DOI-10.53571/NJESR.2019.1.1.65-74

An Investigation On Cyber Security Threats And Security Models

Shejin.T.R
Lecturer In Computer Engineering
Sree Rama Government Polytechnic College
Thriprayar
Thrissur
Kerala

(Received:1January2019/Revised:10 January2019/Accepted:20 January 2019/Published:30 January2019)

Abstract

A plan for defining and implementing security policies is called a computer security model. A formal model of access rights, a computational model, a distributed computing model, or no theoretical foundation at all can serve as the foundation for a security model. Information security and cyber security are often used interchangeably; the former views human involvement as an extra dimension in the security process, while the latter views human focus as a potential target. However, because it centres on the ethical aspect of society as a whole, such a cyber-security conversation has significant implications. Identifying and disseminating information about potential dangers to a given system or network is known as threat modelling. An IT team may comprehend threats and their potential effects on the network by using security threat modelling. Numerous frameworks and strategies have been proposed to handle the cyber security challenge. Additionally, it provides an overview of the structure, personnel, and information pertaining to safeguarding personal computer data. This research examines these models, their shortcomings, and previous approaches to reducing these risks. In addition, the paper offers suggestions for additional research.

Keywords: Computer Security, Computers, Software, Standards, Computational modeling, Computer Science.

Introduction

Information security and cyber security are often used interchangeably; the former views human involvement as an extra dimension in the security process, while the latter views human focus as a potential target. However, because it centres on the ethical aspect of society as a whole, this kind of cyber security conversation has significant implications. There are numerous definitions of the idea of cyber security with varied characteristics such as secured sharing, confidential and access to information. Still, there is a lack of consensus and clarity in the definitions [1]. Cybersecurity encompasses all facets of safeguarding a company, its personnel, and its resources against online dangers. Many cyber security solutions are needed to reduce business cyber risk as cyberattacks become more frequent and sophisticated and corporate networks become more intricate. Organisations can strengthen their cybersecurity posture by adhering to a set of best practices or recommendations known as cybersecurity standards[2]. Cybersecurity standards can assist organisations in identifying and putting into place the necessary safeguards to keep their data and systems safe from online attacks. Guidelines on how to handle and recover from cybersecurity incidents can also be found in standards. Cybersecurity frameworks are generally applicable to all enterprises, regardless of their size, industry, or sector. The common cybersecurity compliance criteria that serve as a solid foundation for any cybersecurity strategy are described in depth on this page. Cybersecurity threats are activities conducted by individuals with ill intent, whose purpose is to steal data, cause damage to or disrupt computing systems.

Different Types Of Cyber Security Systems

The field of cyber security encompasses numerous disciplines. There are seven main pillars to it:

1. Security For The Network

The majority of attacks occur over the network, and solutions for network security are made to find and stop these attacks. To enforce safe web use policies, these solutions include data and access controls like Data Loss Prevention (DLP), Identity Access Management (IAM), Network Access Control (NAC), and NGFW (Next-Generation Firewall) application controls.

The IPS (Intrusion Prevention System), NGAV (Next-Gen Antivirus), Sandboxing, and CDR (Content Disarm and Reconstruction) are among the cutting-edge and multilayered network threat prevention technologies. Network analytics, threat detection, and automated SOAR (Security Orchestration and Response) technologies are also significant[3].

2. Security For The Cloud

As more businesses use cloud computing, cloud security becomes a major concern. Cyber security solutions, controls, policies, and services that assist in protecting an organization's entire cloud deployment (applications, data, infrastructure, etc.) are included in a cloud security strategy. against invasion.

Even though a lot of cloud service providers offer security solutions, achieving enterprise-level cloud security often requires more. In cloud environments, additional third-party solutions are required to safeguard against targeted attacks and data breaches.

3. Endpoint Protection

The zero-trust security model recommends putting data into microsegments wherever it may be. Using endpoint security is one method for accomplishing this with a mobile workforce. Companies can protect end-user devices like desktops and laptops with endpoint security, which includes technologies that provide forensics like endpoint detection and response (EDR) solutions, advanced threat prevention like anti-phishing and anti-ransomware, and data and network security controls[4].

4. Mobile Security

Because mobile devices like smartphones and tablets have access to corporate data, businesses are vulnerable to threats from IM (instant messaging) attacks, zero-day malware, phishing, and malicious apps. These attacks are prevented by mobile security, which also protects operating systems and devices from rooting and jailbreaking. This enables businesses to ensure that only compliant mobile devices have access to corporate assets when incorporated into an MDM (Mobile Device Management) solution.

5. Security For The Internet Of Things (IoT)

While the use of IoT devices certainly increases productivity, it also exposes businesses to new cyber threats. Threat actors look for insecure devices that are connected to the Internet by accident for nefarious purposes, such as opening a doorway into a company network or recruiting a new bot to join a global bot network.

These devices are protected by IoT security, which uses IPS as a virtual patch to prevent exploits against vulnerable IoT devices, auto-segmentation to control network activities, and discovery and classification of connected devices. Small agents can also be added to the device's firmware in some cases to stop exploits and runtime attacks.

6. Application Security

Threat actors target web applications and everything else directly connected to the Internet. OWASP has been tracking the top 10 threats to critical web application security flaws since 2007, including cross-site scripting, injection, broken authentication, and misconfiguration, to name a few.

The OWASP Top 10 attacks can be stopped with application security. Additionally, application security stops malicious interactions with applications and APIs and prevents bot attacks. Apps will remain secure even as DevOps releases new content with continuous learning[5].

7. Zero Trust

The traditional approach to security focuses on the perimeter, erecting walls like a castle around an organization's valuable assets. However, there are a few drawbacks to this strategy, such as the rapid dissolution of the network perimeter and the possibility of insider threats.

A new security strategy is required as corporate assets move off-premises as a result of cloud adoption and remote work. By combining micro-segmentation, monitoring, and the enforcement of role-based access controls, zero trust secures individual resources at the resource level.

Literature Survey

A "Security-aware optimization for ubiquitous computing systems with the SEAT graph approach"[2].

Security has emerged as a new design metric for ubiquitous computing systems, along with other metrics like performance and energy consumption. A security strategy for the application is a combination of selected cryptographic algorithms for the necessary security services [3]. In order to meet the real-time constraint while still achieving maximum overall security strength, we propose methods for the generation of security strategies in this paper. We propose a novel graph model known as the Security-Aware Task (SEAT) graph model to represent real-time constraints and precedence relationships between tasks in order to express an application's security requirements[3-4]. Integer Linear Programming Security Optimization (ILP-SOP), an optimal algorithm, is what we propose, and it is based on the SEAT graph approach. We propose two dynamic programming-based algorithms (DPSOP-path/tree) to generate the best security strategy for special structures like simple path graphs and trees. The accuracy and effectiveness of our suggested method are demonstrated by the results of the experiments. According to the findings of the experiments, the security strength can, on average, be increased by 444.3 percent by employing the strategies we propose. As local descriptors, it has the advantage of being highly efficient in addition to being fixed-size features, as we will see. After converting the image to the HSV system, the proposed method makes it possible to identify the destination [6]. The force field features will then be extracted using the fast algorithm, and the distance for three methods—Manhattan, Euclidean, and Cosine—will be used to classify the data. This will allow for a comparison to be made in order to choose the best resolution, as the accuracy of the two datasets—ORL and UFI—is 99.9%[8].

B "Attack Detection and Identification in Cyber-Physical Systems—Part I:

Models And Fundamental Limitations

Cyberphysical systems interact with humans and the physical world by combining physical, computational, and communication capabilities. Cyberphysical systems are susceptible to malicious attacks in addition to component failures. To ensure system security and dependability, specific analysis tools and monitoring mechanisms must be developed. An integrated framework for evaluating the cyber-physical systems' resistance to omniscient adversary attacks is presented in this paper. Cyberphysical systems and attacks are modeled as exogenous unknown inputs and linear descriptor systems, respectively. Our model includes and generalizes numerous typical attacks, including stealth, (dynamic) false-data injection, and replay attacks, despite its simplicity. It also captures various real-world cyber-physical systems. For the purpose of attack detection and identification, we first define the fundamental limitations of static, dynamic, and active monitors. Second, we provide constructive algebraic conditions for casting attacks that cannot be detected or identified. Thirdly, we describe graph-theoretic conditions for the existence of undetectable and unidentifiable attacks by utilizing the system interconnection structure. Finally, we use a variety of cyberphysical systems, including two electrical power grids and a municipal water supply network, to illustrate our findings[6].

Cyber Security Trends

Most of the time, the current trends in cybersecurity are the result of a combination of responses to major cyber threats, new technologies, and long-term security goals. Some of the most important technologies and trends that will shape cybersecurity in 2024 are as follows:

- **AI Security:** The development of AI has a significant impact on cybersecurity, both offensively and defensively. On the offensive, cyber threat actors have already used tools like ChatGPT to improve and streamline cyberattacks, which has led to a significant increase in attacks all over the place year over year.
- **Hybrid Mesh Firewall Platform:** Combining a variety of firewall types into a single, centralized security architecture, the hybrid mesh firewall platform is increasingly being adopted by businesses. While simultaneously ensuring centralized oversight, administration, and enforcement of policies across their entire infrastructure, this strategy enables organizations to implement firewall solutions tailored to specific environments[8].
- **CNAPP:** The term "Cloud-Native Application Protection Platform" (CNAPP) was created by Gartner to describe security solutions that combine the various capabilities necessary for cloud application security into a single product. Security teams are able to effectively

oversee, administer, and protect their cloud-based applications thanks to this integration of multiple features into a single dashboard and solution. This helps combat security sprawl in the cloud.

• **Hybrid Data Centers:** Some businesses have completely moved their data centers to the cloud, but others have used cloud computing to improve their on-premises data centers. Orchestration is used in a hybrid data center, which makes it possible for applications and data to move seamlessly over the network from on-premises infrastructure to cloud-based infrastructure as needed[5].

• **Comprehensive Protection:** Nowadays, businesses face a wider range of threats and attack vectors than ever before. Cyber threat actors are able to take advantage of weaknesses in IoT systems, mobile devices, traditional endpoints, and remote work infrastructure. Security teams are more likely to overlook the increased complexity of monitoring and securing a large number of systems, which could give attackers access to those systems.

Most of the time, the current trends in cybersecurity are the result of a combination of responses to major cyber threats, new technologies, and long-term security goals. Some of the most important technologies and trends that will shape cybersecurity in 2018 are as follows:

Malware

The term "malware" refers to any program or file designed to cause harm or disruption to a computer. This comprises:

Attacks by Ransom ware Ransom ware are a type of malware that encrypts the information of its victims and demands payment in exchange for the key that decrypts the data. Even if you pay the ransom, you might not be able to retrieve the encrypted data.

Malware that allows an attacker to take control of a victim's computer is known as a "remote-access Trojan." The attacker can then use the victim's webcam to spy on them, install additional software, and access the victim's files. Email attachments and infected websites frequently spread RATs[7].

Bootkits and rootkits Rootkits typically include a number of malicious payloads, such as keyloggers, RATs, and viruses, which enable attackers to gain remote access to the machines being targeted. Bootkits are a type of rootkit that can infect software that loads before the operating system, called start-up code.

Spyware is a type of malicious software that steals personal information and illegally monitors a user's computer activity.

Trojans are a type of malware that, when executed, performs malicious activity while posing as legitimate software[8].

Worms and viruses: A computer virus is a piece of malicious software that infects a computer without the user's permission. By attaching themselves to other computer files, viruses can replicate and spread to other computers. Worms are self-replicating, much like viruses. However, in order to do so, they do not need to join another program.

Security Models: Integrity, Confidentiality And Protection Of The Data

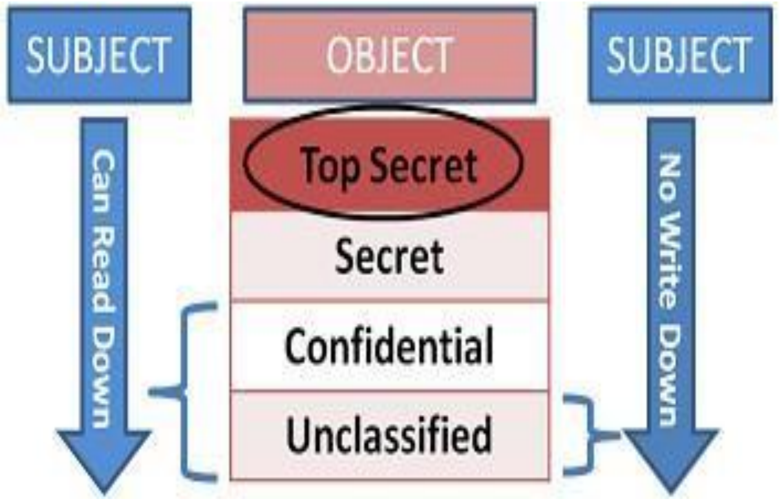
The rules and policies that govern data integrity, confidentiality, and protection are defined by five security models. The main focus and motivation for the implementation of the security models is confidentiality through information integrity and access controls. The primary security models I am addressing are Bell-LaPadula, Harrison–Ruzzo–Ullman, the Chinese Wall model, Biba, and Clark-Wilson. When designing security policies and systems, it is necessary to take these security models into account. They should "define the entities (subjects governed by an organization's security policy)" and "define the access rules necessary to instantiate said policy."[7]

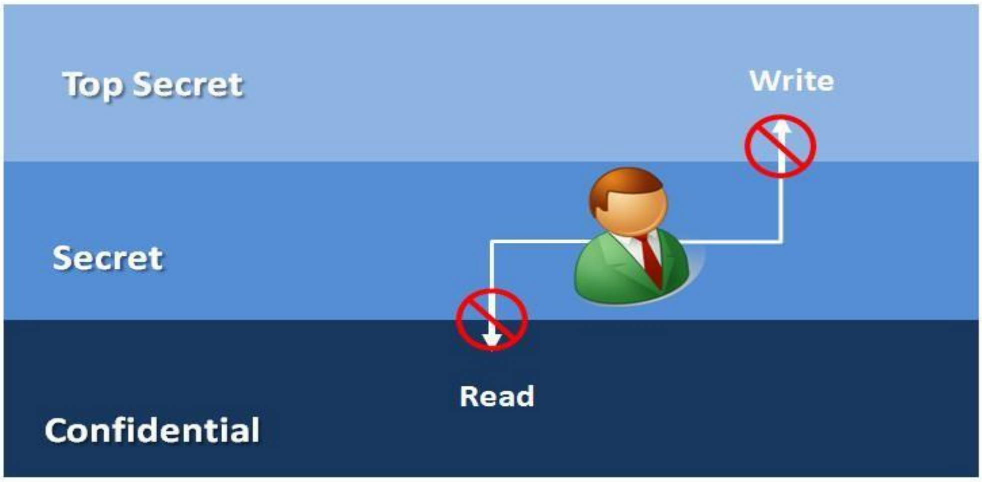
Let me briefly discuss each model and highlight some of its advantages and disadvantages.

Through three primary properties, Bell - La Padula addresses access control. These are discretional security-related ds-property. Ss-property, which focuses on simple security or no "read-down," and *-property, which focuses on no "write-down," are two examples. All of these characteristics should be present in a BLP-secured system. Honeywell Multics was the only genuine implementation of this security model, but it failed to gain traction. This SM has the advantage of preventing subjects from downgrading information and objects, as well as from changing security levels once they have been created[9].

However, one of the implementation-related issues or flaws of BLP is that users can never communicate with "low" users. The model only addresses confidentiality; access control and covert channels are not addressed. The fact that anyone can create an object with a higher classification is another flaw. The military is currently achieving these objectives through the use of discretionary access control and segregation rather than the BLP model, despite the fact that the initial purpose of the BLP model was to meet DOD requirements regarding information security[6].

The Biba Model is similar to Bell-LaPadula in that it emphasizes integrity rather than confidentiality. Reversing BLP's implementation is one approach. Because low integrity cannot be read by high integrity, there is no "read-down." Furthermore, subjects are unable to transfer low integrity data into high integrity environments, so there is no "write-up[10]."





Conclusions

Based on the review, it was discovered that the bulk of research has been done on vulnerabilities, firewalls, and email security. Although there are broad guidelines for password security, the system is not intrinsically protected by any authenticated protocol. Thus, additional research is required to guarantee password security in terms of techniques and models. A security policy is defined inside a framework known as a security model. This security policy was developed with a specific setting or policy instance in mind, such as an authentication-based security policy that was constructed inside the parameters of a security model. Five distinct methodologies have often been used to conduct threat modelling: asset-centric, attacker-centric, software-centric, value and stakeholder-centric, and hybrid. Security models provide a guideline for implementing security in organizations to guarantee data confidentiality for them and their clients. We shall go deeply into the security models and their different varieties in this essay.

References

[1]. CCDCOE. 2017. “Cyber Definitions,” Resources (available at https://ccdcoe.org/cyber-definitions.html; retrieved February 1, 2018)

[2] Abdulrahaman Okino Otuoze, Mohd Wazir Mustafa, Raja Masood Larik, Smart grids security challenges: Classification by sources of threats, Journal of Electrical Systems and Information Technology, Volume 5, Issue 3,2018,Pages 468-483,ISSN 2314-7172, https://doi.org/10.1016/j.jesit.2018.01.001.

[3].Roopak, M., Tian, G. Y., & Chambers, J. (2019). Deep learning models for cyber security in IoT networks. In 2019 IEEE 9th annual computing and communication workshop and conference (CCWC) (pp. 0452-0457). IEEE.

[4. D. Craigen, N. Diakun-Thibault, and R. Purse, ‘‘Defining cybersecurity,’’Technol. Innov. Manage. Rev., vol. 4, no. 10, pp. 13–21, Oct. 2014.

[5] Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees’ cybersecurity behavior. International Journal of Information Management, 45, 13-24.

[6]. Harel, Y. Gal, I.B., and Elovici, Y. 2017. Cyber security and the role of intelligent systems in addressing its challenges. ACM Trans. Intell.Syst.Technol. 8, 4, Article 49 (May 2017), doi: 10.1145/3057729.

[7]. Chen, Zhongqiang, Peter Wei, and Alex Delis. 2008. Catching remote administration trojans (RATs). Software: Practice and Experience, Volume 38, No.7. Pp. 667-703

[8]. Xin, Y. ; Kong, L. ; Liu, Z. ; Chen, Y. ; Li, Y. ; Zhu, H. ; Gao, M. ; Hou, H. ; Wang, C. Machine learning and deep learning methods for cybersecurity. IEEE Access 2018, 6, 35365–35381.

[9]. Bhamare, D., A., Jain, MSamaka A Erbad, 2016. survey on service function chaining,Journal of Network and Computer Applications, Volume 75, 2016,Pages 138-155, ISSN 1084-8045,https://doi.org/10.1016/j.jnca.2016.09.001.

[11]. HONG, G., ZHANG, L., YANG, M., YANG, Z., NAN, Y., ZHANG, Y., DUAN, H., YANG, S., ZHANG, Z., & QIAN, Z. (2018). How you get shot in the back: A systematical study about cryptojacking in the real world. Proceedings of the ACM Conference on Computer and Communications Security, 1701–1713. https://doi.org/10.1145/3243734.3243 840

[12]. Mahdavifar, S., &Ghorbani, A. A. (2019). Application of deep learning to cybersecurity: A survey. Neurocomputing, 347, 149-176.

[13]. Nasir, A., Arshah, R. A., Ab Hamid, M. R., &Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. Journal of Information Security and Applications, 44, 12-22.

[14]. Grammatikis, P. I. R., Sarigiannidis, P. G., &Moscholios, I. D. (2019). Securing the Internet of Things: Challenges, threats and solutions. Internet of Things, 5, 41-70.

[15]. Peng, C., Sun, H., Yang, M., & Wang, Y. L. (2019). A survey on security communication and control for smart grids under malicious cyber attacks. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(8), 1554-1569.