Title Page

Title: Ware to Start?

Contact Information:
Rayford B. Vaughn, Jr.
Department of Computer Science
Mississippi State University
PO Box 9637
Mississippi State, MS 39762
(662) 325-7450; Fax 325-8997
vaughn@cs.msstate.edu

Track to which submitted: "Experiences with course or laboratory development" - GENERAL

Abstract
This paper suggests that the instruction of computer security in the university environment should begin with a through examination of the 1970 Report of the Defense Science Board Task Force on Computer Security, "Security Controls for Computer Systems". Dr. Willis Ware was the chair of this task force in 1970. While the report itself is dated and the architectures discussed no longer exist, the problem identification contained in the report and the technical issues examined remain valid today - some 30 years after the report was released. Students having read this report prior to beginning a semester course appear better prepared to then understand and follow on with formal instruction in models, multilevel security, trusted operating systems, and the need for a holistic approach to the security problem. Teaching Saltzer and Schroeder's principles is made far easier as is the need for trusted development environments, strong process control, policy enforcement, and accountability.

Brief Biographical Sketch of Author

Dr. Rayford Vaughn is currently a professor of computer science at Mississippi State University where he teaches and conducts research in the areas of Software Engineering and Information Security. Prior to joining the University, he completed a twenty-six year career in the Army where he commanded the Army's largest software development organization and created the Pentagon Single Agency Manager organization to centrally manage all Pentagon IT support. While on active duty with the Army, he served a three-year assignment with the National Security Agency's National Computer Security Center where he authored national level computer security guidance and conducted computer security research. After retiring as a full Colonel in June 1995, he accepted a position as Vice President of DISA Integration Services, EDS Government Systems where he was responsible for a wide variety of technical service contracts and customer satisfaction.

Dr. Vaughn has over 40 publications to his credit and is an active contributor to software engineering and information security conferences and journals. He currently has over $1M in information security related funding and leads a security research effort at Mississippi State University. He holds a PhD in Computer Science from Kansas State University.

Ware to Start?

Rayford B. Vaughn, Jr.
Department of Computer Science
Mississippi State University
PO Box 9637
Mississippi State, MS 39762
(662) 325-7450; Fax 325-8997
vaughn@cs.msstate.edu

Abstract

This paper suggests that the instruction of computer security in the university environment should begin with a through examination of the 1970 Report of the Defense Science Board Task Force on Computer Security, "Security Controls for Computer Systems". [1] Dr. Willis Ware was the chair of this task force in 1970. While the report itself is dated and the architectures discussed no longer exist, the problem identification contained in the report and the technical issues examined remain valid today - some 30 years after the report was released. Students having read this report prior to beginning a semester course appear better prepared to then understand and follow on with formal instruction in models, multilevel security, trusted operating systems, and the need for a holistic approach to the security problem. Teaching Saltzer and Schroeder's principles [2] is made far easier as is the need for trusted development environments, strong process control, policy enforcement, and accountability.

1. Introduction

More than 30 years ago, a confidential document was produced within the Department of Defense by the Defense Science Board (DSB), which for the first time, took a comprehensive look at the emerging computer security problem in this country. The report was titled "*Security Controls for Computer Systems*" and the task force that wrote it was chaired by Dr. Willis Ware - then with the Rand Corporation. As a computer security student, lecturer and practitioner for over 15 years, the author of this paper often cited Ware's early work along with a litany of other early papers, but never actually studied the paper itself. This was a mistake. After having recently read the paper in preparation for offering another computer security course for the Spring 2001 semester, I was struck by the applicability of the paper in today's computer security context. Those who teach this subject today and who have also not actually studied this report would be well advised to do so. More importantly, requiring students to read it and then to discuss its applicability serves as a wonderful introduction to the many topics that will be addressed over the course of the semester. The instructor will undoubtedly have many opportunities to return to the

Ware conclusions and cautions during the course of study.

2. The Report Itself

Access to the report for students and faculty is not difficult. It can be downloaded easily by accessing the very useful ACSAC Bookshelf at http://www.acsac.org (please note that this is also a very helpful resource for security students in general) or by accessing the History of Secure Computing at http://seclab.cs.ucdavis.edu/projects/history/ (another excellent resource cite maintained by Dr. Matt Bishop at UC-Davis).

Once acquiring the report, the student has roughly 80 typewritten pages of analysis to read that represents the first comprehensive look at the security problem and lays the basis for research efforts that continue today. The report is divided into four sections:

- *The Nature of the Problem:* A discussion of the security problem itself, threats to systems, architectures and their impact on our ability to secure them, a taxonomy of security problems, and some definitions (most of which hold today).
- *Policy Considerations and Recommendations*: This section lays the groundwork for future discussion of the architectural underpinnings of the DOD Standard 5200.28 (Orange Book) [3] and later ISO Standard 15408 (see http://www.niap.nist.gov/cc-scheme). The need for audit, policy, labels, certification, evaluation, and assurance is addressed here.
- *Technical Recommendation*s: Here the panel members lay out the early concepts of access control mediation, monitoring system security relevant events, leakage points, open versus closed systems, the need to protect system assets while in various states of processing, communication, and storage, and finally, an excellent discussion of areas recommended for research (most still applicable today).
- *Management and Administrative Control*: The briefest of all the sections in that it consists of only two pages. This section points out the vulnerabilities present in the lack of standards, controlled and uncontrolled shutdowns, file control, personnel issues, magnetic storage media, and maintenance issues. Although most of this would fall in the area of physical and procedural security today, nonetheless, the discussion is relevant to today's problem.

This first attempt to codify the principles of the security problem refers to the issue as a "technical-administrative" problem. Later papers and textbooks stress the same lesson when we discuss the need for a "holistic" approach to security or when we use lessons like "security is only as strong as the weakest link in the chain". The Defense Science Board was quick to recognize that the problem reached far beyond technical solutions. In fact, more than half of the report itself addresses management, personnel, procedural, and physical

security issues and stresses that they are just as important as software and hardware technical solultions.

Lastly, the report alluded to the problem we face today in the skill we call "security engineering" when the members of the study group agreed that " *...the security problem of specific computer systems must, at this point in time, be solved on a case-by-case basis employing the best judgement of a team consisting of systems programmers, technical hardware and communications specialists, and security experts*." In this day and age, we often refer to the pursuit of "sufficient security" to meet a customer's needs and we use a team of systems and software engineers to do so - normally with the assistance of a security expert. Security engineering has not changed a great deal since the board issued the finding above.

3. The Seven Conclusions

The conclusions of the DSB report make for interesting class discussion topics in and of themselves. In fact, most discussion surrounding the conclusions reached in 1970, tend to be why the issue remains valid today and why it is still unsolved. Students begin to discover though this discussion just how difficult the computer security problem really is, the fact that it is more than an architectural issue, and that there is a long history of scientific research attached to each issue. Those that teach this subject should contrast this discussion result against simply starting off with a textbook and papers. The DSB report seems to add more credibility in the mind of the student and leaves a more lasting impression. This section of the paper both quotes and paraphrases findings from the report and briefly comments on their applicability today. Apologies are extended to the board members if any part of this synopsis overlooks an important issue.

a. **Conclusion 1**: Providing *satisfactory security controls in a computer system is in itself a system design problem. A combination of hardware, software, communication, physical, personnel, and administrative-procedural safeguards alone are not sufficient.*

This conclusion could quite easily make it into the Federal Best Security Practices list today. The principle of a holistic approach to security that is taught in every computer security class is brought home in this conclusion. It also serves as a springboard for discussions surrounding the various types of security (i.e., physical, communications, personnel, etc.), the Saltzer and Schroeder principles of secure system design [2], the Orange Book [3] architectural considerations for assurance, Gasser's lessons [4] on building a secure computing system, and perhaps even social engineering. A comparison of this conclusion with the DSB report sections on Managerial, Technical, and Administrative controls is appropriate here also.

b. **Conclusion 2**: *Contemporary technology can provide a secure system acceptably resistant to*

external attack, accidental disclosures, internal subversion, and denial of use to legitimate users for a ***closed environment****.*

This finding (coupled with conclusion 3 described below) still largely applies today. It is far easier to secure a system with cleared users, good physical protection, and communication line protection (the report's definition of *closed environment*), then it is to secure a system where the user community is not trusted, the communication lines are insecure, and the security perimeter is unknown (an example of this might be electronic commerce as we exercise it today). This conclusion and classroom discussion is an excellent means to introduce the notions of system high processing (or perhaps dedicated processing), the difficulty of providing multilevel security, the need for PKI implementation, e-commerce security issues, SSL, and security perimeters. Additionally, this presents an opportunity to discuss with the class why this conclusion is essentially still valid today - some 30 years after it was written.

c. **Conclusion 3**: Contemporary *technology cannot provide a secure system in an* ***open environment****.*

This conclusion is closely related to the previous one and the same discussion applies. The DSB defined an open environment as one in which communication circuits and end equipment were unprotected and in which the users were "uncleared". In today's world we might change this definition to say that the user's are unknown and that the communication circuits are either not protected or are minimally protected (which more accurately reflects the e-commerce situation today).

d. **Conclusion 4**: It *is unwise to incorporate classified or sensitive information in a system functioning in an open environment unless a significant risk of accidental disclosure can be accepted*.

While the applicability of this conclusion to today's problems is subject to debate (depending on where one stands on the issue of multilevel security or MLS), the conclusion itself opens the door to a discussion of multilevel security, assurance, the architectural considerations present in DoD Standard 5200.28, and the early attempts at assurance metrics in the form of Orange Book Digraphs. Additionally, one can use this conclusion to discuss the meaning and difficulty of formal methods, models, and policy and why they are important to the creation of an MLS solution. Many would agree that this conclusion is still valid today, albeit to a lessor degree.

e. **Conclusion 5**: *Acceptable procedures and safeguards exist and can be implemented so that a system can function alternately in a closed and open environment.*

This conclusion can be used to discuss the early solution known as "periods processing" and what that entailed (such as concern with residual information, shut down and

restart, processing perturbation, and separation of duty concepts. A good discussion can follow as to why many organizations today which deal with classified information, end up with two or more computers on a single employee's desk. The need to provide multilevel security solutions can be argued quite successfully in such a discussion. Additionally, the conclusion reached can still be applicable today - but with the decline in hardware costs and the proliferation of smaller, more powerful computer, it is really unnecessary.

f. **Conclusion 6**: *Designers of secure systems are still on the steep part of the learning curve and much insight and operational experience with such systems is needed.*

While not a surprising finding in 1970, students find it a bit interesting that this appears to still be the case today. Much progress and understanding has been accomplished since the DSB report was issued some 30 years ago. It is largely because of that progress and understanding, that we realize even more today that we are still on the "learning curve" and that we still need much more empirical study to determine what works and what does not. Using this conclusion to discuss the history of computer security and previous efforts to describe security architectures and then measure conformance to those architectures is an approach that seems to work well in the classroom. While we know much more today about how to design stronger mechanisms in systems, we have also discovered flaws in our reasoning about evaluated trust, formal methods, models, and other false starts. Examples useful in the classroom include security flaws that exist and continue to be reported in *Windows NT* - a product that was purportedly built with security in mind. At least one security product, STAT Analyzer from Harris Corporation,(www.statonline.com) reports over 1000 vulnerabilities in its database associated with Windows NT. These sorts of examples tend to prove that conclusion 6 is still valid.

g. **Conclusion 7**: *Substantial improvement in security controlling systems can be expected if certain research areas can be successfully pursued.*

This conclusion is one that needs no justification - either in 1970 or today. Research is always necessary to improve understanding and to progress. Classroom discussions surrounding this specific conclusion start with the research topics of 1970, move though many of the early operating system research efforts, and culminates with a list of interesting research topics today (e.g., information assurance metrics, intrusion detection, e-commerce security, etc.).

4. Summary

After having taught computer security at three institutions and having worked in the field for over 15 years, this instructor finds the 1970 Defense Science Board Report an excellent vehicle for launching new students into the technical and

managerial aspects of information assurance. It turns out from an examination of the conclusions found then compared with problems faced today, that the basic issues have not changed much. What has changed are the architectures, the ease of attack, and perhaps our collective understanding of the complexity associated with computing security. Students seem to relate to this report quite easily and its organization provides a framework from which many hours of discussion can occur - moving the student from 1970, through key historical events, and into the present. Although perhaps not a technique all instructors might adopt, this author prefers to hand out the DSB report the first day of class and test the students on it the second week of class. Experience has shown that such a rapid start pushes the student into a security concentration much faster than a textbook reading can do and it develops interest in the topic much faster. Nothing in this paper should be construed to indicate that use of a security textbook should be downplayed. There are many good texts on the market (see [5,6,7] for examples) and this instructor has used several with success. Supplementing the text with the DSB reading is suggested however, and using it very early in the class is preferred.

5. Acknowledgements:

I wish to acknowledge the patience of my students in the Mississippi State University CS4243/6243 Computer and Information Security Class, Spring 2001, who read, assimilated, and discussed the Defense Science Board report with great enthusiasm. I also acknowledge support from NSF Grant CCR-0085749 which has provided many ideas useful in this class with respect to the provision of computing security. Similarly, support from this grant has attracted several undergraduates to continue study of this important topic at the graduate level.

6. REFERENCES

[1] Report of Defense Science Board Task Force on Computer Security, "Security Controls for Computer Systems", Department of Defense, February 1970.

[2] Saltzer, J. and Schroeder, M. "The Protection of Information in Computing Systems." Proceedings of the IEEE, v63, n9, Sep 1975, pp. 1278-1308.

[3] Department of Defense Standard, *Department of Defense Trusted Computer System Evaluation Criteria,* DOD 5200.28-STD, GPO 1986-623-963, 1985.

[4] Gasser, M., Building a Secure Computer System, Van Nostrand Reinhold, 1988.

[5] Summers, R., Secure Computing: Threats and Safeguards, McGraw Hill, 1997.

[6] Pfleeger, C, Security in Computing, 2d ed, Prentice Hall, 1997.

[7] Gollmann, D., Computer Security, Wiley, 1999.