Information System Security Engineering: A Spiral Approach To Revolution

Donald M. Howe
Infosec Systems Engineering S9
Fort Meade, Maryland 20755

Abstract

Security criteria is not keeping pace with the Information Revolution. This paper describes an evolutionary, operational experience based approach for advancing criteria to be consistent with modern information systems. Interoperable and flexible systems/components are (and will be increasingly) demanded by users. This is especially true for distributed systems. These demands are not entirely consistent with today's foundational models of security, leading to the conclusion by many individuals that earthquake proportion changes in the foundations of information security are necessary. Fundamental revisions are necessary. There is, however, substantial risk in abandoning models that have been proven to work in many environments . The road to success is based on managing the risk associated with moving toward a new vision of information system security. A spiral approach to resolving information system security issues has been proposed and is now being practiced. It consists of incremental expansion of security theories and practices (based on existing theories) with directions of advancement determined by operational experience. The experience drives theory in a evolutionary, rapid prototype verification manner. This paper presents criteria related background, describes the spiral concept, and presents examples.

1 Introduction

The Trusted Computer Security Evaluation Criteria (TCSEC) [1] forms the basis for the evaluation of the effectiveness of security controls built into automatic data processing system products. The TCSEC identifies application independent (to the extent practical) security feature requirements and assurance requirements. The Trusted Network Interpretation (TNI) [2] extends the assurance requirements, and rating structure of the TCSEC to networks (Local Area Networks, LANs, and Wide Area Networks, WANs). The TNI describes a number of additional security services associated with networks. The TNI does not describe communications security, emanations security, physical security and other measures required of a secure network. The TCSEC and TNI were produced without an emphasis on distributed systems, virtual systems, database systems and shared applications. The Trusted Database Management System Interpretation (TDI) [3] was produced when commercially developed trusted operating systems were becoming available that could provide a basis for hosting secure applications such as multilevel secure Data Base Management Systems (DBMS). The TNI and TDI present valuable network partitioning and database subset-domain security concepts. The scope of the TCSEC, TNI and TDI are to be applied to the set of components comprising a trusted system, and is not necessarily applied to each system component individually. Further, an A1 system could conceivably consist of mostly untrusted products with a strong trusted reference monitor. The security foundation provided by the existing criteria is strong, but there are potential blind spots and ambiguities when the criteria is applied to modern systems.

The European community's Information Technology Security Evaluation Criteria (ITSEC) [4,5,6] has some advantages by explicitly incorporating integrity, availability, communication confidentiality and integrity,and network confidentiality and integrity. The draft Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) [7] provides for the evolving inclusion of information and experience acquired yearly. The (CTCPEC) revisions may take the form of additional criteria elements, clarifications, or reflections of interpretations. The U.S. Air Force Trusted Critical Computer System Certification Criteria (AFTCCSCC) [8] focuses on criticality criteria, in particular, on system integrity and assurance of service. The AFTCCSCC is intended to reduce or prevent high-impact incidents caused by failures, ac-

1993 ACM 0-89791-635-2

cidents, disasters, errors, and or other mishaps. A new U.S. Federal Criteria is being drafted to give guidance for both Department of Defense and Commercial applications.

All of the existing Criteria, Interpretations, and Guidelines have many valuable security features and assurance requirements. Unfortunately, there are criteria/interpretation gaps such as denial-of-service, and ambiguities such as the distribution of security services/mechanisms in modern interoperable and flexible information systems. The prevention and detection of malicious code is a potential blind spot that needs improvement. In addition, there appears to be difficulty in truly integrating communications security with computer security concepts and practice. Ideally, we are moving toward a unified (or set of) commercially available programmable processors and software that can be certified for a broad range of applications. The intent is to be able to perform the full range of distributed and concentrated security services, together with cryptographic functions, at a high level of assurance with cost-effective components in an integrated system.

The challenges are awesome. The opportunities are abundant. Success is mandatory. A structured engineering approach based on empirically derived evidence that builds on existing criteria/interpretations/guidelines appears to be the best approach. The spiral approach toward progress is the best vehicle for managing expectations and risk. It provides for evolutionary progress based on operational experience.

2 The Spiral Approach to Criteria Advancement

The Spiral Model [9,10] of software development is a risk-driven approach for software development. The spiral model proposed for criteria advancement in this paper is related to the software model. It is based on the same premise of managing risk by expanding capabilities by increments in an evolutionary manner, determined by operational experience.

The spiral process gets started by the hypothesis that a particular operational mission could be improved. The mission need is assumed to have some security requirements. If the security requirements and assurance requirements are not sufficiently defined in the existing criteria/interpretations/guidelines, then the project associated with the improving the mission is a candidate for advancing the criteria through operational experience. Ideal candidate systems are rapid prototype or testbed systems that, by their nature, lend themselves to timely resolution of issues.

It is important that the system-development/system- modification chosen to facilitate the advancement of criteria address each step of development. For example, a top level policy must be defined that clearly identifies access, authentication and integrity requirements. A concept of operations is also important. The classical stages of development include: mission identification, concept formulation, function specification, threat analysis, policy definition,vulnerability and risk analysis, architecture selection,concept of operations preparation, design/specification, fabrication/production/integration, installation, accreditation, and operation. The intent is not to require extensive formal treatment of each of the development steps but to insure the critical security feature and assurance requirements are addressed in some manner throughout development. The successful completion of a system(or phase of a system), together with a comprehensive analysis of the treatment of security features and assurance requirements, completes one cycle of the criteria spiral. The operational experience becomes the basis for criteria advancement.

The CTCPEC appears to lend itself to spiral criteria advancement through the annual review, identified in the criteria. The CTCPEC is relatively complete in the security requirements and assurance requirements covered, however, it seems somewhat shallow in its treatment of those topics in its current version.

Adopting an evolutionary/spiral/periodic-review approach to criteria advancement would require a authoritative review process staffed by recognized computer security individuals with credibility.

3 Examples

3.1 MAC Testbed

The Military Airlift Command [11,12] has established a Multi Level Secure (MLS) command center testbed. The testbed was initiated to meet operational requirements and provide a methodology for implementing MLS in other command centers. The objectives include: (1) evaluate emerging MLS commercial-off-the-shelf (COTS) products, (2) develop standards, methodologies, and tools for integrating COTS products into a Trusted Computing Base (TCB), (3) develop standards, methodologies, and tools for rehosting existing applications onto the TCB, and (4) prove

these methodologies by applying them to the migration of a specific, existing C2 system to a MLS environment.

A generic MLS testbed is shown in Figure 1. The Figure illustrates the variety of terminals/hosts and LANs. COTS trusted and untrusted terminals are shown for users, servers, routers, network managers and compartmented mode workstations. Four types of LANs are shown: (1) Management, (2) Trusted Terminal, (3) Trusted Workstation, and (4) Untrusted Terminal. This type of modern information system presents many interesting and critical security issues. The resolution of these issues should correspondingly be feed-back into criteria/interpretation/guideline creation/revision.

To date, there have been several lessons learned through the MAC testbed that should have a an effect on future criteria/interpretations/guidelines. As anticipated, one of the primary findings was that the lack of widely accepted standards can result in expensive, custom systems which can not be readily used interoperably with other systems. Standards and associated criteria are required for labeling, management, communication and integration capabilities. Guidelines for distributing security services would be very beneficial. A great deal of personnel resources could be saved through the introduction of interoperability and system/component flexibility associated criteria. Identifying viable standards and criteria should eliminate the need for dedicated processors for label management, TCB extensions, and ancillary security function processes. The goal is to be able to incorporate these capabilities as a intrinsic features of COTS products. Examining the detailed issues and lessons being learned in the MAC testbed is very useful for advancing criteria/interpretations/guidelines.

3.2 MLS Space Application

SPADOC 4 [13] is a system acquired by the Air Force U.S. Space Command to support space surveillance and space defense. This acquisition included: (1) MLS accreditation, (2) an evolutionary acquisition (spiral phases, each phase using a waterfall model), (3) COTS base, and (4) a need to support complex applications. The acquisition took place while the TCSEC was being circulated for comment. Criteria related issues encountered included: (1) difficulty in identifying and handling nonhierarchical access restrictions, (2) the evolutionary nature of the acquisition presented design-early verses retrofit security feature questions, and 3. audit trail capability at a fine level of granularity can have a severe impact on performance.

3.3 Current Applications

The Information System Security Engineering Office of the National Security Agency is currently working on six systems. The work is intended to apply system security engineering concepts and procedures. Complementary work is underway in the office to develop the methodology for information system security engineering. The lessons learned from the projects will be documented to improve the overall development process and provide a baseline of empirical data for future criteria/interpretations/guidelines.

4 Conclusion

This paper has proposed an approach to Criteria advancement through an iterative, evolutionary, approach based on operational experience. Operational experience is currently being gained through testbed and full scale operational projects. The methodology for advancing the Criteria is termed a spiral approach because of its foundational relationship to the spiral approach to software development.

Acknowledgement

The assistance of 1st Lt. Charles Tracey, USAF, the Information System Security Office MAC Testbed Project Engineer, is gratefully acknowledged. The review and comment contributions of Bruce Bottomley, Paul Boudra, Grant Wagner and Edward Zieglar have been very useful and are greatly appreciated.

References

[1] DOD. *Trusted Computer System Evaluation Criteria (TCSEC).* Department of Defense Standard 5200.28-STD, December 26,1985. (Orange Book.)

[2] NCSC. *Trusted Network Interpretation (TNI).* National Computer Security Center, NCSC-TG-011 Version-1. 31 July 1987. (Red Book.)

[3] NCSC. *Trusted Database Management System Interpretation of the Trusted Computer System Evaluation Criteria (TDI).* National Computer Security Center, NCSC-TG-21. Version2. April 1991.(Lavender Book.)

[4] UK IT CESG. "UK IT Security Evaluation and Certification Scheme." Undated pamphlet.

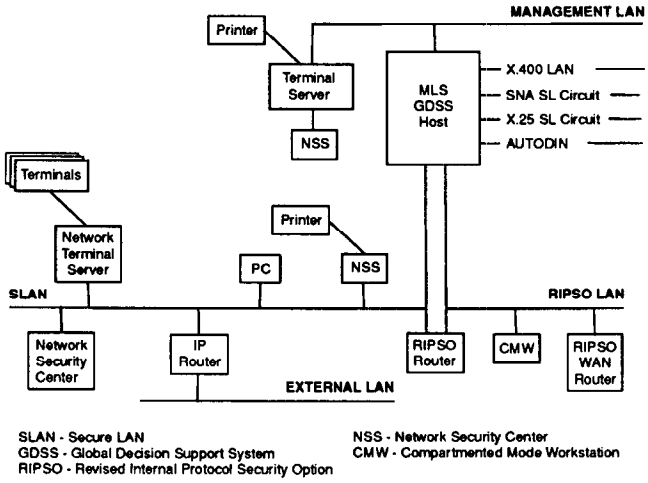

Figure 1: Generic MLS testbed (adapted from MAC)

[5] Branstad M.,Brewer D.,Jahl C., Kurth H., Pfleeger C. "Apparent Differences Between the U.S. TCSEC and the European ITSEC." *Proc. 14th National Computer Security Conference*, pp. 45–58. October 1991.

[6] Neumann P. G.,Proctor N. E. *A Designer's Handbook for Reliable Secure Distributed Systems.* (draft) prepared for Rome Laboratory COAC under contract F30602-90-C-0038.

[7] Government of Canada. *The Canadian Trusted Computer Product Evaluation Criteria (CTCPEC).* Canadian System Security Centre Communications Security Establishment . Version 2.1e. July 1991.

[8] U.S. Air Force. *Trusted Critical Computer System Certification Criteria (AFTCSCC).* Department of the Air Force. 14 August 1991.

[9] Boehm B. W. "Software Risk Management: Principles and Practices." *IEEE Software.* pp 32-41. January 1991.

[10] Boehm B. W. "A Spiral Model of Software Development and Enhancement." *IEEE Computer.* May 1988.

[11] Galik D., Tretick B. "Fielding Multilevel Security Into Command and Control Systems." *Proc. 7th Computer Security Applications Conference.* December 1991.

[12] Doncaster S., Endsley M., Factor G. "Rehosting Existing Command and Control Systems Into a Multilevel Secure Environment." *Proc. 6th Computer Security Applications Conference.* December 1990.

[13] Bodeau D. J., Reece M. J. "A Multilevel-Mode System for Space Applications: Lessons Learned." *Proc. 6th Computer Security Applications Conference.* December 1990.