Data Center Tiers Security Service

S.Janosepah[1],.N.Modiri[2],.M.V.Malakooti[3]

[1]Falculty member in IAU Majlesi Branch and M.s Student in IAU EUA, Isfahan, Iran, safoura.janosepah@iaumajlesi.ac.ir **; [2] Faculty member in IAU Zanjan Branch, Tehran, Iran,** nassermodiri@yahoo.com **; [3] Faculty member in IAU EUM, Dubai, Emirate,** malakooti@iau.ae**;**

Paper Reference Number: 0105-719
Name of the Presenter: Safoura Janosepah

Abstract

The heartbeat of any organization is its Data Centers. Employees, partners, and customers rely on data and resources in the Data Centers to effectively create, collaborate and interact for their business. Over the last decade, the rise of Internet and Web-based technologies has made the Data Centers more strategic than ever, improving productivity, enhancing business processes, and accelerating change. Data centers are the strategic focus of IT efforts to protect and optimize the growth of businesses. Therefore, IT organizations must improve operational efficiency, optimize utilization of Datacenters resources, and release funds for innovative new IT projects that help generate revenue. Data centers have evolved significantly as organizations consolidate servers, applications, and other resources, and as they adopt new technologies as a means to reduce costs and increase efficiency. However, technologies such as Server Virtualization, Virtual Machines and Web services eliminate this coupling and create a mesh of interactions between systems that create subtle and significant new security risks. Consequently, Datacenters managers face several security challenges in fulfilling their goals.

In this paper, we want to present a framework for developing risk-driven enterprise information security and information assurance architectures and for delivering security infrastructure solutions that support critical business initiatives. This paper also discusses multi-tier architecture, This Model comprises four layers, and it follows closely the work done by John A. Zachman in developing a model for enterprise architecture. Each tier has a different role in the process of specifying, designing, constructing and using the building. It has a security service management that has been placed vertically across the other layers which manages other layers.

Key words: Information, Challenge Security, Management, Tier architecture, Frame work.

1. Introduction

Today’s data centers are the central repository of computing resources, enabling enterprises to meet their business objectives. Data centers are evolving quickly in response to operational requirements and new technologies. To reduce costs and gain flexibility, many enterprises

have taken on server, application, and data center consolidations to reduce costs and increase returns on their IT investments. Also many organizations are considering cloud computing as a new infrastructure model to create dynamic scalable resource storages [6].
Consolidating servers, applications, and other resources leads to higher efficiency of these resources and eliminates the need for IT staff in many locations. Outsourcing some applications to the cloud can make it easier to support teleworkers in remote offices who need secure access to centralized resources that are always available [6].

In information systems, security controls address the confidentiality, integrity, and availability of information. As organizations consolidate applications, data, and other resources within a few large data centers, they increase the risk that a single system breach represents. Whereas a single server has conventionally housed one application, virtualized servers today host multiple applications or components or both [3, 4].

Server virtualization is a new technology for data center consolidating, allowing enterprises to compress the most of server resources, and reduce the need for floor space, electricity, and cooling. Each of these operating systems has its own virtual CPU, memory, and I/O resources, creating a virtual machine. In addition, VMs can migrate from host to host, allowing for dynamic resource allocation as demand rises and falls. But this immigration between platforms in VM makes some security risks such as: worm/virus propagation and monitoring and control problem.

In new Data Centers has been used *Distributed Application Architectures*, While these architectures make application development faster and more efficient, they pose security risks by creating highly distributed communication patterns, with multiple flows per transaction. This technology makes it difficult to enforce access entitlements. Data privacy is another security issue in highly distributed application environments. Since client communications are now targeted at a larger set of systems, the possibility of an eavesdropper intercepting a communication stream increases, making encryption a requirement for communication. Therefore it needs to an overall bandwidth.

To effectively manage the risks resulting from new technologies in the *distributed, virtualized systems* of new generation of data centers, organizations must reevaluate their practices and implement new security solutions that includes management consoles from which operations can centrally manage all functions, including defining a unified security policy and aggregating compliance information. Beyond supporting consolidated policy definitions, centralized management systems can significantly reduce security operational overhead in other areas [3, 4].

In this paper, a framework has been represented for developing assurance architecture in data centers. At first we investigate about Data Center Consolidation Phases. Next we want to describe some data center architectures and enterprise frameworks such as: *Cisco Data Center Architecture* and *Zachman Enterprise Architecture*. After that we propose a model for Data Center architecture which combines both of architectures that said above. Finally we express some advantages in conclusion.

2. Data Center Consolidation Phases

Consolidation is a complex project that spans over several months, or even a few years. The process must be split into several phases, and each phase must be managed by a dedicated, detail-oriented, and experienced project manager. Following are the main phases:

- Study and document the current environment.
- Architect the target consolidated environment.
- Implement the new architecture.
- Control and administer the consolidated environment.

Main focus in this paper is about third phase (Implement the new architecture). On the other hand, for consolidating in new generation Data Centers, it should be implemented assurance architecture. Therefore we will discuss Data Center Architecture more in next part [6].

3. Data Center Architecture Overview

The data center is home to the computational power, storage, and applications necessary to support an enterprise business. The data center infrastructure is central to the IT architecture, from which all content is sourced or passes through. Proper planning of the data center infrastructure design is critical, and performance, resiliency, and scalability need to be carefully considered [1].

Another important aspect of the data center design is flexibility in quickly deploying and supporting new services. Designing a flexible architecture that has the ability to support new applications in a short time frame can result in a significant competitive advantage. Such a design requires solid initial planning and thoughtful consideration in the areas of port density, access layer uplink bandwidth, true server capacity, and oversubscription, to name just a few.

The data center network design is based on a proven layered approach, which has been tested and improved over the past several years in some of the largest data center implementations in the world. The layered approach is the basic foundation of the data center design that seeks to improve scalability, performance, flexibility, resiliency, and maintenance. The layers of the data center design are the core, aggregation, and access layers. Figure 1 shows the basic layered design [1].

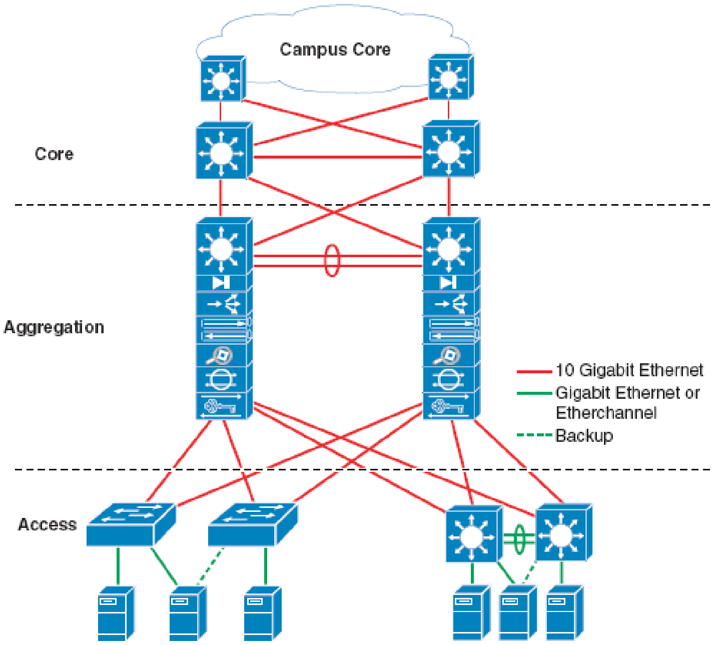

Fig1: basic layered design [1]

3.2. The Cisco Data Center Architecture

The evolving consolidation and virtualization of data center resources requires a highly scalable, resilient, and secure data center network foundation. The network is the fabric that provides secure user access to data center services and an infrastructure for the deployment, interconnection and aggregation of shared data center components as required, including applications, servers, appliances, and storage. A properly planned data center network protects application and data integrity, optimizes application availability and performance, and enables responsiveness to ever-changing market conditions, business priorities, and technology advances [2].

The Cisco Service Oriented Network Architecture (SONA) framework outlines how enterprises can evolve to an Intelligent Information Network that optimizes applications, business processes and resources. Cisco SONA is based on the principle that by making the right investment in the network, an enterprise can dramatically increase productivity, efficiency and business resilience, reduce costs and improve IT alignment with business priorities. Nowhere is this truer than in the data center.

The Cisco Data Center Network Architecture provides a scalable foundation that allows data centers to host a variety of legacy and emerging systems and technologies. Among these technologies are the following: *N-tier Applications*, *Web Applications*, *Blade Servers*, *Clustering/High-Performance Computing and Grid*, *SOA and Web Services and Mainframe Computing*.

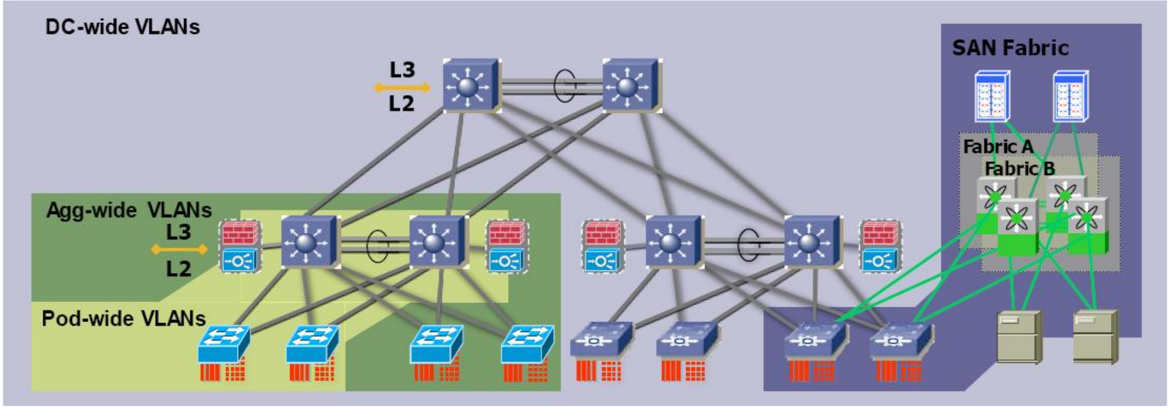

Fig 2: New Data Center Architecture [2]

Figure2 illustrate, the Cisco Data Center Network Architecture comprises the following layers [2]:

- Topology layers
    - Core layer
    - Aggregation
    - Access
- Topology service
- Topology flexibility

3.3. Zachman Framework for enterprise architecture

Today, there is a growing movement among both business managers and Information System 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. Increasingly, when managers talk about the alignment between business processes and goals and Information System applications and middleware systems, they rely on an enterprise architecture to define how the business-IS alignment should be achieved. There are many different approaches to describing the elements of enterprise architecture. One approach that has grown in popularity in the past few years is based on a framework developed by John Zachman.[5]

In fact, the Zachman Framework was designed to provide an architecture that embraces all of the descriptions used by a large organization. It makes more sense for business managers to maintain those aspects of the architecture that they create and for Information System managers to focus on the documentation that they create. To emphasize this, it can be divided the cells in the Zachman Framework to show that the upper rows are primarily the concern of business managers and a lower area that is primarily the concern of various groups of Information System managers; you can see these classification in table 1.

	The Zachman Framework	**DATA** *What*	**FUNCTION** *How*	**NETWORK** *Where*	**PEOPLE** *Who*	**TIME** *When*	**MOTIVATION** *Why*
Business Managers	SCOPE (Contextual) *Planner*	List of Things Important to the Business	List of Processes the Business Performs	List of Locations in Which the Business Operates	List of Organizations Important to the Business	List of Events Significant to the Business	List of Business Goals/Strategies
	ENTERPRISE MODEL (Conceptual) *Owner*	Semantic Model	Business Process Model	Business Logistics System	Work Flow Model	Master Schedule	Business Plan
IT Managers and Developers	SYSTEM MODEL (Logical) *Designer*	Logical Data Model	Application Architecture	Distributed System Architecture	Human Interface Architecture	Processing Structure	Business Rule Model
	TECHNOLOGICAL MODEL (Physical) *Builder*	Physical Data Model	System Design	Technology Architecture	Presentation Architecture	Control Structure	Rule Design
	DETAILED REPRESENTATIONS (Out-of-Context) *Sub-Contractor*	Data Definition	Program	Network Architecture	Security Architecture	Timing Definition	Rule Specification
	FUNCTIONING ENTERPRISE	Actual Business Data	Actual Application Code	Actual Physical Networks	Actual Business Organization	Actual Business Schedule	Actual Business Strategy

Table1: the zachman framework [5]

4. Proposed framework

Given the highly distributed, complex nature of today’s data centers, it is a challenge to implement a consistent set of security policies across the entire data center infrastructure. Organizations need a comprehensive security solution that includes management consoles from which operations can centrally manage all functions, including defining a unified security policy and aggregating compliance information.

A robust, centralized management system gives the ability to define security policies that are detailed enough to apply granular controls to users, applications, and resource domains, but abstract enough that they don’t need to be customized for each enforcement point. With centralized policy creation, managers are spared having to define security policies for each system within the data center, and the potential vulnerabilities created by a patchwork of policies are avoided.

For developing a robust centralized management in Data Centers, we combine two architectures, The Cisco Data Center Architecture and Zachman Framework for enterprise architecture. We use from Cisco Architecture because the *multi-tier* model is the most common design in the enterprise. It is based on the web, application, and database layered design supporting commerce and enterprise business ERP and CRM solutions. This type of design supports many web service architectures, such as those based on Microsoft .NET or Java 2 Enterprise Edition. These web service application environments are used by ERP and CRM solutions from Siebel and Oracle, to name a few. The multi-tier model relies on security and application optimization services to be provided in the network [1].

Also an approach that avoids piecemeal problems is the development of an enterprise security architecture which is business-driven and which describes a structured inter-relationship between the technical and procedural solutions to support the long-term needs of the business. If the architecture is to be successful, then it must provide a rational framework within which decisions can be made upon the selection of security solutions. The decision criteria should be derived from a thorough understanding of the business requirements, including [5]:

- The need for cost reduction
- Modularity
- Scalability
- Ease of component re-use
- Operability
- Usability
- Inter-operability both internally and externally
- Integration with the enterprise IT architecture and its legacy systems.

Furthermore, information systems security is only a small part of information security, information assurance or information risk management, and information security is a part of Data Center security, finally Data Center security is a session of Business security. The enterprise security architecture and the security management process should therefore embrace all of these areas.

4.1. Security Architecture Needs

Many people make the mistake of believing that building security into information systems is simply a matter of referring to a checklist of technical and procedural controls and applying the appropriate security measures on the list. However, security has an important property that most people know about but few pay any real heed to it: it is like a chain, made up of many links, and the strength and suitability of the chain is only as good as that of its weakest link. At worst, if one link is missing altogether, the rest of chain is valueless.

The checklist approach also fails because many people focus on checking that the links in the chain exist but do not test that the links actually fit together to form a secure chain. The chain is a reasonably good analogy, but the problem is actually much worse than this. There are some of the key questions for filling a checklist such as [5]:

- Do you understand the requirements?
- Do you have a design philosophy?
- Do you have all of the components?
- Do these components work together?
- Do they form an integrated system?
- Are you assured that it is properly assembled?
- Do you operate the system correctly?

- Do you maintain the system?

4.2. A Layered Model of Architecture

This Model comprises four layers, the summary of which is in Table 2. It follows closely the work done by John A. Zachman(with considering a *multi-tier* model) in developing a model for enterprise architecture, although it has been adapted somewhat to a security view of the world. Each layer represents the view of a different player in the process of specifying, designing, constructing and using the building.

The Designer's View	Logical Security Architecture
The Builder's View	Physical Security Architecture
The Tradesman's View	Component Security Architecture
The Service Manager's View	Security Service Management Architecture

Table 2: Layered Architecture Views

There is another configuration of these four layers which is perhaps more helpful, shown in Figure 3. In this diagram the 'security service management architecture' has been placed vertically across the other three layers. This is because security service management issues arise at each and every one of the other three layers. Security service management has a meaning in the context of each of these other layers.

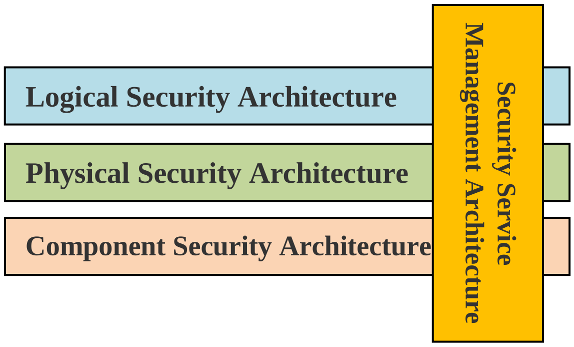
Logical Security Architecture
Physical Security Architecture
Component Security Architecture
Security Service Management Architecture

Fig3: A Model for Security Architecture

4.3. The Model Lifecycle

The Model Development Process can be seen in the context of an overall Model Lifecycle for the security architecture, shown in Figure 4. In this Lifecycle, the first phase of the process is into an activity called *'Design'* which embraces the design of the logical, physical, component and service management architectures. This is followed by an activity called '*Implement'*, followed by '*Manage and Measure'*.

Failure to meet the performance goals is a risk event. Thus the performance goals are also capable as being viewed from the opposite perspective as key risk indicators. It is usual in the framework to set two performance or risk indicators.

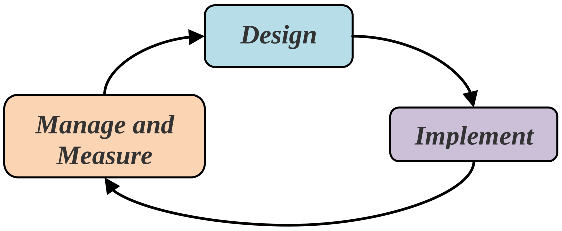

Fig 4: The Model Lifecycle

5. Conclusions

Nowadays organizations rely more than ever on their data centers to enable their operations. The data center continues to evolve as organizations concentrate resources and implement technologies such as server virtualization, distributed application models, and IP-based storage. They adopt new technologies as a means to reduce costs and increase efficiency. But using form new technologies make some new security risks. Therefore, organization should find some solutions for solving these problems.

In this paper we suggest multi layers architecture for developing risk-driven enterprise information security and information assurance architectures. It comprises four layers it follows closely the work done by Zachman framework and Cisco Multi tiers Model in developing a model. Each tier has a different role. Also it has a security service management which has been placed vertically across the other tiers that manages other tiers. Finally, there are some Advantages by Developing of this model such as:

- Cost Reduction
- Modularity
- Scalability
- Operability
- Usability
- Manageability

References

1. Cisco Systems (2007), *"Cisco Data Center Infrastructure 2.5 Design Guide".* Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706 USA.
2. Cisco Systems (2010), *"Next Generation Data center Architecture*", Cisco System. Inc.
3. Dawoud, W. (2010), *"Infrastructure as a service security: Challenges and solutions"* Takouna, I. Meinel, C. Hasso Plattner Inst. .IEEE Inc. page(s): 1 - 8 , ISBN: 978-1-4244-5828-8, INSPEC Accession Number: 11292630.
4. Talukder, A.K. (2009), "*Security & scalability architecture for next generation internet services "*,Prahalad, H.A. , IEEE Inc. page(s): 1 – 4, ISBN: 978-1-4244-4792-3, INSPEC Accession Number: 11207703.
5. John A. Zachman (1987), *"A Framework for Information Systems Architecture." IBM Systems Journal, vol.26, no. 3, 1987. IBM.*
6. Kailash Jayaswal (2006), *"Administering Data Centers: Servers, Storage, and Voice over IP",* Published by Wiley Inc. 10475 Cross point Boulevard Indianapolis, IN 46256.