Global Journal of Computer Science and Technology: G Interdisciplinary
Volume 19 Issue 3 Version 1.0 Year 2019
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

An Approach to a New Network Security Architecture of Nuclear and Research Facilities

By A.B. Ramadan & M. Hefnawi

Abstract- With the growth of information technology (IT) systems, network security is rapidly becoming a critical business concern. Due to the interconnectivity of IT systems, a comprehensive description of all of the key elements and relationships that make up an organization's network security is needed, which can be referred as network security architecture. The value of this architecture is often questioned by organizations in terms of its practical application. This paper has presents a new approach to the network security architecture by using the Zachman Framework capabilities. The network security architecture of nuclear and academic facilities academic centers is discussed to show how a conceptual model can be applied to a real organization. This new approach makes any Local Area Network LAN more secure and more flexible than any conventional security procedures without affecting the performance of the LAN. Applying Zachman matrix provides the answers to what data assets the nuclear and research facilities controls, how they are used, and where they are located.

Keywords: computer network, LAN's security, zachaman, information technology (IT), Information systems architecture (ISA).

GJCST-G Classification: C.2.0

Strictly as per the compliance and regulations of:

An Approach to a New Network Security Architecture of Nuclear and Research Facilities

A.B. Ramadan[α] & M. Hefnawi[σ]

Abstract- With the growth of information technology (IT) systems, network security is rapidly becoming a critical business concern. Due to the interconnectivity of IT systems, a comprehensive description of all of the key elements and relationships that make up an organization's network security is needed, which can be referred as network security architecture. The value of this architecture is often questioned by organizations in terms of its practical application. This paper has presents a new approach to the network security architecture by using the Zachman Framework capabilities. The network security architecture of nuclear and academic facilities academic centers is discussed to show how a conceptual model can be applied to a real organization. This new approach makes any Local Area Network LAN more secure and more flexible than any conventional security procedures without affecting the performance of the LAN. Applying Zachman matrix provides the answers to what data assets the nuclear and research facilities controls, how they are used, and where they are located.

Keywords: computer network, LAN's security, zachaman, information technology (IT), Information systems architecture (ISA).

I. Introduction

The industry is moving toward more formal development and documentation of enterprise architectures based on Enterprise Architecture Frameworks. The term "architecture" has been used for many years within the information technology (IT) community to refer to various types of overviews that provide guidance to software systems and applications developers. The term is obviously a metaphor derived from the building trade [1, 8]. Like a homeowner which is designing a home. Information technology managers work with an architect to provide an agreed upon architectural drawing of the enterprise's information systems and processes. This high-level

Architectural drawing does not change with tactical decisions to deploy improved technology since it is simply built around a framework of business processes and the information that they need [2].

Today, there is a growing movement among both business managers and IT managers to use the term "enterprise architecture" to refer to a comprehensive description of all of the key elements and relationships that make up an organization. Based on this, enterprise information architecture provides a framework for reducing information system complexity and enabling enterprise information sharing. Since most enterprises have existing information systems, the architectural drawing provides the future state and facilitates the best possible strategy to remodel with the least amount of inconvenience to the business [1].

The rapidly growing interconnectivity of IT systems, and the convergence of their technology, renders these systems increasingly vulnerable to malicious attacks. Network attacks cause organizations several hours or days of downtime and serious breaches in data confidentiality and integrity. Depending on the level of the attack and the type of information that has been compromised, the consequences of network attacks vary in degree from mildly annoying to completely debilitating, and the cost of recovery from attacks can range from hundreds to millions of dollars [3].

This paper presents a network security architecture based on the Zachman Framework. The aim of this architecture is to organize the data, process, and technology around the points of view taken by various players instead of representing them as entirely separate entities. For this, we'll consider the Zachman Framework in more detail in Section 2. In Section 3, the relation between network security and the Zachman Framework is discussed. An example for designing security architecture of Nuclear and Research facilities based on the Zachman Framework is presented in this work.

II. The Zachman Framework

The Zachman Framework for Information Systems Architecture (ISA), defined in 1987, is a logical construct to define and control the interfaces and integration of all components of a system. The framework of the Zachman model enables systematic capture of system specific information from the various perspectives with respect to system architecture [4]. Table 1 illustrates the Zachman model, tailored to support a network security system.

Author α σ: Nuclear & Radiological Regulatory Authority, Cairo, EGYPT.
e-mail: mmaazz_2222@yahoo.co.uk

Table 1: The Zachman Framework

	DATA	FUNCTION	NETWORK	PEOPLE	TIME	MOTIVATION
Planner	List of Things Important to the Enterprise	List of Processes	List of Locations	List of Organizational Units	List of Events	List of Business Goals
Owner	Semantic Model	Business Process Model	Network Logistics System	Work Flow Model	Master Schedule	Business Plan
Designer	Logical Data Model	Application Architecture	Distributed System Architecture	Human Interface Architecture	Processing Structure	Business Rule Model
Builder	Physical Data Model	System Design	Technology Architecture	Presentation Architecture	Control Structure	Rule Design
Sub-Contractor	Data Definition	Program	Network Architecture	Security Architecture	Timing Definition	Rule Specification
Functioning	Data	Function	Network	Organization	Schedule	Strategy

In this customization of the model, the system developers have an existing operational system in place. The rows at the top are the most abstract and are oriented toward very broad goals and plans. If we were building a house, this layer would describe the diagrams, pictures, and plans the architect would discuss with the owner. The next level is more specific, but still abstract. These are the diagrams that the architect would discuss with the contractor. In a similar way, the top level of the Zachman Framework, labeled "Scope," is focused on the concerns of senior executives. The second is focused on the slightly more detailed concerns of business managers. A lower level focuses on concerns that business and IS manager's work together on, and then, finally, on a detail that IS managers and developers work on [1]. The columns in the Zachman framework represent different areas of interest for each perspective. The columns describe the dimensions of the systems development effort. The Zachman Framework has two very distinctive features that make it ideal for information modeling. The framework may be applied at any level of abstraction in the system development process, from a global enterprise, to a system, subsystem, or major module level. The framework also gives the modeler latitude in that any data representation technique can be used to model the inner workings of each cell. The system model becomes more implementation specific. However, the requirements traceability between layers can be maintained through backward references to upper layers of cells. This traceability is critical in security requirements engineering, where tracing a global access control requirement may translate into explicit setting of access controls on specific files or directories within an operating system. The framework provides taxonomy: that helps us understand the perspectives of various players in the development of an information system and the descriptions of the system that can be produced during its creation [4].

The model is frequently used as a framework during information systems activities to support the solicitation, identification and mapping of the following information re-engineering associated with an information system's[4] such as goals, objectives, environment, customers served, time constraints, functional description, information architecture, supporting infrastructure. In short, the Zachman ISA can provide a consolidated view of a system, to whatever level of detail a modeler chooses.

III. Network Security and The Zachman Framework

The objective of network security architecture is to provide the conceptual design of the network security infrastructure, related security mechanisms, and related security policies and procedures. The security architecture links the components of the security infrastructure as one cohesive unit. The goal of this cohesive unit is to protect corporate information [3]. The security architecture should be developed by both the network design and the IT security teams. It is typically integrated into the existing enterprise network and is dependent on the IT services that are offered through the net-work infrastructure. The access and security requirements of each IT service should be defined before the network is divided into modules with clearly identified trust levels. Each module can be treated separately and assigned a different security model. The goal is to have layers of security so that a "successful" intruder's access is constrained to a limited part of the network. Just as the bulkhead design in a ship can contain a leak so that the entire ship does not sink, the layered security design limits the damage a security breach has on the health of the entire network. In addition, the architecture should define common security services to be implemented across the network [7].

For security architecture modeling purposes, the first three levels of the perspective hierarchy (planner, owner, and designer) and the Network cell of the Builder's view are useful. They provide the consumer perspective of the system's end user, the perspective of the system "owner" or contracting entity, and the perspective of the designer, or systems engineer. In other words, the "as built" and used in daily operation perspective, the "as desired" operation perspective, and "as actually specified" perspective. The highest level, the Planner View, defines a clear and coordinated boundary (domain) of the system for the purposes of identifying the people, subsystems, and needs impacted by the system. The Owner's View captures the business and organizational relationships, and their external interfaces. It also documents sources of system requirements, including those derived from legacy systems. The Designer's View establishes and documents the security architectural design and provides a basis for system measurement. Finally, the Builder's View provides a detailed description of the

design and methodology for monitoring and correcting system performance [2].

Similarly, the first three columns of the Zachman matrix (data, function, and network) provide the answers to what data assets the organization controls, how they are used and where they are located [5]. As shown in Table 1, these are:

Data: Each of the rows in this column address understanding of and dealing with an enterprise's data. This begins in Row One with a list of the security concerns of the enterprise and its directions and purposes. Row Two is a contiguous model of the security problems seen by the participants in the business. Also, relationships may be shown which themselves have attributes. Row Three provides more of an information based perspective of the network security, resolving the rules and relationships, along with relationships containing their own attributes. Indeed, attributes are more exhaustively defined and unique identifiers are specified.

Function: The rows in the function column describe the process of translating the mission of the network security system of the enterprise into successively more detailed definitions of its operations. Where Row One is a list of the kinds of network security related activities the enterprise conducts, Row Two describes these activities in a contiguous model. Row Three portrays them in terms of data transforming processes, described exclusively in terms of the conversion of input data into output data.

Network: This column is concerned with the geographical distribution of the enterprise's activities. At the strategic level (Row One), this is simply a listing of the places where the enterprise does business. At Row Two, this becomes a more detailed communications chart, describing how the various locations interact with each other. Row Three produces the network architecture for data distribution, itemizing the special security policy for the enterprise. In Row Four, this distribution is translated into the kinds of computer and network facilities that are required in each location to force the security policy.

IV. The Network Security of Nuclear and Academic Facilities

Nuclear and Research facilities, as major users of information and communication technology (especially Internet), also need security; however, because of their special structure and requirements, the traditional solutions and policies to limit access to the Internet are not effective for them. These institutions face concerns about the security of computing resources and information. The security problems in these environments are divided into two categories [3, 6]: problems with research information and problems with administrative information. Although the corporate and research environments face common security problems they can't choose similar methods to solve them, because of their different structures. In a corporate environment, the natural place to draw a security perimeter is around the corporation itself. However, in a nuclear and research facilities research environment, it is very difficult to draw a perimeter surrounding all of the people who need to access information resources and only those people. This is mainly because of different types of information resources in these environments and also different users who want to access them. So if the security perimeter chosen is too big it includes untrusted people and if it is chosen too small it excludes some of the authorized people.

In addition, corporations can put serious limitations on the Internet connectivity in the name of security but research organizations simply cannot function under such limitations. First, trusted users need unrestricted and transparent access to Internet resources (including World Wide Web (WWW), FTP, Gopher, and electronic mail) located outside the security perimeter. Researchers rely on fingertip access to online library catalogs and bibliographies, preprints of papers, and other network resources supporting collaborative work. Second, trusted users need the unrestricted ability to publish and disseminate information to people outside the security perimeter via anonymous FTP, or WWW. This dissemination of research results and papers is critical to the research community. Third, the security perimeter must allow access to protected resources from trusted users located outside the security perimeter. An increasing number of users work at home or while traveling. Research collaborators may also need to enter the security perimeter from remote hosts. If we consider these centers as an enterprise, the security architecture of their network can be designed based on the ZachmanFramework. For the first four rows and first three columns of the framework the cells can be completed as described in the following sections:

a) Planner's View

An overall organizational policy would be implemented in the Planner's View. The first cell is the list of things important to the Nuclear and Research facilities. Research groups often need to maintain the privacy of their work, ideas for future research, or results of research in progress. Administrative organizations need to prevent leakage of student grades, personal contact information, and faculty and staff personnel records. Moreover, the cost of security compromises is high. A research group could lose its competitive edge, and administrative organizations could face legal proceedings for unauthorized information release. On the other hand, nuclear and research facilities and research institutions are ideal environments for hackers

and intruders and many of them are physically located in these places and they are highly motivated to access and modify grades and other information. There are several reports of break-ins and deletion of data from educational institutions [3, 6].

The second cell in this row is the list of the processes important to the enterprise. This can also be divided into two categories: processes done by nuclear facilities, such as radiation monitoring and control; and research processes, such as conducting projects and disseminating information. The next cell (the network cell) is the locations of the entire research and nuclear facilities.

b) Owner's View

The next level down, the Owner's View, considers the groupings of data and means of access available to both internal and external users. For the first cell (data), we can see three categories of information in a university:

1. The information officially disseminated by the nuclear facilities (such as news and events articles).
2. The information gathered and used by network users.
3. The information not allowed to be publicly disseminated.

Based on the above categories, three types of function servers (second cell) may be proposed in the research facilities which are supervised by nuclear facilities:

1. Public servers, which are used to support information dissemination.
2. Experimental servers, which are used for researchers to develop and test their own software packages and protocols.
3. Trusted servers, which are used for administrative purposes or keeping confidential information. These servers are the places where functions occur with respect to the data [9].

The other requirement of a nuclear facilities environment is to let its trusted members access the resources of the network from outside of the security perimeter (e.g., from home or on trips). Another problem that causes serious trouble for the university is network viruses. These viruses are distributed through the network when users are accessing special sites. Proxy servers can be used to control this problem. Of course these proxy servers should be transparent. The network cell of the framework in this layer is shown in Figure 2.

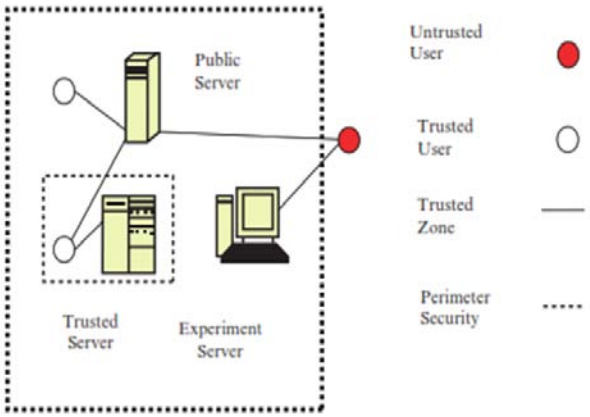

Figure 1: Network layer in Owner's View

c) Designer's View

At the next level, the Designer's View, we introduce mechanisms to protect the network. To achieve the goals described in owner's view, the logical data model (first cell) of the proposed network security policy was designed based on seven basic rules:

1. Packets to or from the public servers are unrestricted if they are from authorized ports. The authorized port is the port that the special service is on. Of course, each public server should be protected itself. The server level security means to enforce stronger access controls on that level.
2. Packets to or from the experimental servers are unrestricted. These servers can be located outside of the security perimeter.
3. Packets to or from the authorized ports of trusted servers are allowed only from or to the authorized clients inside the security perimeter.
4. All of the outgoing packets are allowed to travel outside after port address translation. The incoming packets are allowed if they can be determined to be responses to outbound requests.
5. The packets to or from trusted users of hosts outside the security perimeter are allowed.
6. All of the requests from particular applications such as http should be passed through a proxy server.
7. All the packets to or from outside the security perimeter should be passed through the Intrusion Detection System (IDS).

Rule 1 is based on our need to support information dissemination in a research environment. Public servers must be separated from trusted hosts and protect them at the server level. Because of they may be compromised, so it should make a plan to recover them from information kept securely behind the security perimeter.

Rule 2 follows from recognition that researchers sometimes need to develop and test insecure software packages and protocols on the Internet. Of course they should be alerted that their server is not secure and their information may be corrupted.

Rule 3 is based on the fact that confidential information must be protected. These servers are most important resources to be protected and therefore they should be put in a special secure zone.

Rule 4 follows from recognition that open network access is a necessary component of a research environment. On the other hand it is not allowed to any user to set up Internet servers without permission. The address translation prevents outside systems from accessing internal resources except those listed as public servers.

Rule 5 grants access to protected resources to users as they work from home or while traveling, as well as to collaborators located outside the research group.

Rule 6 is based on the need to block some Internet sites that contain viruses.

Rule 7 follows from recognition that the above rules should be monitored somehow. IDS can be a proper tool to monitor the network and check if there is any violation of proposed rules. The network cell is shown in Figure 2.

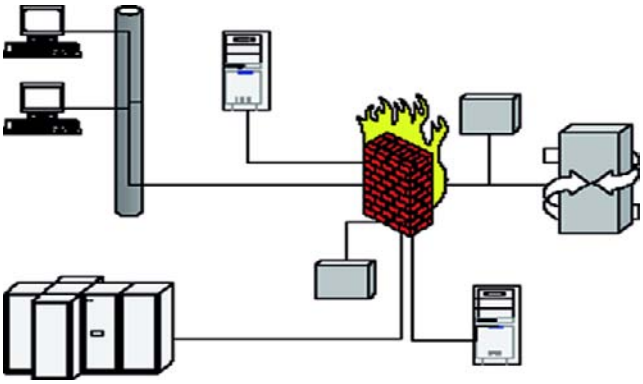

Figure 2: Network layer in Designer's View

d) Builder's View

Finally, the Builder's View describes how technology may be used to address the information processing needs identified in the previous rows. For network security purposes, mainly the network cell is needed. Generally, two ways can be proposed to implement the designed network: first, to use hardware firewalls and caches; and second, to use general purpose servers with proper software packages as cache, proxy, and firewall. In our case study in the nuclear facilities the proxy and cache is used as transparent server, and IPTABLES as the firewall for packet filtering, in which the different zones of the network were defined. Also Network Address is used as Translation of the IPTABLES for implementing the rules in design view. Of course each server in the network had also its own security rules and guards. For restricting access to special websites (mainly to avoid viruses) special software was utilized. SNORT is used as as IDS. The network cell is shown in Figure 3.

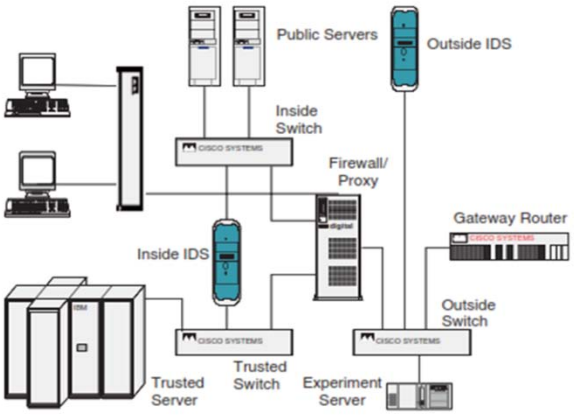

Figure 3

V. Conclusion

Security architecture for computer network makes any Local Area Network LAN more secure and more flexible than any conventional security procedures without affecting the performance of the LAN. Creating Security architecture for nuclear and research facilities, it is possible to develop descriptive security architecture. It provides the "as built" and used in daily operation perspective, the "as desired" operation perspective, and "as actually specified" perspective. Similarly, Creating security architecture for nuclear and research facilities by the Zachman matrix (data, function, and network) provide the answers to what data assets the organization controls, how they are used, and where they are located. Nuclear facilities, as one of the major users of information and communication technology, present a good case study for applying the proposed architecture. The key point of the research is to design the network security architecture of these facilities based on a framework so it provides the consumer perspective of the system's end user, the perspective of the system "owner" or contracting entity, and the perspective of the designer or systems engineer simultaneously.

References Références Referencias

1. Harmon P. Developing an enterprise architecture. Business Process Trends. Available at: http://database.ittoolbox.com/documents/document.asp?i=2385. 2002.
2. DeLooze LL. Applying security to an enterprise using the Zachman Framework. SANSPublications. Available at: http://www.sans.org/rr/paper.php?id=367. 2001.
3. Mohajerani MR, Moeini A. An approach to a new network security architecture for research environments. Proc. Of the 21st International SAFECOMP Conference, Italy.2002.
4. Henning R, Corporation H. Use of the Zachman architecture for security engineering. Proc. of the

19th National Information Systems Security Conference, Baltimore, MD. 1996.
5. Hey DC. A different kind of life cycle: the Zachman Framework. Essential Strategies Inc. Available at: http://www.essentialstrategies.com/documents/zachman2000.pdf. 2000.
6. Greenwald M et al. Designing an research firewall: policy, practice and experience with SURF. IEEE Proceedings of 1966 Symposium of Network and Distributed Systems Security. 1996.
7. Ramachandran J. Designing security architecture solutions. Hoboken: John Wiley and Sons; 2002.
8. Heaney J et al. Information assurance for enterprise engineering. Proc. of the 9th Conference on Pattern Language of Programs, Monticello, Illinois. 2002.
9. Rosenthal M, Coopers P. Three-zone model to depict enterprise security & technology architectures. 28th Annual Computer Security Conference, Washington D.C. 2001.