ITL BULLETIN FOR DECEMBER 2016

RETHINKING SECURITY THROUGH SYSTEMS SECURITY ENGINEERING

Ron Ross, Larry Feldman,[1] and Greg Witte,[1] Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Introduction

Each of us depends heavily upon modern technology in all aspects of our lives. Technology is increasingly integrated into complex "systems of systems" through the convergence of various cyber and physical systems, or cyber-physical systems (CPS), including what many call the Internet of Things (IoT). This innovation – and the associated complexity – is difficult for even seasoned engineers to fully understand, and even more difficult to defend against failures and attackers. As digital solutions are increasingly part of our physical world, including medical and transportation applications, our lives depend on becoming better able to trust the safety, reliability, and security of these technologies.

After four years of research and development, NIST has published a groundbreaking new security guideline, Special Publication (SP) 800-160, *Systems Security Engineering*. The publication draws from proven system engineering processes to address the longstanding problem of how to build trustworthy, secure systems—systems that can provide continuity of capabilities, functions, services, and operations during a wide range of disruptions, threats, and other hazards. Development was led by NIST Fellow Dr. Ron Ross who said he thinks NIST SP 800-160 "is the most important publication that I have been associated with in my two decades of service with NIST."

NIST SP 800-160 addresses the engineering-driven perspective and actions necessary to develop more defensible and survivable systems, inclusive of the machine, physical, and human components that compose the systems and the capabilities and services delivered by those systems. It starts with, and builds upon, a set of well-established international standards for systems and software engineering published by the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the Institute of Electrical and Electronics Engineers (IEEE) and infuses systems security engineering methods, practices, and techniques into those systems and software engineering activities.

[1] Larry Feldman and Greg Witte are Guest Researchers from G2, Inc.

The objective of NIST SP 800-160 is to address security issues from a stakeholder's perspective, considering protection needs, concerns, and requirements and using established engineering processes to ensure that those needs and requirements are appropriately addressed early and throughout the life cycle of the system.

A supplement to International Standard ISO/IEC/IEEE 15288, *Systems and software engineering — System life cycle processes,* NIST SP 800-160 is extremely flexible in its application to meet the diverse needs of organizations. It is *not* intended to provide a specific recipe for execution. Rather, it can be viewed as a catalog or handbook for achieving the identified security outcomes of a systems engineering perspective on system life cycle processes—leaving it to the experience and expertise of the organization to determine what is correct for its purpose. Organizations using this guidance for systems security engineering can select and employ some or all of the thirty ISO/IEC/IEEE 15288 processes and some or all of the security-related activities and tasks defined for each process. Note that there are process dependencies, and that the successful completion of some activities and tasks necessarily invokes other processes or leverages the results of other processes.

NIST SP 800-160 is intended for several key audiences. It is important for engineering professionals in the public and private sectors. Dr. Ross pointed out at a recent meeting, "Just as civil engineers must design a bridge so it can sustain the weight of the vehicles that will cross it, so software engineers need to design code that can't be taken over by hackers. That means we must 'Build [trustworthiness] in, bake it in, don't bolt it on at the end.'" Dr. Ross also pointed out that the academic community is a critical audience in that this integration of systems engineering and systems security engineering must become part of our curriculum as we train the next generation of computer scientists and computer engineers.

Systems and Systems Security Engineering

The need for trustworthy secure systems stems from a wide variety of stakeholder requirements that are driven by mission, business, and a spectrum of other objectives and concerns. Systems engineering provides the basic foundation for a disciplined approach to engineering trustworthy secure systems. Trustworthiness, in this context, means simply worthy of being trusted to fulfill whatever critical *requirements* may be needed for a particular component, subsystem, system, network, application, mission, enterprise, or other entity. These requirements can include, for example, attributes of safety, security, reliability, dependability, performance, resilience, and survivability under a wide range of potential adversity in the form of disruptions, hazards, and threats. Effective measures of trustworthiness

are meaningful only to the extent that the requirements are sufficiently complete and well-defined, and can be accurately assessed.

Systems security engineering contributes to a broad-based and holistic security perspective and focus within the systems engineering effort. This ensures that stakeholder *protection needs* and *security concerns* associated with the system are properly identified and addressed in all systems engineering tasks throughout the system *life cycle*. This includes the protection of intellectual property in the form of data, information, methods, techniques, and technology that are used to create the system or that are incorporated into the system. Systems security engineering activities draw upon the combination of well-established systems engineering and security principles, concepts, and techniques to leverage, adapt, and supplement the relevant principles and practices of systems engineering. Such engineering activities are performed systematically and consistently to achieve a set of outcomes within every stage of the system life cycle, including concept, development, production, utilization, support, and retirement.

Principles and Concepts Associated with Systems Security Engineering

With sufficient understanding of systems security engineering, the context-sensitive application happens as a natural by-product of systems engineering. It is essential that the processes be adaptable and tailorable to address the *complexity* and *dynamicity* of all factors that define the system and its environmental context. This includes the system-of-systems environment where such systems may not have a single owner, may not be under a single authority, or may not operate within a single set of priorities. The approach to system security, described in NIST SP 800-160, can be used for different applications, including any Internet–connected devices that are part of the IoT. For example, a solution to potential security problems resulting from Internet-connected devices with vendor's default passwords should be defined during the systems engineering process before implementation of these devices.

NIST SP 800-160 emphasizes the importance of achieving adequate security, which is a trade space decision or judgement driven by the objectives and priorities of stakeholders. Such decisions or judgements are based on weighing security protection, performance, and effectiveness against all other performance and effectiveness objectives and constraints. The foundation of the reasoning results from having well-defined security objectives and security requirements against which evidence about the system can be accumulated and assessed to produce confidence and to justify the conclusions of trustworthiness. This approach, described in the document, is complementary to other existing models and risk management approaches

such as the six steps of *NIST Risk Management Framework*[2] and the functions, categories, and subcategories of the *Framework to Improve Critical Infrastructure Cybersecurity.*[3]

System Security in System Life Cycle Processes

NIST SP 800-160 describes the security considerations and contributions to system life cycle processes to produce the security outcomes that are necessary to achieve trustworthy secure systems. These security considerations and contributions are provided as systems security engineering activities and tasks—and they are aligned with and developed as security extensions to the system life cycle processes in ISO/IEC/IEEE 15288. The system life cycle processes are organized and grouped into four families. These include: Agreement Processes; Organizational Project-Enabling Processes; Technical Management Processes; and Technical Processes. NIST SP 800-160 lists the system life cycle processes and illustrates their application across all stages of the system life cycle.

Conclusion

As technology becomes further integrated into the systems that our governments, businesses, critical infrastructure, and citizens depend upon, it is critical that we make progress on improving the reliability of products and services. We must create more trustworthy, secure systems through a holistic approach, applying the proven concepts, principles, and best practices of science and engineering. NIST SP 800-160 is the first step toward securing the things that matter to us. It is the flagship publication in a series of planned systems security engineering publications addressing such topics as *hardware security and assurance*; *software security and assurance*; and *systems resiliency*. Each topic will be addressed in the context of the system life cycle processes contained in ISO/IEC/IEEE 15288 and the security-related activities and tasks that are described in NIST SP 800-160.

---

[2] The NIST Risk Management Framework is described in NIST Special Publication 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, available from https://doi.org/10.6028/NIST.SP.800-37r1.

[3] The *Framework to Improve Critical Infrastructure Cybersecurity*, or NIST Cybersecurity Framework, is available from https://www.nist.gov/document-3766.

In addition to the above publications, NIST plans to update its foundational security and risk management publications (NIST SPs 800-30, 800-37, 800-39, 800-53, and 800-53A)[4] to describe how such guidance can be applied at both the enterprise level and within a life cycle-based systems engineering process when component products and systems are in a developmental process.

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

[4] Publications that are part of the Joint Task Force Transformation Initiative supporting the Department of Defense, Intelligence Community, and Civil Agencies.