1999-06-00

The Reference Monitor Concept as a Unifying Principle in Computer Security Education

Irvine, Cynthia E.

Proceeding IFIP TC11 WC11.8 First World Conference on INFOSEC Education

Proceeding IFIP TC11 WC11.8 First World Conference on INFOSEC Education, Kista, Sweden, pp. 27-37, June 1999
http://hdl.handle.net/10945/7200

The Reference Monitor Concept as a Unifying Principle in Computer Security Education

Cynthia E. Irvine
Naval Postgraduate School, Monterey, CA 93943 USA

Key words: Computer Security Education, Reference Monitor Concept, Assurance, Graduate Education

Abstract: For over twenty-five years, the Reference Monitor Concept [1] has proved itself to be a useful tool for computer security practitioners. It can also be used as a conceptual tool in computer security education. This paper describes a computer security education program at the Naval Postgraduate School that has used the Reference Monitor concept as a unifying principle for courses, laboratory work, and student research. The intent of the program is to produce graduates who will think critically about the design and implementation of systems intended to enforce security policies.

1. INTRODUCTION

Since its 1972 introduction in the "Anderson Report" [1], the Reference Monitor Concept has served the computer and network security communities in two ways. First it provides an abstract model of the necessary and sufficient properties that must be achieved by any system claiming to securely enforce access controls. Second, it has been a tool used in the design and implementation of secure automated systems.

As an abstraction, the Reference Monitor Concept does not refer to any particular policy to be enforced by a system, nor does it address any particular implementation. It is up to organisations to articulate the former as a part of the requirements for their computer systems [23]; the Reference Monitor Concept does not judge whether a policy is appropriate. Instantiations of the Reference Monitor Concept can vary from "monolithic"

systems to complex networks. The abstract notion is intended to, and can, encompass all systems required to enforce some access control policy. A particular instantiation of the Reference Monitor Concept will enforce a particular policy.

This paper describes a computer security education program at the Naval Postgraduate School that has used the Reference Monitor concept as a unifying principle for courses, laboratory work, and student research. The intent of the program is to produce graduates who will think critically about the design and implementation of systems intended to enforce security policies. In Section 2 the Reference Monitor Concept will be reviewed. Section 3 will provide and overview of the roles that NPS graduates will play in the architectural plans and construction of secure systems. The computer security program and how the Reference Monitor Concept is used as a pedagogical tool will be discussed in Section 4. A summary follows in Section 5.

2. REFERENCE MONITOR CONCEPT

What elements of the Reference Monitor Concept make it a powerful tool for analysing system security properties?

- First, it states that the access mediation mechanism is always invoked—every access is mediated. If this were not the case, then it would be possible for an entity to bypass the mechanism and violate the policy that must be enforced.
- Second, the access mediation mechanism is tamperproof. In the model, it is impossible for a penetrator to attack the access mediation mechanism such that the required access checks are not performed and authorizations not enforced.
- Third it "must be small enough to be subject to analysis and tests, the completeness of which can be assured" [1]. This must be the case, since if the mechanism could be demonstrated to be flawed, then it would not enforce the policy.

To date, the Reference Monitor Concept is the only effective tool we know of for describing the abstract requirements of secure system design and implementation. No viable alternative has been introduced and it has proven itself effective under close scrutiny[1]. Even if there were no demand for well engineered secure systems, should students learn about the Reference

[1] In 1997, the IEEE Symposium on Security and Privacy held a debate concerning the effectiveness of the Reference Monitor Concept in modern system development environments. The contest was won, by a large margin by those claiming that this abstraction continues to be an effective model for secure systems [15, 3, 20].

Monitor Concept? The answer is simple. It is a paradigm that we know works.

Is an educational program based upon the Reference Monitor Concept relevant? One might argue that market factors in computing today indicate that this model is no longer applicable. Some would ask: “The Reference Monitor Concept was introduced twenty-five years ago. If systems could be more secure by applying that paradigm, then why don't such secure systems exist?” Two factors contribute to the current situation. They are a combination of customer ignorance and management dictates that do not permit engineers to construct systems as well as they could. Customers who do not know better will accept insecure solutions. Given no market demand for security and business profit motives, management will not allocate corporate resources to engineer systems with better security. Clearly a decision not to construct sound secure systems does not mean that engineers do not know how to build them!

It might also be argued that political processes may make engineering of systems based upon the Reference Monitor Concept difficult. Scientists and engineers must recognize that their work is conducted within a political context [5]. Often negotiations are required and a variety of factors can impact the outcome of a project.

Several arguments favor the use of the Reference Monitor Concept as a teaching construct. First, using the Reference Monitor Concept, students will understand how a sound system could be built and can better analyse the impact of competing requirements. Second, it provides a framework for teaching a rigorous, analytical approach to systems that draws from many disciplines: programming languages, software engineering, operating systems, networks, etc. Third, it is a model that is applicable across a broad range of systems and guides students' creative processes when considering new systems.

3. UNIVERSITY CONTEXT

The Naval Postgraduate School (NPS) is a graduate university operated by the United States Navy. It grants MS and PhD degrees in a variety of engineering disciplines including computer science, physics, meteorology, oceanography, mathematics, engineering, and operations research. Most students receive MS degrees. The student population is comprised of U.S. military officers, Department of Defense and U.S. Government civilians, and officers from allied military services. The majority of the students have had from five to ten years of military experience since receiving their BA or BS

degrees. Many enter NPS graduate degree programs based upon aptitude rather than a prior degree in the field. Thus, the MS programs include both the courses and additional time required to compensate for a lack of undergraduate background. In Computer Science, the MS degree curriculum takes two years. In addition to courses, the degree requirement for an MS at NPS includes a thesis.

Graduates continue their careers as military officers. Although some computer science graduates apply their educations in the detailed design and implementation of systems, more often than not they participate in systems-level programs in a managerial capacity. Contractors and DoD civilians often provide the detailed engineering and programming. Among an officer's responsibilities may fall determination of whether or not a system meets DoD requirements. These may include security, fault tolerance, and a variety of performance and operational characteristics. An asset for graduates is the ability to apply their scientific and engineering knowledge to new problem areas while contributing to the soundness of solutions.

4. SECURITY PROGRAM

The Naval Postgraduate School computer security program [9] is intended to address the needs of a variety of students. All students enrolled in the Computer Science, Information Warfare, Command and Control, and Information Technology Curricula are required to take a survey course in computer security. Many also enroll in a course, entitled “Secure Management of Systems,” intended to address practical aspects of computer security such as certification, accreditation, risk analysis, and configuration management. Advanced courses are available for students who wish to pursue computer security as a specialization area. These courses include:

- Security Policies, Models and Formal Methods
- Secure Systems
- Database Security
- Network Security
- Advanced Topics

In the subsections that follow the use of the Reference Monitor Concept as a unifying notion for a security education program will be described. Included will be studies that preceded the articulation of the Reference Monitor Concept, its formulation, and techniques to create instances of the Reference Monitor Concept.

4.1 The Dangers of Penetrate and Patch

Prior to formulating the Reference Monitor Concept the team tasked with producing the Air Force report spent considerable time reviewing existing methods for securing computers. They found that *ad hoc* approaches to computer security were common.

In an introductory security course, students are often motivated through presentations of various system vulnerabilities and threats. An appendix to the Anderson Report provides a review of attacks, giving generic categories of attacks as well as specific examples where each of the attacks had be successfully mounted against an existing system. It described the activities of *tiger teams* engaged in games of *penetrate and patch* with vendors. The tiger team would exploit a system flaw and inform the vendor of the flaw. The vendor's repairs usually introduced additional flaws that were quickly exploited by the tiger teams. The conclusion of this analysis was that systems not *ab initio* designed to be secure, could never be repaired in such a way that users would be confident of system security.

A discussion of contemporary problems with comparisons to those encountered several decades ago illustrates the fact that by ignoring the Reference Monitor Concept, the situation in computer security is little improved over that of 1972.

The problem of malicious code is discussed. This includes not only viruses and malicious macros, but looks forward to code to be used in distributed, web-based systems. The confinement of executables to well-defined domains and analysis of code dependencies are addressed. The Anderson Report specifically addressed executable software. Users of Air Force systems were to be permitted to develop and execute their own software. This can be construed to include the loading of software developed elsewhere as well. Thus, there was potential for users to either accidentally or intentionally load malicious software. These issues illustrate the importance of a mechanism that is always invoked and that cannot be altered without authorization.

In addition, students discuss the problem of system subversion—the intentional insertion of an artifice at some point during a system's lifecycle [16]. Here the notion of assurance of correctness can be introduced. Any number of “Easter eggs” can be used to illustrate subversion of popular commercial products.

4.2 Passwords, Audit, Intrusion Detection

With the Reference Monitor Concept as the model for a system's central policy enforcement mechanism, students are introduced to supporting policies and instantiations of those policies. These include Identification and Authentication, and Audit.

From the Reference Monitor Concept perspective, Identification and Authentication provides the binding of a user's identity to active system entities executing on his or her behalf. Starting with identification and authentication in monolithic systems, discussions are extended to authentication in networks and single-signon support systems.

The notion of accountability is introduced and extended in discussions of audit. It is applicable regardless of the access control policy to be enforced. Students examine password criteria, password and account administration, and the implementation of trusted paths. The last can be illustrated with the Windows NT trusted path, which requires the use of a “secure attention key.”

Audit is an essential component in an accountability scheme. Students can examine traditional audit mechanisms and then expand to intrusion detection systems. An important challenge to be discussed is protection of the audit mechanism, the audit trail, and audit reduction tools. For distributed intrusion detection systems, discussions of the Reference Monitor Concept as applied to a network are pertinent.

4.3 Security Policy

The Reference Monitor Concept is policy neutral, however, in real systems policies are enforced.

One of the most significant problems facing many system developers is extracting a statement of organizational security policy from those who will own and operate the system. Too often a system requirement is stated as “security” and no more. This is meaningless. The computer scientist must ask: “You want security with respect to what?” Generally this is translated into statements regarding access to information by individuals for the purposes of disclosure and modification. This high level statement of policy may also include notions of availability. Availability as a security objective is subjective and students need to understand this.

A challenge is to understand whether the policy to be enforced makes sense and whether it is enforced correctly. Security models permit us to understand the former and provide a mathematical articulation of policy to which system implementations can be mapped for the purposes of verification.

Fortunately, military organizations have well articulated secrecy policies for information of various sensitivity levels. This permits us to examine these policies and determine how they can be expressed as technical policies in formal models. Considerable research has been conducted in the area formal models, for example [2, 4, 15]. Broad classes of policies are introduced to students: discretionary, information flow, work flow, etc. Beginning courses provide an overview of policies and models, while students in advanced courses study selected models in detail. By reading seminal papers, they explore the theoretical foundations of access control and complete laboratory exercises to prove the Basic Security Theorem and simple mandatory and discretionary models. At NPS, PVS [19] is used to introduce students to mechanical theorem proving techniques.

4.4 Secure System Construction

As a study topic, building secure systems allows students to learn about techniques that are applicable to the realization of Reference Monitor Concept objectives.

Students study classic papers such as that of Saltzer and Schroeder [4]. They continue by examining how classic concepts are (or are not) applied in modern systems such as Windows NT. In case studies and hands-on experiments, students test their understanding of protection mechanisms.

To implement a system in which every access to information is mediated by the reference monitor, system designers must determine which aspects of the system will be available directly and which will be virtualized. Virtualization provides a way to insert the reference validation mechanism between system resources and active entities. By examining both software and hardware, students examine hardware platforms and learn that some provide significant support for address space isolation [8, 18, 22], while if other platforms are used, the system developer must construct such isolation mechanisms in software. Students learn how hardware resources can be virtualized so that access checks can be applied [6, 12, 24]. The use of hardware mechanisms to construct isolated address spaces that provide for self protection of a reference validation mechanism and separation of application-level entities is examined. Software to utilize and extend those facilities is discussed.

The Reference Monitor Concept is an ideal; real systems are imperfect. Students explore covert channels and the relationship between assurance and the system development lifecycle. They learn the importance of software engineering techniques as applied to the creation of Reference Monitor Concept instances.

4.5 Network Security

The NPS program includes network security in its introductory as well as an advanced course on network security. Both encompass a wide variety of topics including cryptography, protocols, public key technology, IP-security, virtual private networks, secure mail, web security, etc. Evolving standards and technologies permit (or force) classroom presentations in network security to be refreshed frequently. Yet, the underlying principles have already been established. The full power of the Reference Monitor Concept can be recognized in these distributed contexts.

A physical network may support a logical system, i.e. a virtual network. Some policy will be applicable to that network. The standard requirements apply: the policy enforcement mechanism must always be invoked, must be tamperproof, and it must be correct. Students can discuss how end systems, intermediate nodes, cryptographic mechanisms, and protocols combine to support a distributed policy enforcement mechanism. They can examine how reference monitor instantiations at end systems interact across a network. Each individual reference monitor must have predefined or negotiated cryptography and protocols necessary to ensure its self protection as well as satisfy the requirements for communication with the remote system. The use of virtual private networks to isolate different user groups and the use of mechanisms to protect hosts against tampering places the concepts of secure system design and implementation at the center of network security.

4.6 Database Security

Database security illustrates the application of the Reference Monitor Concept to massive systems with complex security policies. Several case studies, such as SeaView [13], allow advanced students to understand that highly trusted secure systems can be constructed. Students learn how the concept of TCB subsets [21] can be applied in systems that enforce a hierarchy of security policies.

As an aside, it is noteworthy that there are database topics that currently do not fit into our Reference Monitor Concept framework. Statistical database security, inference and aggregation are among the topics covered in the database security course that fall outside of the framework of our unifying notion. They are, however, quite important, particularly for privacy concerns in an era of increased use of knowledge bases and data mining.

4.7 System Evaluation and Management

Critical military systems are subjected to a certification and accreditation process. A study of these processes permits students to examine the criteria and methods used to evaluate the effectiveness of reference monitor instances. They learn the cost of high assurance and some reasonable compromises that can be made with respect to assurance and policies. For example, they learn that a mechanism for enforcement of a weak policy [7] may not merit the extraordinary efforts one might invest in the assurance of a system intended to enforce a critical access control policy.

Configuration management and system administration play an important part in system lifecycle assurance. In both introductory and advanced courses students are exposed to these topics. The advanced course allows students to configure and use a variety of contemporary tools for monitoring and maintaining system health. To ensure that student experiments do not escape from the laboratory and corrupt campus networks, a small, isolated network is used for security tests.

The Reference Monitor Concept and assurance is discussed in the context of legal issues. As connectivity and dependence upon computers expands, the possibility of computer accidents and subsequent litigation will increase. For example if a system has no assurance of correctness of policy enforcement or penetration resistance, can a user be held accountable for actions of malicious software?

4.8 Thesis Research

Thesis research permits students to apply what they have learned in class to current problems. Certain research projects lend themselves to the direct application of the reference monitor concept [10, 11]. Often students are involved research projects involving applications or middleware [25]. In these projects, they learn how dependencies on underlying security mechanisms affect the assurance arguments that can be made for their system. They learn how to implement the reference monitor concept within a TCB subset [21] and how notions of a distributed reference monitor [17] can be applied. In application and middleware efforts that rely upon weakly secure commercial products, students learn the limitations of the underlying systems and are better able to appreciate the value of coherent security architectures.

The thesis program allows students to work with both NPS faculty and staff on current research topics. In addition, students address topics of interest to Department of Defense and U.S. Government sponsors. Thesis

supervision may be collaborative, involving outside experts from government and industry as advisors. These external contributors enrich the educational program and help students to examine the Reference Monitor Concept across a broad range of emerging areas.

5. SUMMARY

For over twenty-five years, the Reference Monitor Concept has proved itself to be a useful tool for computer security practitioners. It can also be used as a conceptual tool for constructing a computer security education program. The computer security program at the Naval Postgraduate School is intended to prepare military officers to participate in the design and implementation of future systems. By introducing students to the Reference Monitor Concept and subsequently describing how it can be realized, graduates are equipped with an essential tool for constructing and assessing the effectiveness and assurance of security policy enforcement in automated systems.

REFERENCES

1. Anderson, J. P., *Computer Security Technology Planning Study*. Technical Report ESD-TR-73-51, Air Force Electronic Systems Division, Hanscom AFB, Bedford, MA, 1972. (Also available as Vol. I, DITCAD-758206. Vol. II DITCAD-772806).
2. Bell, D.E, and LaPadula, L. *Secure Computer Systems: Mathematical Foundations and Model*. Technical Report M74-244, MITRE Corp., Bedford MA, 1973.
3. Blakley, B., and Kienzle, D. M. Some Weaknesses of the TCB Model. In *Proceedings of the IEEE Symposium on Security and Privacy*, pp 3-5, Oakland, CA, May 1997, IEEE Computer Society Press.
4. Denning, D. A Lattice Model of Secure Information Flow. *Communications of the A. C.M.*, 19(5):236-343, 1976.
5. Forman, B. The Political Press in Systems Architecting. In Eberhardt Rechtin and Makr W. Maier, eds. *The Art of Systems Architecting*, pp. 199-209. CRC Press, Boca Raton, FL 1997.
6. Gasser, M. *Building a Secure Computer System*. Van Nostrand Reinhold, New York, NY, 1988.
7. Harrison, M., Ruzzo, W., and Ulman, J. Protection in Operating Systems, *Communications of the A.C.M.*, 19(8):461-471, 1976.
8. Intel, *Intel Architecture Software Developer's Manual, Volume I: Basic Architecture*. Intel Corporation, Santa Clara, CA 1997.
9. Irvine, C.E., Warren, D. F., and Clark, P. C. The NPS CISR Graduate Program in INFOSEC: Six Years of Experience. *In Proceedings of the 20th National Information Systems Security Conference*, pp. 22-30, Baltimore, MD, October 1997.
10. Irvine, C. E., Anderson, J.P., Robb, D., and Hackerson, J. High Assurance Multilevel Services for Off-The Shelf Workstation Applications. In *In Proceedings of the 21st*

National Information Systems Security Conference, pp 421-431, Crystal City, VA, October 1998.

11. Isa, H.R., Shockley, W. R., and Irvine, C. E., A Multi-threading Architecture for Multilevel Secure Transaction Processing, to appear in *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA, May 1999, IEEE Computer Society Press.
12. Karger, P.A., Zurko, M.E., Bonin, D.W., Mason, A.H., and Kahn, C.E., A VMM Security Kernel for the VAX Architecture. In *Proceedings of the IEEE Symposium on Researchin Security and Privacy*, pp. 2-19, Oakland, CA, May 1990, IEEE Computer Society Press.
13. Lunt, T. F., Schell, R. R., Shockley, W.R., Heckman, M. and Warren, D.F. A Near-Term Design for the SeaView Multileve Database System. In *Proceedings of the IEEE Symposium on Security and Privacy*, pp 234-244, Oakland, CA, May 1988, IEEE Computer Society Press.
14. McLean, J. Security Models. In j. Marciniak, ed. *Encyclopedia of Software Engineering*. Wiley and Sons, Inc., New York, NY 1994.
15. McLean, J., Is the Trusted Computing Base Concept Fundamentally Flawed? In *Proceedings of the IEEE Symposium on Security and Privacy*, pp 2, Oakland, CA, May 1997, IEEE Computer Society Press.
16. Myers, P. *Subversion: The Neglected Aspect of Computer Security*, M.S. Thesis, Naval Postgraduate School, Monterey, CA, 1980.
17. National Computer Security Center, Trusted Network Interpretation of the Trusted Computer Evaluation Criteria, NCSC-TG-005, July 1987.
18. Saltzer, J.H., and Schreder. The Protection of Information in Computer Systems. *Proceedings of the IEEE*, 63(9):1278-1308, 1975.
19. Shankar, N., Owre, S., and Rushby, J. *PVS Prover Guide*. Technical Report, Computer Science Laboratory, SRI, Inc., Menlo Park, CA, September 1993.
20. Shockley, W. R., and Downey, J.P. Is the Trusted Computing Base Concept Fundamentally Flawed?: The Case for the Negative. In *Proceedings of the IEEE Symposium on Security and Privacy*, pp 6-7, Oakland, CA, May 1997. IEEE Computer Society Press.
21. Shockley, W. R., and Schell, R.R. TCB Subsets for Incremental Evaluation. In *Proceedings of Third AIAA Conference on Computer Security*, pp 131-139, December 1987.
22. Sibert, O., Porras, P., and Lindell, R. The Intel 80x86 Processor Architecture:Pitfalls for Secure Systems. In Proceedings of the IEEE Symposium on Security and Privacy. pp 211-222, Oakland, CA, May 1995. IEEE Computer Society Press.
23. Sterne, D. On the Buzzword “Security Policy”. In *Proceedings of the IEEE Symposium on Security and Privacy*, pp 219-230, Oakland, CA, May 1991. IEEE Computer Society Press.
24. Wray, J.C. An Analysis of Covert Timing Channels, In *Proceedings of the IEEE Symposium on Security and Privacy*, pp 2-20, Oakland, CA, May 1991. IEEE Computer Society Press.
25. Wright, R., Integrity Architecture and Security Services Demonstration for Management System for Heterogeneous Networks. M.S. Thesis, Naval Postgraduate School, Monterey, CA June 1998.