CYBER SECURITY ARCHITECTURE FOR NETWORKED TELEMETRY

Richard Dean PhD, Wole Akpose DE, Wondimu Zegeye DE, Farzad Moazzami DE
Department of Electrical and Computer Engineering
Morgan State University
Baltimore, MD 21251
Richard.Dean@Morgan.edu

ABSTRACT

This paper presents a Cyber Security Architecture for Telemetry Enterprise Networks. This work follows from Morgan's development of a Cyber Security Testbed for Telemetry networks. It follows from prior work [2] that shows how Telemetry Networks can be modeled after Supervisory Control and Data Acquisition/Industrial Control Systems (SCADA/ICS) which has received significant treatment in past decades. This work is specifically tailored towards Enterprise Telemetry Networks which envision the inclusion of multiple Test Articles spanning multiple Test Ranges over a wide geographic area. The cyber security implications of this structure are significant. The proposed architecture follows the 3 level structure proposed for SCADA/ICS networks. The emphasis here will be in managing the boundaries between each layer and across Test Ranges. The recommendations for SCADA/ICS are adapted to fit the unique applications and security issues for the Telemetry Enterprise.

INTRODUCTION

Telemetry systems have evolved over the past decades. Legacy telemetry was typically a closed system of sensors and radio links. These evolved into simple bus networks, networked Test Centers and now multiple Test Center Enterprise networks. Security issues for these systems began with closed, system-high approaches, added radio link encryption, but now face a fully integrated enterprise network without a clear strategy for security. As outside academics, we can only surmise that today's networked telemetry systems lack a comprehensive cyber security architecture that is uniquely fitted to the nature of these systems. This paper attempts to fill this gap by recognizing the similarity of telemetry to Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition Systems (SCADA), and by tapping into the extensive work that has been done on securing these networks. We also add best practices for cyber security features directed at the most serious threats face by today's network telemetry systems.

APPROACH

There is a large corpus of work in cyber security. It is one of today's most challenging emerging disciplines. Our approach is to focus on the intersection of cyber security for: IT Systems, ICS/SCADA systems and Telemetry systems. There are several well developed guidelines for the design of traditional IT systems from DoD, DoE and NIST [ref 1,2,3] that can guide the design of much of the enterprise. There are also several guidelines for the design of ICS/SCADA(ref 4,5] systems. In light of this best practice, our paper will assume these practices are in place and focus on the unique elements of networked telemetry and the most serious security threats to these networks.

NETWORKED TELEMETRY

Like so many other enterprises, the telemetry community envisions a highly networked environment to both enhance its scope and effectiveness. The Joint Mission Environment Test Capability (JMETC)[1], for example, has integrated operation of several remote Telemetry Instruments across multiple test ranges. Joint testing allows for the incorporation and integration of Test Articles over a wide geographic region that can emulate real operation conditions necessary for testing. Our model for such a scenario is shown in Figure 1 below. This shows two test centers connected over the internet to support a JMETC environment. Each Test Center is shown to have a 3 layer network based on ICS/SCADA [2] modeling of networked telemetry. The Enterprise Network represents public facing network serving the business functions of the test organization with a classical IT network. The Control Network represents a sub-network with a variety of engineering and operator workstations that control the telemetry operations. The Field layer network represents Remote Test Units and Programmable Logic Units that connect to the sensors and actuators in the test equipment.

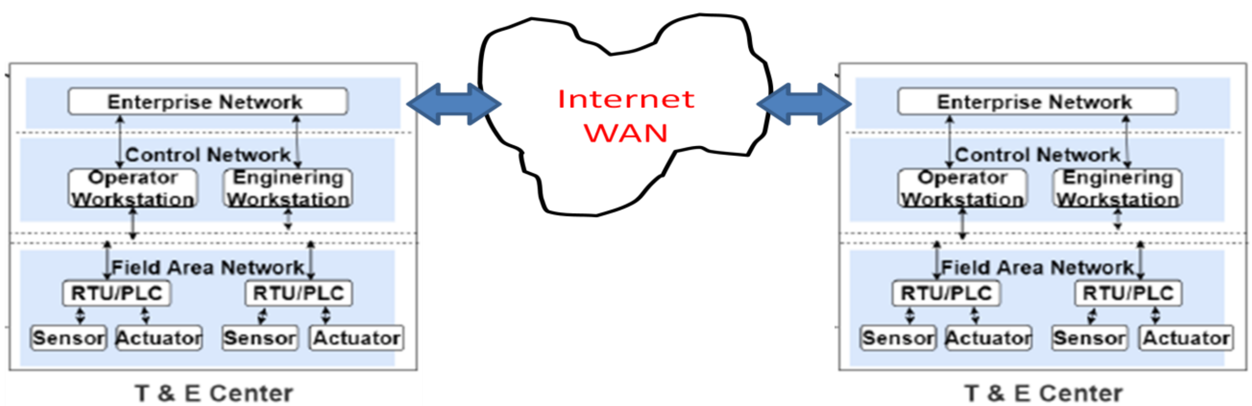

Figure 1 Networked Ted Environment

In support of this JMETC integrated environment, the Test and Training Enabling Architecture (TENA) architecture was developed with middleware, object models, tools / utilities, and collaboration capabilities. These structures require a new look at the cyber security issues inherent in this strategy.

THE NETWORKED TELEMETRY DIFFERENTIAL

This approach is highlights on the cyber security differential that networked telemetry represents. This includes:

Operation across WAN networks – Fully integrated operation across the WAN(internet) introduces additional complexities to a security design. The potential surface of attack expands dramatically. The Test Center is opened to another domain having security architectures with different weaknesses and users with different privileges. It remains to limit access and least privilege in this environment.

Four Layers of operation and design to consider – Figure 1 shows how 3 layer networks are connected over a WAN to create four layers of operation and the need to distinct security solutions for each layer.

The nature of the cyber threat – Threats to the telemetry enterprise might stem from nation states, casual hackers, criminal hackers, malicious insiders and or vendors.

> **Nation states and sophisticated terrorist organizations -** represent sophisticated, motivated and resourced adversaries.
>
> **Inside Attacks** - Penetration of DoD and vendor communities has been widely published. Such adversaries will spend years to infiltrated targeted networks and deeply embed attacks that are difficult to detect. Our work must assume that these attacks are present within today's telemetry networks.
>
> **Insiders** – We cannot expect that our networked telemetry networks will be free from traitors who will compromise our system for either personal gain or attention. USAF National Guard soldier Jack Teixeira, and NSA contract employee Edward Snowden are two examples of insiders that compromised security.
>
> **Vendor and Supply Chain** – Our systems are configured with components from everywhere and operated with teams of vendors. With much of the core components of both our telemetry systems and enterprise compute and network infrastructures coming from disparate foreign suppliers, the supply chain has become a major source of vulnerability as well.

STRATEGY FOR INSIDER DETERRENCE

The security challenges presented by Networked Telemetry are extensive and so our architecture needs multiple structures to succeed. Here is our strategy.

> Use Cryptographic protocols as a Backbone – Cryptography can provide high assurance, zero trust solutions to sensitive applications where Confidentiality, Integrity and Availability can be assured.
>
> Use DoD approved IPSEC and TLS – These protocols are readily available and support custom Public Key Certificate solutions coupled with encryption with high confidence.
>
> Use Trusted Certificate Authority – A trusted Certificate Authority will manage the credentials and privileges needed for a zero trust environment for users, applications and domains. The protocol enables customized choices of the public key distribution method, encryption algorithm, signature and hashing schemes.
>
> Cryptographically Secure Backbone – Establishes and manages boundaries for the Test Center, Zone, User, and Application. Test Center Control layers can be provided end to end authentication and confidentiality to enable the integrated Test Center operation envisioned by JMETC.

Segment network elements – Beyond cryptography, a good security architecture will physically and logically separate network elements by function, privilege, and sensitivity. This creates boundaries that enforces policy and limits visibility and migration.

Strong Authentication across Boundaries – Beyond the IPSec and TLS cryptographic structures, a zero trust environment is developed by adding traditional network tools to build a zero trust environment. Insider attacks are deterred by firewalls and guards that are customized for each layer and zones within layers. The elements can create boundaries based on multilayer inspection of packets and threads. The policies and filtering structure can be constrained to allow only specific applications, protocols and addresses. This will severely limit the attackers options to find and attack sensitive applications.

Identify and Thwart Insider Attacks – This strategy includes additional elements to identify and thwart insider attacks each customized to the layer, zone and function in the network. Intrusion Detection and Protections (IDPS) systems are added at each layer/zone. These elements can identify known attacks or anomalies, log the event, and prevent the attack. The compliment to the IDPS is the Honey Pot which attracts attackers with accessable addresses and availability. Honey Pot detection of attacks come with high confidence and an ability to find new attacks and attackers. A Tripwire product is added for detecting, assessing, reporting and configuration changes. Finally a Security Information Manager (SIEM) system will capture all security related events in the network to help establish the health of the network and aid recovery in the event of compromise.

We propose a zero trust architecture and design around the four zones of the telemetry enterprise; the telemetry(field zone), the control (management zone), the general enterprise zone and the user zone which will encompass casual users and the extension to general WAN or external (internet) users.

The cornerstone of zero trust is access management (for users, devices and codes) as well as continuous monitoring. Access management include holistic credential management using a DoD certified credential management solution; transport protection tools as recommended by DoDD 8420.01. All TLS and IPSec solutions must be at least FIPS 140-3 compliant.

Continuous monitoring and logging is a key resource for effective IDPS, SEIM and firewall solutions. Firewalls are the primary intrusion prevention technology and their effectiveness are enhance by robuts machine learning algorithms.

Integrity management solutions (IMS) such as tripwire serves to help identify and trigger changes to inspected data. IMS settings and placements should reflect the sensitivity of the mission (and data). IMS can monitor changes to logs, system configurations and other data. This can be a key tool in identifying insider attacks as well as incoming attacks. IMS systems should also incorporate anti-spoofing techniques.

Other components of a robust zero trust architecture includes a Security Operations Center which incorporate SEIMS and a security monitoring and control consoles.

FOUR LAYER APPROACH

The Networked Telemetry solution envisions distinct four layers. These are:

- WAN – Public Internet, Open, Unsecured
- Enterprise Layer – The organizations interface to the internet and business operations
- Control Layer – The subnet for Test Center's operational IT and control of the field layer
- Field Layer - The connected telemetry elements

We approach this design by describing features included in each layer following the overall strategies from above for each layer. A JMETC integrated solution would replicate the approach at each organization and Test Center.

WAN Layer - Issues and Approach

The WAN layer represents the connection of Test Centers and Vendors across the internet. Our strategy for this layer is shown in Fig. 2.

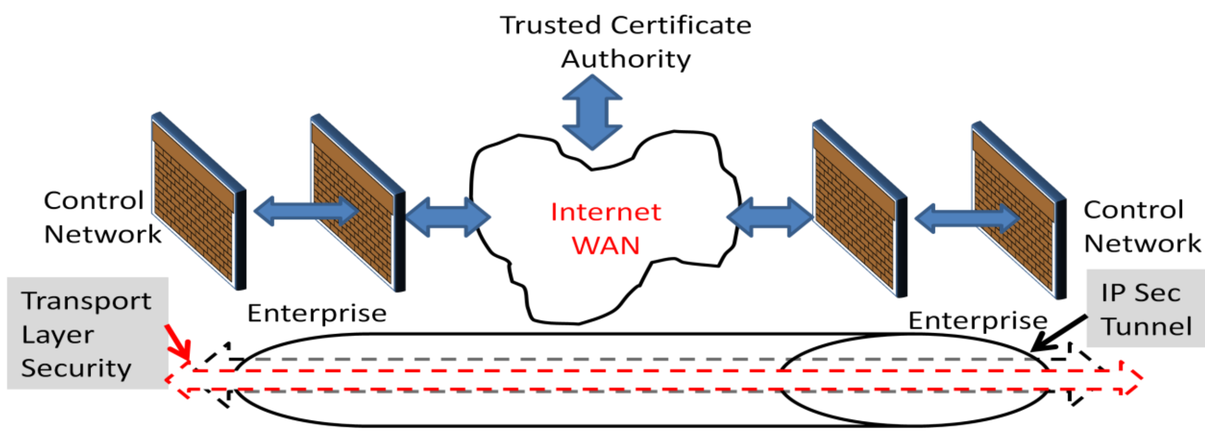

Figure 2: WAN Architecture

This strategy envisions a connection among Test Centers and Vendors over the internet. Security is provided with two cryptographic security tunnels that provide the backbone of the network. Figure 2 shows an IPSec tunnel connecting two Test Centers. Note that the IPSec protocol is terminated at both ends at the boundary of the Control Layer Network. The IPSec tunnel extends the security domain of the two control layer networks across the WAN with cryptographic assurance. The second tunnel is provided by a TLS which extends from two peer applications at each Control Layer Network. This is independent of the IPSec tunnel and protects access and traffic from all other entities. This is a tunnel within a tunnel. Note that each of these protocols are supported by a Trusted Certificate Authority over the WAN. It is assumed that none of these protocols are permanent, but are established and terminated for scheduled telemetry events.

Enterprise Layer Network - Approach and Issues

The Enterprise layer Network is the internet-facing network for the organization and supports the business of the organization. While not necessary for networked telemetry, the presence of an Enterprise layer is both a common and practical reality. It is common for attacks to originate in this layer as it is most accessible, more diverse, and less protected than the other layers. Our approach to security for this layer follows from best practice for DoD and Federal agencies. These are captured in Table 1 and left to the reader to pursue in detail.

REQUIREMENTS	PROCESS	CONTROLS
FIPS 199 Sec Cat Fed Information Systems	DoD Cyber Reference Architecture V5.0 [3]	NIST 800-53 Security Controls Fed Info Syst
FIPS200 Sec Req't Fed Information System	NIST Engineering Trust Worthy Security System[4]	SANS 20 Critical Cont Effective Cyber Def
	NIST 800-82r2 Guide Industrial Control Sec [5]	CIS Critical Security Controls V8
	DoE C2M2 CyberSec Capability Sec Model [6]	
	NIST Framework Impr Critical Infrastructure [7]	

Table 1 Best Practice Requirements, Processes, and Controls

Following the strategy identified earlier we organize the enterprise into multiple security zones shown in Fig. 3

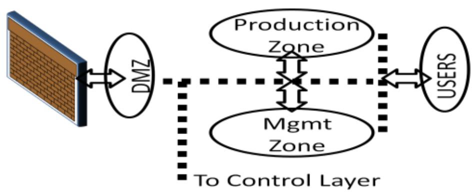

Figure 3 Enterprise Layer Architecture

The security elements included in these zone are shown in Table 2.

DMZ	USERS	Production	Management
Firewall	Firewall	Firewall	Firewall
IDPS	IDPS	IDPS	IDPS
Honey Pot	VLAN	Servers	TripWire
Proxy	TripWire	TripWire	SIEM

Table 2 Enterprise Network Zones and Security Features

Control Layer Network - Approach and Issues

The Control Layer network is the specialized layer in Telemetry networks where managers and operators control elements and capture and process data in the Field Layer. Additional security features are added here consistent with our zero trust model and the strategy described above. The architecture for the Control Layer is shown in Figure 4.

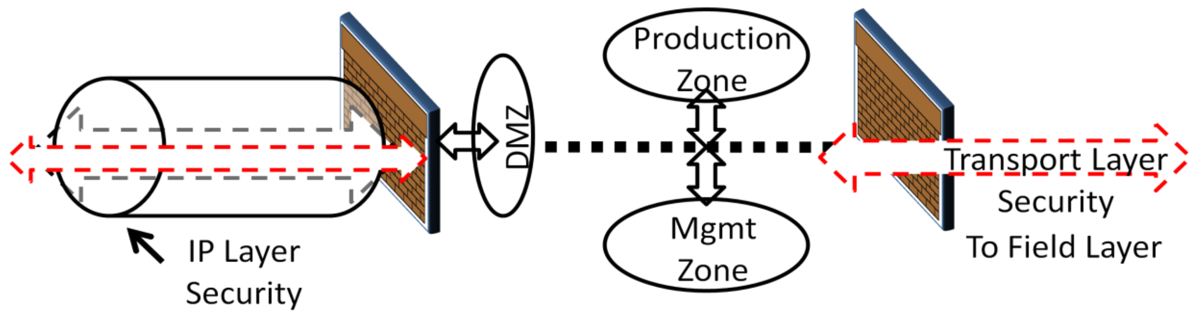

Figure 4 Control Layer Security Architecture

As described above the traffic from other Test Centers and vendors are carried under a TLS protocol within an IPSec tunnel on the left. The IPSec protocol is terminated at the Control Layer firewall and the TLS traffic is carried into the Prodcution Zone to a peer entity, or perhaps to a Field Layer entity exiting on the right. Likewise TLS traffic may originate in the Production Zone and exit to the Field Layer. The security features included in the Control Layer Zones are shown in Table 3

DMZ	Production	Management
Firewall	Firewall	Firewall
IDPS	IDPS	IDPS
HoneyPot	Data Server	TripWire
	Tripwire	SIEM
	Honey Pot	Security Manager

Table 3 Control Layer Zones and Security Features

Field Layer Network - Approach and Issues

The Field Layer networks are a mix of legacy and modern systems that were never intended to be fully attached to networked applications. It is difficult to definitively quantify these networks collectively so our strategy needs to be adapted to specific configurations. Our overall strategy however can be applied with these systems with careful attention to their limitations. The architecture for the Field Layer is shown in Fig. 5. This shows TLS traffic coming into the Field Layer where is can be terminated at the peer application in the Production zone. The Field Layer has a local component which would be the Telemetry Ground Station(GS), and a remote section which would be the Test Article (TA). A Management Zone is included here which would include Security Manager, SIEM, and TripWire.

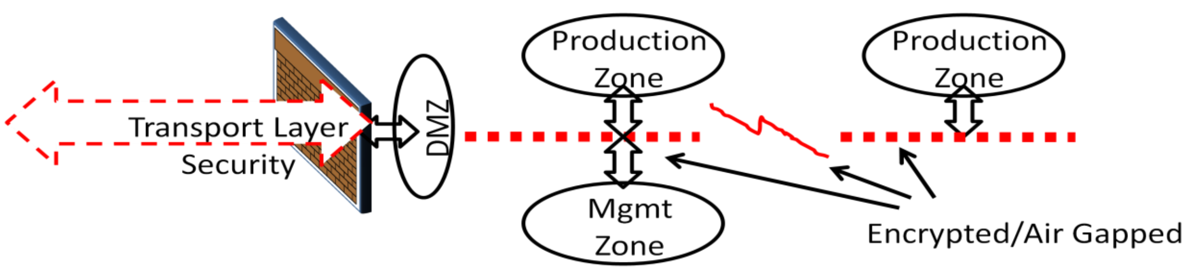

Figure 5 Security Architecture for the Field Layer

The allocation of security features are shown in Table 4. These should be taken as objective features where the functionality may be integrated into other modules.

DMZ	Production	Management
Firewall	Firewall	SIEM
IDPS	TripWire	Traffic Monitors
Honey Pot	Message Authentication	Security Manager
		TripWire

Table 4 Field Layer Security Zones and Features

Illustration of this approach will come from two examples, the legacy 1553 field layers and modern iNET field layer. From Figure 5, the Ground Station (GS) represents an opportunity for security enhancement. The GS boundary system shown as the DMZ can incorporate a firewall, IDPS and Honey Pot features.

Legacy 1553 Bus LAN Approach

The 1553 Bus LAN structure has been foundational to telemetry systems for decades and is installed in a number of existing systems. The 1553 Bus was intended for use in trusted closed systems where few security features at the TA. A security strategy for this system means adding features where possible without major disruption. Assuming that the GS security features are in place, two enhancements are suggested. The first is an enhancement in Message Authentication which would verify the source of all messages. A Message Authentication Packet could be added to all sensitive 1553 packet transmissions with a secure hash in a supplemental data packet. The second enhancement would come in the form of Traffic Monitoring. This could be incorporated into the Bus Monitor which captures all of the bus traffic. The Traffic Monitor could enhance security with the identification of unauthorized, anomalous, or dangerous traffic on the bus.

TCP/IP and iNET LAN Approach

The presence of a TCP/IP fabric at the TA enables the addition of security features within the framework of these network protocols. Assuming the GS security features are present as above the addition of Message Authentication and Traffic Monitoring is indicated. In this case the choices are straightforward. The TLS protocol can be readily added to the fabric of the TCP packet structure enabling both authentication and data integrity. Short of that a secure hash can be appended to sensitive packets to assure authentication and data integrity. In addition a traditional Traffic Monitor with classic IDPS capability is indicated.

CONCLUSIONS

The networking of today's telemetry as envisioned for example by the JMETC with the integration of multiple Test Centers with the ability to remotely configure and operate test resources requires a new look at the cyber security of these systems. This paper presents a strategy for such an architecture. The focus here is the unique issues within telemetry applications and networks as well as the unique threats presented. A focus on the insider attack created emphasis on developing a zero trust environment where insider attacks would be greatly diminished. This is just a start. We hope this paper inspires interest in this important topic.

REFERENCES

1.The Tena And Jmetc Solution For Telemetry In Distributed Ranges And Facilities Gene Hudgins and Juana Secondine ITC 2017
2. Modeling Telemetry Networks for Cyber Security Analysis, Zegeye, W, International Telemetering Conference 2021
3. DoD Cyber Reference Architecture V5.0 https://dodcio.defense.gov/Portals/0/Documents/Library/CS-Ref-Architecture.pdf
4. NIST Engineering Trust Worthy Security System https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1r1.pdf
5. NIST 800-82r2 Guide Industrial Control Sec https://csrc.nist.gov/pubs/sp/800/82/r2/final
6. DoE C2M2 CyberSec Capability Sec Model https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2
7. NIST Framework for Improving Critical Infrastructure https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf