SECURITY ARCHITECTURE FOR TELEMETRY NETWORKS

Daryl Moten, Sekaran Jambureskan
Faculty Advisors: Richard Dean, Farzad Moazzami, Yacob Astatke
Morgan State University
Baltimore, MD 21251

ABSTRACT

This paper develops a Security Architecture for a network of telemetry networks as is envisioned for future telemetry systems. We show a model for an aggregation of Test Centers as might be deployed for the envisioned network telemetry. We build a security architecture grounded in best practices for security design as captured in the NIST family of standards and guidelines captured in the SANS 20 critical controls.

TELEMETRY NETWORKS AND SECURITY THREATS

Today's telemetry networks are transitioning from a hub and spoke links to an integrated network of telemetry networks. This transformation promises great improvement in performance, capability, and efficiency. Figure 1 illustrates the nature of an interconnected telemetry environment where multiple test ranges collaborate on a test mission. A networked radio environment as proposed in the iNET standard, for example, offers the potential of increased data rates and more timely access to test data.Connecting across test centers enables use of remote resources and shared testing for complex systems. These benefits come at a price. The connection of previously dedicated links to data networks, which are connected over the internet, dramatically expands exposure to threats.

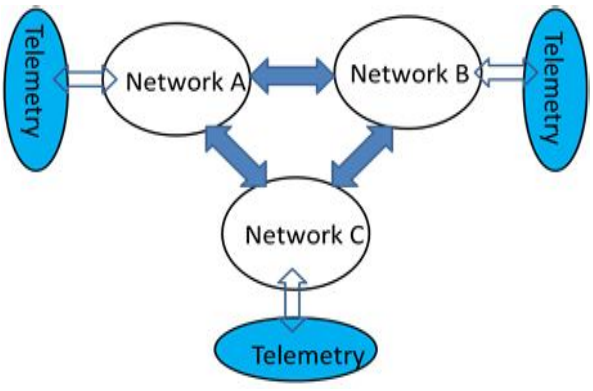

Figure 1: Interconnected Telemetry Network

Cyber Security threats are pervasive. Attacks by cyber hackers, criminal organizations, and nation states are reported in the papers every day. This prompted the director of national intelligence, James Clapper, to tell a congressional committee [1] "We all recognize [cyber attacks] as a profound threat to this country, to its future, to its economy, to its very being". Defense infrastructure and contractors are a prime target for nation states. It has been reported that China [2] is actively attacking defense facilities to capture technology for emerging weapon systems. Telemetry networks represent an attractive target for such attempts. Furthermore, the nature of modern cyber attacks are not limited to probes at the network boundary. The best attacks manage to leverage internal network resources to find an exfiltrate sensitive data.

SECURITY SOLUTIONS AND THE 20CRITICAL CONTROLS

Network Security solutions are complex, evolving and extensive. There is little science to Network Security and a plethora of ad hoc solutions. There are so many strategies proposed to address this that confusion prevails. Some have focused on a few components such as intrusion detection or the firewall, while others have an abundance of overlapping and conflicting schemes. For this reason a complete set of features organized into an architectural framework is proposed here as a strategy. We chose the SANS 20 Critical Controls [3] as a definitive set of requirements and features. This work is an aggregation of work that reflects the best practices from NIST, NSA and Industry experts. We take these controls and then organize and map them into an architectural framework based on the best security design principles. These 20 Critical Controls include:

1. Inventory of Authorized and Unauthorized Devices – this detects unauthorized penetration of devices on to your network by intent or by error.

2. Inventory of Authorized and Unauthorized Software – this detects insertion of unauthorized software on your machines by intent or by error.

3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers – this verifies that hardware and software have the latest security updates.

4. Continuous Vulnerability Assessment and Remediation – these are the tools that find weaknesses in your network including your network devices and host devices. Such tools can be centralized or distributed, and include alerting and remediation..

5. Malware Defenses – these are the various security software tools that find malware like viruses and worms, or attacks like port scanners. These include virus scanners, Intrusion Detection and Prevention Systems (IDS, IPS), and firewalls that can be at multiple locations in the network tailored to the domains and application.

6. Application Software Security – these are all the processes, tools and testing needed to design and test software for high assurance. These include the training and skill in personnel developing software as well as the processes to validate software developed by third parties.

7.Wireless Device Control – these are the tools needed to detect and mitigate the unauthorized connection of wireless devices to the network.

8. Data Recovery Capability – these are the capabilities needed to capture, store and recover data that might be compromised by a successful attack of the network.

9. Security Skills Assessment and Appropriate Training to Fill Gaps – these represent the policies and practices of the network owners to insure that the necessary security skills and awareness are present at all levels of the organization.

10. Secure Configurations for Network Devices such as Firewalls, Routers, Switches – these are the tools necessary to test and verify that all networks devices are protected from the latest potential attacks.

11. Limitation and Control of Network Ports, Protocols, and Services – these are the tools necessary to limit and manage access to sensitive machines on the network from potential internal and external attackers.

12. Controlled Use of Administrative Privileges – these are the tools necessary to manage access control to sensitive machines to limit access to authorized users and to monitor all access.

13. Boundary Defense – these are all the tools necessary to isolate the internal network from the external network with mechanisms such as firewalls, DMZ;s, IDS, and proxies.

14. Maintenance, Monitoring, and Analysis of Security Audit Logs – these are the tools and processes necessary to manage security for the immediate and long term potential for security compromise.

15. Controlled Access based on the Need to Know – these are the tools necessary to insure that sensitive information is available only to users with the necessary authorization.

16. Account Monitoring and Control – these are the necessary tools and processes needed to insure that only current and authorizer users have accounts on the network.

17. Data Loss Prevention – these are the necessary tools needed to identify, deter, and recover from the exfiltration of sensitive data to unauthorized parties.

18. Incident Response Capability – These are the policies, practices and resources needed to provide timely responses to a security compromise in the network.

19. Secure Network Engineering – these are the policies, practices, and resources needed to maintain a skilled and active technical community to design and manage sensitive networks.

20. Penetration Tests and Red Team Exercises – these are the practices and resources necessary to maintain an independent skilled team of expert who routinely test the networks security health.

These controls are useful in that each addresses a set of potential attacks, includes a set of recommended tools to implement the control, and ways to test their effectiveness. These controls are better seen in the context of a typical network. For this purpose we organize these controls into network elements as shown in figure 2. There are four segments shown in figure 2 for this structure into which each control may be mapped. This mapping is illustrated in figure 3 and summarized below by the five elements.

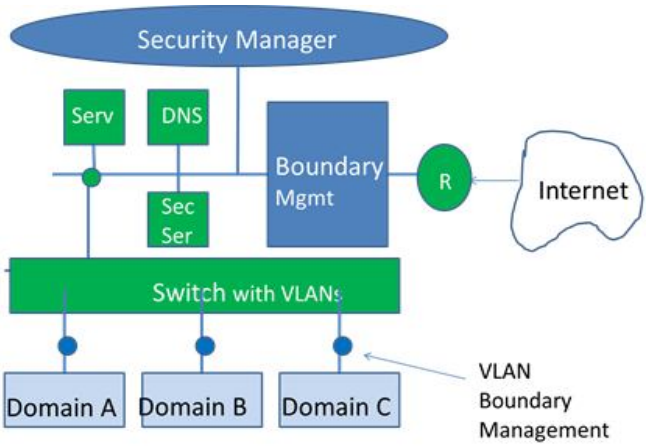

Figure 2: Security Controls Placement

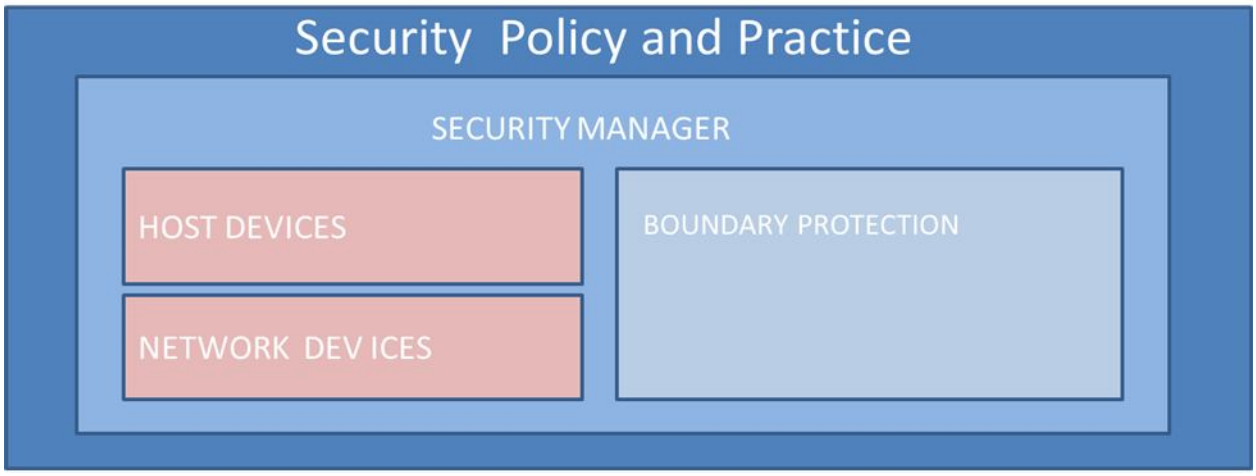

Figure 3: Security Controls Mapping

Security Policy and Practices – These are the set of controls that are endemic to the operation of the enterprise that owns the network. These include controls 9, 18, 19 and 20. Note that these controls reflect capabilities of the network owner and are not present on the networks as hardware or software.

Security Manager - The security manager consists of hardware and software within the network in the background that executes and verifies security controls. These include controls 1,2,3,4,6,7,8,10,11,12, 14, 15, 16. Note that these capabilities might be bundled into several hardware and/or software packages that operate collaboratively. Several are configured to control and collaborate with packages on hosts, network devices, and servers.

Boundary- These are controls that are included in hardware and software elements that reside at the boundary between the inside and the outside network. These are the classical security mechanisms such as firewalls and DMZ's that isolate the inside network from the outside internet. These boundary capabilities collectively satisfy the controls below. Note that these controls may map into several mechanisms that might be configured in numerous ways. The

proposed architecture that follows is a preferred ways to execute these controls. These include controls 5, 10, 11,12, 13, 17, and 19.

Network –these are the hardware and software components that enable the network to operate and include the routers, switches, hubs, and servers on the network. These include controls 3, 4, 5, 7, 10, 11, and 19 which are Secure Configurations; Continuous Vulnerability Assessment; Malware Defenses; Wireless Device Control; Secure Configuration of Network Devices; Control of Network Ports; Secure Engineering, respectively.

Host - these are the controls that reside on each host machine for users and servers. These controls are hardware and software that work independently or in conjunction with the Security Manager, e.g., inventory of hardware and software. These include controls 1, 2, 3, 4, 6, and 17.

ARCHITECTURE

The 20 Critical Controls identify security features and constraints, but do not describe or imply the structure needed to support these controls. This section now proceeds to develop a network architecture where these controls are populated. Together these represent a network security architecture that can inspire real hardware and software designs.

Design Principles

While agreement on security design detail is absent, there is clear consensus among security experts on security design principles capture in the NIST family of standards and guidelines. These include:

Boundaries – Security design follows from the definition of clear boundaries in software, systems and networks. Boundaries and associated gateway management enable design, analysis and verification of security properties. In the context of this work we develop a set of domains within the network, and boundaries among these domains that maintain their security integrity. Security design follows from the constraints established by these boundaries.

Security in Depth – This follows a long tradition in security design. It assumes that security failures are common and that high assurance security design develops layers of security, where each layer is independent, and all layers must be compromised for a security failure to occur. In this context the probability of a security failure, Pf, is the product of the independent layer failures ,Pf_n, which for n layers yields to$Pf = \prod_n Pf_n$

This creates the illusion of strong security solutions from multiple sub-layers. In practice it is difficult because independence of layers is difficult to design and harder yet to prove. In this architecture security in depth is accomplished by the creation of multiple domains and boundary controls such that multiple boundary security failures are necessary for a successful attack.

Verification and Risk Management – Security design verification represent a final layer for each security sub-layer. Security designs are only effective if the design is present, active, and functional. In operational systems a verification function tests these properties before during and after operations. This verification operates at multiple levels, from the hardware and software module, to the subsystem and system. Included in the 20 Critical Controls are numerous

verification functions. These include control 4, continuous vulnerability assessment, control 10, up to date secure configuration of hosts etc., and control 14, maintenance of security audit logs.

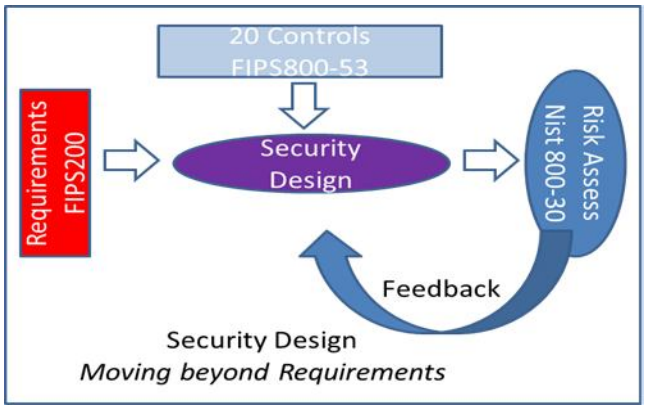

Figure 4: Security Framework

NIST and IBM Redbook Design Methodology [4] – with the constraints and requirements set by the 20 Critical Controls, and with the design principles established above, the next step is a design methodology. There is a large set of design guides available in the public domain but few if any methods that can be applied systematically. The NIST [5,6,7] family of standards and guidelines represent the best overall design guidance. The composite of guidance from NIST approaches the methodology shown in figure 4 and will be used here. A similar framework appears in the IBM RedBook [4].

Best Practice – Security designs are ephemeral. Attacks, applications, and tools change on a regular basis. In 2005, for example, most attacks and solutions were focused on boundary devices while in 2014 emphasis has moved to application software vulnerabilities. The notion of Best Practice captures a methodology that varies dynamically over time with ongoing peer review and support.

DESIGN

ORGANIZATION OF DOMAINS

Security design is driven by organizing users and data into domains by virtue of a common set of privileges, function, and location in the network. Domains enable the development of security policies that can be enforced at domain boundaries. Such policies may prescribe who has access, allowable packet types, and required security features. By organizing entities into domains more sensitive functions and data can be isolated from less privileged users and functions. For telemetry network five distinct domains are established as shown in figure 5. These include:

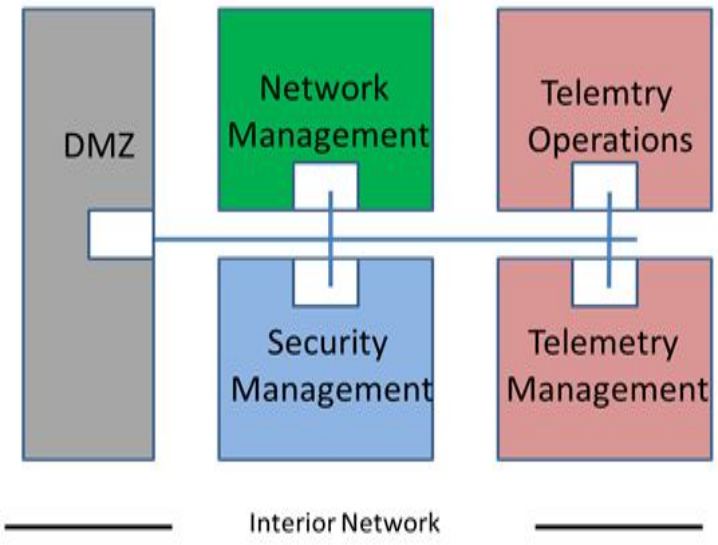

Figure 5: Distinct Security Domains

The Boundary Network – This is a boundary network which separates internal functions and elements from the outside internet users. This will typically host a DMZ, outside service web servers, outside mail servers and proxy servers. Boundary security devices such as firewalls and intrusion detection systems are normally part of the boundary network.

Network Management – This is the collection of entities that manages the operation of the overall network such as the routers, switches and Domain Name Server.

Telemetry Operations – These are the operational telemetry elements including the links and networks associated with the telemetry.

Telemetry Management – These are the networks that host the telemetry developers, managers, and operators that configure and manage telemetry operations.

Security Management – These are the elements of the network that configure and manage the overall security of the network.

Note that each domain in the network may be physically or logically isolated from the other domains. Such isolation can include separation by physically separate LAN's or by virtual VLAN's incorporated into network switches. This separation will also include a boundary gateway. In this context the gateway would incorporate security mechanisms customized for this gateway between domain (i) and domain (k) where the connection (i,k) is established. A gateway system might include a firewall, intrusion detection, and IPSec. Two cases of boundary gateways can be developed. The first case is the Boundary network and gateway between the outside network (internet) and the inside sub networks (domains) as illustrated in figure 6. This network includes services that connect to the outside internet such as the mail server, domain name server (DNS), a web server, and proxy servers. These are services that are especially subject to attack and are isolated into a boundary network referred to as the DMZ. These also include a firewall at both the input to the DMZ and the output to the sub-networks. These firewalls are different in that they apply different rules and filters to allow the traffic beyond the firewall in both directions. The DMZ also includes an Intrusion Detection System and a Honeypot which work in tandem to identify traffic and attack conditions on the boundary. The focus of this boundary network is to isolate more sensitive domains from direct attacks and to place more outside facing servers away from sensitive networks. The second case is the boundary to the sub-network or domain as illustrated in figure 7. This gateway is also connected through a firewall. This firewall is customized to this specific domain and can have rules and filter for each of the other domains tailored to the specific

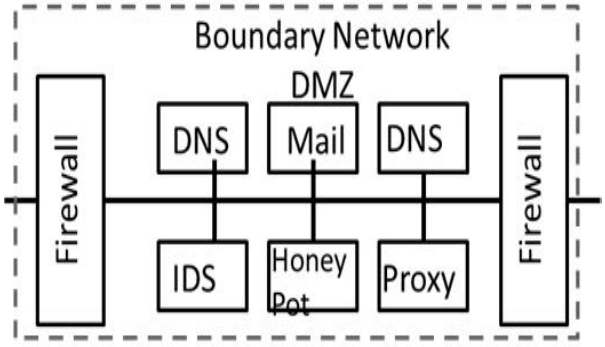

Figure 6: Boundary Design 1

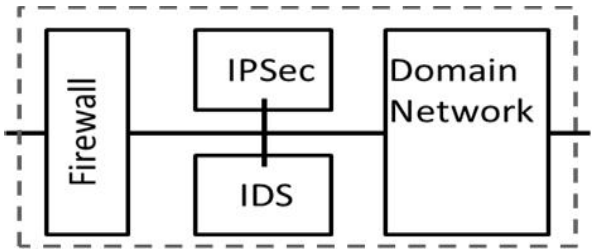

Figure 7: Boundary Design 2

security needs of the domain. Telemetry operation sub-networks may limit traffic only to the telemetry management domain even though it is logically connected to the other domains, and even though it is less sensitive than the security manager, or may limit the packets from the Security Manager to a small subset of packet types from specific network addresses. The domain boundary also includes a separate intrusion detection system (IDS) which is tailored to the traffic and features of this domain. The boundary may also include IPSec which would create a virtual private network with other domains, or peer domains on other networks. With IPSec in place the firewall might severely limit traffic to only domains with a peer security relationship.

SECURITY MANAGEMENT DOMAIN

Critical to this architecture is a security management domain which can configure and deploy the security controls identified above. A suite of hardware and software security applications are envisioned for this domain. Its operation and management would be severely limited by its boundary gateway which would limit access to a small set of security manager administrators, and to authorized traffic to other domains. The firewall and IDS associated with the Security manager would be narrowly configured to limit traffic to authorized security applications and administrative controls. As seen above the Security Manager hosts many of the security applications dictated by the 20 Critical Controls. These controls might be separate applications, or more likely, bundled into a security suite. Think of the Security manager as a hydra of links the reach into the system and initiate, probe, and validate the security status of the system. This manager is at once highly protected from access by other sub-networks, and yet connected to the rest of the networks. This is made possible with highly refined firewalls and security associations (with encryption) to the various security modules distributed over the network. The Security manager is also the place where a Security Operations Center (SOC) would reside with visualization of the security status of the many applications, and administrators at the ready to address security alerts.

HOST OPERATIONS

The host operation would include user host machines and applications as well as servers within the network. The host machine may also include boundary security features as shown in figure 8. These may include yet another firewall that is tailored to the specific applications and vulnerabilities of this host. If for example the host was a sensitive administrator in the Telemetry management domain, it might limit traffic from all other domains and peer domains from other telemetry networks by the incorporation of a Secure Socket Layer (SSL) or IPSec (Virtual Private Network) requirement. This would allow only connections to other authorized telemetry centers and applications.

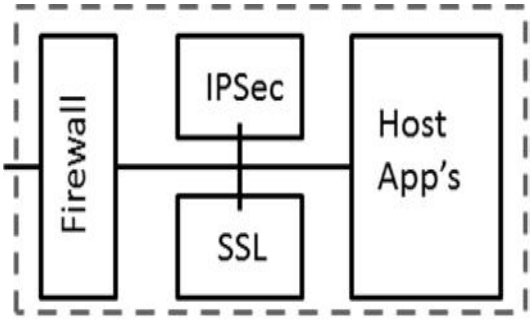

Figure 8: Host Configuration

VERIFICATION AND RISK MANAGEMENT

The final layer of security lies in the process of verification that the security elements of the system are functional and the residual risks and new risks are managed. This element is the key as the threats and vulnerabilities of the network are dynamic and the security must adapt to changes if it is to be effective. Verification is accomplished for every control. Many of the components of verification are accomplished in the Security Manager. These elements however do not address the dynamics of the threats and vulnerabilities. Constant reassessment, as illustrated in the NIST model of figure 4, is a critical component in the design methodology. The risk management component includes a best practices activity that looks for new vulnerabilities, new attacks, and fixes that happen on a daily or hourly basis. The Security Manager envisioned here includes a SOC whose role would include operational management of alerts and risks. Beyond that, Control 18, Secure Network Engineering, would tap into the larger security community to identify and address emerging risks on a continuing basis.

CONCLUSIONS

The security framework and architecture presented here is intended to lay down some markers for the journey that the telemetry community has begun. Moving into the world of Networked Telemetry is essential for the capabilities and efficiency envisioned for future test systems. The security complexity that comes with networked solutions is a challenging, but manageable piece of this journey. Fortunately the best practices of the 20 Critical Control and the NIST/IBM architectural guidelines captured here are a well traveled road that will make this journey more productive and less risky.

BIBLIOGRAPHY

[1] Lisa Daniel, *"Intelligence Leaders Urge Congress to Act on Cyber Laws,"* Defense.Gov/News/NewsArticle, Feb 2, 2012.[online]. Available: http://www.defense.gov/news/newsarticle.aspx?id=67035.[Accessed July 1, 2014]

[2] Charles Riley, "Second Chinese Military Unit Linked to Hacking", CNN Money, June 10, 2014

[3] *"Critical Controls for Effective Cyber Defense"*, SANS Corp, Version 4.1, March, 2013,

[4] *"IBM Security Solutions Architecture for Network, Server, and Endpoint,"* IBM International Technical Support Organization, March, 2011

[5] *Minimum Security Requirements For Federal Information And Information Systems* FIPS 200, National Institute of Standards and technology, Mar, 2006

[6] *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, Rev 4, NIST, April 2013

[7] *Guide For Conducting Risk Assessments, National Institute of Standards and technology,* SP 800-30, September 2012