

INFORMATION SYSTEMS SECURITY ENGINEERING

The Need for Education

By

Richard K. McAllister

Senior Scientist

Sparta Inc.

Columbia MD

rmcall@sparta.com

410-381-9400 ext. 231

Abstract: Several aspects of problems with the state of information systems security are presented; the main points concern incorrect marketing and customer expectations. They are followed by identification of solutions; the main point being education. The last section explains what efforts Sparta Inc. and the NSA have accomplished and are doing to fix the problems cited.

POSITIONS

Products Not Systems

The information systems industry or information technology (IT) industry, as it is often called, is a product selling business. Vendors press to corner the market for their products and extend the marketability by selectively adding features to enhance interoperability with other popular products.

Services Not Systems

The information systems industry is a services selling business. Service providers including communications (telephone, cable, satellite, wireless), Internet services (Web, email, messaging, etc.) compete for the market.

Customers Buy Products and Services Not Systems

The information systems industry has trained customers to buy individual products and services. We are all beta testers of the combinations of products and services available from vendors. There is little or no emphasis on the engineering of information systems. Customers view systems engineering as additional cost and unnecessary delays in becoming operational.

Information Security Is No Different

Information protection product and services vendors are behaving the same as all other vendors. Customers have been trained to buy firewalls, guards, crypto mechanisms, intrusion detection systems, security administration packages, etc.

System Security Is Not An Amateur Sport

Customers and vendors are rarely capable of engineering systems¹. In fact, neither are most information security engineers. Even the known processes for certification and accreditation of systems have little guidance for the engineering of information protection into systems.

Information Systems Security Engineering (ISSE) is a specialization of systems engineering. If you listen to systems engineers in any specialization they all have similar complaints about inadequate attention to a systems approach in design.

Products Are Not Designed To Be Composed

Since the earliest days of computer security and communications security, information security products have not been designed to be integrated or composed with other products such that the resulting security could be measured or even estimated. There is no common framework in any current evaluation scheme or criteria that directly supports measuring the combined security effectiveness of products. One danger is that so called "systems integrators" can put things together and make adjustments to make a system work but produce no knowledge about the risks incurred in operation.

¹ "Systems" meaning combinations of products not all specifically designed and tested to work together.

WHAT NEEDS TO BE DONE?

Educate ISSEs

Given the above positions, the uninitiated ISSE has an enormously difficult task and needs to be prepared to deal with:

- Customers who don't understand their needs for protection
- Customers who are impatient to get their business or mission underway
- Products with widely varying notions of security utility
- Systems engineers with little appreciation for security design
- Security engineers who don't know how to design for compose-ability
- Customer Certifiers who are unable to deal with complex systems evaluations
- Customer Accreditors who accept systems without proper risk assessments.
-

The ISSE must be educated in and trained to employ a systems engineering process. That process must address the difficulties listed above. Systems engineering has a few well known activities from requirements analysis to operational acceptance. Some authors² believe that systems architecting is a different activity that draws more upon inductive skills than the deductive skills of engineering but I include that as a design step in systems engineering. There are important principles that the ISSE must learn to observe and must impart to customers such as separating the problem from the solution.

Educate Customers

Customers must be convinced that systems engineering is beneficial. They must be shown evidence of cost, schedule, and performance enhancement because of systems engineering. ISSEs and the systems they develop are the sources of that evidence. Most customers of information systems have never seen a systems approach to solving their problems and therefore have no appreciation that their systems could be better. They simply accept the world of IT as delivered by product vendors and service providers. Customers must learn that searching catalogs and composing products without professional help is problematic and may be dangerous to their business or mission.

Define Needed Product Specifications

Vendors must be shown how to design their products to be composable and to be evaluated for their contribution to the effectiveness of the systems' overall protection. Information security in 2002 has become primarily the business of detection rather than prevention. Information protection requirements based on security services must be translated by ISSEs and security engineers into specifications for security mechanisms in products. There is much research necessary to be able to apply metrics to composing security mechanism strengths but a systems approach today can identify weaknesses and holes in the security design. ISSEs must also learn that the set of security mechanisms

² "Systems Architecting" Rehtin

includes physical and administrative security elements that are part of the security architecture.

WHAT HAS BEEN DONE?

My colleagues and I at Sparta, the NSA, and elsewhere in the "INFOSEC" business have been working for many years (at least 25) at defining, practicing, and teaching Information Systems Security Engineering. Of course we ask ourselves why haven't we been able to bring about wide acceptance of ISSE. The answer is that security has been a hard sell. Business losses have been affordably passed on to customers. We sense a change. In government, communications security has been well practiced. Closed systems linked by cryptographic mechanisms served well for a long period. Open systems communicating over public networks are a whole different set of problems. The industry is thrashing about in computer security, criteria for product evaluation, public key cryptography, firewalls, intrusion detection, virus detection, biometrics, and stenographics in an attempt to acquire safe systems. We have been developing an approach that pulls together the problem definition and the solutions systematically. What follows is a very brief description of all of the aspects we are working to build better solutions.

Courses

ISSE Introduction: NSA has produced an introductory course on ISSE based on five system engineering activities of:

- Discover Needs
- Define System
- Design System
- Implement System
- Assess Effectiveness

In each activity the role of an ISSE or ISSE team is defined. The course gives students the opportunity to experience methods that can be applied to bring about systems with known and acceptable information protection.

ISSE Protection Needs Elicitation: NSA has produced a practitioner level course that teaches ISSEs how to "Discover (protection) Needs". The steps presented are:

- Approaching the customer
- Information management modeling
- Applying least privilege
- Information threat analysis
- Customer priorities
- Information protection policy development
- Customer acceptance

The methods taught here are based upon many successes and failures in both government and private industry programs. Probably the most significant point here is how to deal with the propensity of customers and engineers to define the requirements based upon available solutions.

ISSE Architecting: NSA is developing a practitioner level course in systems security architecting. The course begins with "Define System" in which a context is developed for defining the scope of the target systems to be developed and which parts of the information protection policy are allocated to them. The course will focus on:

- Understanding the proposed or existing system architecture
- Understanding some basic "security physics" of what is possible
- Allocating security services and strengths where needed
- Defining the types of security mechanisms to provide the services
- Performing a security mechanism interdependency analysis
- Defining the types of components that include the security mechanisms
- Preparing a preliminary security concept of operation
- Practicing on example systems

Mentoring

There are very few ISSE qualified engineers and those that can are assisting in the on-the-job training of new ISSEs. We expect this to bring about more and better ISSEs.

Program Execution

In addition to the direct training we are engaged in several government and a few commercial programs where we are applying the ISSE process that we preach. Programs include national key management and public key infrastructures, multinational joint force information sharing, upgrades to existing cryptographic systems, and many more. These are vehicles for demonstrating how ISSE works and how it benefits programs.

Certification

The NSA is under pressure to satisfy the needs of many customers. It has defined the need to be able to point customers to qualified ISSE services in private industry to expand its coverage. A process has begun to certify individual ISSEs.

Master Task List: The first step in certification was to identify the tasks performed by the individual ISSE. A master task list was composed and reviewed by subject matter experts in government and private industry. The list was compared to information compiled under the System Engineering, and Security Systems Engineering Capability Maturity Models. The NSA has had exchanges with ISC² to discuss relationships to CISSP certification and what additional requirements there would be for an ISSE certification.

Testing: The NSA is currently considering options to produce test material as part of the ISSE certification.