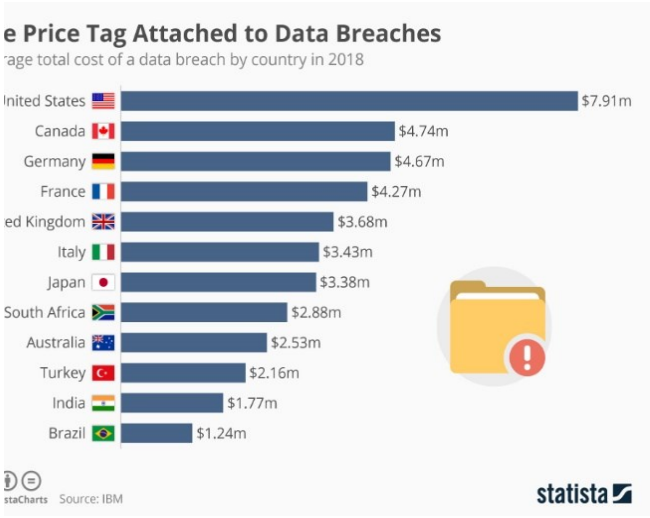
Security, Trust and Privacy In Cyber (Stpc Cyber)

Ayesha Maqsood, Dr. Muhammad Rizwan and Dr. Fahad Ahmad
Department of Computer Science, Kinnaird College for Women, Lahore

DOI: 10.29322/IJSRP.9.02.2019.p8682
http://dx.doi.org/10.29322/IJSRP.9.02.2019.p8682

Abstract- **Cyber security is a dimension in the world of Internet revolution, where rapid increase in cyber-crimes and cyber-warfare is occurring to a level where national and international economy and security is at stake and destabilizing. Cyber-security, in short, is the protection from unauthorized access of data over the Internet and the prevention of exploitation of hardware and software vulnerabilities. Various strategies, techniques, models and frameworks have been established to address the issue of cyber security This paper gives an overview of various cyber threats, its related concepts and principles, effects of cyber-attacks on individual, national and global level, the models, frameworks and steps taken to cater cyber security, with there limitations and recommendations for improvements in cyber security measures.**



I. INTRODUCTION

Cyber-attacks and terrorism do not know borders. With an increasing Internet revolution, the hidden way of cyber warfare and cyber threats is also getting paved and reaching to devastating results. With innovations in technology and networks, the cyber-crimes are becoming more often, complex, sophisticated, expensive and more exploitive which is causing severe potential damages to world peace, national and international destabilization, economic downfall and disrupting international relations[1]. Figure 1.1 shows the average cost that the countries had to pay for a data breach i.e. a type of cyber-attack.

Fig 1.1 Average cost of data breach by country.

To cater with the rising threat of cyber-attacks, a dimension of Cyber Security is emerging. Cyber security is referred to as an integration of principles and methods, security models and protocols, frameworks and models which ensures the protection of the computer systems, networks and information stored on these networks from unauthorized access, exploitation of hardware and software vulnerabilities, and secure data transmission without any interception from the intruder and safe online identity[2].

Fig 1.2 Some Functions of Cyber Security and System

The various types of cyber-attacks includes data breach, phishing, man-in-the middle attacks, brute-force attacks, malware, ransomware etc [2]. The cyber attackers exploit the vulnerabilities in the computer system and the networks, cause damage to the data, and use it for criminal purposes [2]. Fig 1.3 shows some of the most common cyber-attacks.

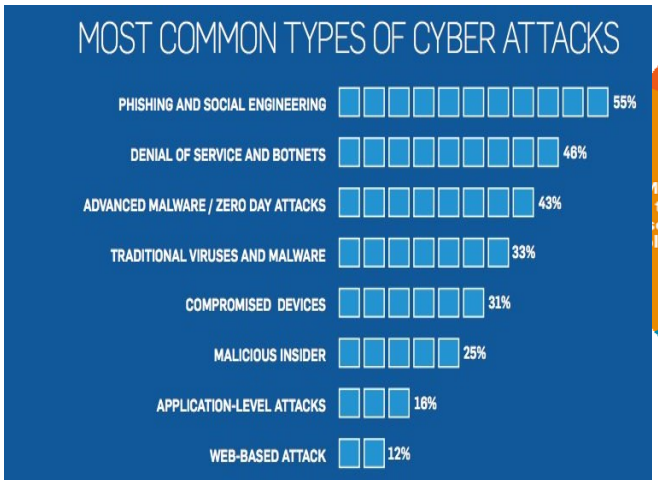


Fig 1.3 Most common cyber-attacks

Protection of cyber space from unauthorized access and exploitation of system vulnerabilities, both hardware and software. There are two aspects in ensuring cyber security: The first is to deal with the protection of the hardware and the softwares eg authentication, encryption, LAN analyzer softwares etc. The second aspect deals with the workforce that needs to be trained to deal with the complex security of the cyber space.

Fig 1.4 An overview of the different areas in cyber security

Cyber security covers there important aspects:

1) Protecting and security of the Information Technology (both the hardware and the software).
2) Integrity and security of the data.
3) The transmission of data over physical or wireless media and the processing of data [2].

This paper gives an overview about the cyber challenges that are being faced at individual and national levels, various ways through which cyber criminals penetrate into the system and the existing cyber security models and policies that are used for cyber protection. The paper also covers the limitation of the existing models and provides with recommendations for future research in cyber security.

II CYBER SECURITY

With the increase in time, data and information is being produced in a huge amount at a high velocity, each versatile and in nature. The Information Systems used to manage this huge data are often complex and require network access such as Internet. Automation of everything and storing data on cloud and networks has benefitted in many ways but it hides under it a dark world of cyber crime which is catered with cyber security mechanisms and policies. Cyber Security is the set of all the mechanisms and policies which are implemented for the security

III PHASES OF A CYBER ATTACK

Cyber security is a domain that has huge impact on the concept of security at individual and national level. Cyber threats are being faced at all levels and has lead the safety of our information assets at stake [1]. Cyber-attacks are conducted with some specific intent of exploiting the vulnerabilities and using them for causing damage to the security at all levels.

The cyber-attacks are considered to be of different phases, as how they are conducted [1]:

The first phase is that the cyber attackers observe the operations being done on the system through various applications as spyware and determining the points of target [1].

The second phase is penetrating into the system. Until the attacker does not penetrate into the system, it cannot do much than making certain services inaccessible or unavailable to others [1].

The third phase is examining the resources and the rights in order to access the system and the information stored on it [1].

In the fourth phase, the attacker exploits the information and causes damage to it or steals important data [1].

IV DIFFERENT CYBER THREATS

Now a days, cyber-attacks are conducted by sending malicious codes and messages through emails that is known as **phishing**. Intercepting the data and modifying or deleting the data. Denial of service to create obstacles in accessing the network. Recording passwords by recording the keystrokes that is known as ***brute force attack***. Stealing and modifying the encryption keys used to encrypt the information that is known as ***key-reinstallation attacks*** and many other ways are being used in cyber-attacks[2].

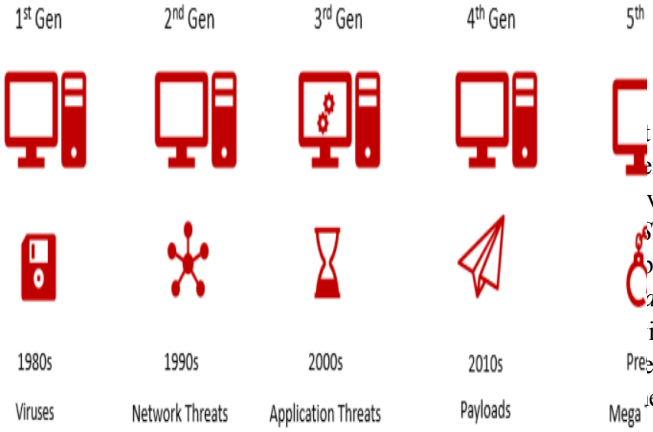


Fig 1.5 Generations of cyber threats

V PREVENTION AGAINST A CYBER ATTACK

The significant steps that are to be taken towards securing the cyberspace and the confidential and important information on cyber space are to use encryption and decryption and its protocols like WPA and WPA2, when sending data over a network, avoid using public networks and using *Virtual Private Network(VPN) [4],* setting up a passphrase is recommended over password, setting up different passwords for different online accounts, use anti-virus and anti-spywares, keep the firewall on, keep installing the updated versions for the Operating system/Windows and application programs installed on the system[2].

VI PRINCIPLES OF CYBER SECURITY

When designing a framework for cyber security the following principles are to be considered:

- *Increase Trust by Limiting and Isolating Functionality* emphasizes that "less is more" and calls for smaller components with well-defined interfaces. This principle is based on well-established security principles such as the Principle of Least Privilege[3].
- *Adaptive Multiple Layers of Security* (abbreviated as Independence Principle) applies the Isolation Principle both logically and dynamically by dividing systems into several layers[3].
- *Artificial and Natural Diversity* (abbreviated as Diversity Principle), emphasizes the need for diversity defenses that present attackers with unpredictable targets[3].
- *Learning Systems* (abbreviated as Learning Principle), emphasizes the need for systems to dynamically learn from past activities, data and even from users[3].

VII CYBERSECURITY FRAMEWORKS

different frameworks designed for cyber security do not the requisite level that is required to completely secure the em and its data from intruders due to the rapid technological vations and the lack of facilities [2]. The *National Institute Standards and Technology (NIST)* made an agency to olish a framework for cyber security named *National ative for Cybersecurity Education (NICE).* It focuses on iding with awareness on cyber security and training for ecting the assets on cyberspace. *NICE* established a ework named *Cybersecurity Workforce Framework*[2].

It comprised of an infrastructure for securing the cyberspace but it was not much efficient as it lacked the factor of coping up with the technological advancements that caused the cyber-attacks to be more complexed and difficult to detect [2].

Cyber-crimes also include sending virus and spams to disrupt the normal operations of the system and cause damage.

According to the studies it has been said that these methods are based on text categorization methods and do not claim to provide an ideal solution with 0% false positive and 0% false negative. The Rnd is an email spam classification algorithm that has been proved to give 99% accurate results for spam detection [2].

Usage of firewalls, anti-viruses and anti-spywares, using *Intrusion Detection Systems (IDS)* to diagnose computer system attacks and many more [2]. Checksum algorithms are executed over the data that is sent over the networks.

In this, a hash value is calculated of the data, that is sent over the network, before and after it is sent. If the hash values calculated before and after transmission are same then it means that data was safe but if not then it means that an intruder has intercepted it.

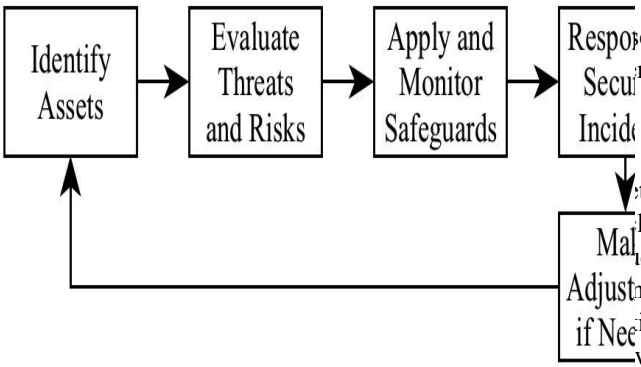


Fig 1.5 General operation flow of cybersecurity prevention.

VIII CYBER SECURITY STRATEGIES

The strategies in cyber security can be categorized into four categories[3][4]:

1) Prevention Strategies.
   - Proactive defense techniques
   - Reactive defense techniques
2) Detection Strategies.
3) Data Driven Science for Detecting and Mitigating Attacks.
   - Text Analysis to Detect Emerging Cyber Threats
   - Detecting Attacks using Graph Grammars
   - Detecting Attacks Using Stream-based Classification

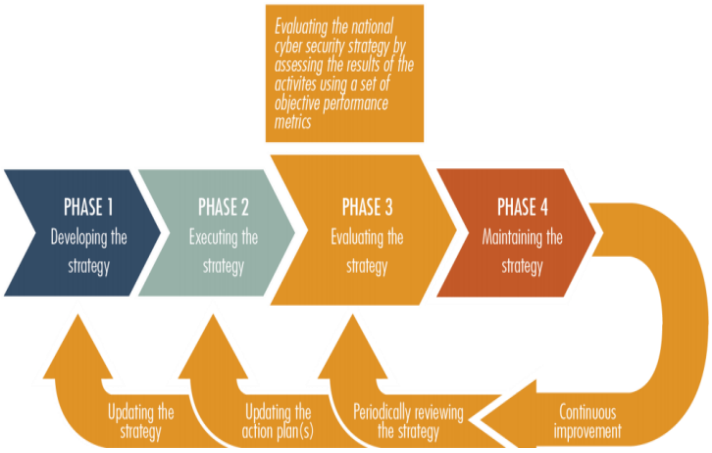


Fig 1.6 A general flow when designing a cyber-security strategy

1. Prevention Strategies

e includes methods taken in advance for prevention against r attacks. These are further classified into[4]:

a) Proactive defense techniques:

tration testing, Ethical hacking and simulation, in this, a test k is conducted to detect any system vulnerabilities. It also ides regular training exercises on social engineering niques. Keeping computer system up to *date* is required all ime whenever a new updated version of a software or of ware is released. This reduces the loop holes in the existing system and protects it from exploitation and cyber attacks to a considerable extent.

Furthermore, designing the computer securely and its applications is an important task because the settings in the Web Browse verify what happens when you visit websites on the internet and keep track of the cyber activities a user performs.

In addition, Vulnerability Assessment includes identification of the expected threats and the equipment and its assessibility, quantification and prioritization of vulnerabilities. Data Encryption is which the plain text is converted to an encrypted form known as cipher text which can be accessed only by the authorized person through a key. It is helpful because even if the data goes in wrong hands it will be impossible to decipher the text or information. Creating strong passwords and changing them after some time is highly recommended as it can keep the damage within bounds which is caused by someone who has already gained access to your account. Never send personal or confidential information via email or instant messages as these can be easily intercepted[4].

b) Reactive Defense Technique

Anti-DNos and Anti-bot Detection Systems are the softwares designed, which detects bots and Distributed Denial of Service (DDNoS) attacks and can block communications. Intrusion Prevention Systems are designed to detect, report, log any unusual activity taken place on the computer system and blocking connections from malicious systems.. Firewalls are supposed to monitor open connections. This includes checking attachments in email, blocking unauthorized and unwanted traffic or disable internet add-ons such as cookies, pop-ups etc[4].

Antivirus scans the files or packages in your system for viruses. They clean or delete any such infected files if found. Ensuring Clean Pipe- Clean Pipe is the term for communication channel through which the user employs or delivers services.

2. Detection Strategies

Tripwire softwares are designed to take snapshots of the behavior of the system before and after an operation. These then can be compared with the system screenshots after the operation to diagnose any changes. This enables to provide evidence against the hackers as they make alterations while installing backdoor entry points. ***Honey pot*** refers to fake accounts that are created by cyber security experts as to show that they contain sensitive data to keep the intruders busy in hacking those files and during that time the experts then can identify the intruder. ***Anomaly Detection System*** focus on odd patterns of activity. They analyze user profiles and user activity and immediately informs if there is something different than the usual activity.

3. Data Driven Science for Detecting and Mitigating Att

To identify unusual activities over cyber and generating mes to inform about those activities, State-of-the-art intr detection and prevention systems (IDPSs) are used. They m the cyber activities on the basis of signatures[3].

The two drawbacks of the current systems are that they are u to detect attacks of which the signatures are unknown an they are designed in manner that can protect only a single ta

In more sophisticated systems (SIEMs), notifications warnings from individual components are combined and rec in an operations center. These are then analyzed by the ne security analysts and allowing professional analysts to analy different segments of the information and check if they d any pattern notifying a cyber attack. This process is watchstanding[3].

a) Text Analysis to Detect Emerging Cyber Threats

The first source for the information about new software vulnerabilities exploits and cyber-attacks is the web. Other than the web, there are many other informal sources of information such as hacker blogs and forums, chat rooms and social media. For the early detection of emerging vulnerabilities and tracking the progression of existing vulnerabilities, data mining is done and is then integrated for analysis. It is required to create a framework which collects text from new streams dynamically which can then be analyzed to identify potential new vulnerabilities and threats[3].

b) Detecting Attacks using Graph Grammars

The graphs that are used to represent cyber activities are called Graph Grammers which are based with a dynamic graph entailed by its OWL representation. The entities such as programs, ports, users are represented by nodes and the edges symbolize events and interactions such as running a program, opening a port, an attacker initiating a campaign. The graphs are updated in real time whenever a new interaction occurs consisting of an unknown or new resources or there is an update in the information about entities. It is required to lay emphasis on this method in order to develop powerful new methods for representing, reasoning about, and identifying attacks[3].

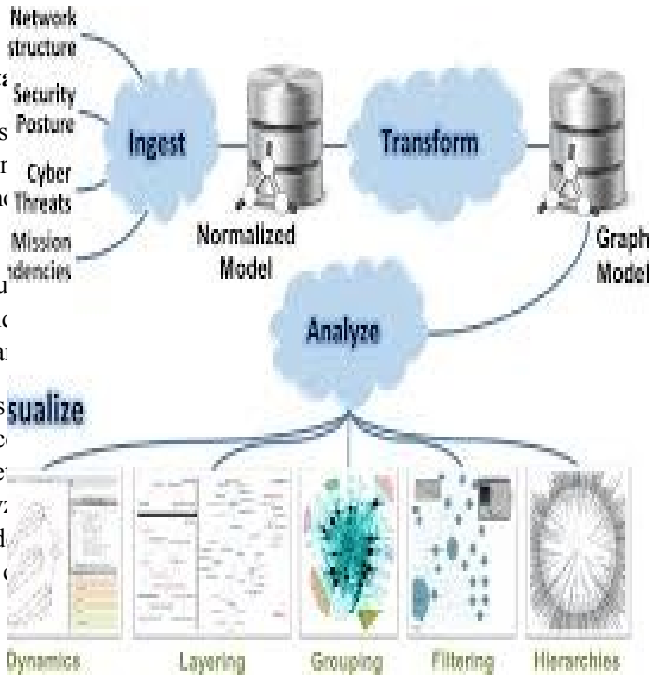


Fig 1.7 A graph based detection and analysis of a cyber-attack

c) Detecting Attacks Using Stream-based Classification

The cyber-attack detection is considered as a data stream classification problem. These are of dynamic nature due to which the problems of concept-drift and concept-evolution arise. The problem occurring due to the change in the underlying concept of the data is referred to as “concept-drift”.

As a result of this, the previous models become quaint and require to be updated continuously in response to the new data incoming. In contrast to this, the emergence of novel classes over time is referred to as “concept-evolution”. For example, a new APT with new attack methodology and objectives would typically fall into this category.

In our approach, it is assumed that the data stream (e.g. sensor information) is decomposed into chunks of equal sizes. An ensemble of classifiers will be the core of the system. When a new unlabeled test instance arrives, which is a part of a chun instance is then classified with the help of the ensemble. If th instance is identified as an outlier, it will be temporarily stored in a buffer for further investigation. If the test instance ... outlier, then it will be classified with a known label. The l will be checked periodically to see whether a novel clas appeared.

If a novel class is found, then the instances belonging to the class will be identified and tagged accordingly. It is also requ to apply collective classification over multiple data sources based on Markov network in order to facilitate inference. The outputs will be another type of input to the stream based reasoning tools[3].

IX CONCLUSION

In this technological era where everything is being converged over the internet and things are being automated, a rapi... in more complex and sophisticated cyber-attacks is occurrin... prevent systems and data from exploitation and making cy... safe place various cyber security strategies and frameworks have been established, are being implemented and massive work is being done in the domain of cyber security. In this paper, we have discussed about cyber security domain, the threats in cyber space, various cyber security strategies and frameworks and the steps that can be taken at an individual level for protection against cyber-attacks.

REFERENCES

[1] I. Duić*, V. Cvrtila**, T. Ivanjko*** *Croatian Radiotelevision, Zagreb, Croatia **University of Applied Sciences Vern, Zagreb, Croatia ***Faculty of Humanities and Social Sciences/Information and Communication Sciences, Zagreb, *"International cyber security challenges"*.https://ieeexplore.ieee.org/document/7973625. (May22-26, 2017).

[2] Kutub Thakur1, Meikang Qiu2∗, Keke Gai3, Md Liakat Ali4 *"An Investigation on Cyber Security Threats and Security Models."* IEEE 2nd International Conference on Cyber Security and Cloud Computing (CSCloud 2015), At ... New York, USA.

[3] *A Data Driven Approach for the Science of Cyber Security: Challenges and Directions* Bhavani Thuraisingham, Murat Kantarcioglu, Kevin Hamlen, Latifur Khan University of Texas at Dallas Richardson, TX, USA Tim Finin, Anupam Joshi, Tim Oates University of Maryland, Baltimore County Baltimore, MD, USA IEEE 17th International Conference ... Information Reuse and Integration (IRI), ... https://ieeexplore.ieee.org/document/7785719 ,July 2016

[4] Niral Shah #1 , Naveen Vaswani *2 # Student, *Cyber Crime and Security- Challenges and Security Mechanisms* Department of Computer Engineering, Watumull Institute of Electronics Engineering and Computer Technology, Worli, *Assistant Professor, Department of Computer Engineering, Watumull Institute of Electronics Engineering and Computer Technology, Worli, June 2016

[5] L. J. Janczewski and A. M. Colarik, Cyber warfare and cyber terrorism. Hershey: Information Science Reference, 2008.

[6] H. Liu, M. Qiu, J. Li, T. Grant, D. Taylor, and S. McCaleb et al. A review on cloud computing: Design challenges in ... architecture and security. J. of Computing and Info. Tech., ... 19(1):25–55, 2011.

[7] S. Subashini and V. Kavitha. A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1):1–11, 2011.

[8] F. Liu, H. Lo, L. Chen, and W. Lee. Comprehensive security integrated model and ontology within cloud computing. J. of Internet Technology, 14(6):935–946, 2013.

[9] Z. Duan, P. Chen, F. Sanchez, Y. Dong, M. Stephenson, and J. Barker. Detecting spam zombies by monitoring outgoing messages. IEEE Transactions on Dependable and Secure Computing, 9(2):198–210, 2012.

[10] S. Delany, M. Buckley, and D. Greene. SMS spam filtering: methods and data. Expert Systems with Applications, 39(10):9899–9908, 2012.

[11] C. Ten, C. Liu, and G. Manimaran. Vulnerability assessment of cybersecurity for scada systems. IEEE Transactions on Power Systems, 23(4):1836–1846, 2008.

[12] Natural Hazards, 77(1):405– 428, 2015. [28] X. Ye, J. Zhao, Y. Zhang, and F. Wen. Quantitative vulnerability assessment

of cyber security for distribution automation systems. Energies, 8(6):5266–5286, 2015.

[13] H. Sun, Y. Chen, and Y. Lin. opass: A user authentication protocol resistant to password stealing and password reuse attacks. IEEE Trans. on Info. Forensics and Security, 7(2):651–663, 2012.

[14] M. Masud, L. Khan, J. Han, et al. Classification and Adaptive Novel Class Detection of Feature-Evolving Data Streams. IEEE Trans. Knowl. Data Eng. 25, 2013.

[15] A. Joshi at al. Extracting cyber-security related linked data from text. 7th IEEE Int. Conf. on Semantic Computing. IEEE Computer Society, Sept. 2013.

[16] V. Mulwad et al. "Extracting Information about Security Vulnerabilities from Web Text" Web Intelligence for Information Security Workshop. IEEE 2011.