Using Enterprise Architecture Framework to Design Network Security Architecture

MAHDIREZA MOHAJERANI and ALI MOEINI
Informatics Center and School of Engineering
University of Tehran
No. 286, Keshavarz Blvd, Tehran
IRAN

Abstract:-In the recent years, Information Technology (IT) has come to play an important, and often vital, role in almost all aspects of the life and so there is a growing role and importance for the enterprise architecture (EA) in the management of the organizations. Network security architecture, which can be referred as a comprehensive description of all of the key elements and relationships that make up an organization network security, is a critical business concern, due to the rapidly growing of vulnerabilities in the systems. This paper presents an approach to use enterprise architecture models as a framework to design network security architecture. The network security architecture of academic centers is discussed as a case study to show how a conceptual model can be applied to a real organization.

Keywords: - Enterprise Architecture, Security Architecture, Zachman framework, Network Architecture, Network Security

1 Introduction

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. Much like a homeowner designing a home, information technology managers work with an architect to provide an agreed upon architectural drawing for the information and processes in the enterprise. 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]. 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][10]. 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 using enterprise architecture model and as a practical model, 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 discuss the architecture models in network security in more details in section 2. An example for designing security architecture of academic centers based on Zachman framework is presented in section 3 and section 4 is the conclusion of the paper.

2 Architecture Models in Network Security

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 network 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]. To design network security architecture one approach is to use software development architecture models. These models attempt to describe a system and its architecture from multiple viewpoints, each supporting specific functional and non-functional requirements thereby simplifying the apparent complexity of the system. Each view might require its own notation and analysis. The implementation of the system requires resolution of the pairwise view interaction and verification that the architecture supports all requirements [7]. An example for this model is Kruchen's 4+1 View Model. This model describes four main views of software architecture plus a fifth view that ties the other four together. The views are as follows:

- The logical view describes the objects or object models within the architecture that support behavioral requirements.
- The process view describes the architecture as a logical network of communication processes.
- The physical view maps software onto hardware and network elements.
- The development view focuses on the static organization of the software in the development environment and deals with issues configuration management, development assignments, responsibilities, and product constructions.
- The scenario view is organized around all four of these views. Its definition is driven by the system's use case.

The problem with these models is that most software definitions lump security into the same class as other non-functional system requirements, such as availability, portability and performance. However, security does not belong within a system in the same manner as the other requirements and cannot be treated in a uniform manner [7].

Using enterprise architecture frameworks is another approach to design network security architecture. One of the frameworks that is widely used in information system architecture is 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. 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 on the slightly more detailed concerns of business managers. Lower levels focus on concerns that business and IS managers work together on, and then, finally, on details 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

Table 1. Zachman Framework

	DATA	FUNCTION	NETWORK	PEOPLE	TIME	MOTIVATION
Planner (Scope)	**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

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.

3 The Network Security of the Academic Centers: A Case Study

Academic centers as one of the major users of the 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 is 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 academic 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 an academic environment, it is very difficult to draw a perimeter surrounding all of the people whom they 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 is chosen 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, FTP, Gopher, electronic mail, etc.) located outside the security perimeter. Researchers rely on fingertip access to on-line 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, World-Wide-Web, etc. This dissemination of research results, papers, etc. 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 Zachman framework. For the first four rows and first three columns of the framework the cells can be filled as follow:

4.1 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 academic centers. Research groups often need to maintain the privacy of their works, 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. In other hand, academic 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: academic processes, such as examinations, and research processes such as conducting projects and information dissemination.

The next cell (the network cell) is the location of the academic center. For some universities with central campus, it is much easier to develop their network security architecture, rather than universities with several branches.

4.2 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:

- The information that is officially disseminated by the university (such as news and events, articles and …)
- The information that is gathered and used by network users.
- The information that is not allowed to be disseminated publicly.

Based on the above categories, three types of function servers (second cell) may be proposed in the university: Public servers, which are used to support information dissemination. Experimental servers, which are used for researchers and students to develop and test their own software packages and protocols. Trusted servers, which are used for administrative purposes or keeping confidential information. These servers are the places where the function occurs with respect to the data [9].

The other requirement of an academic environment is to let its trusted members to access the resources of the network from outside of the security perimeter (for example from home or in the trips).
Another problem, that causes serious troubles for the university is the network viruses. These viruses are distributed through the network after users access the special sites. The 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 can be shown in Fig 1.

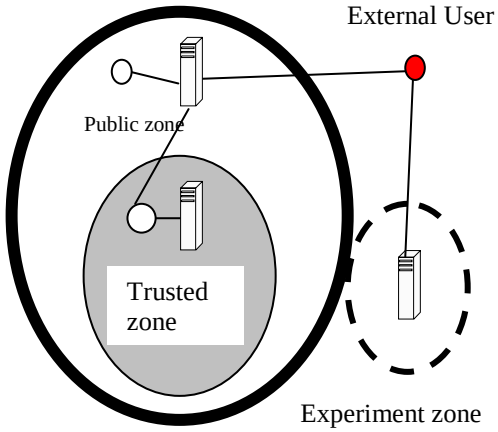

Fig 1. Network Layer in Owner's View

4.3 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 [3][11]:

i. 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 it. Of course, each public server should be protected itself. The server-level security means to enforce stronger access controls on that level.

ii. Packets to or from the experimental servers are unrestricted. These servers can be located outside of security perimeter.

iii. Packets to or from the authorized ports of trusted servers are allowed only from or to the authorized clients inside the security perimeter.

iv. 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 request.

v. The packets to or from trusted users of hosts outside the security perimeter are allowed.

vi. All of the requests from particular applications such as http should be passed through proxy server.

vii. All the packets to or from out of the security perimeter should be passed through Intrusion Detection System.

The *rule i* is based on our need to support information dissemination in a research environment. We have to separate the public servers from our trusted hosts and protect them in server-level and accept this fact that they may be compromised, so we should have a plan to recover them from information kept securely behind the security perimeter.

The *rule ii* follows from our recognition that researchers and students 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.

The *rule iii*, is based on this fact that we want to protect the confidential information. These servers are our most important resources to be protected and we put them in a special secure zone.

The *rule iv* follows from our recognition that open network access is a necessary component of a research environment. On the other hand we don't want to allow the users to setup Internet servers without permission. The address translation prevents the outside systems to access the internal resources except the ones, which are listed as public servers.

Rule v 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 vi is based on the need of blocking some sites in the Internet, which contains viruses.

Rule vii follows from our recognition that the above rules should be monitored somehow. Intrusion Detection System (IDS) can be a proper tool to monitor the network and check if there is any violation from our proposed rules. The network cell can be shown in Fig 2.

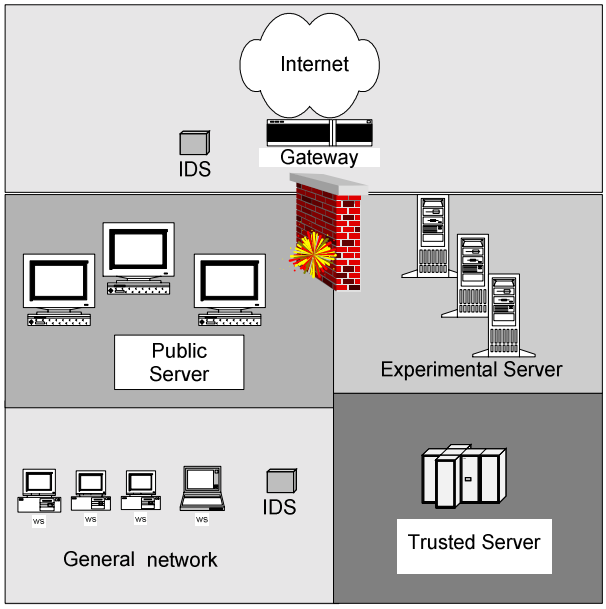

Fig 2. Network Layer in Designer's View

4.4 Builders View

Finally, the Builder's View describes how technology may be used to address the information processing needs identified in the previous rows. For the 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 (such as Cisco PIX, Watchguard, etc) and caches, and second, to use general purpose servers with proper software packages as cache, proxy and firewall. In our case study in the University of Tehran we used a server with Linux operating system (Redhat 7.3 upgraded to Redhat 8.0) with a normal hardware specification (800 MHz CPU, 1 GB RAM). We used SQUID as the transparent proxy and cache server, and IPTABLES as the firewall for packet filtering which the different zones of the network were defined in it. Also we used Network Address Translation (NAT) of the IPTABLES for implementing the rules in our design. Of course each server in the network had

also its own security rules and guards. For restricting the access to special websites (mainly to avoid viruses) the SQUIDGUARD software was utilized. We used SNORT as our Intrusion Detection System (IDS). The network cell can be shown in Fig 3.

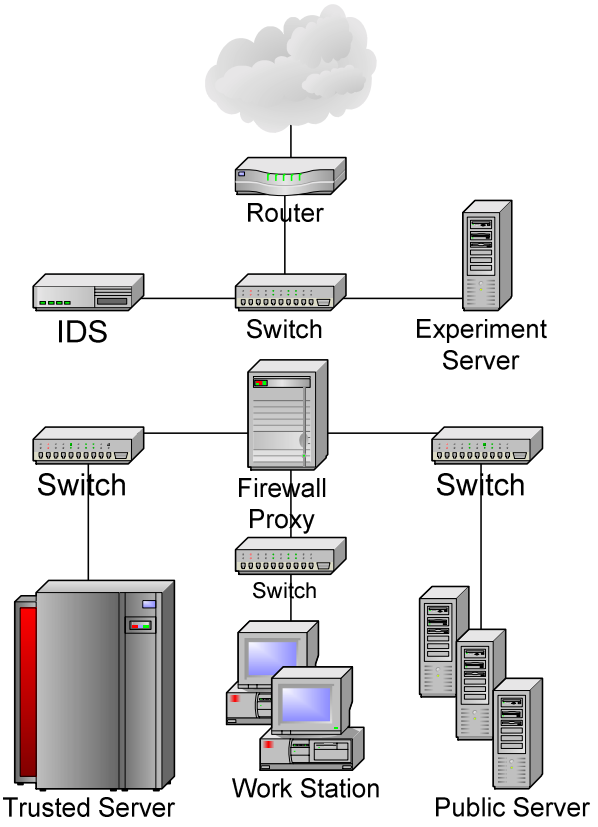

Fig 3. Network Layer in Builder's View

5 Conclusion

As an enterprise architecture framework, the Zachman Information Systems Architecture framework for systems modeling provides a commonly used technique that can be applied to network security architecture modeling early in the system requirements definition process. By applying the top three levels of the Zachman hierarchy, it is possible to develop descriptive security architecture. They provide the "as built" and used in daily operation perspective, the "as desired" operation perspective, and "as actually specified" perspective. 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. Academic centers as one of the major users of the information and communication technology can be a good case study for applying our proposed architecture. The key point of the research is to design the network security architecture of these centers 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:

[1] P. Harmon, Developing an Enterprise Architecture, Business process Trends, http://database.ittoolbox.com/documents/document.asp?i=2385, Nov. 2002

[2] L. L. DeLooze, Applying Security to an Enterprise using the Zachman Framework, *SANS Publications*, Sep. 2001 http://www.sans.org/rr/paper.php?id=367

[3] M.R. Mohajerani, A. Moeini, An Approach to a New Network Security Architecture for Academic environments, *Proc. of the 21st International Conference SAFECOMP*, Italy, Sep. 2002

[4] R. Henning, H. Corporation, Use of the Zachman Architecture for Security Engineering, *Proc. of the 19th National Information Systems Security Conference*, Baltimore, MD, Oct. 21-25, 1996

[5] D. C. Hey, A Different Kind of Life Cycle: The Zachman Framework, *Essential Strategies Inc.*, www.essentialstrategies.com/documents/zachman2000.pdf, 2000

[6] Greenwald, M., et al., Designing an Academic 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*, John Wiley and Sons, 2002

[8] J. Heaney, et. al, Information Assurance for Enterprise Engineering, *Proc. of the 9th Conference on Pattern Language of Programs*, Monticello, Illinois, 2002

[9] M. Rosenthal, P. Coopers, Three-Zone Model to Depict Enterprise Security & Technology Architectures, *28th Annual Computer Security Conference*, Washington D.C. , Oct. 2001

[10] G. Santana, et. al., Modeling a Network Security Systems Using Multi-Agents System Engineering, 4th WSEAS Int. Conf. on Information Science, Communications and Applications (ISA 2004), Miami, Florida, April 21-23, 2004

[11] Nor Badrul Anuar et. al., RedAlert: Approach for Firewall Policies Update Mechanism, 4th WSEAS Int. Conf. on Information Science, Communications and Applications (ISA 2004), Miami, Florida, April 21-23, 2004