Threats and Emerging Developments in Cyber Security

M. Murugesan
Department of Computer Science and Engineering, Anurag Engineering College, Ananthagiri, Telungana.
E-mail: murugeshvim@gmail.com

P. Balamurugan
Department of Information Technology, College of Engineering and Technology, Faculty of Engineering and Technology, SRM Institute of Science and Technology, SRM Nagar, Kattankulathur, Kanchipuram, Chennai, TN, India.
E-mail: pookumbala@gmail.com

J. Santhosh
Department of Computer Science and Engineering, Vel Tech Rangarajan Dr.Sagunthala R &D Institute of Science and Technology, Chennai.
E-mail: j.santhoshme@gmail.com

G. Arulkumaran
Department of Computer Science and Engineering, Vel Tech Rangarajan Dr.Sagunthala R &D Institute of Science and Technology, Chennai.
E-mail: erarulkumaran@gmail.com

Received July 16, 2020; Accepted September 18, 2020
ISSN: 1735-188X
DOI: 10.14704/WEB/V17I2/WEB17053

Abstract

Cyber security plays a significant role in science. Data or information security is one of the crucial issues facing the world, when there is discussion about the rapidly growing cyber-crimes, the government and many corporations are taking many steps to stop such crimes. Driven by several different measures, cybercrime continues to expand day by day. In this review, the problems confronting cyber security from emerging technological advances and developments are briefly discussed and, in turn, the paper also reflects on the newest cyber security technologies, trends and other ethics throughout the cyber security field.

Keywords

Cyber Security, Cybercrime, Threads, Encryption and Attacks.

Introduction

In modern era, with just one click of a button, people are able to send and receive any type of data or information such as video and electronic mails. Is there any attention provided to the secure sharing of data without leakage of some sort? One of the best ways to solve the aforementioned issue is cyber security. The internet is the rapid growing industries for that, and several recent technologies are totally transforming the network. Owing to the growing advances in technology, people are not able to monitor their valuable data and this is why crime is growing. For an instance, people are using online mode to transfer the amount, which is why high data security is necessary for the successful and complete protection concern. Not only is the scope of cyber security restricted to data protection, but there is also the requirement to add various fields such as the network house and much more [1-2].

In recent years, many advancements have made like smart phones, cloud storage and online transactions, often required high degree of protection. Since these solutions keep users ' private information and their security is very important. We also acquired customer trust by improving information protection and completely securing critical records, and it is very important for the defense structures of all countries and also beneficial for economic well-being. Securing the security is important to government operations [3].

Combating cybercrimes requires a very detailed and secure strategy. By giving technical measures alone is not sufficient to prevent this crime, and it is very difficult that law enforcement agencies are permitted inspect and prosecute cybercrime effectively. A lot of countries are now attempting to enforce the stringent cyber security regulations to avoid the loss of any critical information. Even everyone should be educated in this problem to protect themselves from rising levels of crimes.

Cybercrime

Cybercrime is a type of illegal operation that utilizes a computer a network or a networked device, and the increasing number of such crimes involves crimes that are generated by using machines like network surveillance and spreading of laptop viruses as well as other crimes including well as computer-enabled crimes such as stalking and bullying. The term cybercrime can be defined in simple words as a crime perpetrated by the use of computer device. Often, use the internet to snatch some person's identity and peddle the illegal drugs. When more technology and creativity progresses, more offences are growing as well.

Cyber Security

One of any government's main concerns is data security and now more information is being handled all over the world in digital versions or in cyber form. Several social networks provide a good environment where people should feel protected while connecting with others around the globe. The crimes being discussed have their main social media target for evaluating the unlicensed data. Besides social network, people also required to take necessary steps while online banking.

Network Security

In order to determine the last degree of protection for the system analyzed, the basic and extraordinarily common strategies were established in which the protection master initially made what should be broken down and then their master would work out the relevant considerations with an easily sensible approach. Subsequence, the stste of system stability as well as many methods, it varies over period. Most existing ways are subject to hazard investigation for the security of a system action, in which the hazard of a safety is portrayed as a component of hazard and hazard.

$$\text{Risk} = \text{Vulnerability} * \text{Threads} * \text{Impact} \quad (1)$$

Equation (1) indicates the probability is the product of the potential impacts and the current risks, and selected network insecurity, too. Quite generally, that is sued to clarify the network evaluation criteria. But when applied as a solution to the real-life problem, these variables are Real and Real Difficult to represent with certain values.

Trends in Cyber Security

Cyber Security in Companies

Cyber security is a increasingly growing sector that is currently generating new employment for the next decade, as both government sectors and private sectors are making major investments in data and information technology defense. Norton's annual Cybercrime reported that around 143 million people in the U.S. became victims of cybercrime, and in 2017 it cost $110 billion in cybercrime [18]. The US President recently announced that "Cyber attacks are one of the most major strategic and economic difficulties confronting us as a world" and that "the economic stability of America in the twenty one century and must hang on cyber security [19].

The White House has reported that the United States government alone will need as many as 30,000 new Cyber security professionals in the coming years. Many cyber security adjustments are expected to be new kinds of information science and research skills. The normal increase in the information will mean that the human-made reasoning may likewise be necessary. Versatile capabilities will be one of the biggest keys for the cyber security era ahead.

Web Servers

The possibility of threats on the network client to physically get the information by inserting malicious file is strong, and the hacker can spread malicious file on the internet by using any legal secers. It is also high risk to have the acquisitions that are not approved for data and many of them get the media coverage. Protection of the servers and all applications is required.

Web server and its components are illustrated in figure.1. Web server is the one of the easiest components to enter with these malicious codes, so people need to make straightforward transactions with the safer browsers to remain safe[5].

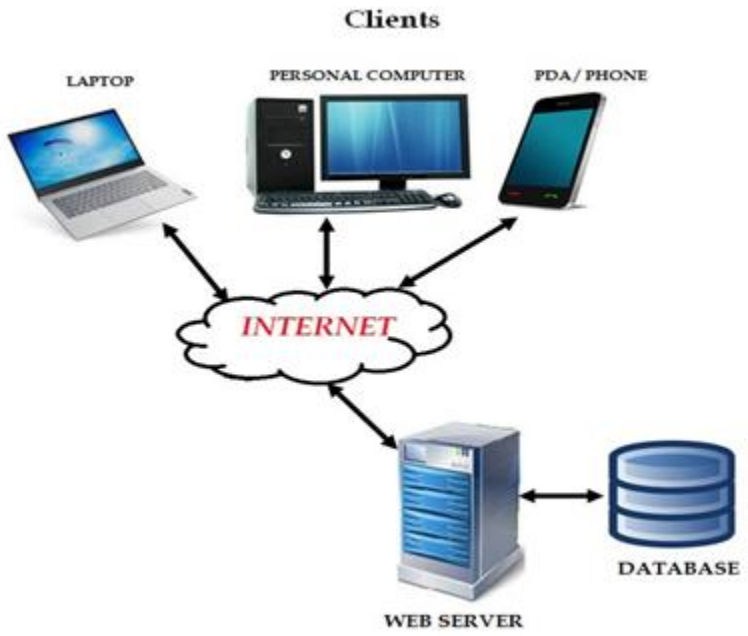

Fig. 1 Web server and its components

Cloud Computing with Services

Recently, most of companies are promoting the utilization of cloud infrastructure, and the entire environment is rapidly shifting towards clouds, this phenomenon is presenting a

huge challenge to cyber security. Besides this, because most of the applications down are like in the cloud, the internet and information development approach still needs to broaden as it expects the lack of data available. Could solutions make the different strategies and several security problems are observed, the cloud services could offer many opportunities and it should be observed that the security issues are also increasing as the cloud progresses.

Advance Persistent Threads

APT is normally a new Cybercrime ware platform. Computer network system is employed for many years as the major part of assessing target attacks. A majority of threats utilize sophisticated approaches, network protection will cooperate with other defense tools to detect threats in a timely manner. This is why monitoring measures [5] should be developed to secure the network from external threats.

Mobile Communication Networks

In modern era, people can communicate with others around the globe and the network security is a major problem. Diverse kind of protection measures are not enough, because people use electronic apps such as cell phones , laptops that need more protection than those included by default in the products. It is necessary to consider the problems of smart phones and in order to contribute to this, the mobile communication network is at high risk for cybercrime advertisements, users should be sought to open any links or ads.

Internet Protocol (IPv4 and IPv6)

IP was being upgraded to IPv6 since IPv4 became the primary machine network and communication internet protocol. Protecting this not only requires the uploading of IPv4 functionality, however it is a major turning change in the creation of IP addresses, there are some major important modifications to this procedure that must be included in protection rules. This is why upgrading to IPv6 as early as possible is really silly to lessen the chance of cybercrime [6].

Encryption

Encryption transforms information into a form meaning it can be read only by those with access to concealed information by using key or password. Encrypted documents are usually called cipher-text, at present in ICT, data encryption is one of powerful methods to provide data security. Encryption is an extremely fundamental level for data protection and data integrity. But more usage of this means that more cyber security issues arise. The

transmitted data is secured with the help of encryption and data transmitted over communication network, for example [7], can also be realized if the information is leaked through code encryption.

Applications of Data Security

There is also a new prospect in application security however it is not taken advantage of by most companies because it is very expensive. So it's now necessary to find it out the right way to assess the safety and nest method value to explain that to the firm. In turn, DevOps[8] can also become the DevSecOps[9] and concentrate on protection. This is a good time to combine the activities and the advances. Time to the market has been made less of a considerable measure and it makes the interminable association between progress and activity which shows that it is exceptionally vital to stop running these parts in a different mode. Time has come to bring the security to DevOps.

IT Risk Assessment

The framework for ordinary evaluation of IT risk management is used in organization such as organizational simple danger and helplessness management. In fact, there are considerably more approaches, such as Central Computer and Media Transmission Office[10] analysis of danger and procedure for administration (CRAMM), from which stage moreover comes the risk assessment of target and bi-functional and CORAS, which is a kind of model-based threat assessment method for the general system. However, there is also a wide range of the idea that is scholastic in nature, such as the ISRAM-known data protection chance analysis technique.

Furthermore, risk analysis and vulnerability measurement and benchmarking Sprint is a tactic that is reordered as a chance inquiry method; and, in turn, business process chance management named as BPM approach [11]. Numerous techniques available for the test fire, and some examples of the SCADA mechanism other than the IT game plan mentioned here and used to restrict the application of the IT business infrastructure threat evaluation of the SCADA frameworks. The system must be concerned with being configured in the framework of SCADA systems in the IT hazard evaluation and all aspects in terminology; the hazard is delineated as follows.

The assessment of hazard in SCADA’s systems should be especially helpful in coordinating in an appropriate manner between the frame segments as to their role and importance in the system operation, and in turn as to the nature of the threat they have and their probability of validation. The evaluation of the threat is helpful in assisting the

administrators and experts in a SCADA environment alongside strengthening critical monitoring arrangements in the construction in defense networks and also rationally allocating the finite resource [12].

It's also useful to promote contact between SCADA's defense, industry, and experts. It was articulated in 2004 that, considering the interdependent network networks, there is a desperate need for getting the ideology that is essential for applying the protection to the SCADA scheme. There have been a range of risk evaluation approaches developed for SCADA systems over the last few years and these have been motivated by the value of monitoring and exposure to cyber security threats in SCADA systems. The key objective of this research work is to demonstrate the current cyber security pattern and also to demonstrate the potential solutions.

Most of the literature on SCADA security and cyber security problems are available, but not many of them focus on the solutions to risk assessment [13]. Detailed review of the methods of risk assessment was presented by [14] in 2016, but very few approaches were listed in it. It is very difficult to categorize risk management in general and for the SCADA system. The categorization system must be polygon and it should focus upon various system factors. Our systemic architecture of the categorization method remains an open subject under review. It is helpful to check and analyze the specific and duplicate methods [7] in the scheme and that it is useful to find and elaborate the same system characteristics.

Cyber Security Threats

Normally, there are two categories of threats related to cybersecurity that are referred to as activity aimed at having detrimental effects on digital media networks and certain acts that are necessary to hack network infrastructure or other malicious reasons without doing any damage that may have consequences at once.

The internet abuse includes the integration of using the network and another software agreement to apply some sort of coercion such as stealing, organizing a mental oppressor and copyright violation, sending dubious communications that combine political and loathe speech, and providing the provocative enthusiasm of restricted children or distinguishing content. Close proximity the augmentation of the available hacking devices and creations which are not above the top like viruses and malware and RF surveillance systems, in case one person uses the email and game plan of his or her PC, he should be targeted at any level.

Software Tools for Attacks

There are many programming tools are available and utilized to robotize many threats and by using this software and pre-installed attacks, a lone guilty party can attack a wide range of computer systems in a single day using a single computer. In which the accused party should have in any case one PC at the entry. Since most product devices are available, however, the attack strategy does not result in the attacks being fruitful. customers should now update their job systems and regularly implement them, as them decreases the risk of yielding to such expansive based attacks because the company now makes security programming tests assaults tolls as they are also fully prepared for the threats.

Cyber Security in Social Media

Social media is increasingly being used aloeously and most companies are now considering using social media to advance. This forum plays a tremendous role in increasing the issue of cybersecurity, and even leads to rising risks of cyber attack. In the general public, the use of this stage is always with the malevolent assaults. This stage is used by different people in several organizations and is one of the easiest targets for programmers and individual information hacking and has some unauthorized access to sensitive or hidden data.

People's desire to convey the knowledge to others coincides with the underlying question that web-based social networking exists within the enterprise. In fact, it also offers everyone the ability to submit the incredibly private business information. Conjointly, social media often offers the same ability to expose the incorrect details that could hurt the company. Social networking allows data dissemination at a very high pace that can significantly increase a company's risk[15].

Techniques for Cyber Security

The following are few cyber-attack security strategies.

Login Protection and Authentication

A mechanism for using the username and password is a very simple data protection strategy and this is one of the most common cybersecurity steps. It's no longer possible to only use username and password. Attacker can quickly guess, or use password cracking methods. Even though there are plenty of password protection methods are report, strong password means hard to guess. Password may be used to provide enhanced access

protection in addition to other types of access management methods such as biometrics or two-step authentication.

Data Authentication

Data Authentication is the crucial cyber security method which intends to verify the uniqueness of the baseline and this verification heavily relies on the attributes which are put away in the framework area. One of the most commonly known methods of administration of hidden core invention and there are distinctive separate executions, such as SIM cards inserted in the telephone of another person. Equally, SIM cards are filled with such each-of-a-kind ID numbers that the covered communication line overlooks in order to acquire the distinctive proof procedure for a given number.

The most important issues associated to this protocol is that the unapproved individuals are undergoing foiling efforts to listen stealthily to the message. This watchword transmitting through the unpredictable medium is at risk of being catched by the untrustworthy individuals who might use it to treat the first customer. The utilization of encryption methods listed in next section will rectify this issue. It is important to ensure that the documents which you obtain are authenticated before uploading them. One needs to make sure the paper comes from a known, reliable source. Using tools such as antivirus to ensure they are not malicious files will normally authenticate those documents. For this reason it is necessary to install the good antivirus[16] to protect the systems from viruses[17].

Malware Scanner

Malware has become one of the serious threats to cyber security in the last few decades. Nearly any issue in the cyber world such as viruses, denial - of - service, somewhere linked to malware. The malware scanner is a program which we used to search for any malicious information on the records and data that are stored in a computer network. One example of that includes horses from Trojans.

Though there are many spam detection methods reported in the literature, they , they often suffer significant flaws. Such as signature-based methods can easily be bypassed with the use of obfuscation and network call-based strategies can also be stopped with reordering attacks from the system call. In the other side, such identification strategies are often effective based on complex analysis, yet their execution is sluggish and incompetent in the detection of malware on end-user machines in real time. Selection of an efficient and

appropriate technique to attack classification for end-users should be considered carefully [20].

Firewall

It is often a program that is used to identify malicious data or individuals who try to access the content through the internet or network in an inappropriate manner. All the information sent or received from the device usually passes through the firewall, which is used to analyze the files, or to view and block data which may be dangerous to the device [21]. The firewall is crucial component in detecting malware codes in the network in this way [22]. Fig 2 provides a general description of how firewall is exploited to defend SCADA from cyber-attacks.

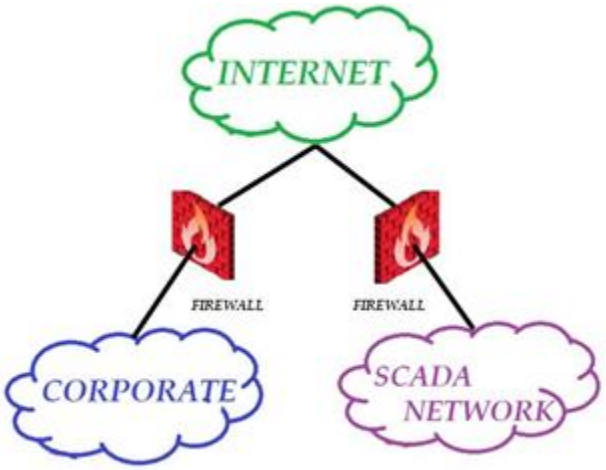

Fig. 2 SCADA and corporate network

Antivirus Programs

Antivirus software detects and avoids computer malicious files. Most ant viruses have the feature of auto-updating that helps us to have all the information about the viruses and detect new viruses as they reach the device.

Conclusion

It is a critical trend as the world grows more interconnected. Gradually, Computer devices are being used to render critical trades. Along with the development of sophisticated information security instruments and distinguished global hazards every day, innovative developments impact companies to recognize the reliability of their Computer networks and need make better stages and tools to support their systems. There is no terminal

response for automated assaults. In every case, we will make every attempt to restrict cybercrime.

References

Thakur, K., Qiu, M., Gai, K., & Ali, M.L. (2015). An investigation on cyber security threats and security models. *In IEEE 2nd International Conference on Cyber Security and Cloud Computing*, 307-311.

Mann, B. (2009). *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards.* Cabinet Office, London.

Byres, E., Leversage, D., & Kube, N. (2007). *Security incidents and trends in SCADA and process industries.* The industrial ethernet book, *39*(2), 12-20.

Cárdenas, A.A., Amin, S., Lin, Z.S., Huang, Y.L., Huang, C.Y., & Sastry, S. (2011). Attacks against process control systems: risk assessment, detection, and response. *In Proceedings of the 6th ACM symposium on information, computer and communications security*, 355-366.

Cheminod, M., Durante, L., & Valenzano, A. (2012). Review of security issues in industrial networks. *IEEE transactions on industrial informatics*, *9*(1), 277-293.

Chittester, C.G., & Haimes, Y.Y. (2004). Risks of terrorism to information technology and to critical interdependent infrastructures. *Journal of Homeland Security and Emergency Management*, *1*(4).

Coles, R.S., & Moulton, R. (2003). Operationalizing IT risk management. *Computers & Security*, *22*(6), 487-493.

Bass, L., Weber, I., & Zhu, L. (2015). *DevOps: A software architect's perspective*. Addison-Wesley Professional.

Myrbakken, H., & Colomo-Palacios, R. (2017). DevSecOps: a multivocal literature review. *In International Conference on Software Process Improvement and Capability Determination*, *Springer, Cham*, 17-29.

Yazar, Z. (2002). *A qualitative risk analysis and management tool–CRAMM*. SANS Info Sec Reading Room White Paper, *11*, 12-32.

Campbell, P.L., & Stamp, J.E. (2004). *A classification scheme for risk assessment methods*. United States. Department of Energy.

Saltuk, Y., & El-Idrissi, A. (2015). Impact Assessment in Practice: Experience from leading impact investors. *JP Morgan Global Research*, *4*.

Sajid, A., Abbas, H., & Saleem, K. (2016). Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges. *IEEE Access*, *4*, 1375-1384.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & security*, *56*, 1-27.

Jabee, R., & Alam, M.A. (2016). Issues and challenges of cyber security for social networking sites (Facebook). *International Journal of Computer Applications*, *144*(3), 36-40.

Annam, S.R. (2001). An Overview of Computer Security. arXiv preprint cs/0110043.

Thakur, K., Ali, M.L., Kopecky, S., Kamruzzaman, A., & Tao, L. (2016). Connectivity, Traffic Flow and Applied Statistics in Cyber Security. *In IEEE International Conference on Smart Cloud (SmartCloud)*, 295-300.

Ali, M.L., Thakur, K., & Atobatele, B. (2019). Challenges of Cyber Security and the Emerging Trends. *In Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure*, 107-112.

Kolbitsch, C., Comparetti, P.M., Kruegel, C., Kirda, E., Zhou, X.Y., & Wang, X. (2009). Effective and efficient malware detection at the end host. In *USENIX security symposium*, *4*(1), 351-366.

Thakur, K., Tao, L., Wang, T., & Ali, M.L. (2017). Cloud Computing and its Security Issues. *Application and Theory of Computer Technology*, *2*(1), 1-10.

Ahmad, A. (2012). Type of security threats and it's prevention. *International Journal of Computer Technology and Applications*, *3*(2), 750-752.