Information Systems Security Engineering: A Critical Component of the Systems Engineering Lifecycle

James F. Davis
University of Maryland University College
3501 University Blvd. East
Adelphia, MD 20783
1-800-888-UMUC
jim@thedavisnetwork.com

ABSTRACT

The purpose of this research paper is to illustrate the industrial and federal need for Information Systems Security Engineering (ISSE) in order to build Information Assurance (IA) into a system rather than the current costly practice of fixing systems after production. Extensive research was performed by collecting information from throughout the World Wide Web to include sites such as the National Security Agency's Homepage, the Information Assurance Technical Framework Homepage, the Workshop for Application of Engineering Principles to System Security Design, as well as many others. This research realized the following findings: (1) IA is dangerously left out of systems engineering processes; (2) a consortium from academia, industry and the federal government have formalized ISSE and its processes; (3) federally sponsored and industrially sponsored professional certifications exist for security engineers practicing ISSE; (4) ISSE, however, is not greatly used today due to a lack of understanding and a perceived high cost; (5) end-users are beginning to understand IA and are calling for more secure systems. This paper was written to illustrate a way forward, a method to bring ISSE to the frontlines of systems engineering and bring to life a notional concept of Designing for Security. This paper does not provide quantitative analyses as to the benefits of ISSE vs. the initial up front costs; however, further research should be accomplished in the future to address this. In conclusion, I recommend that ISSE must be identified as a critical component of the systems engineering lifecycle and be properly utilized to ensure that future products meet the IA demands of the end user. To achieve this, academia must build degree programs to educate ISSE and incorporate ISSE into existing degree programs; industry and the federal government must both embrace these principles and apply these techniques to their post-production, active engineering as well as new program developments.

SIGAda 2004, November 14-18, 2004, Atlanta, Georgia, USA.
Copyright 2004 ACM 1-58113-906-3/04/0011…$5.00.

Categories and Subject Descriptors

D.2.0 [**Software Engineering**]: General – *protection mechanisms, standards*.

General Terms

Design, Security, Theory, Verification.

Keywords

IA, Assurance, Engineering, ISSE, Security

1. INTRODUCTION

In September 2003, Mr. Eugene Spafford, Professor and Director, Purdue University Center for Education and Research in Information Assurance, stated during a testimony before the US Congress, "it is clear that there is a large and growing problem with the security of our cyberinfrastructure," and that "nowhere is this more apparent than in the computing systems used within the Federal government" [15]. He continued to describe how alarming the trends are "in the way software is produced, acquired, deployed, and then used" [15]. In particular he focused on the concerns with Commercial Off-the Shelf software [15]. The problem Mr. Spafford is describing is the fact that there exists a severe lack of focus and understanding in regards to information assurance (IA) during software systems development. Although his testimony is in regards to software, the same applies to systems that incorporate hardware solutions as well. With respect to these trends of software development as well as the ever increasing system and software complexities of today, limited are the days of *post hoc* security, and enter the need for a systematic and secure approach to incorporate information assurance—Information Systems Security Engineering (ISSE) [1].

As evidenced by Mr. Spafford's testimony as well as countless papers, research and discussions—of which, a select few have been cited in the references that follow this document—it is a well-known fact that there exists a severe lack of understanding regarding the risk of IA. The risk mentioned here refers to both the risk of including as well as excluding IA within a systems development. The risk of including IA is the budgetary, schedule and performance costs that IA could possibly place on a system. On the other hand, leaving IA out could bring about critical system failures due to system vulnerabilities which would then potentially reveal an enormous cost to repair, patch and cleanse the system. It is the mission of ISSE to balance these risks along with others to ensure some acceptable level for the customer and/or end user [9].

The purpose of this research paper is to illustrate the industrial and federal need for ISSE in order to build IA into a system rather than the current costly practice of fixing systems after production. In particular, this paper will describe what ISSE is, how it is used today within academia, industry as well as the federal government and why it must be recognized and treated as a critical component of the systems engineering lifecycle. Finally, a challenge and roadmap will be presented to illustrate an approach to satisfying the need for ISSE within academia, industry and the federal government.

2. WHAT IS INFORMATION SYSTEMS SECURITY ENGINEERING?

Historically, due to the ability to cheaply and easily deploy a system with limited to no IA capabilities and thus provide a greater amount of features, convenience and performance that consumers demand, IA has typically been left out of the development processes to be integrated in *post hoc,* i.e., after production [1]. This method has since been accepted as common practice, however, the ability to accurately and efficiently counter all of the inherent vulnerabilities of a system, post production, is extremely difficult and costly (Cowen et al.). Thus, the growing need for IA directly conflicts with these current practices [1,15]. This growing need requires a revolution in the methods that IA is conceived, applied and endorsed. The proper application of ISSE to a systems engineering process is one of the results of this revolution.

In summary and for the purposes of this paper, ISSE is the systematic approach to building IA techniques and tools within a systems engineering process. Another common and more detailed definition in use today by the Information Assurance Technical Framework (IATF)—a group of federal, industrial and educational communities brought together to raise IA issues and provide guidance for solving IA issues—as well as the NSA defines ISSE as “the art and science of discovering users’ information protection needs and then designing and making information systems, with economy and elegance, so they can safely resist the forces to which they may be subjected” [9]. The commonality between these two definitions and the overall objective of ISSE is that IA must be addressed from the very beginning of a systems development and that IA is not only serve as a component engineering role, however it permeates throughout the systems engineering lifecycle to build the tools and techniques to satisfy the IA need of the system [9].

ISSE is applied to both an overall systems engineering process as well as component level and sub-component level engineering processes as required [9]. IA considerations must be provided during the earliest phases and throughout a systems engineering lifecycle such as when defining the overall need of a system, developing the concept of operations of a system, during requirements engineering, during system design, implementation and during other post production activities [9]. The IATF describes the application of ISSE through a generic systems engineering lifecycle and is best illustrated by figure 1 [9]. The IATF also provides a set of overarching principles for guiding ISSE: (1) Always maintain separation between the problem and solution; (2) Problem space is driven by the customer’s need; (3) ISSE defines the solution space based on the problem space [9]. Thus ISSE is much more than the current reactive approach to security by applying fixes, the goal here is to proactively apply IA to systems to prevent the need for theses fixes.

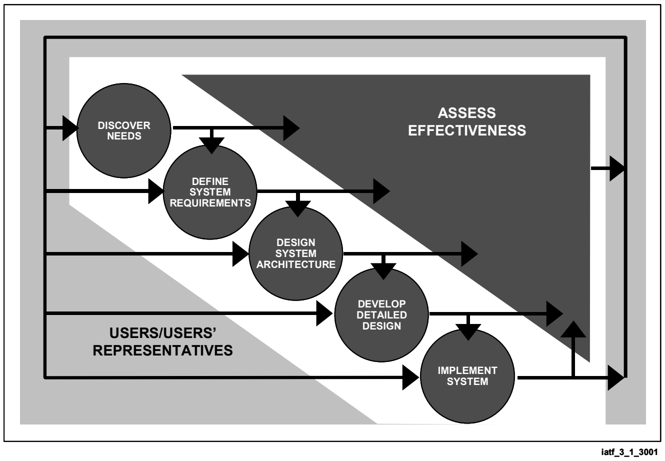

Figure 1 - The generic systems engineering framework from which the NSA sponsored IATF (2002) builds the ISSE processes from as extracted from Chapter 3 of the IATF [9].

3. HOW IS ISSE BEING USED TODAY

ISSE, although growing in demand and popularity, is currently only being sporadically used and when used is not being applied correctly or throughout a systems engineering process. Due to the increased upfront cost of applying ISSE early on to an engineering process and the end user’s inability to correctly realize the potential future costs of skipping out on IA—both in terms of maliciously identified faults as well as the application of *post hoc* security—the motivation and demand for ISSE is severely limited [1]. However, as the federal government continuously strives to improve its IA awareness and use, this will hopefully lead the way as an example for industry and academia.

3.1 ISSE within the Federal Government

The federal government is actively utilizing ISSE, for example the NSA provides ISSE support to government systems engineering efforts as well as in support of Department of Defense system certification and accreditation processes [13]. The NSA also is the sponsoring agency of the IA Technical Framework (IATF), a document that, in great depth, defines what ISSE actually is [9]. The IATF is a product from a wide variety of persons throughout the federal, industrial and academic sectors [13]. Although additional improvements and changes will have to be made to further support ISSE development processes, the federal government is making progress and is moving to system-wide acceptance of ISSE.

3.2 ISSE within Industry

Industry is realizing the need for systems security engineers as well [3]. Demand for security engineers and ISSE principles is rapidly growing in support of federal and commercial missions which in turn have been increasingly requesting security engineers and ISSE principles for systems engineering. This growing demand is a direct response to the continual lack of security with regards to software applications development, network systems as well as many others [15]. Also a cause for this realization is that increasing residential bandwidth and access to global information repositories has led to IA failures and the need to apply more protection to systems, including home systems [2]. The use of network firewalls and other filter devices have spread to home users, virus software and the notion of secure software has also spread to residential neighborhoods. With this spread and increased awareness of IA, users have begun to demand better IA from the commercial world. Finally, with increasing systems complexities and thus cost to apply *post hoc* security, the application of ISSE principles and techniques are beginning to look much more appealing [1].

The growing demand for systems security engineers led to a lack of an ability to formally distinguish those persons that had the experience and expertise to perform ISSE functions vice those that did not. This lack of a formal ability to validate the skills of those personnel applying for positions to meet the demand of both industrial and federal ISSE positions led to federally sponsored certification programs via the International Information Systems Security Certification Consortium, Inc., also known as $(ISC)^2$ [5]. The formal ISSE development program, as established by the $(ISC)^2$ has become the industrial and federal standard for certifying systems security engineering professionals [6]. The certification track consists of a broad-based, limited depth of knowledge certification in Information Assurance, Certified Information Systems Security Professional (CISSP), as well as three different tracks of concentrated depth-based knowledge certifications: (1) Information Systems Security Engineering Professional (ISSEP); (2) Information Systems Security Architecture Professional (ISSAP); (3) and Information Systems Security Management Professional (ISSMP) [7]. These certification programs serve as basic credentials for persons desiring IA careers both within federal and industrial markets.

3.3 ISSE within Academia

Academia's response to the need for IA awareness and education has been broadened by federal ventures such as the NSA's National IA Education & Training Program (NIETP) [14]. This program builds governmental, industrial and academia partnerships to advocate IA education and awareness [14]. The NIEPT's direct partnership with colleges and universities is via another program called the NSA's National Centers of Academic Excellence in Information Assurance Education (CAEIAE) [11]. Within the CAEIAE program, universities and colleges may apply for certification-type lauds from the NSA and be recognized as a Center of Academic Excellence that then enables students of those universities and colleges to be eligible for federal scholarships and grants, such as the Department of Defense Information Assurance Scholarship Program as well as others [11]. These programs represent just one aspect of growing IA education within academia, however, much more is needed to solidify and promote the overall ISSE principles of designing IA into a system rather than *post hoc* security [1].

Another academic response to the need for IA in current and future systems is the idea of "Design for Securability," where the assumption is that no system can be designed secure; rather, the focus is on securing the system during its operation [4]. This concept greatly contradicts the ISSE approach in that the objective of ISSE is to do what this idea has stated as impossible [4,9]. In fact, the idea of "Design for Securability" calls for the implementation of design features during the operation of a system which still ends up producing a *post hoc* security solution [1,4]. However contradictory to ISSE, this critical analysis of different methods of securing a system is greatly needed as these analyses may potentially discover a better method to apply security solutions to a system.

4. ISSE: A CRITICAL COMPONENT OF THE ENGINEERING LIFECYLCE

The systems engineering lifecycle is the evolution of a system or product with specific and identified phases that address need, development, test, production, operations, support and maintenance, as well as training and terminating at disposal of the system or product [8]. For example, DoD 5000.2-R framework incorporates a DoD standard for systems engineering lifecycles as does the IEEE 1220-1998, Standard for Application and Management of the Systems Engineering Process, both of which are illustrated in the IATF appendix J [9]. The ISSE lifecycle is designed to fit perfectly within a systems engineering lifecycle and is also illustrated in the IATF and the same appendices [9].

Due to the nature of IA and how it permeates throughout an information system's design and implementation, ISSE must be considered more than a component engineering discipline and rather as a critical attribute and function of the overall systems engineering lifecycle [9]. In contrast to the standard component engineering disciplines such as Software Engineering, Civil Engineering, etc., ISSE does not only provide products to satisfy system-level requirements, rather ISSE provides both products and guidance for other component engineering disciplines during the systems engineering lifecycle [9]. For example, ISSE is responsible for engineering specific IA products in support of the overall system, such as: cryptography devices, key management services for the cryptography, etc [9]. ISSE is also responsible to provide constraints and guidance in regards to the methods that component disciplines build their products, such as building a component to meet certain IA certification guidelines or restricting the types of personnel that are authorized to work on a product (i.e., US only, persons/organizations with a certain amount of known trust, or persons/organizations who hold certain certifications such as ISO 9000 or Capability Maturity Model Indices) [9].

ISSE must also be integrated into a systems engineering lifecycle from the beginning as it plays a critical role in facilitating system-level requirements, design and analyses [9]. The ISSE process, as captured by the IATF, is intimately involved within every phase of the systems engineering lifecycle [9]. For example, during a standard DoD 5000.2-R systems engineering lifecycle's requirements analysis phase, ISSE is defining system security requirements and in particular, developing a systems security concept of operations, defining the IA boundaries for the system as well as much more [9].

5. ISSE AND ITS IMPACT ON LIFECYCLE COSTS

Although the upfront cost of performing the tasks of ISSE during a systems engineering lifecycle may seem great due to uncertainty and time or budget constraints, the cost if compared to applying the security, changing system designs and possibly rebuilding components *post hoc* is extremely low [1]. In fact, if ISSE is properly utilized from the beginning of a systems engineering process, ISSE may provide additional benefits such as identifying and mitigating system risk in regards to cost, schedule and performance earlier on and thus further enhance a system's ability to remain on target [9]. However, due to the extreme difficulty of properly measuring IA effectiveness and because IA is not always a black box that can be engineered, procured and just simply placed on a system and expected to solve all IA worries, it is extremely difficult to warrant the need of ISSE without stating 'just because' or relying on corporate or governmental regulations.

6. RECOMENDATIONS

In order to build IA into today's systems, the current, most systematic and cost effective method is ISSE. ISSE must be identified as a critical component of the systems engineering lifecycle and be properly utilized to ensure that future products meet the IA demands of the end user. To do this, we must build security engineers from the ground up. Academia must provide degree programs for ISSE as well as incorporate ISSE principles in current component level and system level degree programs such as Systems Engineering, Software Engineering, etc. Through this education process, engineers, customers and the end users will realize the current methods of cost analysis regarding IA are extremely flawed and will be able to better analyze the IA need with respect to their constraints. By building ISSE and ISSE aware personnel from the ground up, future programs will be able to withstand the current and ever growing threat to IA.

Due to the latency of academics reaching industry, it is imperative that ISSE principles and tasks be incorporated into today's systems engineering processes as well. Spinning up ISSE educated experts will take time, so a solution to the ISSE gap must be identified. The recommended solution to this is to incorporate the $(ISC)^2$ certification processes as a guide to building top down security engineers. This would provide both a means to measure person's capabilities as well as provide a structured guide to understanding ISSE and thus fill the academia-to-industry transfer gap.

7. CONCLUSION

In conclusion, there exists a fundamental need for ISSE within the overarching systems engineering process for federal, industrial as well as academic purposes [15]. The purpose of this paper was to illustrate this need by defining what ISSE is, how it is in use today by federal, corporate and academic worlds as well as to discuss why it must be treated as a critical component of the systems engineering lifecycle. As Mr. Spafford stated the need for IA within software development processes and as *post hoc* security becomes more impractical, the need for ISSE becomes unmistakable [1].

As the systematic approach to building and incorporating IA principles, techniques and solutions into a systems engineering process, ISSE is the foundational IA process to protect current and future information systems and must be accepted as such [9]. Without the system level security engineering, systems will continue to be developed that must incorporate *post hoc* security as a major portion of their maintenance phase of their lifecycles [1]. As was illustrated in this paper, this form of applying IA solutions is extremely costly and increasingly difficult as systems and software increase in complexity [1]. Another concern with *post hoc* security or poorly implemented component-centric ISSE is the possibility that a system-level defined process may be the root cause of an IA failure, however, due to the lack of IA focus at the system-level, this failure is not realized until testing or possibly even implementation of the system [1]. To make a correction of this magnitude would cost an incredible amount of time and money. The paramount principle of ISSE is that security engineering is done from the system-level and spiraled into the components in concert with the developmental lifecycle [9].

As is evidenced in academia, industry as well as the federal government, ISSE principles are beginning to plant roots and build their foundation from which to build on. The NSA's drive of boosting IA awareness via the CAEIAE program & IATF Forum is a major player in the world of security engineering. The results of the CAEIAE program are evident as 50 colleges and universities have been certified by the NSA as Centers of Academic Excellence. Industry has also taken notice as the demand for security engineers begins to quickly rise and security concerns flow to the general civilian populace. For instance, due to the increasing bandwidth to the residential users, more and more users are utilizing firewalls or other Internet security mechanisms—a clear sign that IA awareness is spreading [2].

Finally, the way forward; how do we protect the systems that have already been designed and implemented, those in their maintenance phases; what about those systems that are just starting up; and those that are nearing a critical design milestone. We must embrace the principles of ISSE and make use of the academics available now, utilize certification processes to provide structured training and then integrate those ISSE principles within every phase of a systems lifecycle. A formalized and baselined set of ISSE principles is publicly available as chapter 3 and appendix J of the NSA's IATF [9]. The tools, techniques, knowledge and training is available; get it, learn it, do it, be an IA aware engineer or an Information Systems Security Engineer

8. ACKNOWLEDGMENTS

My thanks to the University of Maryland University College's Professor Louis Blazy for his assistance and teachings during his Spring 2004 Systems Engineering course for which this paper was originally written.

9. REFERENCES

[1] Cowan, C., Hinton, H., Pu, C., & Walpole, J. (2000, October). *The Cracker Patch Choice: An Analysis of Post Hoc Security Techniques.* Presented at the National Information Systems Security Conference, Baltimore, MD. Retrieved April 4, 2004, from http://www.cse.ogi.edu/~crispin/crackerpatch.pdf

[2] Entman, R. M. (1999). *Residential Access to Bandwidth: Exploring New Paradigms.* Washington, DC: Communications and Society Program. Retrieved April 23, 2004, from http://www.aspeninstitute.org/aspeninstitute/files/Img/pdf/access.pdf

[3] Google Inc. Google Search For Systems Security Engineer. Retrieved April 23, 2004, from http://www.google.com/search?hl=en&lr=&ie=UTF-8&oe=UTF-8&q=%22systems+security+engineer%22+

[4] Hunstad, A., & Hallberg, J. (2002, November). *Design for securability -- Applying engineering principles to the design of security architectures.* Presented at the ACSA Workshop on the Application of Engineering Principles to System Security Design. Retrieved February 22, 2004, from http://www.acsac.org/waepssd/papers/04-hunstad.pdf

[5] International Information Systems Security Certification Consortium, Inc. (ISC)^2. (2004, April). *(ISC)^2® And Booz Allen Hamilton Present Preview Of New NSA-Sponsored Certification.* (ISC)^2® Press Releases. Retrieved April 11, 2004, from https://www.isc2.org/cgi-bin/content.cgi?page=388

[6] International Information Systems Security Certification Consortium, Inc. (ISC)^2. *About (ISC)^2®*. Retrieved April 11, 2004, from https://www.isc2.org/cgi/content.cgi?category=7

[7] International Information Systems Security Certification Consortium, Inc. (ISC)^2. *Frequently Asked Questions.* Retrieved April 11, 2004, from https://www.isc2.org/cgi/content.cgi?page=8#cat06

[8] Kossiakoff, A., & Sweet, W. N. (2003). *Systems Engineering Principles and Practice* (pp. 449-50). Hoboken, NJ: John Wiley & Sons, Inc.

[9] National Security Agency. (2002, September). *Information Assurance Technical Framework Release 3.1.* Fort Meade, MD: Author. Retrieved April 23, 2004, from http://www.iatf.net/framework_docs/version-3_1/zipfile.cfm?chapter=version-3_1

[10] National Security Agency. (2003, December). *Information Systems Security Engineer Professional (ISSEP).* Las Vegas, NV: 2003 Annual Computer Security Applications Conference. Retrieved February 22, 2004, from http://www.acsac.org/2003/case/thu-c-1530-Oren.pdf

[11] National Security Agency. *Centers of Academic Excellence.* Fort Meade, MD: Author. Retrieved April 23, 2004, from http://www.nsa.gov/ia/academia/caeiae.cfm

[12] National Security Agency. *Centers of Academic Excellence: Institutions.* Fort Meade, MD: Author. Retrieved April 23, 2004, from http://www.nsa.gov/ia/academia/caemap.cfm#completelist

[13] National Security Agency. *Information Systems Security Engineering.* Fort Meade, MD: Author. Retrieved April 23, 2004, from http://www.nsa.gov/ia/government/isse.cfm?MenuID=10.3.2

[14] National Security Agency. *National IA Education & Training Program.* Fort Meade, MD: Author. Retrieved April 23, 2004, from http://www.nsa.gov/ia/academia/acade00001.cfm

[15] Spafford, E. H. (2003, September). *Exploring Common Criteria: Can it Ensure that the Federal Government Gets Needed Security in Software?* Washington, DC: Testimony before the House Government Reform Committee Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census. Retrieved February 22, 2004, from http://www.cerias.purdue.edu/homes/spaf/usgov/tipirc.pdf