PROPOSED INET NETWORK SECURITY ARCHITECTURE

Author: Renata Dukes
Advisor: Dr. Richard Dean
Morgan State University

ABSTRACT

Key Words: iNET, Authentication, Confidentiality, Integrity, Network Security Architecture

Morgan State University's iNET effort is aimed at improving existing telemetry networks by developing more efficient operation and cost effectiveness. This paper develops an enhanced security architecture for the iNET environment in order to protect the network from both inside and outside adversaries. This proposed architecture addresses the key security components of confidentiality, integrity and authentication. The security design for iNET is complicated by the unique features of the telemetry application. The addition of encryption is complicated by the need for robust synchronization needed for real time operation in a high error environment.

INTRODUCTION

INTEGRATED NETWORK ENHANCED TELEMETRY

The Integrated Network Enhanced Telemetry (iNET) study was created to address several of the current telemetry issues by incorporating advanced network technologies. The critical needs to be satisfied are outlined by the Major Range and Test Facility Base (MRTFB) report. These needs were generated based on the collection of scenarios from users who have experienced these kinds of telemetry issues. The discernment needs of the iNET study range from optimizing the allotted shared spectrum for effective transmission of data over the horizon. The most critical need which will be addressed in this paper is the need to protect the integrity of sensitive telemetry data with the appropriate government approved Information Assurance technologies for classified information and/or commercially accepted technologies for company proprietary information [1].

The goal of iNET is to enhance reliable data delivery by creating a bi-directional link between the ground station (GS) and test articles (TA's) so that data is effectively and efficiently transmitted as illustrated in Figure 1.

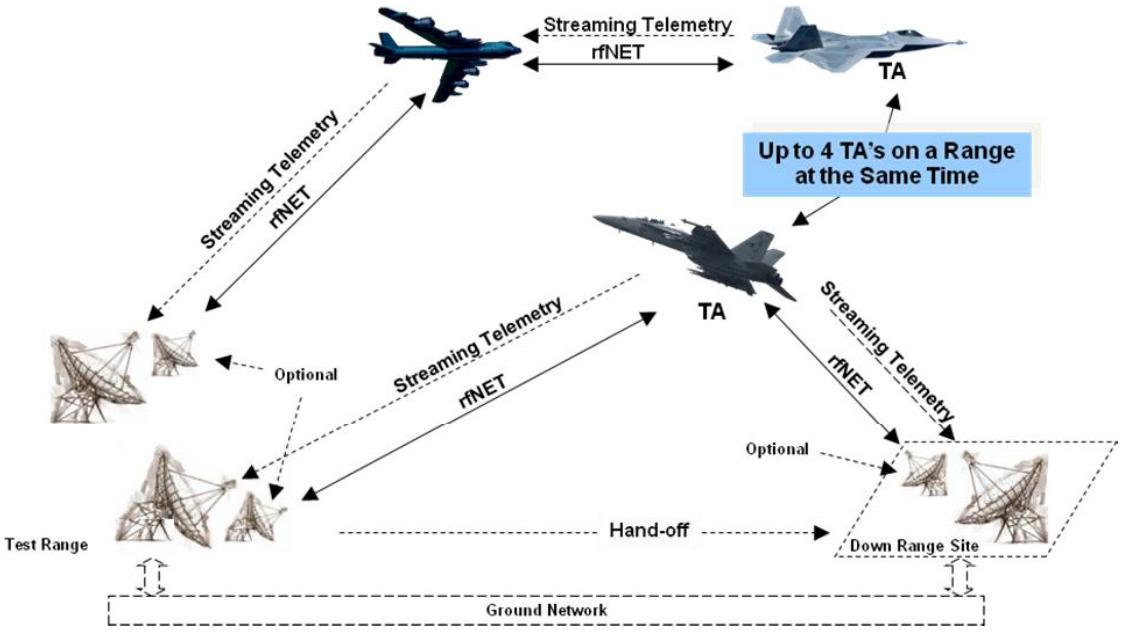

Figure 1: Existing Telemetry Infrastructure [1]

By creating a bi-directional link, time delays in data transmission will be reduced which allows for multiple pieces of information to be transmitted over the same channel. It will also help with TA to TA communication for mobile and over the horizon (OTH) transmission.

SECURITY GOALS AND THREATS

There are several requirements that need to be met in order to ensure the safe delivery of information to its intended recipient. Security requirements include confidentiality, integrity, authentication, non-repudiation, availability and access control. Confidentiality refers to protection from disclosure to unauthorized persons. Integrity refers to keeping data unmodified in transmission. Authentication refers to the assurance of identity of the person or the originator of the data. Non-repudiation refers to the ability to validate transactions. Availability refers to legitimate users having access when they need it. Finally, access control ensures that unauthorized users are restricted access. These six requirements ensure that there is protection from any unauthorized users, data consistency is maintained, access is made available to all authorized parties and unauthorized users are kept out [2]. With the iNET design, confidentiality, integrity and authentication are the goals in which need to be met for sensitive data in a shared spectrum environment as illustrated in Figure 2.

Figure 2: "Security Goals of iNET" at the Intersection of the 3 circles [3]

If any of these requirements are not completely satisfied, unauthorized users can attack the system. These attacks are categorized as passive and active attacks, where passive attacks allow data to be observed and active attacks allow for modification. As a result, data may be intercepted, interrupted, modified and fabricated as illustrated in Figure 3.

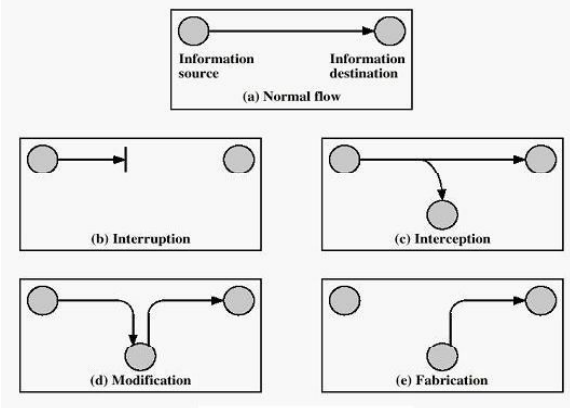

Figure 3: Network Security Threats [3]

As a result of passive and active attacks which may occur on an unsecure network, there are security mechanisms which have been put in place in order to eliminate such attacks from occurring in the future. The encryption mechanism can provide confidentiality, authentication and integrity protection. The digital signature mechanism provides authentication, integrity protection and non-repudiation. Finally, the checksums/hash algorithms provide integrity protection and some authentication. The encryption mechanism will be looked at here in order to address the goals of iNET's security design. Additional study will follow.

Encryption refers to an algorithm that is used to translate the plain text into encrypted form. Conventional encryption uses a shared key between the sender and receiver that allows for successful decryption of the message while the message is transmitted on an open channel. The plaintext, encryption algorithm, secret key, cipher text, and decryption algorithm are the five ingredients, which are used to ensure the security of information [4]. There are several types of

encryption methods, which have evolved including the Data Encryption Standard, Advanced Encryption Standard, Blowfish and Skipjack.

INET ARCHITECTURAL DESIGN

Traditional telemetry designs place encryption points at the connection with the radio interface (rfNET). This is the conventional location for link encryption and is consistent with current telemetry designs. This protects the data from outside adversaries but does not restrict unauthorized inside users from being able to access information from inside the vNET or inside the gNET, i.e., before the encryption stage and after the decryption stage as illustrated in Figure 5.

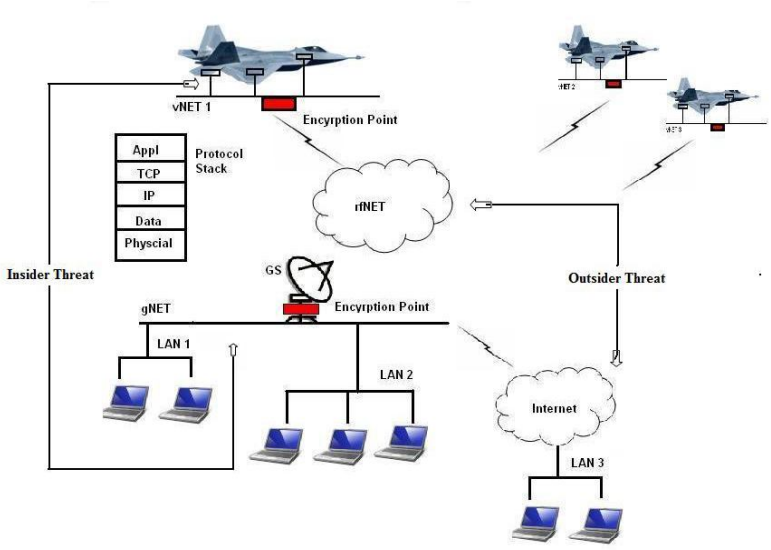

Figure 5: Current Security Architecture Design of iNET [5]

This network architecture utilizes a link encryption mechanism which is suitable when information is being transmitted directly from the sender to the receiver. However, this design has major weaknesses when the transmission of data is being sent over a network versus a peer to peer link. As a result of the architecture using an open network, the susceptibility of attacks within the LAN connections is very high. These attacks are exaggerated when LANs are extended over the internet as is envisioned. These attacks can range from interception of packets to the forging of packets. Furthermore, the existing design illustrates major issues with confidentiality, integrity and authentication. The broadcasting of packets through this system revokes confidentiality and allows all entities on the LAN to monitor what is being sent [5]. This architecture design allows for any inside or outside adversaries to gain easy access to all information thus limiting the amount of authentication and integrity provided by the design.

Since the goal of this new design is to maintain authentication, confidentiality and integrity from inside and outside security threats, the addition of encryption at every data point internally rather than externally and the distribution of keys to domains groups is needed. This will allow for

multiple pieces of information to be sent over the shared spectrum more efficiently while maintaining robust security as illustrated in Figure 6.

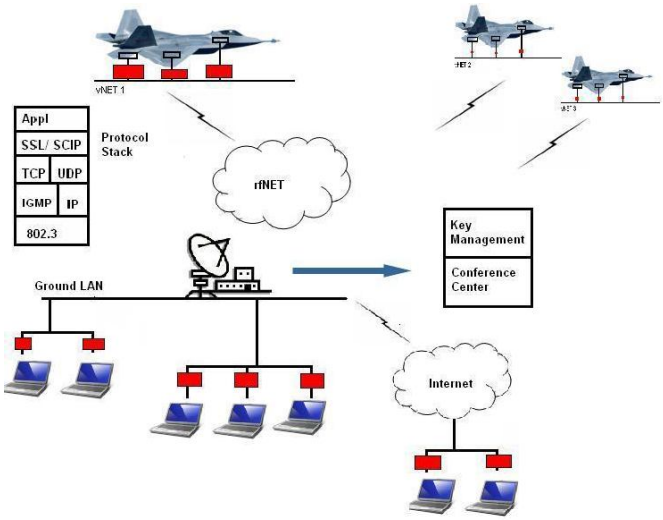

Figure 6: Proposed Security Architecture Design for iNET [5]

This proposed design will call for a shift in utilizing the link encryption design to using an end to end encryption design. Furthermore, it uses the addition of the Secure Communications Interoperability Protocol (SCIP) within the protocol stack because it will maintain security within each application as well as support security within the multicast operation. Meanwhile, this design protects users from inside attacks through the LAN as well as outside threats within the spectrum.

BACKGROUND

SECURE COMMUNICATIONS INTEROPERABILITY PROTOCOL

The Secure Communications Interoperability Protocol (SCIP) is a security protocol developed by the National Security Agency (NSA). This protocol covers wide areas of security schemes for both voice and data transmission which can enhance the functionality of a network [5]. SCIP outlines the necessity to use framing in order to transport data in a high error environment. In addition, SCIP provides the capability for a user to communicate with other compatible instruments using a secure overlay on a variety of digital networks. SCIP is an ideal protocol for iNET because it supports multicast conferencing and compatibility with the Internet Group Multicasting Protocol (IGMP).

ANALYSIS

In order to design a more efficient network security architectural design for iNET, confidentiality, integrity and authentication must be satisfied. It is crucial for a security

architecture design to satisfy these requirements because there is high susceptibility to unauthorized users being able to access important information.

The first step used to attack these issues is to generate a key management center which will distribute public and private keys to the necessary parties based on the information they will need to receive as illustrated in Figure 7. Figure 7 shows an example illustration which states that clients 1 and 3 will be the only ones receiving aeronautical information and clients 2 and 4 will be the only ones receiving weapons information after the information has been encrypted and decrypted at the necessary data points.

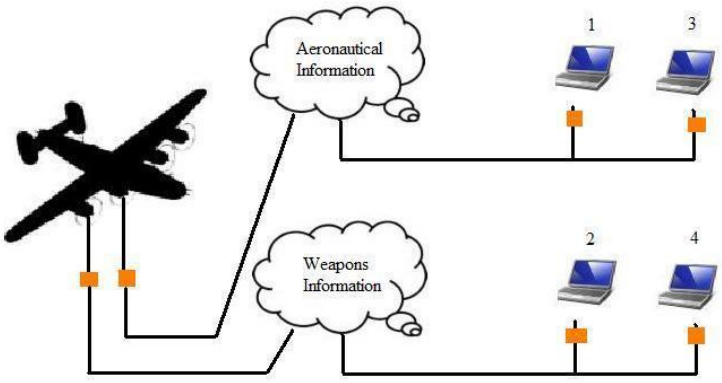

Figure 7: Illustration of Key Management in Proposed Security Architecture

The development of a key management center will also allow authorized clients to request to be added or deleted from any key session. Figure 8 illustrates the key generation process which identifies the management center (MC), security center (SC), certificate authority (CA), test articles (A, B) and host (N). This follows from commercial Public Key schemes in current use. Once clients enter or exit a particular domain session, new keys will be generated by the key management center to avoid any parties tampering with information or prevent any unauthorized users the ability to gain access to new information.

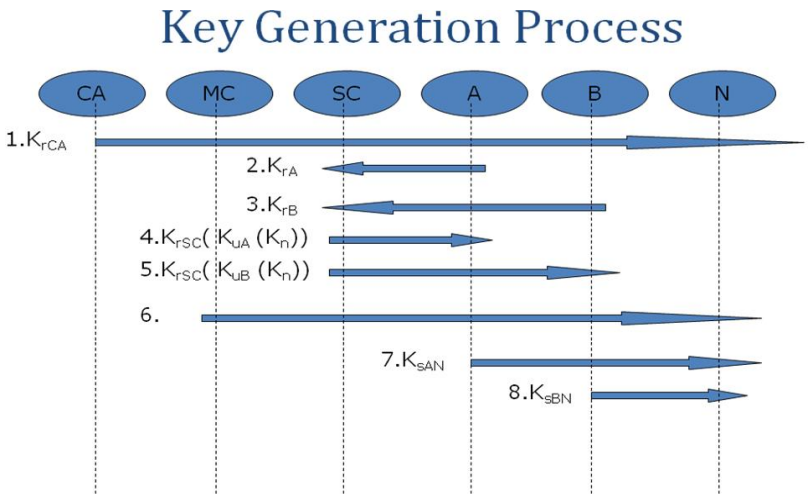

Figure 8: Key Generation Process [5]

First, the CA transmits a certificate to host N. Next, A and B request keys in order to prepare to transmit data. Keys are then generated and sent to the TA's so transmission of data can take place. The MC then makes sure than N is still included in the domain session and will monitor the transmission process between A, B and N. Finally, the information needing to be transferred from A and B to N takes place safely and securely. Each of the entities included in the key generation process are essential because it allows for a checks and balance system of security. The SC closely monitors the transmission process between TA's and host networks and generates keys using the multicast methodology to assist in the rapid transmission of data.

CONCLUSION

This paper proposes a Security Architecture for iNET suited to the network environment that is inherent to this design. The focus of this work is the nature and the location of the encryption to protection of sensitive data. An end-to-end encryption strategy was presented to address the confidentiality, integrity and authentication needed in this system. The application of an existing security design provided by SCIP is proposed to fit the requirements of real-time data and for multicast application. Additional work is needed to show how SCIP and multicast can be successfully integrated into this design.

ACKNOWLEDGEMENTS

The author appreciates the support of the DoD CTEIP and INET program offices for their support of this work. The author appreciates the contributions of Mr. Wayne Ross whose original report [5] develops much of this work.

REFERENCES

[1] iNET Study. *iNET Needs Discernment Report*, Version 1.0. 19 May 2004.

[2] Johnson, Henric. *Network Security*. Blekinge Institute of Technology, Sweden. www.its.bth.se/staff/hjo/.

[3] Johnson, Henric. *Conventional Encryption Message Confidentiality*. Blekinge Institute of Technology, Sweden. www.its.bth.se/staff/hjo/.

[4] Khalifa, O.O., Islam, M.D.R., Khan, S., Shebani, M.S. *Communications Cryptography.* RF and Microwave Conference, 2004. 5-6 Oct. 2004. 220 – 223.

[5] Ross, Wayne. *iNET Architectural Security Design*. Morgan State University. December 2008.

[6] General Dynamics (for National Security Agency). *SCIP Signaling Plan*, Revision 3.2. 19 Dec. 2007.