JES
Journal of Engineering Sciences

Vol 13, Issue 05, May /2022

ISSN NO:0377-9254

SECURITY MODEL BASED ON NETWORK BUSINESS SECURITY

[1]Boda Sindhuja, [2]S. Bhanu Prakash Raju, [3]S. John Kennedy, [4]G. Karthik, [5]A. Anil Kumar, [6]D. Venkata Sai

[1,2,3,4,5,6] Dept of CSE, Gokaraju Rangaraju Institute of Engineering & Technology, Hyderabad, Telangana 500090

*Corresponding Author: sindhuboda777@gmail.com

Abstract:

As well as serving as a platform for information sharing and exchanging, the Enterprise Network Information System serves as a platform for both the Enterprise Production Automation and Management Systems to work as a single system. Enterprise Network Information System security includes not only network and data security, but also network business security, such as confidentiality, integrity, continuity, and real-time availability of network business, which are all aspects of network security. Network business security is proposed in this study based on Enterprise Network Information System security. There are three components to the topic of information security in this paper: the definition of data security, network system security, and network business security, as well as a description of the network business security model. An enterprise's automated production system and its management information system can both benefit from theoretical groundwork laid out in the concept of "network business security."

I. introduction:

The convenience of computers and networks has led to a rise in security concerns, which are becoming more and more significant. As computer applications have grown in popularity and network technology has advanced at a rapid pace, a growing number of security threats have emerged, making the issue of information security one that must be addressed immediately. After the defences of the sea, land, air, and space, network information security has risen to the position of number five. An enormous amount of theoretical and technical study on information security has been conducted in recent years. Data

and network security are two of the most important aspects of information security today [1]. According to the security theory based on data (information) protection in a network context, [6] information security has been built. Using the theory of cryptography, data security studies the secrecy, integrity and availability of data. The BLP [7] model, the Biba [8] model, and the PDR [9] model are three of the most important models for guiding the security defence process when it comes to data confidentiality, integrity, and availability. Security protocol, security mechanisms, and security services [10] are the three pillars of Open Systems Internet Security Architecture (OSIA), which aims to provide a theoretical foundation for creating a safe network system. Figure 1 illustrates the current theoretical framework for information security. A public information network, such as the Internet, Chinanet, and Cernet, can facilitate the exchange of information and facilitate the sharing of information, while an enterprise information network, such as the Electric Power Data Network (SPDnet) and the Electric Power Integrated Data Network (SPInet), can facilitate information sharing and exchange. Sharing and exchanging data is what the information system on the public information network is all about. As a result, it places an emphasis on safeguarding network and data security. As a platform for information exchange and information sharing, the Enterprise Network Information System is also a platform for the Enterprise Production Automation and Management Systems to function together in tandem. Consequently, enterprise network information system (ENIS) security defences encompass data security, as well as protecting the networks that host the businesses that use those networks. This paper's "network business security" concept is based on the preceding analysis and the security defence of Enterprise Network Information System. Data security, network system security, and network business security are defined in this study as three distinct aspects of information security. Enterprise Network Information System security can be protected by the theoretical foundation provided by the notion of "network business security."

In the computer network, big data has been widely exploited, which has disrupted the traditional models of numerous businesses and created a new socio-economic development model [1]. People's lives have been greatly enriched as a result of big data, which has made computer network technology an increasingly important part of society, economy, and daily life. Despite this, there is a flaw in the network: because of the network's high degree of openness, a

large volume of virus-infected data is spread throughout it at random [2]. Computer network security is currently under attack from a variety of sources, not just the usual suspects such network viruses, hacker attacks, and weak network systems. Big data and cloud computing have created a slew of new dangers that are continually changing. As a result, computer network security technology is becoming increasingly important. For the sake of long-term computer network security, the research content will conduct a detailed analysis of computer network security and propose specific strategies to prevent and control it [3].

The global economy relies heavily on the building industry. In 1996, construction volume in the United States exceeded $500 billion, with more than a million construction companies engaged in the industry (U.S. Bureau of the Census 1997). But unlike other manufacturing businesses, such as automobiles or personal computers, the construction industry is often focused on producing a singular and unique final product, rather than mass-producing vast numbers of units. The word "project format" refers to the way in which these projects are accomplished (Halpin and Woodhead 1998). The management of resources within the scope of the project is the primary concern in this structure. Despite the importance of project management in the construction industry, strategic management is often overlooked. Strategic management focuses on the issues of running a construction company rather than a single project in this context. However, because of the emphasis on project management needs, strategic management is given far less consideration. In particular, there are considerably less options in existing literature and research papers for construction professionals to learn about strategic management (Goodman 1998). Research was conducted to analyse strategic management techniques in the construction sector and to identify strategic areas that should be given more attention by the industry as a whole.

Rapid development and widespread use of information technology has led to an ever-increasing reliance on information systems in national economies, military affairs, and social development. However, there will be a slew of security issues. If the information systems are breached by threats from the outside or within the network, the state, organisations, or individuals will suffer enormous losses[3]. Information system security problems can be avoided if appropriate risk assessment and active defence security threats are implemented[4]. Information security is a multi-faceted endeavour that requires

expertise in a variety of fields. [5,6] In general terms, the theory and technology of information security are concerned with the security of information in terms of confidentiality, integrity, availability, authenticity, and controllability. Natural disasters, accidents, computer crime, human error, such as improper use and poor safety awareness, hacker behaviour, external leaks, internal leaks, data loss, electronic espionage, such as information flow analysis, information theft, and so on are the main sources of information security threats. Network protocol flaws like the TCP/IP protocol security issue[7] are also included. One of the first things an organisation should know about an intruder's attack strategy is what kind of data they're after[8]. Regardless of the attack method, the intruders employ the four security characteristics as a means to their end aim. Information integrity, availability, and controllability are all significant aspects of information security, but confidentiality is the most critical. Information security, from a technological standpoint, means that the data does not objectively satisfy security risks. The assessment of information security risks is the topic of this article. You will learn about how information security risk assessment has evolved on a national and worldwide scale, as well as a general review of the many methods used to conduct such assessments. It outlines the overall procedure for assessing information security risks. The proposed risk assessment technique is based on the Analytic Hierarchy Process[9,10]. We may determine the current state of the system's security through an information security risk assessment, and from there, we can take the necessary steps to lower the system's risk to an acceptable level.

Information security policies, standards, and practises are the first step in developing an information security programme. After that, the blueprint for future success will be created through the selection or creation of an information security architecture and the development and use of a complete information security blueprint. – With the help of the company's information security policy, the blueprint for the organization's information security initiatives can be realised.– With no policies, plans, or planning, the business cannot meet the information security needs of its numerous stakeholders. – In order to manage resource allocation and prepare for business environment risks, businesses should at the very least engage in some form of planning.

II.literature survey:

Behrouz A. Forouzan, Tata McGraw-Hill," INFORMATION AND NETWORK SECURITY"

Understand the duties and role of management in the formulation, maintenance, and enforcement of information security policy, standards, practises, procedures, and guidelines. It is important to be aware of how the organization's overall information security policy differs from individual policy needs and objectives. In order to better understand an information security plan, familiarise yourself with its components. Know how education, training, and awareness initiatives help a company establish its standards, rules, and procedures. • Take a look at what a feasible information security architecture is and how it is employed. What is contingency planning and how does it relate to incident response planning, disaster recovery planning and business continuity plans?

Zhu Guohua JIANGHAN UNIVERSITYWuhanHubei,"
Enterprise Information Security Risk and Countermeasure Research under Network Environment"

Increasing expectations for information security have made network and information security a critical issue to resolve. Information security risk assessment system based on the Analytic Hierarchy Process (AHP) is offered based on actual demands. It is possible to determine the system's security level by performing a risk assessment of the system's information security. Lastly, a company's risk assessment is used to test the validity of the suggested scheme and the results reveal that the scheme is effective.

Paul S. Chinowsky1 , Associate Member and James E. Meredith2" STRATEGIC MANAGEMENT IN CONSTRUCTION"

The capacity to plan and execute projects is highly valued in the construction industry's conventional management philosophy, which can be found in both academia and industry. The building business, on the other hand, hasn't given strategic management the same focus. These broad contexts make strategic management important for construction companies even though project performance can conceal these areas from time to time because of their importance to the construction industry. Social and technical changes are generating a professional environment that will be vastly different in the future decades from what is currently being experienced by businesses. Construction companies' strategic management techniques are examined in this article. To compete in today's global economy, firms need to focus on strategic management and the areas they need to address. A summary of an industry survey and the background research that

motivated the exploration of these themes are given.

Guoyu Luo1, *"Research on Computer Network Security Problems and Protective Measures under the Background of Big Data"

Because of the massive amounts of data generated on a daily basis in the age of information, we now live in the era of big data. People's daily lives are increasingly reliant on computer networks. Networks and information systems are critical building blocks in the development of social infrastructure and economic progress. In the event of a network attack that fails due to a malicious attack, the public interest and the national economy will be protected. In order to secure the controllability of core technical equipment and the establishment of a national network security system, cyberattacks must be studied and strengthened. Big data, network security models, and intrusion detection frameworks are examined in this article, which then examines the present state of computer network security. In order to keep computer users from experiencing significant losses, protective measures are put in place to decrease the number of security issues that may arise as a result.

III. methodology:

The Enterprise Information Network is not only a means of disseminating and exchanging information, but also a means of conducting a company's business and working together. As a result, EIN security is not just about protecting data on the network, but also about protecting the security of businesses that operate on it. The current philosophy of information security is centred on the protection of data and the protection of networks. Security theory and model centred on data protection may be at odds with actual security defensive requirements in particular enterprise application environments. Dispatching Automation System security is a critical responsibility in power energy enterprise information security defence applications (which is in the highest security level). It's also necessary to get real-time data from dispatching data networks to meet production command and management requirements in a power electrical organisation. Because data is transmitted from a high-security network to a low-security network, the secrecy principle of BLP is violated. There are two separate defence objects in the dispatching data network, one of which is the business of Dispatching Automation System, and the other is data. The current notion of network security does not distinguish between corporate data on networks and personal information on networks. Enterprise

Information Systems now rely heavily on network business security as a key component. This study offers a security concept based on network business security and provides a theoretical explanation of it, considering network business as the defensive target. The Enterprise Information Network's network business security defence is built on network security and data security, which primarily protects network business. Network businesses of varying security levels will be held to the same set of confidentiality and integrity requirements as a result of this initiative. Figure 2 depicts a brand-new mechanism for protecting sensitive data. As part of the definition of information security, defence objects include data protection, network protection, and network business protection. Information security is the study of how to protect computer network information systems, including hardware, software, and data; how to prevent accidental or malicious destruction; and how to ensure that the content of network information cannot be disclosed, network services cannot be interrupted, and network business can run continuously and reliably. Security of data, the network, and the business network are now the three main focuses of the new definition.

The Enterprise Information Network's network business security defence is based on establishing a security concept based on network business security. Network security and confidentiality and integrity limitations between networks of differing security levels are the primary objectives. As a result of this, this paper will provide a formal definition of the network business and network business security model.

A. The Network Business Security Model:

This paper's definitions of network business and network business security lead us to the conclusion that networks, data, and process operation sequence sets make up network business. The security of network process sets and data sets, more specifically, the security of network processes operating and writing operations on data sets, is the security of the network business security. The following is a description of the network security model based on the information provided above about network business and network business security:

Here's a breakdown of the model:

a) Process Set: P=p0,p1,p2,,pn On the Enterprise Information Network, piP is a running process. b) Data Set: D=d0,d1,d2,,dm. dm is not included. djD is the data that is processed when someone has access to it. access set f = f0, f1,..., fn. fi = f, fi = fF (p,d). f(p,d) is the model of a

process's access to data d, as defined by p. There are several possible components to the access matrix A, which is made up of the access set F as a whole.

- r— process p can read data d.
- w—process p can write data d
- r/w—process p can not only read data d but also write data d.
- ϕ—process p can neither read data d nor write data d.

d) S=G(P+) is the process sequence set. It's important to remember that H+ denotes the set's subset for every set H. G(P+) stands for a well-ordered series of actions. It is possible to express a G(P+) in terms of G(P1 + P2 +,Pk +) as G(P+). G(P+) reveals the logical order in which a business's operations should be performed. e) Business Set: B=› (P+ ,D+ ,F+ ,S). A business is made up of all the processes and data necessary to complete the business, as well as the properties that allow processes to access data and the sequential order in which these activities occur. The entire network application system that the model defends is made up of all enterprises.

Constraints on the model:

The following properties of network business and network business security are abstracted in this study based on the previous description: No need for a defence of data's reading operation. x Property 1: Defending data is only necessary for the defence of data's writing action. x Property 2: The order in which network businesses need processes to be completed must not be tampered with. Using these two characteristics, we can describe the model constraint as follows:

Property 1: The access class for process p is defined as pclass(p), and the access class for data d is defined as dclass(d). To put it another way, you can only write data d if the access class of the data you're working with is higher than the access class you've got. Formula for securing a network:

$$\text{For all } p \in P,\ d \in D \quad \text{if } w \in f(p,d) \text{ then } pclass(p) >= dclass(d) \qquad (1)$$

No matter whether business enterprise you're running, the order in which procedures are completed must remain the same. Security comes down to this:

$$\text{For all } b \in B \quad S=G(P^+)=(P_1^+,\ P_2^+,\cdots,P_k^+) \qquad (2)$$

3) Security Status is defined as:

The f(p,d) and G(P+) constraints are met for each business, hence we believe the business is safe. The application system in the network is safe if all of the businesses in the network system are safe.

B. Network Business Security Analysis

An important part of the concept of network business security has been accomplished in the model above, which is to construct network business security defences. The

following two aspects are the foundation of the model that may guarantee network business security: x "The safe beginning state" ensures the safety and credibility of all processes in Process Set P. In concrete terms, we gather as much information about safe processes as possible in a secure and closed environment in order to create the "Credible Network Process List." A process can only run if it is listed in the list of registered processes. Mandatory Running Control technology has solved the problem of maintaining "Credible Network Process List" and intercepting illegitimate processes by "Credible Network Process List." x According to the specifics of the Enterprise Information Network, a network security model has been presented that distinguishes between the defence of reading and writing data. Despite the fact that the model does not specifically stipulate that data content be protected, the data confidentiality attribute has been defended according to business requirements. As a result, the model only includes explicit restrictions on data writing operations. Another significant aspect of the security concept based on network business security is the confidentiality and integrity limitations between networks businesses that have various security levels.

The Enterprise Information System can be separated into distinct business areas based on the importance and reliability of the business running on the network. Enterprise management and production command need the conveyance of data at multiple levels, all of which must adhere to strict security standards. It will be addressed in future study.

v. results:

V. conclusion:

As a result of in-depth research into the current state of the Enterprise Information System network security defence, this paper proposes the concept of "network business security," dividing the protection object of information security into three distinct categories: data privacy and security, and network and business continuity. Using a new information security model, the problem of Enterprise Information Systems can be explained by focusing on network business security. This paper focuses on the definition of network business security and provides a formal explanation of the network business security model, which serves as a theoretical foundation for the creation and design of Enterprise Information Systems.

References:

[1] YuNing Wang. Current Situation and Defense of Network Information Security[J]. Modern Commerce Industry , 2008

[2] DongHui Jiang. Security Offense and Defense Testing and Analysis of LAN[J]. Science&Technology Information, 2009

[3] XingHua Chen. Enterprise Network Information Security and Countermeasure Study[J]. Agriculture Network Information ,2009

[4] Chi Hu. Strategy Choice of Enterprise Information Construction.[J]. China Science&Technology Investment,2009

[5] YuanFei Huang, LiYong Ji, LiPing Jin. Investigation of Network Information Security Situation and Hot Issues[J]. Telecommunications Science, 2009

[6] Chao Li. Simple Exploration of Network Information Security[J]. Scientific&Technological Information Development and Economic, 2009

[7] D.E.Bell, L.LaPaDula. Secure Computer Systems: Mathematical Foundations and Model[J]. Technical Report M74244, Mitre Corp. , Bedford, MA, May 1973.

[8] K. J. Biba. Integrity Consideration for Secure Computer Systems[J]. Technical Report ESD-TR-76-372,Mitre Corp. , Bedford, MA, April 1979.

[9] Winn Schwartau. Time-Based Security Explained: Provable Security Models and Formulas for the Practitioner and

Vendor[J]. Computer&Security, USA, 1998:693~714.

[10] HongSheng Yan, XueLi Wang, Jun Yang. Computer Network Security and Defense[M]. Beijing: Electronics Industry Press,2007

[11] R.Sandhu,V.Bhamidipati,E.Coyne. The ARBAC97 Model for Role-Based Administration of Roles: Preliminary Description and Outline. In Proceedings of Second ACM Workshop on Role-Based Access Control, Fairfax, Virginia, 1997:41~49.

[12] GuangQiong Wang. Comprehensive Study of Access Control Based on GFAC[J]. Journal of AnQing Teachers College,2004