An Investigation on Cyber Security Threats and Security Models

Kutub Thakur[1], Meikang Qiu[2*], Keke Gai[3], Md Liakat Ali[4]

***Abstract*—Cyber security has been used interchangeably for information security, where later considers the role of the human in the security process while former consider this as an additional dimension and also, focus person has a potential target. However, such discussion on cyber security has important implication as it focuses on the ethical part of the society as a whole. To address the issue of cyber security, various frameworks and models have been developed. It also introduces the concepts of cyber security in terms of its framework, workforces and information related to protecting personal information in the computer. This paper reviews these models along with their limitations and review the past techniques used to mitigate these threats. Furthermore, the report also provides recommendations for future research.**

***Index Terms*—Cybersecurity, frameworks, workforces, threats, techniques**

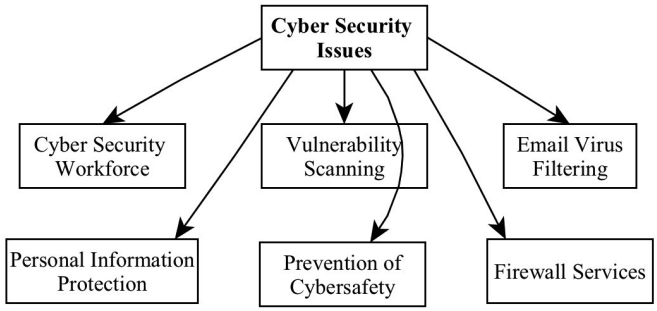

Fig. 1: Viewpoints of cyber security issues reviewed in this paper

I. Introduction

Cyber security has been used interchangeably for information security, where later considers the role of the human in the security process while former consider this as an additional dimension and also, focus person has a potential target. However, such discussion on cyber security has an important implication as it focuses on the ethical part of the society as a whole. There are various definitions of the concept of cyber security with varied aspects such as secured sharing, confidential and access to information. But still, the definitions lacks clarity and consensus.

Moreover, cyber security measured with regards to access, integration of data, security, storage and transfer of data through electronic or other modes [1], [2]. Cybersecurity indicates three important factors. The methods of protecting *Information Technology* (IT), the data itself, the data being processed and transmitted together with physical and virtual setup, the level of protection obtained by applying such measures and the professional aspects associated [3].

We define that the cyber-security as a measure protecting computer systems, networks, and information from disruption or unauthorized access, use, disclosure, modification or destruction [4]–[6]. In the context of this review cyber security has been defined as the integration of policies, security measures, approaches to risk management, protocols, technologies, process and training which can be utilized in securing the organization and cyber setup along with user assets [6].

This paper focuses on the issues of cyber security threats and summarizes the existing security models. Fig. 1 represents the main viewpoints reviewed in this paper, which include cyber security workforce, vulnerability scanning, email virus filtering, personal information protection, prevention of cybersafety, and firewall services. The significance of this paper are assisting both academics and professionals gain a holistic view about contemporary cyber security field. The main contributions of this paper have two aspects:

1) This paper summarizes crucial issues in cyber security domains by a literature review.
2) This paper proposes a number of research directions for future explorations in the field.

The remainder of this paper is organized by the following orders. Section II reviews and organizes crucial issues in cyber security. A number of aspects are addressed in this section. Next, a discussion about future researches is given in Section III. Finally, we present our conclusions in Section IV.

II. Crucial Issues in Cyber Security

Cyber security relies upon the care that individuals can take and conclusions they conduct while they organize,

[1]K. Thakur is with Department of Computer Science, Pace University, New York, NY 10038, USA, kt68851n@pace.edu.
[2]M. Qiu (Corresponding author) is with Department of Computer Science, Pace University, New York, NY 10038, USA, mqiu@pace.edu.
[3]K. Gai is with Department of Computer Science, Pace University, New York, NY 10038, USA, kg71231w@pace.edu.
[4]M. L. Ali is with Department of Computer Science, Pace University, New York, NY 10038, USA, ma03901n@pace.edu.
*This work is supported by NSF CNS-1457506 and NSF CNS-1359557.

manage and utilize systems and internet [7]. Numerous efforts have been made to find the solution for cyber security evaluation challenge and various frameworks have been constructed. However, the frameworks encounter different difficulties though it was working fine initially at the time of development [8]. The restrictions derive from different aspects, such as emerging technologies [9] and facility limitations. Security issues are often considered a tradeoff between security requirements and other benefits [10], [11].

A. Cyber security workforce

The framework of *National Initiative for Cybersecurity Education* (NICE) is an inter-agency attempt by the *National Institute of Standards and Technology* (NIST). The agency focuses on awareness, cyber security education, awareness, training and professional development. NICE Came up with the Cybersecurity Workforce Framework. This framework insists on recognition by the process of training. Also, accomplishes secure cyber infrastructure as defined in the context. Also, the framework has not included the factor new technologies are rapidly emerging that enhances the challenges in cyber security threats [12].

The scholars also mention that there need to be enough cybersecurity standards and procedures, which need to be frequently reviewed [8]. The researchers further indicate the frameworks has not included the aspects of threats that exploit vulnerable and hence strategies of risk management needs to be addressed [13]. Also, the authors recommend that cybercrime legislation is not in place to handle the criminals. Finally, an effective security strategy can be active in collaboration with modeling business processes [14].

B. Cyber safety for protecting personal information in computer

Cyber-safety is a concept that has been used to explain a set of measures, practices, and actions that help in the protection of computer and privacy from various attacks [15], [16]. At any company, there is a *Cyber-safety Program* policy, PPM 310-22, which establishes that all devices connected to any company electronic communications network must meet certain security standards. As required by the system, most departments offer annual reports defining their levels of the compliance. Also, various services are in place to assist all faculty, staff and students to meet the cyber-safety standards. Specific information about these services is provided.

The cyber safety threats can be caused due to viruses, hackers, identifying thieves, spyware [17]. The virus infects the computer through the email attachment and file sharing. One infected computer can cause problems to all the computer networks. A people who "trespass" the computer from a remote location are considered as Hackers. These people use a computer to send spam or viruses or do other activities that cause computer malfunction. In the case of identifying thieves, the people who obtain unauthorized access to the personal information like social security, and financial account numbers are considered [18]. Spyware is software that "piggybacks" on programs that are downloaded and gathers information about online habits and transmits personal information without the users knowledge.

In addition to the above-discussed problem, a company may face a number of other consequences if they fail to take actions to protect personal information and user's computer. The consequence indulges such as loss in the access of campus computer network, confidential information, integration and access to valuable University data, research on personal electronic data lawsuits, loss of public trust and offer opportunities, pursuit, internal conflict action and or employment termination.

C. Studies of email virus filtering

Several studies have been conducted on the filtering of email virus Prior study had addressed various existing spam detection methods and finding the useful, precise, and dependable spam detection process [19]. The applications that are currently applied by various anti-spam spam software are considered to be static, which mean that it is quite easy to elude by tweaking the messages.

To perform this, the spammer would evaluate the current anti-spam methods and determine the modes to play around [20]. To combat the spam effectively, it is important to adopt a new technique. This new approach needs to be complete the spammer's strategies as they are changed from time to time [21]. It must also able to adapt to the particular organization that it is protecting for the answer lies in Bayesian mathematics. The study findings indicated that some of the spam detection method and the numerous issues associated with the spam. From various studies, it is understood that we will not be able to stop the spam and will be a limit them effectively using Bayesian method when compared to other methods.

Moreover, prior research also explored various problems associated with spam and spam filtering methods, techniques. The different methods determine the incoming spam methods are Bayesian analysis, Blacklist/Whitelist, Keyword checking and Mail header analysis [22]. The different spam filtering techniques adopted Distributed adaptive blacklists, Rule-based filtering, Bayesian classifier, K nearest neighbors, *Support Vector Machine* (SVM), *Content-based Spam Filtering Techniques - Neural Networks*, *The multi-layer networks*, *Technique of search engines*, *Technique of genetic engineering*, *Technique of artificial immune system*. The study findings revealed that many of the filtering techniques are based on text categorization methods, and there is no technique can claim to provide an ideal solution with 0% false positive and 0% false negative. There are a

lot of research opportunities to classify multimedia and text messages.

Kumar et al. [23] indicated that the spam dataset is examined with the use of TANAGRA data mining tool which determine the efficient classifier in the classification of email spam. Firstly, feature selection and feature construction is conducted to obtain the required characteristics [24]. After that different classification algorithms would be applied to the dataset and a cross-validation would be done on each classifier. In the end, the best classifier in email spam is determined on the aspects of precision, error rate and recall. From the obtained results, fisher filtering and runs filtering feature selection algorithms performs better classification for many classifiers. The Rnd tree classification algorithm applied to relevant features after fisher filtering has produced more than 99% accuracy for spam detection. This Rnd tree classifier is also tested with test dataset which gives accurate results than other classifiers for this spam dataset.

D. Studies of firewall services

Al-Fayyad et al. [25] evaluated the performance of personal firewall systems by organizing an arranged walk-through to determine the design factors that could violate the usage standards. In the study of personal firewalls usability on Windows XP platform, four modern firewalls namely Norton 360 V. 2.0.0.242, Trend Micro Internet Security Version 16.00.1412, Zone Alarm V. 7.1.248 and ESET Nod32 Smart Security. The study results indicated that Personal firewalls encounter poor usability that could lead to vulnerabilities in security. The usability problems could be due to the issue that the data given by the firewalls (could be during the process of installing, configuration or during interaction) was not clear or misleading. Various usability problems have been noticed because of the reduced clarity of alerts.

Li [26] evaluated the issues in placing the firewalls in the topology of networking design and how to frame the routing tables in the process so that a maximized firewall rule set could be minimal that helps to avoid performance bottleneck and limits the security loopholes. There have been two significant contributions that the problems are NP-complete, and that a heuristic solution has been proposed and illustrate the efficiency of algorithms using simulations. The outcome of the test indicates that the suggested algorithm has limited the multi-firewall rule set than other algorithms.

E. Studies of vulnerability scanning

Sudha Rani et al. [27] analyzed *Intrusion Detection System* (IDS) methods to identify an attack of a computer network. In order to prevent vulnerable virtual machines network, intrusion detection system is proposed. In addition, the study has taken potential security risks as well as the security considerations taken into account for implementing a virtual private network [3]. The study findings revealed that there is two types of intrusion detection system host based and network based. In addition proposed solution provides information on how to use programmability of software switches based on the solutions that improve the detection accuracy and defeat.

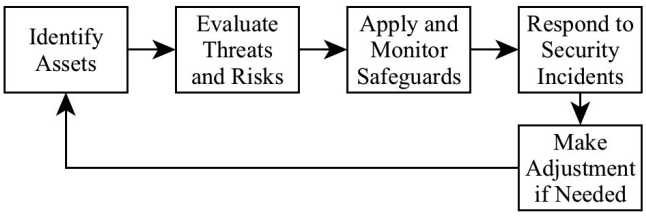

Fig. 2: General operation flow of cybersafety prevention

Other research [25] focused on the vulnerability assessment for automatic environments along with the web applications and various threats which are detected during the vulnerability assessment for different networking products. The study has adopted OpenVas tool with exploratory research method. The study findings revealed some of the methods that can fix vulnerability for removing threats using the function PHP info () and other methods like Trojan helps in keeping networking systems safe.

Ye et al. [28] studied the quantitative vulnerability assessment model in cyber security for DAS. The evaluation process is distinguished into three sections namely vulnerability adjacency matrix formation, attack processes modeling, and physical consequences analysis. The increasing smart grid merits cyber security problems has enhanced because of the higher integration of cyber systems to the physical power systems. It has been found that DAS is highly exposed to cyber attacks when compared to various control systems in substations or power plants.

However, it has to make sure that each DAS is secure and economically not favorable and technically not essential. The theory involves creating ADG models, evaluation of potential physical effects due to cyber-attacks and suggesting vulnerability adjacency matrix to show the connection among various weaknesses. Numerous case studies on account of RBTS bus 2 indicate the effectiveness and validation of the proposed vulnerability assessment model.

F. Prevention of Cybersafety

There are seven significant cyber-safety actions which are Running Anti-virus Software, Installing OS/Software Updates, Preventing Identity Theft, Switch on the Personal Firewalls, Prevent Adware/Spyware, protection of Passwords and Backing up Important Files [29]. Fig. 2 represents a general operation flow of the cybersafety prevention.

1) Install OS/Software updates:

- Installing software updates are also known as patches that helps to fix issues of operating system (OS) (e.g., Mac OS X , Windows Vista, Windows XP,) and software programs such as Microsoft applications.
- Many of the latest operating systems are arranged to download updates automatically by default. Once the updates have ben downloaded, a confirmation prompt is displayed for installation. Click yes
- Once the updates are complete, make sure to restart the computer for the patches to be applied.

2) Running Anti-Virus Software:

- In order prevent computer virus issues install and then run the anti-virus software such as Sophos and check the last updated date.
- Make sure to check periodically if the installed anti-virus is up to the date which helps to block current and future viruses. The anti-virus application removes detected viruses, quarantines it and finally repairs users system infected files.
- The students of UC Davis, staffs and faculty members can download Sophos software for both homes and work computers for free from the Internet Tools CD, which you can obtain from the Shields Library's IT Express.

3) Preventing Identity Theft:

- Don't give out financial account numbers, Social Security numbers, driver's license numbers or other personal identity information unless you know exactly who's receiving it. Protect others people's information as you would your own.
- Never send personal or confidential information via email or instant messages as these can be easily intercepted.
- Beware of phishing scams - a form of fraud that uses email messages that appear to be from a reputable business (often a financial institution) in an attempt to gain personal or account information. These often do not include a personal salutation. Never enter personal information into an online form you accessed via a link in and any email from an unknown email id. Generally authentic businesses do not request personal details online.

4) Switching on Personal Firewalls:

- Find under system's security setting for a default personal firewall and switch it on. Mac OSC and Microsoft Vista have installed built-in firewalls. After turning on the firewall, check it for any open ports which would allow hackers and viruses.
- Firewalls work as the protection layers between the internet and computers.
- The standard process of hackers would be to send pings(calls) to various computers at random and check for their responses. The functionality of Firewalls is to block your computer which prevents any response calls from a computer.

5) Protecting passwords:

- Make sure that not to share your passwords, and make sure to create new passwords which are hard to guess. Avoid any dictionary works and establish a password by with mixed number, alphabets, and punctuation marks.
- Be sure not to use any common passwords or its variations such as abc123, iloveyou1, let me in, qwerty1, (yourname1), password1 and baseball1.
- Change passwords periodically.
- When choosing a password:
  - Mix upper and lower case letters
  - Use a minimum of 8 characters
  - Use mnemonics to help you remember a complicated password

III. Discussions

From the review it was observed that, there are various studies conducted on cyber safety especially earlier studies have tried to attempt the problems linked to spam and spam filtering techniques [19]. In specific, spam dataset is analyzed using TANAGRA data mining tool to explore the efficient classifier for email spam classification [23]. Further studies also analyzed various existing spam detection methods and identified an efficient, accurate, and reliable spam detection method [19].

The usage of personal firewall systems by performing a cognitive analysis in determining design elements which would violate the principles of usability [30]. The issue of how to arrange the topology of firewalls in a network design and how the frame the routing tables in execution so that the max firewall rule set could be limited [26]. Attribute-based solutions can be an option for specific security requirements [31].

The usage of *Intrusion Detection System* (IDS) [32] procedure to find a computer network attack [27]. The vulnerability assessment in automatic setups together with web applications and other threats, such as data validations [24], [33]. An innovative quantitative vulnerability assessment model on cyber security for DAS is evaluated [28]. Further the analysis indicated various safety and prevention functionalities.

IV. Conclusions

From the review, it was found that majority of the studies have been conducted on the email security, firewalls, and vulnerabilities. Yet, not many studies from the perspective of password security. There are general recommendations on how to secure the password but not any authenticated protocol to protect the system inherently. Therefore, there

is a need for more studies in terms of technics and models from this perspective to ensure that passwords are protected.

REFERENCES

[1] J. Blackburn and G. Waters. *Optimising Australia's Response to the Cyber Challenge*. Kokoda Foundation, 2011.

[2] L. Bennett. Cyber security strategy. *ITNOW*, 54(1):10–11, 2012.

[3] M. Qiu, L. Zhang, Z. Ming, Z. Chen, X. Qin, and L. Yang. Security-aware optimization for ubiquitous computing systems with SEAT graph approach. *J. of Computer and Syst. Sci.*, 79(5):518–529, 2013.

[4] M. Gallaher, A. Link, and B. Rowe. *Cyber Security: Economic Strategies and Public Policy Alternatives*. Edward Elgar Publishing, 2008.

[5] F. Pasqualetti, F. Dorfler, and F. Bullo. Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control*, 58(11):2715–2729, 2013.

[6] Y. Yan, Y. Qian, H. Sharif, and D. Tipper. A survey on cyber security for smart grid communications. *IEEE Communications Surveys & Tutorials*, 14(4):998–1010, 2012.

[7] A. Tonge, S. Kasture, and S. Chaudhari. Cyber security: challenges for society-literature review. *IOSR Journal of Computer Engineering*, 2(12):67–75, 2013.

[8] 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.

[9] K. Gai and S. Li. Towards cloud computing: a literature review on cloud computing and its development trends. In *2012 Fourth Int'l Conf. on Multimedia Information Networking and Security*, pages 142–146, Nanjing, China, 2012.

[10] M. Qiu, H. Su, M. Chen, Z. Ming, and L. Yang. Balance of security strength and energy for a PMU monitoring system in smart grid. *IEEE Communications Magazine*, 50(5):142–149, 2012.

[11] M. Qiu, W. Gao, M. Chen, J. Niu, and L. Zhang. Energy efficient security algorithm for power grid wide area monitoring system. *IEEE Transactions on Smart Grid*, 2(4):715–723, 2011.

[12] F. Hu, 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.

[13] S. Ahmed, M. Elsholkami, A. Elkamel, J. Du, E. Ydstie, and P. Douglas. Financial risk management for new technology integration in energy planning under uncertainty. *Applied Energy*, 128:75–81, 2014.

[14] Y. Badr, F. Biennier, and S. Tata. The integration of corporate security strategies in collaborative business processes. *IEEE Trans. on Services Computing*, 4(3):243–254, 2011.

[15] O. Boric-Lubecke, X. Gao, E. Yavari, M. Baboli, A. Singh, and V. Lubecke. E-healthcare: Remote monitoring, privacy, and security. In *IEEE Int'l MTT-S*, pages 1–3, Tampa, FL, USA, 2014.

[16] K. Gai, M. Qiu, L. Chen, and M. Liu. Electronic health record error prevention approach using ontology in big data. In *17th IEEE International Conference on High Performance Computing and Communications*, pages 752–757, New York, USA, 2015.

[17] 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.

[18] Yibin Li, Wenyun Dai, Zhong Ming, and Meikang Qiu. Privacy protection for preventing data over-collection in smart city. *IEEE Transactions on Computers*, PP(99):1, 2015.

[19] 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.

[20] F. Benevenuto, T. Rodrigues, A. Veloso, J. Almeida, M. Gonçalves, and V. Almeida. Practical detection of spammers and content promoters in online video sharing systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 42(3):688–701, 2012.

[21] M. Cha, F. Benevenuto, H. Haddadi, and K. Gummadi. The world of connections and information flow in twitter. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, 42(4):991–998, 2012.

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

[23] R. Kumar, G. Poonkuzhali, and P. Sudhakar. Comparative study on email spam classifier using data mining techniques. In *The International MultiConference of Engineers and Computer Scientists*, volume 1, pages 14–16, Hong Kong, China, 2012.

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

[25] B. Alfayyadh, J. Ponting, M. Alzomai, and A. Jøsang. Vulnerabilities in personal firewalls caused by poor security usability. In *IEEE Int'l Conf. on Infor. Theor. and Infor. Security*, pages 682–688, Beijing, China, 2010. IEEE.

[26] J. Li. The research and application of multi-firewall technology in enterprise network security. *Int'l J. of Security and Its Applications*, 9(5):153–162, 2015.

[27] N. Rani, A. Satyanarayana, and P. Bhaskaran. Coastal vulnerability assessment studies over india: a review. *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.

[29] 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.

[30] H. Hu, G. Ahn, and K. Kulkarni. Detecting and resolving firewall policy anomalies. *IEEE Transactions on Dependable and Secure Computing*, 9(3):318–331, 2012.

[31] K. Gai, M. Qiu, B. Thuraisingham, and L. Tao. Proactive attribute-based secure data schema for mobile cloud in financial industry. In *The IEEE International Symposium on Big Data Security on Cloud*, pages 1332–1337, New York, USA, 2015.

[32] K. Gai, M. Qiu, L. Tao, and Y. Zhu. Intrusion detection techniques for mobile cloud computing in heterogeneous 5G. *Security and Communication Networks*, pages 1–10, 2015.

[33] L. Tao, S. Golikov, K. Gai, and M. Qiu. A reusable software component for integrated syntax and semantic validation for services computing. In *9th Int'l IEEE Symposium on Service-Oriented System Engineering*, pages 127–132, San Francisco Bay, USA, 2015.