Telemetry Network Testbed – Prototype Network Elements

WiNetS Research Lab

Author: Tobechukwu Osuzoka, Uchenna Emerson

Department of Electrical and Computer Engineering, Morgan State University

Faculty Advisors: Dr. Mulugeta Dugda, Dr Farzad Moazzami, Dr. Richard Dean, Dr Wondimu Zegeye.

ABSTRACT

Telemetry is the automated transfer of measurements or other data from a remote or unavailable locations to receiving equipment for monitoring. Network devices send real-time data to one or more centralized locations for storage, processing, and analysis in network telemetry. By configuring a cloud computing network, we will be able to create a virtual database that consists of a variety of network elements. This paper describes the network elements that are used in a telemetry testbed system. There are various elements that are used in a network configuration. These components include but are not limited to routers, switches, connectors, firewalls, and LAN. VMware is a complicated piece of software that performs best when run on a device with the highest possible specifications. A VMware workstation will be built to accommodate these attacks over two hosts namely a kali Linux and windows XP host. By using a vSphere software, we will be able to create these elements. Through it, each of these network elements will be taken through a series of attacks in which we will analyze and modify each to be improved on. We will be reporting an in-depth analysis of each element, the kind of components they consist of, and the results of each element after attacks are done.

Keywords: Telemetry; VMware; Testbed System; Networking

INTRODUCTION

The Wireless Network System (WiNetS) at Morgan State University is building a Testbed that models telemetry enterprise networks and provides modeling and simulation for the testing of cyber-attacks and defenses. The project is centered on developing a workstation suited to supporting the VMware network simulation, and this will involve the creation of a workstation suited to VMware with many hosts, switches, routers, and firewalls. It will include a high performance multi core, multithread processor with high capacity and high-speed RAM and hard drive allocation. One of the many sub-components of the project includes developing a prototype network which will include a LAN kali Linux host and windows host that will demonstrate one attack over the LAN of the XP host. The project will also include the installation of a virtual switch, virtual router, virtual firewall and demonstrate a connection between the hosts.

One important contribution of this project is that it will demonstrate that networked telemetry has a set of new threats and vulnerability that traditional telemetry does not. In the past decade, the telemetry community's initiatives to implement network-centric solutions have been the focus of their initiatives. The development of the Integrated Network Enhanced Telemetry (iNET) protocol and network operation strategy improves the performance and efficiency of telemetry operations. The challenge associated with this plan is the increased vulnerability of telemetry networks to cyber security attacks. Foreign adversaries like China have excellent cyber-attack capabilities, a history of active participation, and a successful record of penetrating and extracting data from the US government and industry networks. It is reasonable to assume that such opponents have successfully penetrated our network. The telemetry network, like most commercial networks, faces many challenges related to cyber-attacks. However, telemetry networks have several unique attributes that can make threats and vulnerabilities more relevant, and the framework can provide insight into security solutions. Telemetry networks are a form of supervisory control and data acquisition companies (SCADA), like power grids.

Working in this area can inspire our work. Furthermore, the network architecture defined in the iNET standard can limit the focus of our approach.

In one of the other ITC 2021 network modeling articles, we submitted (Zegeye et al., 2021), we show in detail that the appearance and functions of a telemetry network are like a supervisory control command and data acquisition (SCADA) network, and that SCADA architecture can be applied to a network. telemetry. In turn, this approach opens the door to a wealth of analysis, strategies and solutions for telemetry networks that have been developed entirely in the SCADA field. In our investigation, we visualized the current telemetry network. The idea is to build a general telemetry network security network test platform. The platform initially combines traditional network security control with the industrial control system framework (ICS-SCADA) built with telemetry components. One of the primary goals of our research is to provide a telemetry network architecture framework for our test platform to meet the requirements of current and future network operations. Describes and classifies the current modules and components of the telemetry network system. Describes the system architecture to help lay the foundation for the analysis of telemetry network system vulnerabilities that lead to security solutions. This is our contribution to the broader telemetry network security community, where we capture the reach of these networks and build this environment. This architecture will also allow us to explore machine learning and artificial intelligence to enable real-time data streams to predict unique traffic patterns in telemetry networks.

The proposed research focuses on network security solutions that are customized to the form and structure of telemetry networks, as well as the risks and vulnerabilities they face. The growth of the Supervisory Control and Data Acquisition (SCADA) system over the last decade has resulted in a slew of safety issues. The development of the Supervisory Control and Data Acquisition (SCADA) system in the past decade has created considerable problems related to its safety. Some of the reasons for its vulnerability to cyber-attacks include the implementation of open communication standards, the connection of control

systems to other networks, the limitations of existing security technologies, remote access, and the availability of control system technical information. Due to its important role in the industry, the security of the SCADA system is very important. Modern systems supporting SCADA are based on Internet Protocol (IP) and Ethernet technology. The application layer (including presentation and data model) is developing a specific SCADA protocol and using the IP protocol stack. SCADA systems are generally integrated into a public IP-based network. The network designed this way has certain weaknesses and vulnerabilities familiar to malicious users. The development of the Integrated Network Enhanced Telemetry (iNET) protocol and the use of network telemetry applications have introduced many potential network security risks inherent in modern networks.

APPROACH

The elements that would be tested in the VMware workstation include two hosts, switches, routers and firewalls. The need for two hosts is to see how the attacks will fair in both operating systems and give the user the option to experience both operating systems and research more with the operating system they are most comfortable with. The two operating systems are almost identical and to reduce configuration issues be sure to make use of the operating system that is easy for you. The switch used was the KVM (Keyboard, video and Mouse) switch to allow another user to access the machine. The switch is a Cybex Longview series that consists of units such as the advocent switch, the Longview transmitter, and the Longview receiver. For the router we would need to set up the connection to the first host network, and then to the second host network. Then stop the VMware DHCP server service, install the router software on the host system and configure networking in the first two virtual machines to use addresses on the appropriate host network. After that assign IP addresses and ping the router machines from the first and second virtual machines. For the firewall a different iso image file is required for its installation and setup. Configuration of the virtual network interface is the next step, then

the deployment of the firewall and installation. All these elements will be simulated on the host machines.

NETWORK TELEMETRY

Network Telemetry is defined as how information from various data sources is collected using a set of automated communication process and transmitted to receiving equipment for analysis purposes. While network telemetry is not new, it is becoming increasingly important as the volume of data continues to grow. Network telemetry collects data from different sources, pulls the information together and funnels it for easier analysis. It can also help administrators gain a better picture of the health of a particular device. Organizations can receive real-time information about the status of their devices, helping them perform more accurate and faster root cause analysis to pinpoint problem areas. Network telemetry can improve outcomes in use cases beyond COVID-19 response. For example, military operations often depend on the quick consumption and analysis of multiple data streams. Network Telemetry is a critical component of modern IT data center operation. Having visibility into what a network is doing and how it is being utilized is the basis for effective network automation and analytics. Telemetry, or streaming telemetry to be accurate, has the potential to help accelerate network troubleshooting, anticipate network capacity growth, and baseline network performance. The right kind of telemetry data enables network operators to address network blind spots proactively and keep their business systems operating efficiently.

A typical network telemetry setup consists of three key components which include Data exporter, Data Collector and Data Analyzer. Data Exporter can be any type of network device that generates data. In many modern telemetry systems, the user can configure the exact type of flow data that needs to be exported. Data Collector is the part of a network

management system that gathers data from one or more data sources, processes the data, and stores it in a suitable format. Data analyzer processes data from one or more data collector and provides actionable insight. Network telemetry uses a push approach achieving more efficient data collection. The data collector 'subscribes' to data from one or more data sources and is streamed network health and performance data in near real-time. Standards based data models allow the user to subscribe to specific data items they need, thus helping the data collector further achieve better efficiency and optimization. The telemetry system can be enhanced with data from multiple data sources. For instance, data from multiple networks, storage, and computing devices as well as other environmental data can be collected as time series data and correlated to provide system wide insights and analytics. The general telemetry architecture proposed consists of different test and Evaluation centers that are interconnected via the global grid. The global grid shows two T&E centers connected to the global grid. These two centers can communicate via internet which is secured via VPN across the global grid.

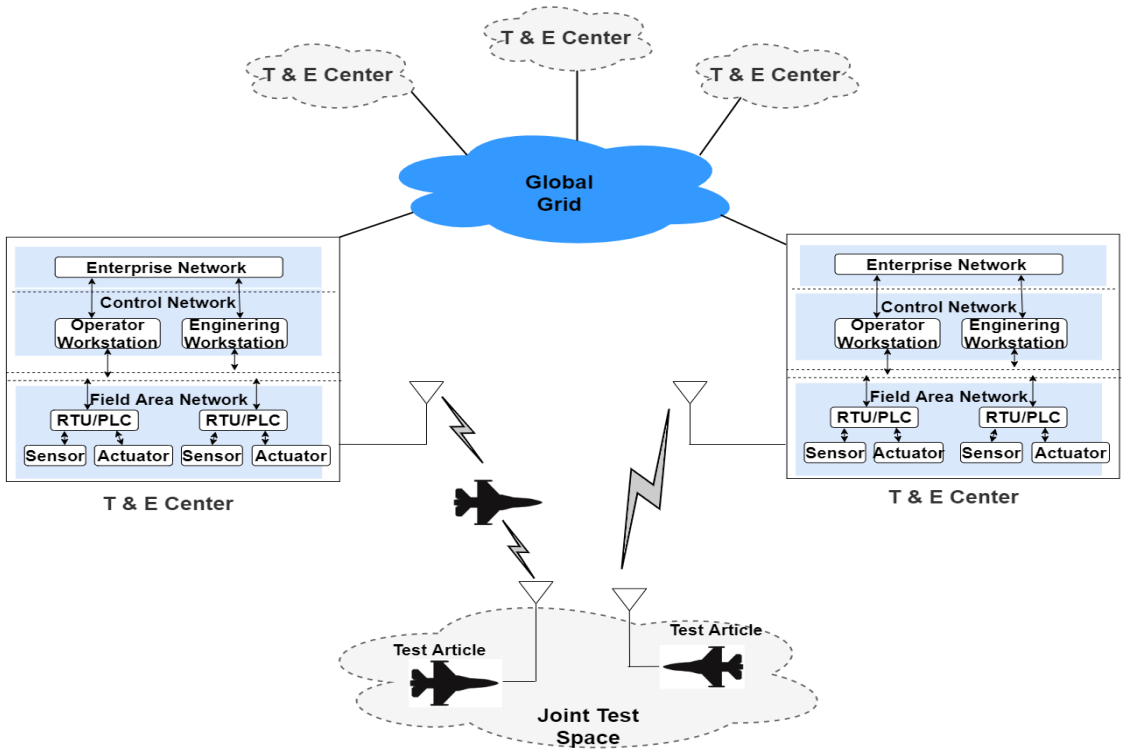

Figure 1. *General Telemetry Architecture*

TESTBED

The testbed consists of hardware and software that functions to form an isolated cyber security testing lab. The testbed includes a computer as the processor of the intrusion detection system. After the model is completed, this PC will become the main node for alarm data analysis and generation. The traffic generator is a software system that can construct effective network data packets. The streaming player can record network traffic for later playback. This allows small physical networks to appear larger by recording traffic from the larger network. The testbed will employ the use of a network switch in place of hubs, and the switch would allow simulation of multiple sub-networks using data routing between virtual local area networks.

TECHNICAL APPROACH/EXPERIMENT

A workstation being developed will support VMware network simulation. It will be outfitted with a high-performance multi-core processor, high speed RAM and hard drive. There are basic requirements for different components involved in the workstation mentioned above.

HARDWARE REQUIREMENT

Processor

For the processor, the system will require a processor launched in 2011 or later. For the 64bit requirement operating system, the host must use either an AMD CPU with MAD-V support or an intel CPU with VT-x support. If an Intel CPU is chosen, the user must verify that the VT-X support is enabled in the host system BIOS. When the operating system is installed, it performs checks to make sure the host system has a supported processor. The chosen CPU for this research was the Intel Xeon Scalable Silver 4114 Skylake 10-core 2.2GHz(3.0GHz) LGA 3647 85W Server Processor. It provides 10 cores of processing power which when overclocked can boost up to 20 threads that can be effectively utilized.

This processor is made for handling server-based program and workload. It has a higher TDP which means they generate more heat, the higher the clock speed the more heat gets generated. Stability and power efficiency are what is important when building a workstation computer that is one of the few reasons this processor was the choice. This processor also allows for higher maximum capacity, more memory channels and ECC (error checking and correction) memory support, which eliminates the most common cause of software crashes which is corrupted memory data.

Figure 2. *Intel XEON Silver Processor*

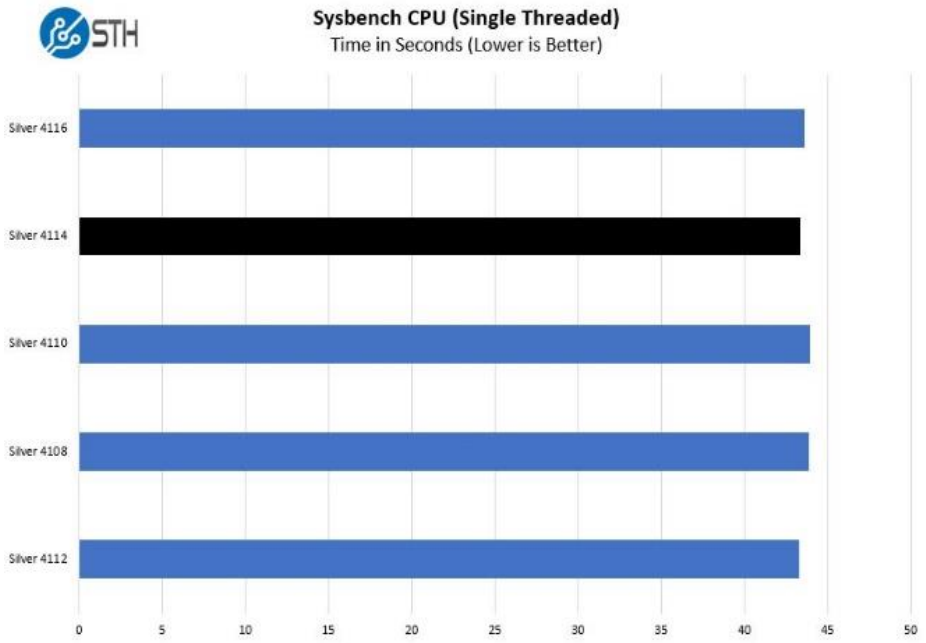

Figure 3. *Comparison of CPU Thread Performance*

Memory

The host system must have enough memory to run the host operating system, the guest operating systems that runs inside the virtual machines on the host system, and the applications that run in the host and guest operating system. For this workstation, the choice was the SAMSUNG 256GB RAM (4x64GB) DDR4- 2666MHz. This was chosen because of the large memory it provides and it has the required ram speed of 2666MHz which would be more than sufficient for the workstation output. The minimum memory required on the host system is 2GB which means 256GB would be more than enough. If the host machine has a physical solid-state drive, the host informs guest operating systems they are running or an SSD.

Figure 4. *Samsung 256GB 4x64GB DDR4 RAM*

Disk Drive Storage

For the storage system, the host must meet certain disk drive requirements. Guest operating systems can reside on physical disk partitions on in virtual disk files. For the hard disk requirement, both NVMe and SATA drives are supported and should have at least 1GB free disk space is recommended for each guest operating system and the application

software used with it. For basic installation, 1.5GB free disk space is required on both windows and Linux. For this workstation, we chose the WD Blue NAND 2TB internal SSD-SATA III 6GB/s Solid State Drive. This storage capacity will allow to all documents and server to get the required storage needed to complete their tasks.

Figure 5. *Western Digital Solid State Hard Drive*

Motherboard

For the motherboard, we chose the ASUS Z11PA-D8 CEB Server Motherboard Dual LGA 3650. This motherboard was chosen because of the compatibility with the CPU to ensure the smooth running of programs and fluency in operation. It is a dual channel motherboard that can accept two Intel Xeon CPU's and it is able to contain up to 8 RAM sticks. For this motherboard, ASUS Z11PA-D8 server motherboard fan and heatsink would also be needed to cool the system and the arctic silver 5 high density polysynthetic silver thermal compound is the thermal paste used to cool the CPU. A decision had to made between an ATX motherboard and an EEB motherboard. This was as a result of the space in the case, the ATX is a relatively small motherboard and would fit in most cases, but the EEB would be more compatible with the purpose of the research which is to build a server type workstation testbed.

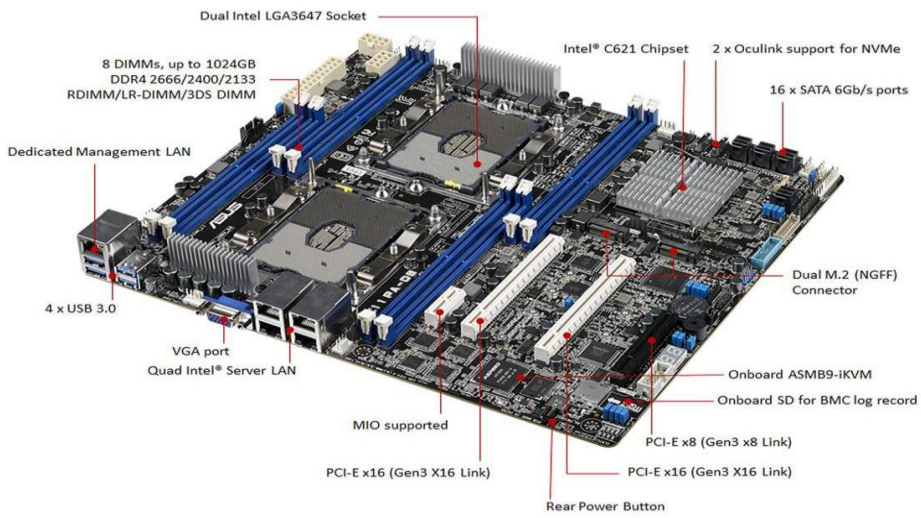

Figure 6. ASUS Dual XEON CPU Motherboard

OTHER PERIPHERALS:

Some other important components that were selected were the GIGABYTE GeForce GTX 1050Ti 4GB GDDR5 PCI Express 3.0 graphics card and 1200W Power supply unit.

ANALYSIS AND SCHEDULE

In this project, the workstation will be built with this hardware in mind. During this shortage in Computer peripherals, the hardware build process has been drawn back but is picking up pace again, by July we should have all components assembled and in august the machine should be built and functioning well.

CONCLUSION

This paper introduces the hardware components that will be used in building and designing the workstation that will house the entirety of the project. The various hardware was assembled because they were compatible, and the connection is seamless.

ACKNOWLEDGEMENT

This work is funded by a grant from the International Telemetry Foundation (IFT). Authors and others WiNetS Laboratory members in the School of Engineering at Morgan State University thank the IFT for their support of this research.

REFERENCES

1. Co-operation, V., 2021. *Virtual Machine Features and Specifications*. [online] Docs.vmware.com. Available at: <https://docs.vmware.com/en/VMware-Workstation-Pro/16.0/com.vmware.ws.using.doc/GUID-5A20BB16-6400-4D4B-9ED2-66C5BE124285.html> [Accessed 23 June 2021].
2. VMware, vSphere. "Performance Best Practices for VMware vSphere 7.0, Update 2." *VMware*, 18 June 2021, www.vmware.com/techpapers/2021/vsphere-esxi-vcenter-server-70U2-performance-best-practices.html.
3. Admin, Posted by. "Install PfSense Firewall in VMWare Workstation with Internet Access." *GNS3 Network*, 15 June 2021, www.gns3network.com/how-to-install-pfsense-firewall-in-vmware-workstation/.
4. Ward, Brian. The Book of VMware: The Complete Guide to VMware Workstation. San Francisco: No Starch Press, 2001.
5. Munro, Jay. "Virtual Machines & VMware, Part I." 21 December 2001 URL: http://www.extremetech.com/article/0,3396,s%253D1027%2526a%253D20 322, 00.asp
6. Daryl Moten, Testbed Server Upgrade Design , 23 June 2021.
7. Network telemetry is becoming the new normal -- GCN
8. Network Telemetry - An IT Executive's Guide | Netreo
9. Wondimu Zegeye, Andargachew Bezabih, Richard Dean, Farzad Moazzami, Mulugeta Dugda, "Modeling Telemetry Networks for Cyber Security Analysis", ITC 2021.