TRACEABLE ENTERPRISE INFORMATION SECURITY ARCHITECTURE METHODOLOGY

Charlotte A. Brown-Moorer
Department of Electrical and Computer Engineering
Morgan State University
Dr. Richard Dean
Faculty Advisor

ABSTRACT

With the introduction of networking into telemetry applications, these systems have become increasingly complex. This imposes significant strain on information security for architecture designs. It has been recognized that an organized or structured approach to developing security architectures is needed. Several enterprise architecture frameworks are available today that address system complexity. However they fall short of addressing security at a high enough level in the enterprise and address security too late in the design process. In this paper a methodology is proposed that bridges the gap between security requirements and architecture design development at the enterprise level.

This approach is consistent with and traceable to the original needs of the customer. This paper introduces a systems engineering approach to develop an enterprise level methodology, and presents a worked example of this approach for the integrated Network Enhanced Telemetry system.

INTRODUCTION

The complex nature of computer and network systems requires an organized approach to addressing network security. Several system of system (SoS) and enterprise architecture tools are available today that address system complexity, however security is hidden in the architecture and is not addressed early enough in the design process. This often leads to an information security design that is not a complete solution. This leads to holes and inconsistencies in the security architecture design. Most of the systems tools which address risk and uncertainties in the system use Bayesian theory which requires prior historical data and knowledge to obtain probability information for risk assessment. This information may not be available for the new complex systems of today.

This paper addresses the complexity of information security in SoS engineering. It especially focuses on using tools and techniques that help to properly characterize information security

architectures. In this work security information was collected about integrated Network Enhanced Telemetry system using iNET Revision 1 documentation. We also walk through an exiting SoS architecture design and illustrate a logic based approach, to quantify the information related to the system's information security.

BACKGROUND

This section gives a brief background on information that will be needed to understand terminology in this paper.

System of System definition

A system is defined as set of interrelated components working together for a common objective. A system of system (SOS) is understood to be an assemblage of components that produces behavior or functions not available from any component individually [1].

Both component system's and SOS's have inputs from other external elements. In either case the input feeds into the functionality of the system which helps in the design process. Boundaries play a key role in making distinctions between simple component systems or complex system of systems. The contributions of external elements that feed into the system boundary are very important in making this distinction. If the external elements have enough features to qualify it as a complex system in itself then we would have a SOS, if not we have a single simple or single complex system.

Initially one would have argued that all systems are a part of a larger system of system. However, after reading Maier's articles [1] which identify the characteristics of a true system of system, one could now say that most systems tend to have a systematic nature. This means that the interaction of some elements may appears to create a system of systems, however, they are just that, interactions which will do not necessarily qualify as a true SoS. Maier identifies a set of discriminating factors which defines the true characteristics of a complex SoS in his landmark article. This is an old article but the key factors of managerial and operational, as well as the concept of emergent behavior still hold true and play a key role in the development of SoS.

SoS and Enterprise Architecture Frameworks

There are several holistic representations of enterprise in existence; however, the frameworks and methodologies are still evolving. Furthermore, security is generally accounted for in the later stages of the system design. Some of the more common frameworks and methodologies in practice today include:

1. The Zachmann Framework [2]
2. The Open group architecture framework [3]
3. The Federal Enterprise Architecture (FEAF)[4]

After examining each of these methodologies in depth it become obvious through observation

that none of these methodologies provide a complete solution to develop information security architectures. Each tool has strengths in some areas and weaknesses in others.

Computer Networking

The iNET project that we are using as a worked example is a 'network of networks' and 'system of system' architecture. To understand how the work is applied in this section, we cover some of the fundamentals of computer networking necessary to understand network security.

A network is a collection of host computer-like devices that can communicate across a common transmission medium. A network passes the request for data from one computer across the transmission media to another computer. Computer X must be able to send a message or request to computer Y. Computer Y must be able to understand computer X's message and respond to it by sending a message back to computer X.

A computer interacts with the world through one or more applications that perform specific tasks and manages inputs and outputs. If that computer is part of a network some of those applications must be capable of communicating with applications on other network computers. If the internet is connected through a local *Internet Service Provider* (ISP), it is actually connecting the computer to one of their networks, which is connected to another, and so on. The Internet is made up of a wide variety of hosts, from supercomputers to personal computers including every imaginable type of hardware and software. These computers understand each other and typically work together using *TCP/IP* (Transport Control Protocol/Internet Protocol). TCP /IP protocol system is subdivided into layered components, each of which performs specifies duties.

Network access layer - provides an interface with the physical network. Format the data for the transmission medium and address data for the subnet on the physical hardware address, provides error control for data delivered on the physical network.

Internet Layer (IP Layer) **–** provides logical hardware–independent addressing so that data can pass among subnets with different physical architectures. Provides routing to reduce traffic and support delivery across the internet.

Transport Layer (TCP Layer) - provides flow control error control and acknowledgement services for the network. It also serves as an interface for network applications.

Application Layer - provides applications for network troubleshooting, file transfer, remote control, and internal activities. Also supports the network application programming interface (APIs) that enable programs written for a particular operating environment to access the network.

NETWORK SECURITY

Security is a difficult topic because everyone has a different idea of what security is and what levels of risk are acceptable. The key for building a secure network is to define policies that define what security means to the organization it will be applied in [5]. Once these have been

defined, everything that goes on with the network can be evaluated with respect to those policies. Projects and systems can then be broken down into their components, and it becomes much simpler to decide whether what is proposed will conflict with the defined security policies.

Potential threats for distributed systems can be protected by the following security service requirements- [6].

1) **Confidentiality** is the assurance to an entity that no one can read a particular piece of data except the receiver(s) explicitly intended.
2) **Data Integrity** is the assurance to an entity that data had not been altered in transmission of the information.
3) **Authentication** is the assurance to an entity that another entity is who they claim to be.
4) **Non-Repudiation** is the ability to ensure that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

Networks may use cryptographic or non-cryptographic mechanisms or both for protection. The intent of security mechanisms is to protect sensitive data and access, and to discard messages that are improper or hostile. Security mechanisms may also provide identification of an event and possibly the source of the improper or hostile message to provide intrusion detection.

iNET PHYSICAL ARCHITECTURE

INET is a "Network of Network" and "System the System" designs.
The physical iNET architecture itself is composed of two component systems: the ground station network illustrated in figure 1 and the test article networks illustrated in figure 2. The two systems communicate on a network through the protocol layer as illustrated in figure 3.

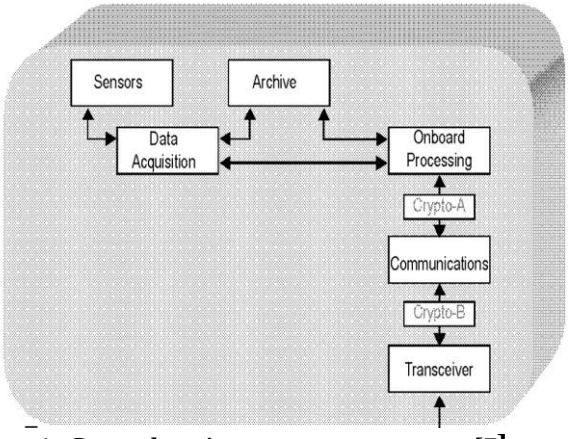

Figure 1: Ground station component systems [7]

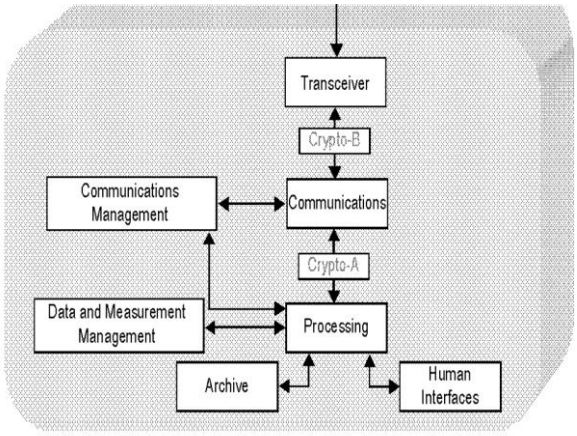

Figure 2 Test article component systems [7]

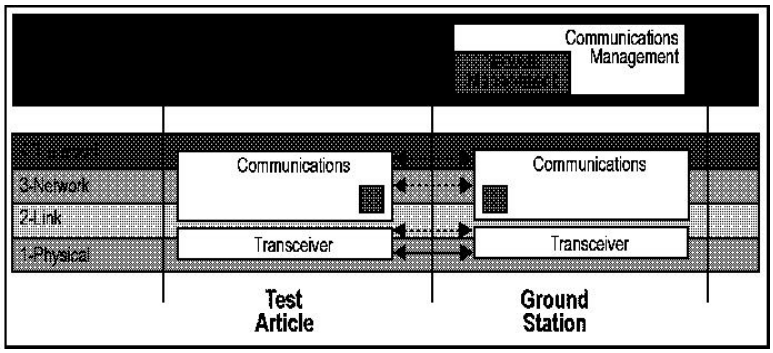

Figure 3:" SoS" "Network of Network" protocol layout [7]

PROBLEM DESCRIPTION

Systems engineering is the process of defining the desired architecture of a system; exploring performance requirements; ensuring that all system components are identified and properly allocated; and system resources can provide the desired performance [8]. However the security aspect of existing architecture tools fall short of taking a holistic approach to incorporating security in their designs. Many complex systems of today have little to no historical security information to represent the systems comprehensive perspective, therefore a better method for quantifying the security information associated with the system and component systems need to be identified.

By quantifying the information about security we can;

- Identify the gaps in the information security associated with this design.
- Analyzing risk associated with the project at the SoS level.

- Use various tools to help understand and associate risk of the security architecture design due to emergent behavior.

It is difficult to quantify most systems because they require years and years of probabilistic information that is not in many cases readily available. Bayesian probability is used in many systems to analyze risk and other entities. However Bayesian theories require a great deal of prior knowledge about the system. This project proposes replacing the Bayesian approach with logic based approach to identifying risks and uncertainties in an information security design.

The iNET Rev1 SoS architecture is a good worked example because it provides information about the security design during the very early developmental stages. This work will focus on the information security aspects of the architecture design.

APPROACH

The approach in this project is to use logic based reasoning to quantify uncertainties in information security systems. In some instances the behavior of how the component systems will work together can not be predicted. Logic based reasoning can be used when specific probability values cannot be assigned to the possible outcomes of the systems behavior. This means that there is no idea of the relative likelihood of the different outcomes of events and therefore probability values cannot be assigned. Logic based reasoning can be applied instead because specific probability values are not necessary be evaluate the systems behavior [9].

The methodology is composed of three phases.

Phase I - In this phase we collect information about the security aspects of the system. The more information that is collected the better the analysis will be.

Phase II – In this phase we quantify information as it relates to the security design. A logic based approach to identifying uncertainties will be applied in situations where there is not enough historical data.

Phase III - In this phase decisions are made based on security information collected. Decision analysis is very challenging because systems engineers and architects must meet the needs of the overall SOS.

PRELIMINARY RESULTS

In phase I information was collected about the security aspects of the iNET design at a very high level. In this work we identified security requirements that fell into the operational or managerial category in the system as defined in Maier's work.

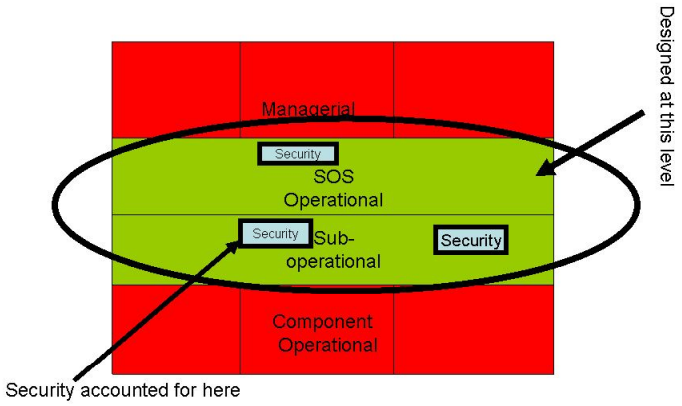

Figure 4: Demonstrates holes in layers of the system engineering development [8]

Figure 4 gives a pictorial representation of how the security is distributed within the security design. The operational layer addresses information related to the physical architecture from a SOS level to a subsystem level. Managerial layer addresses information pertaining to the business and programmatic aspects of the architecture development. This figure illustrates notionally that there are a significant amount of gaps in the security design. Security was not accounted for from a managerial perspective. Security was addressed from an operation perspective but it wasn't addressed comprehensively. From this analysis it was determined that there were potential significant gaps in the information security architecture.

Information was gathered to investigate how the security requirements were associated with the key capabilities and functionality. It is obvious based on this information that the security definition is incomplete. Figure 5 is a clip of the key capabilities and it shows that security features were not grouped at a high enough level. The security service requirements authentication and cryptography are seen as separate security issues.

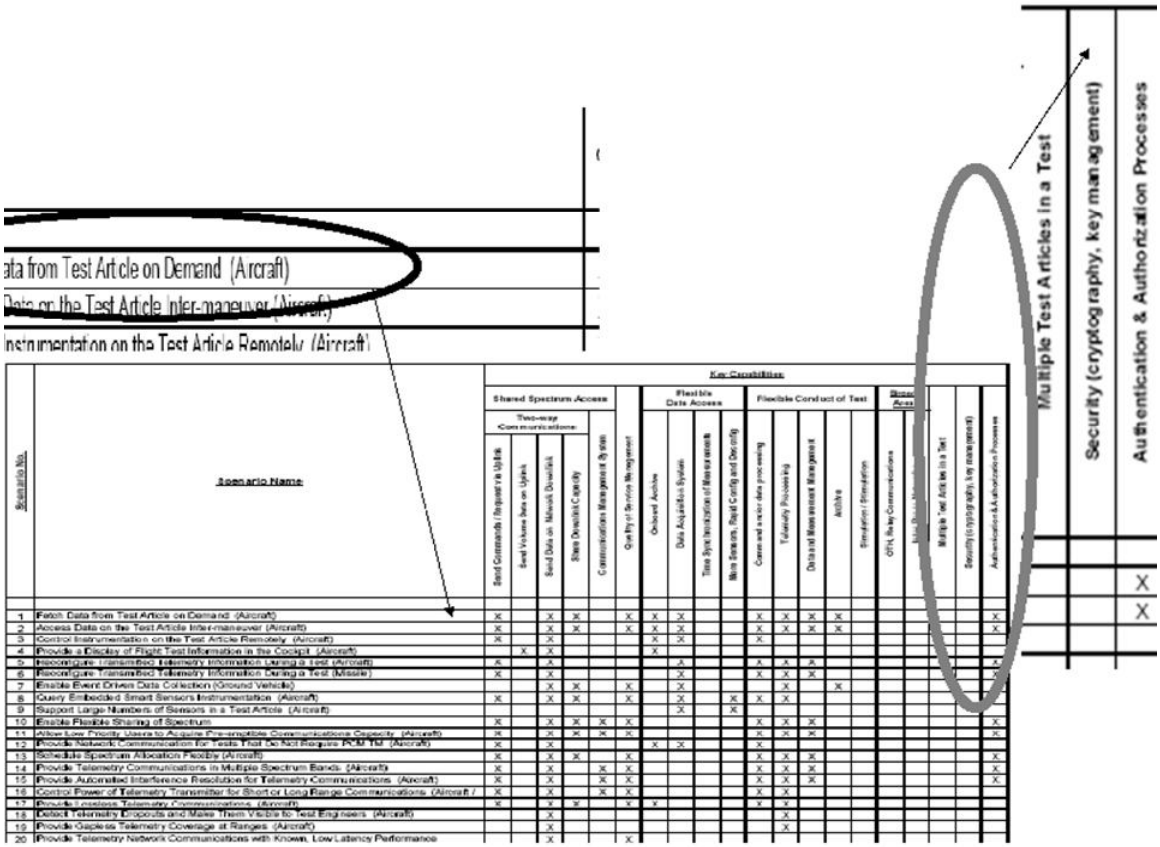

Figure 5: Clip of key capabilities table form iNET Rev1 document [7].

The information collected in phase 1 will be used to develop a logic table such as the one shown in table 1. The purpose of this table is to demonstrate how security information can be quantified. The weights give a number value to the percentage of the service requirements that were identified for the ground station and test article component system. This information is carried over to the decisions analysis phase. This diagram is a very high level representation and gets more involved with the collection of more information as the system evolves.

Table 1 Security requirement weight factors

	Weight (%)			
Security Service Requirement	**25.**	**50.**	**75.**	**100.**
Integrity	0.25	0.5	0.75	1
Non repudiation	0.25	0.5	0.75	1
Confidentiality	0.25	0.5	0.75	1
authentication	0.25	0.5	0.75	1
Do not apply	1	1	1	1

The decision tree in figure 6 was created in phase III. The component systems of the iNET SoS were related to logical information. The component systems must meet security service criteria to determine whether or not the system is secured.

More information needs to be collected to make any logical and quantitative conclusion. This work was conducted using the two dimensional analytical tool set in Excel. However, a more

advances toolset needs to be identified to perform analysis and to realize the impact of applying logic.

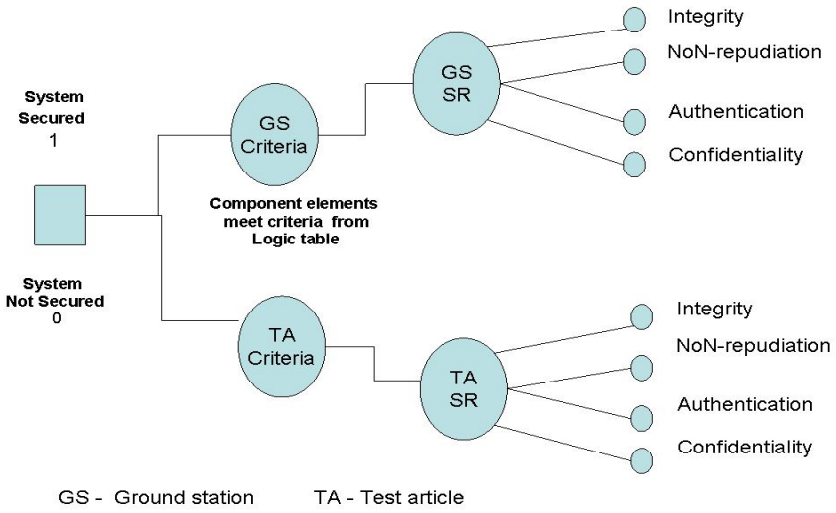

Figure 6 Decision analysis applying security service requirements to the logic.

CONCLUSIONS

The intent of this work was to introduce logic based analysis as a method to understand risks and uncertainties in information security architecture designs. This work showed that a logical approach can be used to point out uncertainties in security architectures. This conclusion was based on sampled data for the first iteration in the process. More information needs to be collected to draw more accurate conclusion about the system. As the models begin to drill down into sub-level components details uncertainties about the system will be identified with more precision.

This work was successful in developing a logic based approach to identifying uncertainty in an information security design. More scenarios and information is needed to see the true effects of this approach. This methodology provides a method to quantify information security within a system design.

We have shown that;

- iNET security is not being addressed at a high enough level in the enterprise development.
- The iNET used DoDAF architecture framework to develop the architecture however, DoDAF AF may not be the proper tool to address information security.
- In many cases security requirements were not identified properly.

- INET's legacy system can be defined as a simple component system. It has now evolved into a complex 'system of system' therefore information security has to be addressed at the enterprise level.

The intent of this work is to introduce the concept that logic based rather than Bayesian probability based approach could be used to identify and address uncertainties in complex information security architectures.

The next step in this work will be to;

- Collect and correlate security information and data about the iNET system.
- Determine how other environments will affect the security information architecture and design.
- Identify physical tool to help analyze the data because the systems are to complex to address with a two dimensional tool such as excel.

ACKNOWLEDGMENTS

I would like to thank the iNET staff and CTEIP program office for allowing me to pursue this work. I would also like to thank my advisor Dr. Richard Dean, director of the Signals Communications and Networks (SCN) Lab at MSU, for all of the time he spends with me to develop this project.

REFERENCES

[1] Maier, Mark "Architecting Principles for System –of -Systems" John Whiley, 1999.
[2] Zachmann A.J., "A Systems Architecture" IBM Systems Journal, Vol. 31, No 3, pp 445-470, 1999.
[3] The Open Group, The Open Group Framework, s.l:, The Open Group 2003 TOGAG.
[4] http//wikipedia.org/, Federal Enterprise Architecture Framework, FEAF.
[5] http//wikipedia.org/, Enterprise Information Security Architecture.
[6] Stallings W. Cryptography and Network Security Principle and Practices, 4th Edition Prentice - Hall 2002.
[7] NAVAIR, "iNET Needs and Discernment Document", 2004
[8] Sweet, W., Systems Engineering Principles, Second Edition, John Wiley, 2003.
[9] Ye Chen , Divakaran Liginlal, Bayesian Networks for Knowledge-Based Authentication, IEEE Transactions on Knowledge and Data Engineering, v.19 n.5, p.695-710, May 2007.