Changing Security in a Distributed Heterogenous Network

Mitchell Rutigliano

***Abstract*— Increased devices being added to networks with different operating systems, different monitoring mechanisms, and different access points provide a challenge for security professionals. These ever-changing ICT infrastructures are more demanding and require more flexibility then current security models. An attempt to fix this issue is to put more focus on a multi-tier architecture that follows the trend of virtualization, automation, software-definition, and hardware/software disaggregation.**

I. Introduction

Finding new ways to approach security is imperative due to the rapid change in how networks are structured. Current practice involves the "security perimeter" model. This model employs a hard exterior, soft interior strategy from implementing firewalls, intrusion detection systems, and virtual private networks. The model is important because these systems do a good job of monitoring networks. However, with distributed heterogenous network implementation, it becomes challenging to monitor everything inside a network with a variety of different operating systems and logging mechanisms [1].

A. Background

A distributed network is a system where the operational data is spread over multiple end points. This differs from systems in the past where there was a centralized computer. Distributed systems provide an advantage to business since data moves more efficiently [2]. Distributed systems are important and necessary in large environments because they are scalable and fault tolerant. Scalability means that a system can expand if more resources are needed. Fault tolerance means that if a part of a network or system goes down, the environment will still function as if nothing happened. The emergence of cloud computing has presented solutions for enterprise distributed networks.

A heterogenous network is a network with a wide variety of access nodes in a wireless network. This comes in the form of different operating systems, IOT (internet of things) devices, and mobile phones where each system may have its own monitoring solution. Due to the varying types of devices inside of an environment, managing traffic flow can become increasingly difficult every time a device is added. An example of the potential types of devices that may be seen in an environment is database servers, web servers, routers, printers, mobile phones, and user computers [3].

This paper is divided into the following sections: Section 2 explains the topic presented. Section 3 explains existing research issues on the topic. Section 4 talks about possible future research issues. Section 5 concludes the paper.

II. Approach to explain the topic

This section is going to be used to talk about in detail what the perimeter security model is. The perimeter model puts an emphasis on security individual systems. As mentioned previously, the perimeter model uses a hard exterior, soft interior strategy. This strategy implements firewalls, intrusion detection systems, and virtual private networks as the primary system for security. However, this model presents itself with potential breaches. The first of the potential issues at present is the externalization and offloading of devices. The introduction of the cloud has made it so that enterprises and customers use third party infrastructures where data is frequently shared. The multiplicity of heterogenous domains have added more devices into environments with limited processing capabilities. This exposes them to compromise inside a network due to the number of potential exploits. Allowing personal and mobile devices increase the number of devises inside of a network. Inflexible defenses make the flow of high rates of traffic difficult to manage and cause security threats to go unnoticed [1].

Current defensive technologies have limitations that weaken security. Some of the limitations include the following: difficult to change the architecture and system configurations, inefficiency due to how network traffic flows through appliances, detection systems that have a narrow scope that limits what can be monitored, and outdated models that doesn't encompass the broad availability of

devices[1].

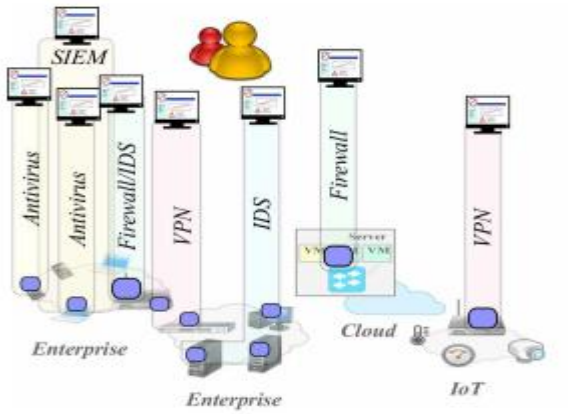


Figure 1 Current Security Model [1]

Figure 1 shows an example of the perimeter model, where there are a bunch of independent applications present [1].

III. Existing Research Issues

Researchers from universities in Italy, working on project Matilda for the European Commission, have proposed a solution to move away from the perimeter model. Their solution is to use a multi-tiered framework that transitions from independent appliance to a common framework.

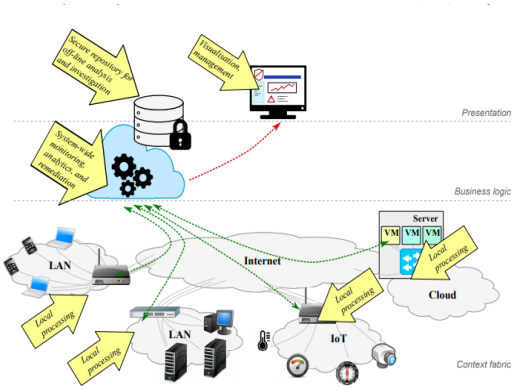


Figure 2 Proposed Mult-Tiered Framework

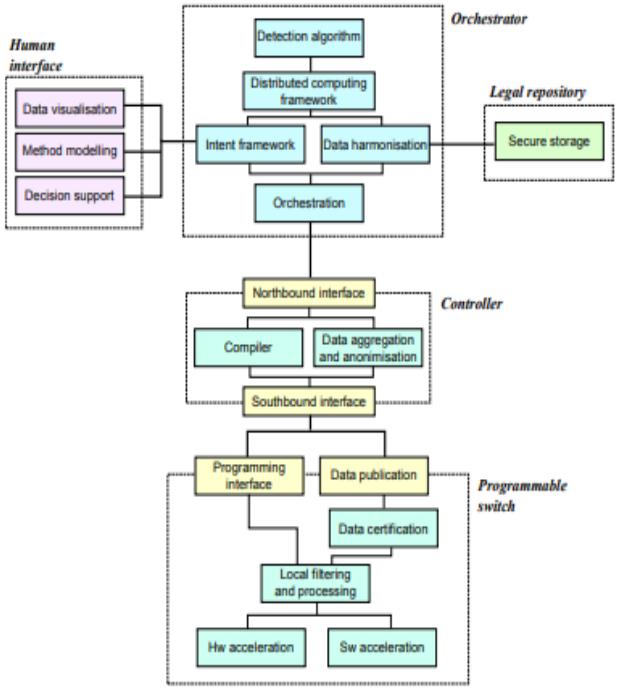
The proposed framework looks very different from the model in figure 1. In the framework, there are three main layers. The layers being: the presentation layer, the business logic layer, and the context fabric layer.

The context fabric layer is where the main monitoring is done. The monitoring includes the "classification, filtering, and processing of network packets". In other words, this layer collects information for threat identification. This layer performs lightweight tasks which allows an increase in sophisticated techniques that can be pushed to endpoints. The framework splits the bottom layer into two different planes, the data plane and the control plane. The data plane is where "lightweight filtering and inspection tasks handle packets without putting significant stress to the computing resources needed." This can be achieved by using a programmable network protocol (OpenFlow) or a network management protocol (NETCONF) for flow programmability, or by using a variety of hardware/software frameworks that create fast paths for faster packet processing. The second part of the context fabric layer, the control pane, extends protocols and interfaces in order to build a common abstraction of the data planes such as, Openflow and NetConf. The abstraction covers the need to "discover, configure, and manage heterogenous resources."

The business layer is used to "extract knowledge from the multiplicity and heterogeneity of data collected by the context fabric." The difficulty with the layer is finding innovative algorithms that work for both space and time dimension to provide metrics. Machine learning techniques help define detailed graphs and models for predictive analysis. Current security models considered with machine learning and big data allow for innovated algorithms. Information needed for forensic investigations need to be considered as well. Storing data and events to be used in an investigation is important. A note to look out for is the importance of protecting user privacy laws. Collecting full contents of network packets can reveal personal information that violates law, so any implementation of innovated algorithms needs to not violate privacy rights.

The Presentation layer displays all the information needed to cleanly display vulnerabilities, risk, and threats. These displays help management and security members make intelligent decisions regarding security threats. The management pane is where "visualization solutions may rely on multi-layer software architectures and REST-based APIs for accessing threats and attacks database by multiple devices, flexible graphical layouts defined by templates and style-sheets to adapt the representation to heterogeneous devices and platforms, event-driven publish/subscription mechanisms for real-time notification of threats, anomalies, and attacks." The graphics should also provide functionality to fire remediation actions. It should also support the creation of new actions based on new identified threats.

The design of the platform uses functional elements that are necessary to implement the framework. The following image explains the conceptual architecture for the framework.



The architecture is split into five sections described below.

- *Programmable Switch*: Responsible for implementing the data plane and context fabric for traffic inspection and analysis. A programming interface sets configurations to offload information to the controller.
- *Controller*: Compiles programs and configurations to SDN protocols. Responsible for managing network topologies, recovery, and data collection.
- *Orchestrator*: Automates and abstracts the infrastructures configurations. It splits detection algorithms and mitigation policies in computing tasks.
- *Legal repository*: Responsible for the storage of data and events useful to a lawful investigation in a secure, trusted manner.
- *Human Interface*: Displays the tools to give a visualization of the security landscape. Allows for a quick and intuitive response to threats.

The advantage of moving to a three-tiered security architecture provides environments with stronger protection against threats. It allows for easy analysis and a quick response. It limits the existing vulnerabilities existing in perimeter model. Although this model outdoes the current perimeter model, there are disadvantages to the framework. Any infrastructure change for a distributed heterogenous network can in many cases, be unachievable [1].

IV. POSSIBLE FUTURE RESEARCH ISSUES ON THE TOPC

Future research on the topic needs to find a cost-effective solution to limit vulnerabilities in a network and to effectively collect valuable data. The continual switch to cloud based environments with thousands of nodes making up a heterogenous network opens the path to new security techniques. However, instead of a straight switch to a new innovative framework, there should be a framework that focuses on transitioning an environment. This would give an environment the flexibility of slowly transitioning to a new model while enhancing current models in a cost-effective manner. The three-tiered framework, from the researchers in Italy, would be a difficult transition for an environment to make. Further research should address a transition phase for this framework.

V. CONCLUSION

The landscape of networking is growing in complexity with the number of distributed heterogenous networks increasing every day This complexity provides holes inside of environments that current security models do not cover. Covering these holes means new models need to be researched to protect environments from security threats. This article talked about the specific challenges that the perimeter model presents and current research on frameworks to shift how security is done. Although there is not a perfect security model that exists, the three-tiered framework is a good step in the direction of innovating security in distributed heterogenous environments.

REFERENCES

[1] Raffaele Bolla, Paolo M. Comi, Matteo Repetto "A distributed cyber-security framework for heterogeneous environments," vol. 2058, ITASEC 2018

[2] Praveen Balda, Sh. Matish Garg "Security Enhancement in Distributed Networking," IJCSMC, Vol. 4.4, April 2015, pg.761-767

[3] Krishna Narayanaswwamy, Bryan Burns, Venkata Rama Raju Manthena"Protecting Against Distributed Network Flood Attacks," US 8,789,173 B2, US 2011/0055921 A1 Mar. 3, 2011