



Information Assurance Requirements Management Approach (IRMA)

Engineering Security into a System to Meet a Set of Specified Requirements

Problem

Currently, security engineering, Certification & Accreditation, and re-evaluation of certified systems are primarily accomplished by many organizations using a non-structured methodology that can vary greatly between projects. This ad-hoc methodology results in an inability to effectively articulate and defend the system's Security Support Structure (S3)/security architecture and makes it more challenging to certify (or re-certify) and accredit (or re-accredit) systems. Other limitations of the current security engineering method include: (1) inability to effectively track and manage requirements within a program that involve multiple organizations and/or interfaces; (2) lack of repeatability, a key factor in contracts concerned with Capability Maturity Model - Integration (CMMI); (3) difficulty in ensuring that "high assurance" IA requirements are completely, correctly, and consistently addressed in the system design, implementation and testing; and (4) inability to understand and document in an S3 the implementation of security requirements and use the S3 to assess the security impact of system changes.

Solution

SPARTA established an innovative security engineering approach called IRMA, which is integrated into SPARTA's system engineering process and used by SPARTA's system security engineers. It can be adapted to serve program objectives. IRMA provides a comprehensive, standardized IA engineering process to define the system's security requirements, build the system to meet these requirements and thus achieve a low-risk system certification & accreditation and/or approval to operate. IRMA aids a program in addressing numerous IA engineering challenges faced during system development efforts such as ensuring coverage

and traceability of requirements through the system-life cycle (across organizations and interfaces); articulating the security design; documenting the implementation of security features; defining and conducting security tests; efficiently reporting security test results; and implementing an effective delta verification program. Government programs are frequently established with short time-lines and low budgets. IRMA can help programs meet their aggressive objectives. Further, programs are also frequently expected to use and seamlessly integrate into infrastructure services, which are typically installed, implemented, and managed by organizations outside of the program office. The figure on the next page illustrates IRMA, and highlights the benefits the approach provides to the system development activities.

IRMA includes the use of a requirements management tool to capture requirements, policies, and standards, and manage the interpretation, derivation, decomposition, and tracing of requirements through the development phases. The tool is also used to allocate requirements and system components (e.g., functional components, physical subcomponents) to organizations involved in the system development/integration effort. For large complex programs it is expected that a full-featured COTS requirements management product (e.g., DOORS) is used by the program. SPARTA is looking into the feasibility of integrating IRMA and its artifacts into the SEACAT capability and investigating other tools to help analyze and test the S3.

Applicability

SPARTA developed the IRMA process, methodology, and tool to help its security engineers, either as a SETA contractor supporting the government customer or as a security engineering support contractor to the prime developer, enable creation of a system which meets all of its security requirements in a



Information Assurance Requirements Management Approach

Engineering Security into a System to Meet a Set of Specified Requirements

readily certified and accredited implementation. We use IRMA to help government personnel to identify, specify and track requirements throughout development life cycle. We use IRMA to help the prime contractor respond to the RFP, and then to architect, design, implement, and test the system against specified security requirements.

SPARTA is currently developing an IRMA specification (or "how to" guide) providing specific details for implementing IRMA, lessons learned, tips, examples, alternative strategies, and a complete data model for employing a COTS requirements management tool to support IRMA.

Benefits

IRMA can be integrated into any system engineering process and adapted to serve the program's objectives. It adds structure to the security engineering and integration process, ultimately lowering the end-to-end costs of the security engineering/integration effort, and it provides assurance that all requirements are addressed (especially important for complex integration efforts). IRMA provides an innovative technique for documenting the system's security design and a means to define and assign IA requirements responsibility across multiple development/integration organizations and interfaces. It ensures that security requirements

are satisfied with sound, well engineered, documented, and tested solutions, thereby making C&A a cost effective confirmation and residual risk analysis process.

IRMA can be used to track requirements and responsibilities (as determined during the requirements definition phase). It helps system stakeholders bring together the requirements traces from all teams/organizations into a single central requirements management database at periodic intervals to track the status of requirements implementation through development and into test and re-certification/re-verification. This enables the program to manage and track risk associated with designing, implementing/integrating, and testing complex systems.

Conclusion

IRMA significantly reduces risk in system engineering, integration, and C&A by ensuring that all requirements are allocated and tracked throughout the system's life cycle). IRMA establishes a structured approach for security requirements analysis and interpretation, security engineering and re-evaluation. It builds confidence with the system stakeholders (project management office, certifier, accreditor, mission owner, and system user) that the system was correctly designed and implemented to meet its security requirements.

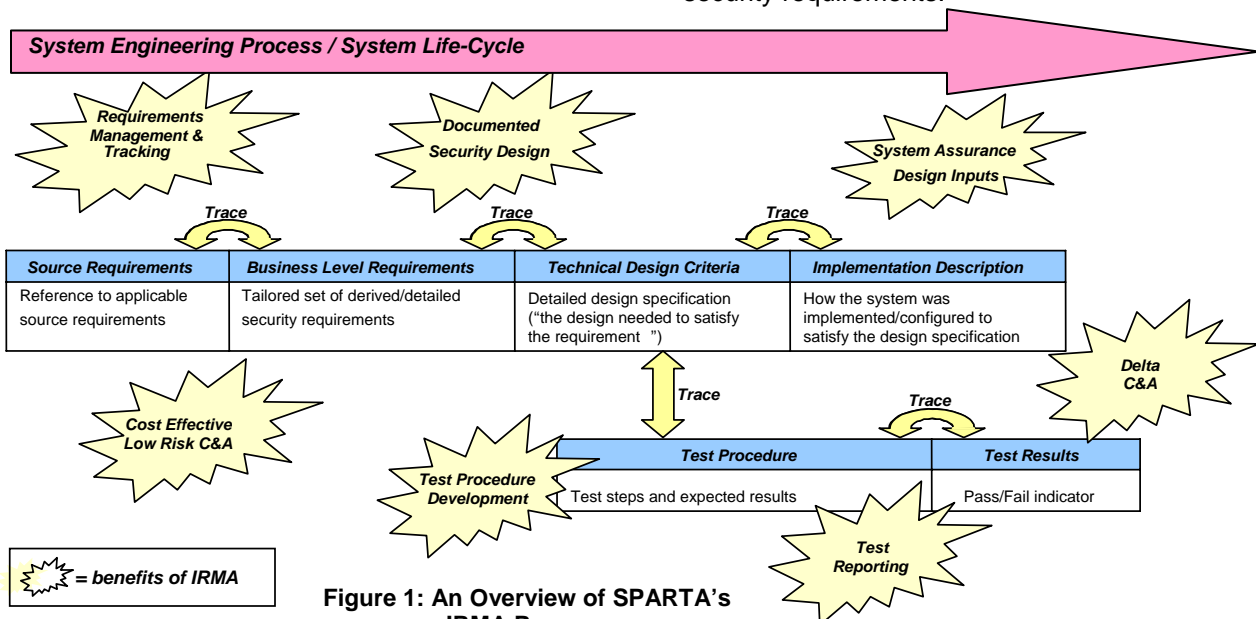


Figure 1: An Overview of SPARTA's IRMA Process