Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 03, March -2018

A Survey on Cyber Defense Architecture

[1]Akshay G, [2]Dr.Sheela S.V

[1]*Student Department of Information Science And Engineering ,BMSCE*
[2]*Associate Professor, Department of Information Science And Engineering, BMSCE*

Abstract—*The swift development of cyber threats around the world has challenged the traditional design of the defense system mechanism.This paper discuss about the need of lithe structure to inform the development of cyber security solutions that are not adaptable for the unknown threats that affect the system .This paper consists of several reference architecture used for their defense by certain companies in public and as well as the private sectors.*

Index Terms—*cyber defense, cyber security, systems security, security architecture*

INTRODUCTION

The phrase architecture is commonly used to describe the practice of designing and building physical structure and as well as designing the defense system and implementing a complex system in the information technology as well as communication etc. [1].In all these realm we are concerned with the describing the system components and their relationship and the guidelines and principles used in designing the architecture that drive the desired functionality or capabilities of the architecture. A key difference about this is that the design of the building remains constant and the successful architecture should constantly adapt to the need of the business.The swift growing of threats around the world has set a challenge to all the architectures designed.

A crucial challenges for organizations is selecting among the hundreds of available cybersecurity providers and their products by maximizing their investment to protect against the threats which can affect the system in future from 2010 to 2015 it has been found that around 8 billion dollars was invested globally in over 900 cybersecurity companies including start-ups [2].

In this paper , we discuss the role of different architecture in providing structure to the design in cybersecurity and we will discuss few models that are used widely across the world today. As stated by Cloutier et al. [3], the concept of Reference architecture can have different meanings and we use their proposed working definition:

"Reference Architecture capture the essence of existing Architecture and the vision of future need and evolution to provide guidance to assist in developing new system Architectures".

Thus , a Reference architecture is not a description of a specific system implementation but it is rather a tool used as a part of the system engineering process to help and ensure the completeness in the design and unity in the approach. Reference Architecture have become important boon to the enterprise due to many factors which includes :1)the trending transition from single site systems to distributed, multi-site systems including cloud deployment, 2) the need to maximize synergy in technology and resource 3)the need to decrease the integration cost and time, 4)the need to capture business and mission value along side the technical decisions [3].Some architectures are more accurately described as Reference Models in that they standard definitions and terms. Altogether both the Reference Architecture and Reference Models are both used to design and plan its implementation [4].

By this cyber domain, a cyber defense reference architecture should seize proven concepts that satisfy specify security requirements and add those concepts within a operation context that guides the implementation and integration of cyber capabilities.A single specific architecture system should be able to carryout multiple system architecture that may have different business needs [1].In this paper we will conduct a literature review and we compare different Reference Architectures that specifically marks the cyber defense.

II .COMPARISION OF CYBER REFERENCE ARCHITECTURES

A. NIST Cloud Computing Security Reference Architecture

The NIST Cloud Computing Security Reference Architecture (SRA) [5] is derived from the NIST Reference Architecture for Cloud Computing and it identifies the components which are in need to be secured for each cloud actor as well as the stakeholder.The SRA shown in the fig

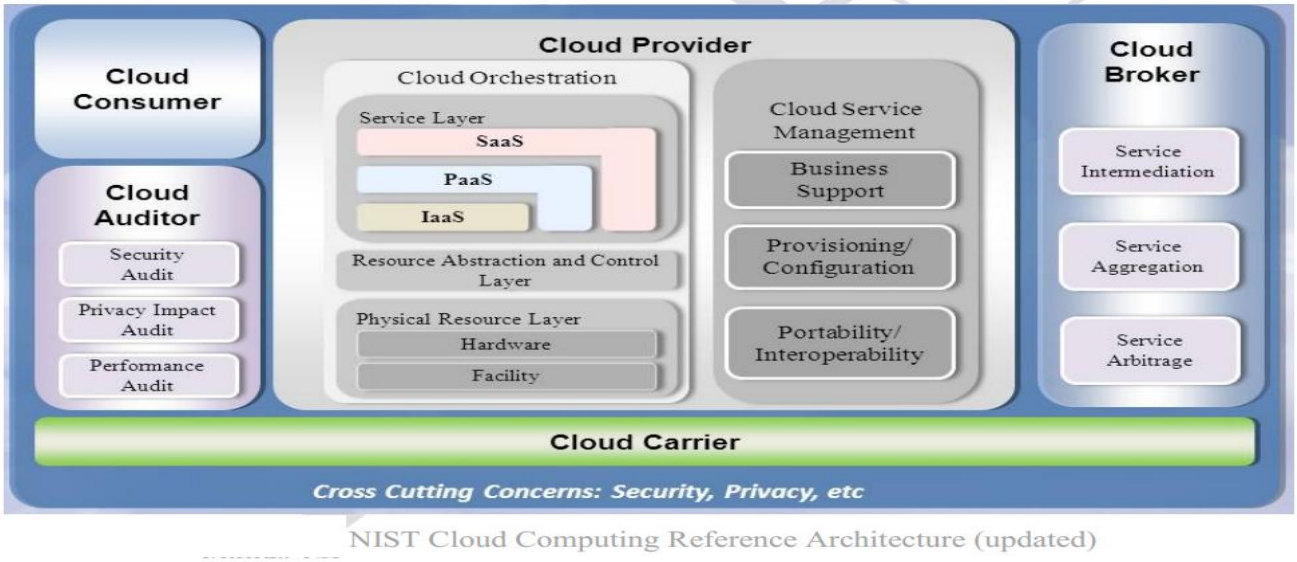

Fig. 1.The NIST Cloud Computing Security Reference Architecture.

components which are in need to be secured for each cloud actor as well as the stakeholder. The SRA shown in the fig 1.depits a layered approach with the cloud actors in the background and the architectural components in the frontend.
Here some of the architectural components extend across the multiple actors. This depends on the some of the cloud deployment factors which are selected by the cloud consumer namely SaaS, PaaS and IaaS. As we don't know how to read the architecture but the cloud consumer has the following list of security architectural components.

- Secure Cloud Consumption Management

  Secure Configuration
  Secure Portability and Interoperability
  Secure Business Support
  Secure Organizational Support

- Secure Cloud Ecosystem Orchestration
- Secure Functional Layers

This SRA leverages the Trusted Cloud Initiative -
Reference Architecture (TCI-RA) [6] by extracting the capabilities allocated to four root domains (Business Operation Support Service[BOSS], Information Technology Operational Support [ITOS], and Security, Technology Solutions (with sub-domains for Presentation, Application ,Information and Infrastructure Services), and Security and Risk Management controls, and capabilities. A comprehensive matrix maps the NIST SRA to the TIC-RA and assigns accountability for implementing each security components to each Actor for each type of cloud deployment.

A closer look between the SRA and TCI-RA depicts that there are only few cases in which a security component cannot be implemented or the component is not secure for implementation by the Cloud Consumer or by the Provider.The exceptions are as expected in cloud deployments. For example ,front-line or the front-end components such as the Presentation Services

and some of the Reporting Services are the responsibility of the Consumer and the back-end components such as the Infrastructure services are the responsibility of the Provider. The main value of the NIST SRA is in providing support when evaluating and selecting a cloud business model rather than designing and implementing a secure system architecture.

B. NATO CIS Security Capability

The NATO communication and Information Agency (NCIA) Communication and Information System (CIS) Security Capability Breakdown [7] is designed to facilitate NATO , multi-national discussion, coordination and capability development related to CIS security and cyber defense. It is structured as a hierarchical decomposition of capabilities to extend necessary to support their development and introduction into operations to address recognized requirements. As a multi-nation body, NATO capabilities depend on the infrastructure provided by many member nations and they are actively involved in an IT modernization process that includes cloud-based services. Although the CIS breakdown does not explicitly depend on cloud computing, it does include a significant component addressing trust in CIS
Components and managing the supply chain security without any specific deployment solution.

There are many rich features of the NATO capability breakdown. It considers both the construction phase of the cyber defense (areas for "Govern CIS security and "Design and implement CIS Security") it also recognizes the improvement which should be made to the final cyber defense instantiation("Enable CIS improvements"). The breakdown lends itself to use a measurement of design, implementation, and operation steps. Version 2 of the NATO capability breakdown was used as a comparative architecture [8] where the top level design was used as a visual for assessing the completeness of a architecture.

In the fourth revision, the main modification from the previous versions of the CIS capability breakdown is that "Cyber Defense" is no longer a separate component , but is integrated into a wider security framework under the capability of " Operate CIS Security ". As other high level capabilities deal with the governance, management and

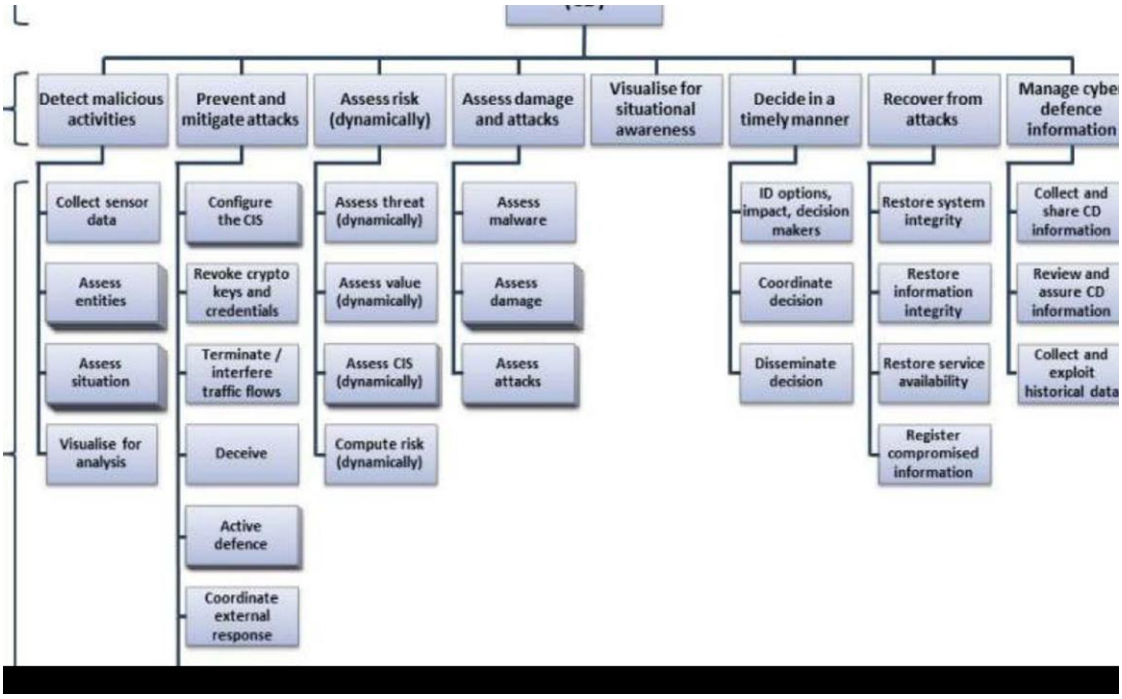

Fig. 2. Cyber Defense capabilities from the NATO

engineering process we now focus only on the Cyber Defense as shown in the fig 2.

However there are some limitations recognized with in the model. The IST-096 NATO Technology Research Committee Final Report [9] noted, in the section of further work the more complete framework would include a maturity model.

III. OTHER CYBERSECURITY FRAMEWORKS

A. Architecture Frameworks

In the previous discussion we have excluded many frameworks such as IBM Security Framework[10], HP Enterprise Cyber Reference Architecture[11], CISCO SAFE and Security Control Framework[12], Department of Defense Architecture Framework[13], The Open Group Architectural Framework[14].

In the contrast to the concepts of Reference Architecture ,these frameworks present various methodologies includes guidance and rules for designing and organizing the architectures.

B. Security Design Patterns

Architecture frameworks are also closely related to security design patterns .
The Cisco safe use defense-in-depth pattern, a perimeter focused perspective that focuses on security configurations at each layer of defense to minimize access to critical infrastructure and prevents attackers from cross over several security levels at once. A recent variation of this perspective is the defense-in-breadth it's an approach in which multiple tools or products with the overlapping functionality but with different capabilities[15].

C. Security Controls

The Reference Architecture as well as the architecture frameworks we presented are commonly mapped to the lists of security controls such as NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations [16] and the Center of Internet Security (CIS) Critical Security Controls (CSC)[17]. Security controls are recommended technical or administrative sets of actions that have been demonstrated to have immediate high impact on improving security posture. The chosen controls defend against most of the cyber threats and are described to have an 80% solution to the present cyber defense.

D. Maturity Models

Maturity models are used throughout information technology and systems engineering disciplines to indicate the ability of an organization to execute continuous improvement. A maturity model provides several benefits such as 1)Recommendation on how to improve, 2) Compare solutions with each other and 3) support for the independent assessment against the accepted benchmarks.

The HPE Security Operations Maturity Model (SOMM) is based on the Capability Maturity Model Integration (CMMI) model for process improvement.

IV . Conclusion

Reference architectures are a staple of good systems engineering. Cyber Security and Cyber Defense being the newer fields, the system engineering approaches and historical knowledge are least. Our survey and analysis provides important knowledge and provides comparisons that will allow cyber architects to better design and evaluate cyber defenses. All the reference architecture we have earlier discussed recognizes the important of building security into the design of a complex system, using analytics for risk management, compliance and reporting, integrating more automated and proactive cyber defense techniques.

References

[1] B. P. Gallagher, "Using the architecture tradeoff analysis method toevaluate a Reference Architecture: a case study," Carnegie Mellon Software Engineering Institute, tech. Rep., 2000.Architecture DRAFT," Natl. Inst. Stand.Technol. spec. Publ., 2013.
[2] Cloud Security Alliance, "Trusted Cloud Initiative Reference Architecture," 2011.Available.: https://cloudsecurityalliance.org/wpcontent/uploads/20 11/10/TCIReference-Architecture-v1.1.pdf
[3] R. Cloutier, G. Muller, D. Verma, R. Nilchiani, E. Hole, and M.Bone, "The concept of Reference Architectures," Systems Engineering,vol. 13, no. 1, pp.14–27, 2010.
[4] "Cybersecurity report: Financing, trends, and companiesanalysis,"CB Insights, Tech. Rep., 2015.

[5] R. Sessions, "Comparison of the top four Enterprise Architecture methodologies," 2007.[Online]. available:https://msdn.microsoft.com/en us/library/bb466232.aspx.
[6] NIST Cloud Computing Security Working Group, "Special Publication 500-299. NIST Cloud Computing Security Reference Architecture draft," Natl. Inst. Stand. Technol. Spec. Publ., 2013.
[7] G. Hallingstad and L. Dandurand, "Communication and Information System Security capability breakdown rev. 4," NATO Communications and Information Agency (NCIA), The Hague, 2013.
[8] D. McCallam, "An analysis of cyber reference architectures," in Presented at NATO 2012 Workshop with Industry on CybersecurityCapabilities, 2012. [12] "STO-TR-IST-096. NATO information assurance/cyberDefence Research Framework (RTG-046/IST-096),"NATO Science & Technology Organization, 2014.
[10] Buecker et al., Using the IBM Security Framework and IBM Security Blueprint to realize Business-Driven Security. IBM Redbooks, 2013.
[11] D. Gahafer, "Cyber security," in FedInsider Tampa Tech Day, 2016.
[12] Cisco SAFE Reference Guide. Cisco Validated Design, 2010.
[13] Department of Defense, "The Department of Defense Architecture Framework Version 2.02," 2011. [Online]. Available: http://dodcio. defense.gov/Portals/0/Documents/DODAF/DoDAFv2-02 web.pdf.
[14] V. Haren, TOGAF Version 9.1, 10th ed. Van Haren Publishing, 2011.
[15] "Special Publication 800-37. Guide for applying the Risk Management Framework to federal information systems," Natl. Inst. Stand. Technol. Spec. Publ., 2010.
[16] "Special Publication 800-53. Security and privacy controls for federal information systems and organizations," Natl. Inst. Stand. Technology spec.Publ., 2013.
[17] The Center for Internet Security, Inc., "The CIS Critical Security Controls for effective cyber defense Version 6.1," 2016.[Online]. Available: https://www.cisecurity.org/critical-controls/download.cfm.

