VIVA-TECH IJRI
ANNUAL RESEARCH JOURNAL
VIVA-TECH INTERNATIONAL JOURNAL FOR RESEARCH AND INNOVATION
ANNUAL RESEARCH JOURNAL
ISSN(ONLINE): 2581-7280

A review on the protocol systems for security enhancement of administrative devices

Yash Pandhare[1], Aditya Bawa[2], Pawan Pujari[3], Ashwini Save[4]
[1](Department of Computer Engineering, VIVA Institute of Technology, India)
[2](Department of Computer Engineering, VIVA Institute of Technology, India)
[3](Department of Computer Engineering, VIVA Institute of Technology, India)
[4](HOD, Department of Computer Engineering, VIVA Institute of Technology, India)

Abstract : *With the increased number of people on the internet, the extent of crimes committed has seen a drastic increase as a direct effect. Most enterprises enhance their security at the primary level by using some form of multi-factor authentication usually limited to Phone or Access card based MFA (Multi-Factor Authentication), although adequate in the past, as with the increasing attack vectors, and types of attacks. Nevertheless a system cannot be completely secure to all possible threats now or in the near future, these risks need to be minimized to the lowest extent possible. One method of minimizing this risk is Proper access control. Moreover, a thorough research on the existing systems shows that the systems used in enterprise solutions are still vulnerable to attacks due to the lack of factors. This paper shows the brief of the existing technology used to overcome the threats posed by the existence of administrative devices that have privileged access across a system.*

Keywords - *Cyber security, host security, multi-factor authentication, access control, enterprise security*

I. INTRODUCTION

Authentication is the Backbone of the Security and Integrity of a system, especially systems of significant importance, which are responsible for proper and safe interaction between the employees and the sensitive information traversing the network at any given, due to the constant movement for use of this data, it becomes highly crucial to protect this data, when at rest or in motion, this can be accomplished in part by only allowing authenticated users to interact with this system. Thus it becomes conspicuous that a host's security plays a pivotal role in enterprise security and a breach in a host's system can cause huge losses to an organization.

II. BACKGROUND

The premise of this review paper revolves around prevention of threats posed to the Admin systems at larger corporate level environments. These threats can cause the complete decimation the systems and subsystems of servers and which can lead to financial collapse and more over in severe cases a possible loss of life, in cases where, these attacks target Hospital systems and Health Care infrastructure on the whole Administrative Systems require a large amount of protection against tamper, as they change the very behavior and all shared data that, is being used, as most systems environments use Active Directory which may allow the attacker to compromise the entire system if an initial foothold is gained, thus it should be top priority to be further protected by the using multi factor authentication, but the currently available technologies only usually offer 2 factors for authentication those being through the Password and an Application or by using SMS features, although other factors are available, these factors are not properly integrated into a singular application.

III. REVIEW OF LITERATURE

To simplify the process of the review of literature, the review has been split into three distinct categories, refining and systematizing the topic at hand and to better understand the advantages and shortcomings of the technology being currently used and in implementation, these categories are:

1 Multi Factor Authentication
2 Network Security
3 Steganography

1 MULTI FACTOR AUTHENTICATION

Multi Factor authentication is in the practice of spreading out the authentication over multiple factors, these factors are normally limited to two, i.e Passwords and Mobile authenticator apps, this means that the both these factors are only governed by either remembering or by possession, which leads it to be vulnerable to threats that are more perverse as compared normal threats.

Sanjar Ibrokhimov et al. [1] proposed the future scope of Authentication methods that would be applicable to business machines and other devices such as services provided on the cloud, in this paper the authors have listed 4 possible methods that Multi Factor Authentication can be improved upon. Their first method uses a Fingerprint based and user-specific random word projection. Their second method focuses mostly on Threshold cryptography using Shamir's Secret algorithm. The Third proposal is based on Cloud based systems. Shengyu Yang et al. [2] delves deep into the use of SMS based verification code generation, to transfer over GSM networks so as to secure the code while on the wire against any possible tampering or manipulation by a third party. This paper further defines an algorithm which is used to send these SMSes and Includes an explanation of the Random code generator used to create these codes, in great depth while their constituting function allows them to create around 95 unique numbers, each 6-digit long for their verification apparatus, they also discuss, the possible use of Smart cards and other owned devices to further improve security. Linjiang Xie et al. [3] explains a system based upon Multifactor authentication, using a technique that is truly unique to the system that is used authenticate systems, usually based around mobile devices using their Gravitational sensors are fields of input to a pre decided password that can be entered by orienting the device in a certain way and hold it there, to what the authors have concluded of being around 1.5 secs per letter and 5 secs of space between two consequent letters.

Shahriar Rahman Fahim et al. [4] have tackled mostly the issue of sensitive documentation and it's transport as well as physical access of these said Documents. This is mostly done through a 3 Factor Authentication model which is run using a base station, the factors of authentication are as follows: 1. Global Positioning System (GPS), 2. Biometric Scanning and 3. Authenticity method based on location.Wiphop Pomak et al. [5] mainly focuses on the Authentication of devices in an Enterprise setting where the culture of BYOD(Bring Your Own Device) is very prevalent and the fact that these personally owned devices and also be vulnerable, Multifactor security is required here. The authors of this paper go in depth about the risks around bringing your own device operations and suggest two methods of MFA, These are : 'Authentication using WLAN and Hybrid cryptosystem' and 'Authentication using NFC'.Bandar Omar ALSaleem et al. [6] discuss methods involving Multi-Factor Authentication to Systems Login, a feature that is available as an add-on. The main disadvantage of knowledge-based mode is that it is susceptible to guessing, dictionary attacks, keyloggers, shoulder surfing, social engineering, and screening capture. As a result, multi-factor authentication may be the best option. It also protects the user against dangerous programmes that contain Trojan or Malware, as these bad programmes capture whatever the user types on the keyboard as well as the user's screen. Abhishek K Roshan et al. [12] explains how an authentication system determines how a user is identified and verified by the computer. Verification of the user's identity is the main goal behind an authentication system, that is the user is actually who they say they are. The degree of authentication increases exponentially when there is an increase in the number of factors in the verification process.Asim Balarabe Yazid et al. [7] proposes a multi-factor authentication algorithm which makes use of QR code, GPS, and Facial recognition. Authentication identifies the object based on who that person is by using biometrics such as fingerprint, facial recognition and retina scan. Identity based authentication is very difficult.

2 NETWORK SECURITY

A lot of these attacks are targeted towards various organizations with an eclecticism of motives ranging all the way from causing annoyance to taking down an entire enterprise. The latter being more menacing. Considering the amount of damage that could've been prevented by implementing simple measures at the rudimentary level, it wouldn't be a daunting task for enterprises to strengthen their systems. Xiao-Si Wang et al [8] explains that tech giants and large enterprises or even small startups outsource their security needs to a third party service provider in general. This might weaken the system with more vulnerabilities. Even Though various MSS service users do not want to share data among themselves because of various reasons, citing various

confidentiality concerns, even when they are using the same MSS platform.Thus, before suggesting or proposing any such mechanism this issue must be considered. In this paper, the authors have proposed a new architecture that is use case driven to private, confidential and secure data sharing among various customers under the same MSS platform. Yue Guo et al [9] explains as information technology slowly penetrates into people's daily lives, the application range of computer networks has become wider and wider, becoming one of the indispensable communication methods for people. The popularization of computer networks in the information age has brought great convenience to people on the one hand, but also has major hidden dangers that damage public privacy and safety. Enterprises must not only rely on computer networks and databases to share data, but also protect sensitive and valuable data from being stolen or tampered with.

Yifan Liu [13] proposes Software-Defined Networking as a trending domain for future network development that implements the different layers of control and data planes respectively. The "three-layer two-inferface" provides a high degree of openness and easy programmability, changes the traditional network and increases nodes in the network, thus resulting in new security issues. The background, architecture and working process of SDN is discussed in the first part. Secondly, and recapitulate the security issues that are likely to arise from: application control and data layers, and northbound and southbound interfaces. The latest research progress along with its analysis is carried out, mainly including: authorized authentication module, application sandboxing, defense against DoS attacks, multi-controller deployment and flow rule consistency detection.

3 STEGANOGRAPHIC MODELS

Image steganography is performed for images and the data is also decrypted to retrieve the message image. Since this can be done in several ways, image steganography is studied and one of the methods is used to demonstrate it. Image steganography refers to hiding information i.e. text, images or audio files in another image or video file. Arnold Gabriel Benedict et al. [11] discussed an innovative strategy for slicing the secret data and storing it on numerous cover pictures is proposed in this paper. The extraction of this secret data from the destination side's cover images has also been addressed. Data slicing ensures secure delivery of sensitive information, making it nearly hard for an intruder to decipher the data without knowing the encryption keys.

With the dependency on the internet and smart gadgets, security of data has become a major concern in today's time. Steganography is a technique for enhancing data security by encrypting the message behind a cover, which can be a text, image, or audio/video. Images are the most preferred medium to apply steganography as it contains large amounts of redundant data. Dipti Watni and Sonal Chawla [10] discussed Jpeg steganography as a good option, as jpeg images can act as an innocuous cover to hide the data because of their popularity. To apply jpeg steganography, three important parameters of image steganography i.e. embedding capacity, robustness and Undetectability are considered.

IV. ANALYSIS

Table 1 represents, a representational view of the Techniques, Advantages and Limitation of each paper, thus further simplifying the review process and providing clear descriptions of Different types of Authentication methods while also providing the disadvantages that come with said methods, this providing a more holistic view of these systems, as implemented an in action, this inturn makes the study more realistic as they also account for easy of usability and the inherent safety of the data being shared as a factor of authentication

Table 2 [9] provides a much required quantification of the effect of various techniques and their subsequent effects on the overall security of a system, represented in terms of factors.

TABLE 1
ANALYSIS TABLE

Sr No	Title	Techniques	Advantages	Limitations
1	Multi-Factor Authentication in Cyber Physical Systems: A State of Art Survey	Biometric, Smart cards and Cryptography	Biometric capability provides ease of use	Biometric capabilities carry inherent risk

2	Research on Multi-factor Bidirectional Dynamic Identification Based on SMS	SMS based authentication, with random code generation	SMS based approach makes it efficient with location based logins	SMS efficiency comes with the cost of adding an additional point of possible failure
3	G-Key: An Authentication Technique for Mobile Devices Based on Gravity Sensors	Gravitational Sensors using Mobile Device	Gravitational sensors are a unique method	Gravitational sensors mean that the learning curve is steep
4	Development of a Remote Tracking Security Box with Multi-Factor Authentication System with a Biometric Sensor.	GPS Location authentication, Biometric authentication and Simple passwords	GPS Location as a factor of authentication can be really useful	GPS Location sensing can be inaccurate and Biometric sensing can be inherently risky
5	Enterprise WiFi Hotspot Authentication with Hybrid Encryption on NFC- Enabled Smartphones	Authentication using WLAN and Hybrid cryptosystem and Authentication using NFC	WLAN and Cryptosystem with NFC can be of great use to secure system	WLAN can be spoofed if not configured properly
6	Multi-Factor Authentication to Systems Login	Python, SQLite, simple passwords and biometrics	It might overcome security threats, such as key-loggers, screen capture attacks or shoulder surfing	Efficiency of the 2nd factor might be a possible failure
7	Enabling Cyber Security Data Sharing for Large-scale Enterprises Using Managed Security Services	Third party security services, privatized data security liabilities	Alleviates the resources spent by the enterprise	Outsourcing adds a vulnerability as the security is dependent on the service provider
8	Improved File Security System Using Multiple Image Steganography	File security, Batch Steganography	Implementation of steganography on multiple image files using encoding and decoding	Improvement in the image hashing technique can be followed
9	Research on Enterprise Computer Network Security Protection Technology Based on Information Technology	Enterprise security types;physical security and network security methods.	Compares the degree of security achieved from the following methods: Physical security, Cyber security technologies and host security	Host security was lacking the amount of security with catastrophic consequences.
10	A Comprehensive Study on Multi Factor Authentication Schemes	Ownership Factor, OTP, Biometrics, RSA SecurID	Compares and evaluates types and stages of authentication.	The described fourth factor of authentication was vague.

In a survey conducted considering pertinent data about computer attack behaviour [9] , the authors performed weighted correlation and calculated the risk value for each system. The results are shown in Table 2.

TABLE 2 [9]

Information System	Physical Security	Cyber Security Technology	Host Security
Surveillance System	1.00	0.85	0.95

Office System	1.00	0.97	1.00
Access Control System	1.00	0.93	0.82

Thus it from the review of the previous literature it becomes abundantly clear that host's security plays a crucial in enterprise security, furthermore it also quantifies that Multi-Factor authentication is a very reliable method, owing to its flexibility and the low amount of flaw only brought along by the quality or quantity of the Factors used, which depend on how the specific deployments are created and administered.

V. CONCLUSION

In this paper it is conspicuous that, although more number of factors might be redundant for systems that are used at home or as consumer systems, It is evident that the systems used in enterprise solutions are still vulnerable to attacks due to the lack to factors, the limitation of current technologies identified here is the lack of including more than two factors, and only focusing on Authentication of users while, there are is a lack of focus on Machine authentication and inclusion and implementation of the factors that relate to the time of access and hardware authentication.

In the past decades, cyberattacks have advanced and evolved rapidly due to technical advancement. But yet, most organizations have not grown with time and are still using old cyber security measures. This paper discussed the existing Multi-factor Authentication techniques, Computer Network Security techniques, and Steganographic techniques, and their use in preventing cyber attacks. Although these might be adequate in containing the preliminary attacks, advancements need to be made in order to secure the modern-day systems.

VI. REFERENCES

Proceedings Papers:

[1] Sanjar Ibrokhimov, Kueh Lee Hui, Ahmed Abdulhakim Al-Absi, Hoon Jae Lee and Mangal Sain Multi-Factor Authentication in Cyber Physical System: A State of Art Survey, *21st International Conference on Advanced Communication Technology (ICACT) 17-20 Feb. 2019, PyeongChang, Korea (South), DOI 10.23919/ICACT.2019.8701960*

[2] Shengju Yang, Jie Meng Research on Multi-factor Bidirectional Dynamic Identification Based on SMS, *IEEE's 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), 12-14 Oct. 2018, Chongqing, China, DOI 10.1109/IAEAC.2018.8577505*

[3] Linjiang Xie, Hequn Xian, Xuyue Tang, Wei Guo, Feilu Hang, Ning Fang G-Key: An Authentication Technique for Mobile Devices Based on Gravity Sensors, *IEEE's International Conference on Power Data Science (ICPDS) 22-24 Nov. 2019, Taizhou, China, DOI 10.1109/ICPDS47662.2019.9017188*

[4] Shahriar Rahman Fahim, Saquib Shahriar, Omar Kamrul Islam, Md. Ilias Rahman, Subrata K. Sarker, Shahela Akter, Development of a Remote Tracking Security Box with Multi-Factor Authentication System Incorporates with a Biometric Sensing Device, *5th IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE) 15-16 Nov. 2019, Bangalore, India, DOI 10.1109/WIECON-ECE48653.2019.9019973*

[5] Wiphop Pomak, Yachai Limpiyakom, Enterprise WiFi Hotspot Authentication with Hybrid Encryption on NFC- Enabled Smartphones, *8th International Conference on Electronics Information and Emergency Communication (ICEIEC) 15-17 June 2018, Beijing, China, DOI 10.1109/ICEIEC.2018.8473476*

[6] Bandar Omar ALSaleem; Abdullah I. Alshoshan, Multi-Factor Authentication to Systems Login, *2021 National Computing Colleges Conference (NCCC), 27-28 March 2021, Taif, Saudi Arabia, DOI 10.1109/NCCC49330.2021.9428806*

[7] Asim Balarabe Yazid; Moussa Mahamat Boukar; Salisu Yusuf Ibrahim; Isa Muslu, Four-Factors Authentication Algorithm For Preventing Fake Attendance, *2019 15th International Conference on Electronics, Computer and Computation (ICECCO) 10-12 Dec. 2019, Abuja, Nigeria DOI: 10.1109/ICECCO48375.2019.9043287*

[8] Xiao-Si Wang; Ian Herwono; Francesco Di Cerbo; Paul Kearney; Mark Shackleton, Enabling Cyber Security Data Sharing for Large-scale Enterprises Using Managed Security Services, *2018 IEEE Conference on Communications and Network Security (CNS), 30 May-1 June 2018, Beijing, China, DOI 10.1109/CNS.2018.8433212*

[9] Yue Guo; Jie Xu; Hui Yuan; Yan Zhuang; Guowei Zhu; Yintie Zhang, Research on Enterprise Computer Network Security Protection Technology Based on Information Technology, *2020 IEEE 3rd International Conference on Automation, Electronics and Electrical Engineering (AUTEEE) 20-22 Nov. 2020, Shenyang, China, DOI 10.1109/AUTEEE50969.2020.9315704*

[10] Dipti Watni; Sonal Chawla, A Comparative Evaluation of Jpeg Steganography, *2019 5th International Conference on Signal Processing, Computing and Control (ISPCC), 10-12 Oct. 2019, Solan, India, DOI 10.1109/ISPCC48220.2019.8988383*

[11] Arnold Gabriel Benedict, Improved File Security System Using Multiple Image Steganography, *2019 International Conference on Data Science and Communication (IconDSC), 1-2 March 2019, Bangalore, India, DOI 10.1109/IconDSC.2019.8816946*

[12] F. Jaafar, G. Nicolescu and C. Richard, ”A Systematic Approach for Privilege Escalation Prevention,” *2016 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), 2016, pp. 101-108, doi: 10.1109/QRS-C.2016.17.*

[13] A. Zaytsev, A. Malyuk and N. Miloslavskaya, "Critical Analysis in the Research Area of Insider Threats," *2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud), 2017, pp. 288-296, doi: 10.1109/FiCloud.2017.16.*

Journal Papers:

[14] Abhishek K., Roshan S., Kumar P., Ranjan R. (2013) A Comprehensive Study on Multi Factor Authentication Schemes. In: Meghanathan N., Nagamalai D., Chaki N. (eds) *Advances in Computing and Information Technology. Advances in Intelligent Systems and Computing, vol 177. Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-642-31552-7_57*

[15] Yifan Liu; Bo Zhao; Pengyuan Zhao; Peiru Fan; Hui Liu, A survey: Typical security issues of software-defined networking China Communications *(Volume: 16, Issue: 7, July 2019), Page(s): 13 - 31, 19 July 2019, DOI: 10.23919/JCC.2019.07.002*