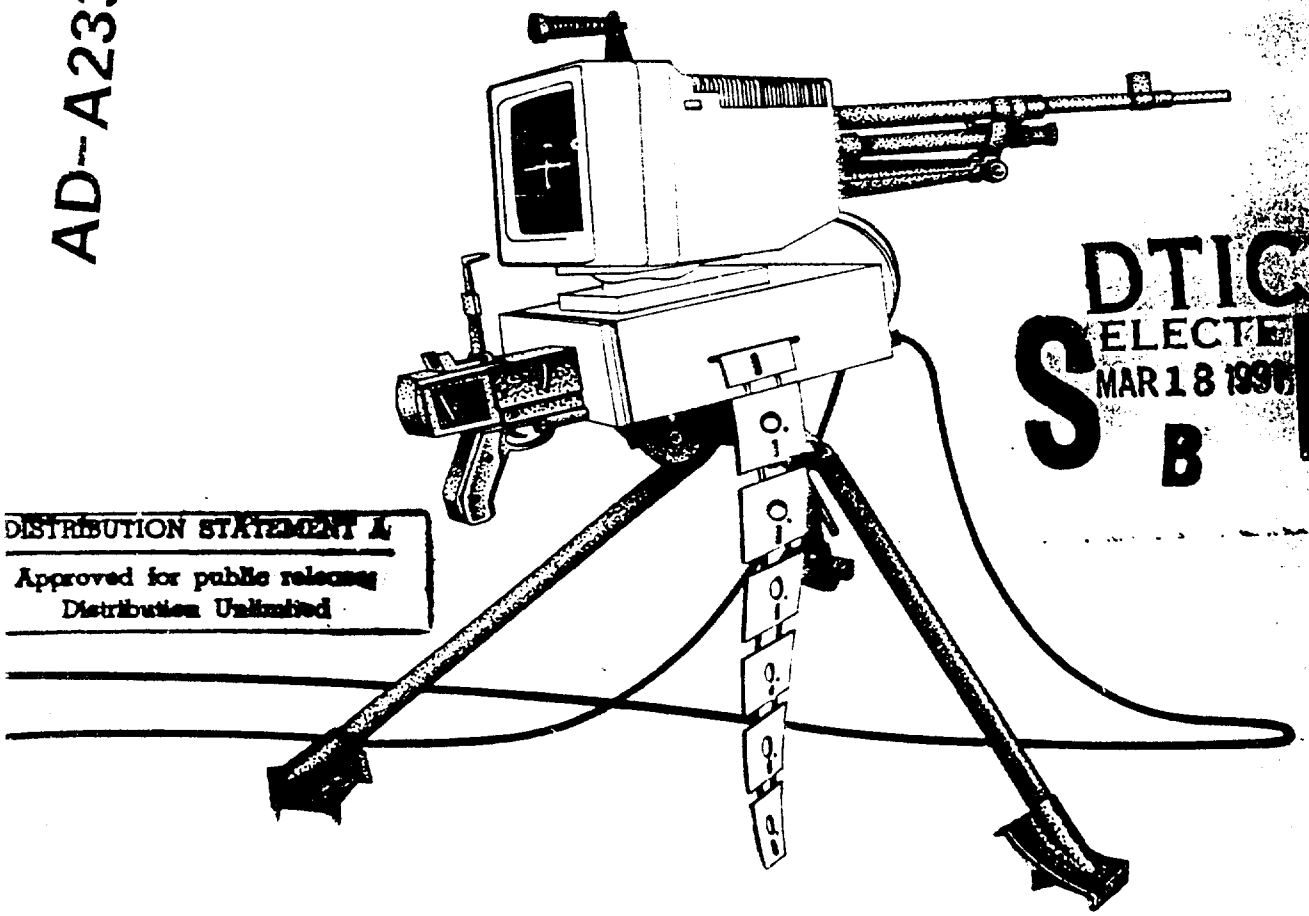
An Analysis of Trusted Computer Evaluation and Certification

Maj Eric C. Lewallen, USAF



REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	DEC 90	

4. TITLE AND SUBTITLE

An Analysis of Trusted Computer Evaluation and Certification

5. FUNDING NUMBERS

6. AUTHOR(S)

Maj Eric C Lewallen, USAF

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

AUCADRE/PTP
Maxwell AFB AL 36112-5532

8. PERFORMING ORGANIZATION REPORT NUMBER

AU-ARI-89-13

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Public Release

12b. DISTRIBUTION CODE

A

13. ABSTRACT *(Maximum 200 words)*

14. SUBJECT TERMS

15. NUMBER OF PAGES

41

16. PRICE CODE

NONE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLAS	UNCLAS	UNCLAS	

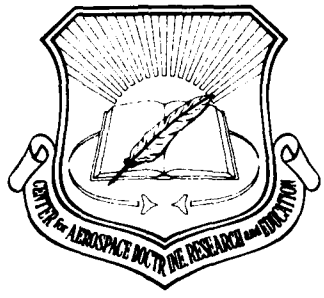
Cut along dotted line

After you have read the research report, please give us your frank opinion on the contents. All comments—large or small, complimentary or caustic—will be gratefully appreciated. Mail them to: CADRE/RI, Building 1400, Maxwell AFB AL 36112-5532.

An Analysis of Trusted Computer Evaluation and Certification

Lewallen

Thank you for your assistance



Research Report No. AU-ARI-89-13

An Analysis of Trusted Computer Evaluation and Certification

by

ERIC C. LEWALLEN, Maj, USAF
Research Fellow
Airpower Research Institute

Air University Press
Maxwell Air Force Base, Alabama 36112-5532

December 1990

DISCLAIMER

This publication was produced in the Department of Defense school environment in the interest of academic freedom and the advancement of national defense-related concepts. The views expressed in this publication are those of the author and do not reflect the official policy or position of the Department of Defense or the United States government.

This publication has not been reviewed by security and policy review authorities and is not cleared for public release. It is the property of the United States government and is not to be reproduced in whole or in part without the permission of the commander, AUCADRE, Maxwell Air Force Base, Alabama.

Contents

Illustrations

Foreword

At the very heart of our war-fighting capability is computer systems. We depend upon these machines as a key force multiplier to defeat a larger and more heavily armed adversary. Yet these machines are vulnerable to many security threats. Progress in developing and acquiring trusted computer systems—hardware and software together that enforce a security policy—has been slow over the past 10 years, providing users with few products. Clearly, this situation must improve. Our command, control, and communication systems need trusted computer systems to counteract the growing threat to our systems and provide a multilevel secure processing capability.

Maj Eric C. Lewallen has thoroughly examined the trusted computer evaluation and certification processes. Although there are significant problems in developing and acquiring trusted systems, Major Lewallen's report reveals an increase in interest and support at all levels to resolve this important issue. His recommendations address actions the Air Force can take to assist computer security personnel in the difficult job of developing and acquiring these systems.

DENNIS M. DREW, Col, USAF
Director
Airpower Research Institute

About the Author

Maj Eric C. Lewallen

Maj Eric C. Lewallen completed this study while assigned to the Airpower Research Institute (ARI), Air University Center for Aerospace Doctrine, Research, and Education (AUCADRE) at Maxwell AFB, Alabama. In 1976 Major Lewallen completed helicopter flight training at Fort Rucker, Alabama. After completing helicopter transition training at Kirtland AFB, New Mexico, he was assigned to the 71st Aerospace Rescue and Recovery Squadron at Elmendorf AFB, Alaska, as an HH-3 rescue helicopter pilot. In 1980 Major Lewallen went to the 1550th Aircrew Training and Test Wing at Kirtland AFB as an HH-3 instructor/flight examiner. In 1981 he was selected for fixed-wing transition. After completing his transition training, he served as a T-37 instructor pilot and academic instructor at Columbus AFB, Mississippi, from 1982 to 1985. In 1985 Major Lewallen was assigned to Scott AFB, Illinois, where he worked as a search and rescue controller, executive officer, and communications program manager. In 1988 the commander of the Air Force Communications Command selected him for the AUCADRE research fellow program.

Major Lewallen holds a master's degree in business administration and is a graduate of Squadron Officer School and Air Command and Staff College. He is currently assigned to the Standard Systems Center, Gunter AFB, Alabama, as the Air Force Defense Data Network program manager. He and his wife, Alice, have two children, Elizabeth and Clay.

Preface

This paper represents one person's view of the trusted computer system evaluation and certification processes. I formed my viewpoint based entirely on one year of research, having no previous background in trusted systems. I did not deal with the technical issues of trusted system evaluation or certification, but rather addressed what the Air Force can do to help those who are attempting to develop and acquire trusted systems.

The significant time lag between accomplishing this paper and its publication has given me time to evaluate what I wrote against the test of time. As my boss, John Gilligan, suggested, it appears that I was overly optimistic about the progress that would be made in trusted system development. The Air Force has not fielded regulations as fast as originally predicted, nor has the forecasted number of evaluated trusted systems materialized. It will be interesting to see if efforts in trusted systems continue to develop or if they will be another fatality of the budget process. I feel the methodology of trusted systems is basically sound and now has widespread support both inside and outside of the Department of Defense (DOD). Trusted systems can provide the needed capability to enforce a security policy and provide multilevel secure capabilities.

Trusted systems are not a panacea for the problems in computer security programs today. They can, however, significantly strengthen a sound computer security program. In addition, trusted systems can remove the restriction and frustration caused by a "system high" mode of operation.

The objectives of my research were to help users understand the benefits of trusted systems, to explain the problems associated with the current evaluation and certification processes, and to identify ways to make it easier to develop and acquire trusted systems. I believe we can make significant progress toward these objectives through education and networking.

Several people spent many hours helping me with this research report. First, I would like to thank John Gilligan for his active interest and support of my efforts. Second, I would like to thank at AUCADRE, Lt Col Manfred Koczur, chief of the Command Research Division, for his administrative and moral support; Dr Bynum Weathers, my research adviser, for helping me focus my research topic; and Dianne Parrish, my editor, for her pep talks, reminders of missed suspenses, and her ability to make something readable out of my attempts at writing. Finally, I am truly indebted to my wife Alice

and my children who endured many evenings and weekends looking at my back while I worked at the computer.

ERIC C. LEWALLEN, Maj, USAF
Research Fellow
Airpower Research Institute

Introduction

Surprise is one of the key principles of war. To achieve surprise, commanders must protect their war planning information. However, today, with the advent of computers, the military has a whole new set of problems in trying to protect classified information. Computer systems, as we are well aware of, are vulnerable to exploitation and intrusion. If a computer system is to process secret information, it must be protected to handle that level of information without being compromised.

One example of the military's effort to protect a computer system is the interservice agency automated message processing exchange (IS/A AMPE). This system was designed to provide automated message processing using the Defense Data Network. A multiservice effort, it was also required to process all levels of message traffic from unclassified to top secret. To accomplish this task, the computer needed the most sophisticated security features available. However, developing these security features turned out to be more difficult than expected.

The problems centered around the development and certification of security features in accordance with DOD Directive (DODD) 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria*.[1] The DOD criteria were written in very general terms to avoid driving hardware or software design. As a result, the user needed someone or some agency to determine if the intent of the criteria was met.

The National Computer Security Center (NCSC) was established to "study and implement secure computer technology and encourage the widespread availability of trusted computer systems."[2] A trusted system is one that will enforce a security policy through internal security features. A trusted system is defined in terms of the hardware and software it runs. DODD 5200.28-STD prescribes the security features and the types of assurances (that the security features will perform as specified) a trusted system must have. There are different levels of trust according to the types of security features and assurances a system has, with "A" as the highest and "D" as the lowest.

For the IS/A AMPE program, NCSC provided computer experts to help develop the security features according to these criteria. As the program proceeded, the differences in interpretation of the criteria between the contractors and the NCSC experts continued to grow. The IS/A AMPE program was canceled, but the difficulties in trying to develop and acquire the computer security features for this system indicated real problems in the ability to develop trusted systems.

The purpose of this report is to determine what the Air Force can do to help users develop and acquire trusted systems. This report does not offer technical solutions; however, it provides a general understanding of the trusted system evaluation and certification processes and the policies and regulations that direct them.

Having a trusted computer system does not automatically guarantee security in a particular operating environment. Application software must be written or modified so as not to compromise the security features of the computer system. The trusted computer system, however, is foundational.

I have two objectives for writing this report. The first is to educate those who are or will be involved in acquiring or developing trusted computer systems. They need to understand how the process works and to be aware of the pitfalls encountered in attempting to acquire a trusted computer system. My second objective is to provide recommendations that the Air Force can implement to reduce or eliminate current problems. By doing so, I hope to provide policymakers with suitable evidence for revising guidance so that users can have a clear and practical road map for the development of a secure computer system.

Chapter 1 discusses problems with security in general, provides a brief history of the development of trusted computer standards, and describes the evaluation and certification processes.

Chapter 2 examines current problems faced in our evaluation and certification of computer systems. Some of these problems include lack of user understanding and the complexity of the processes themselves.

Other government agencies have been developing practical applications of the trusted computer system methodology. In addition, the National Computer Security Center and the Air Force Cryptological Support Center Computer Security Office have initiated several positive changes over the last year. Chapter 3 looks at these initiatives and alternatives.

Chapter 4 discusses the relationship between industry and the Air Force in the development of trusted computer systems. Also included are my comments and recommendations on the Air Force role in developing and acquiring such systems.

Notes

1. DOD Directive 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria*, December 1985, 116.
2. National Computer Security Center, "National Computer Security Center," Fort Meade, Md., n.d., 1.

Chapter 1

Security and the Evaluation/ Certification Processes

Before I begin my discussion of the trusted computer system evaluation/certification processes, it is important to recognize a few facts about security in general. First, although most people acknowledge the need for security, they are often not willing to put up with the restrictions imposed for security's sake. Second, the operator wants free access to the equipment, whereas the security manager wants limited or protected access to the equipment. Figure 1 clearly shows this relationship. Point A indicates the operator's desire for maximum accessibility to the equipment. Point B indicates the security manager's desire for maximum security on all equipment. In fact, most security managers would like to place each piece of classified information in a safe and throw away the combination while the operators would like to declassify all information and keep it in their desk. Obviously the answer to the security versus accessibility problem calls for a balanced approach (point C). In other words, the operator has to accept some security restrictions that will reduce accessibility and the security manager has to accept some risk to give the operator the needed accessibility.

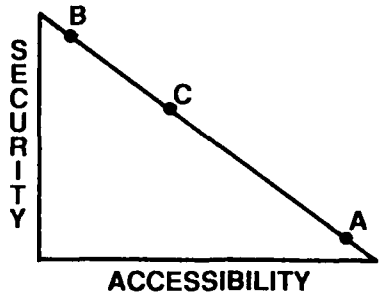


Figure 1. Security versus Accessibility

Computer Security

The problem of security versus accessibility also exists in the computer security arena. Although there has been a need for computer security since the invention of computers, operators have balked at such practices. Before the 1970s computer security was accomplished primarily through physical

means, with large computer systems and operators kept behind locked doors. Also, machines that processed different levels of classified information were separated physically. The computer security environment was relatively easy to control. In the late seventies the environment became harder to control with the addition of terminals. The physical area to control expanded and the number of people with access to computers increased. Thus, the computer security issue became more complex. Remote terminals and telecommunications systems further complicated the security problem. Obviously, as the military becomes more and more dependent upon computers, the problem continues to take on greater significance.[1]

The primary threats to computer systems today are: (1) the threat from outside the organization, (2) the threat from within the organization, and (3) the threat caused by the lack of a multilevel processing capability. An example of an outside security threat is what the media calls *computer viruses*. A computer virus is like a human virus in that it transmits through contact and has a reproductive capability. It can be harmless or harmful depending on the code instructions from the author. Some viruses just leave a message. Others destroy the data on the disk by causing the computer to overwrite when it should not. The media has covered the subject of viruses quite extensively.

An illustration of what can happen occurred in 1988, when a virus caused the unclassified segment of the Defense Data Network to shut down over a weekend.[2] The danger to the military becomes critical if these programs disrupt its command and control systems.

Our second security threat is the authorized user. From 1978 to 1985, authorized users committed almost 80 percent of computer crime or abuse.[3] Robert Courtney, a noted computer security expert, explains:

> Giving numerous people unmonitored, unaudited access to records, while assuring them of complete and continuing anonymity to do whatever they can and wish to do from their terminals, exposes data to all, including the least trustworthy of the people using the terminals. When people know they will not be held accountable for their actions, it is unreasonable to expect everyone, including those who use data processing systems, to be meticulously careful, completely honest, and to always maintain a high degree of integrity.[4]

Finally, the third security threat arises from the inability to accomplish multilevel processing; that is, the processing of different levels of classified information by individuals having different clearance levels.[5] Our present methods of dedicating computer resources to one classification level and forcing all users to be cleared to that level is not only a waste of resources but also creates a potential problem with data security. As we become more and more dependent upon computer systems as a force multiplier, we will tend, during times of crisis, to pass all levels of data by the most efficient means possible through the available systems. The classification of the data or the system will be changed to fit the needs of the moment without regard to long-term consequences. Such actions will significantly increase the vulnerability of the data to both outside and inside threats. With multilevel

processing, however, the system will have the capability to process data with different classification levels and restrict a user's access based on his or her clearance.

In 1967 a scientific advisory board met to determine how these remote access, resource-sharing computer systems could be secured.[6] They developed policy and technical recommendations to reduce the threat of compromise to classified information. In the seventies these initial recommendations were further developed into a list of criteria. These criteria specified, in general terms, the security features and assurances needed to secure the systems. Assurances consist of documentation, system and code architecture, and testing requirements. Additionally, the criteria were graduated to determine the amount of trust to place in the computer system. For instance, the more extensive the security features and assurances, the greater the trust.

DOD Trusted Computer System Evaluation Criteria

Interpreting the criteria was a task that fell to the Department of Defense Computer Security Center which was formed in January 1981. Its charter was "to encourage the widespread availability of trusted computer systems."[7] Renamed the National Computer Security Center (NCSC) in 1985, it became the agency responsible for the development of secure systems and the evaluation of commercially developed systems using the DOD standard.

In 1985 the NCSC published criteria as DODD 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria*, commonly referred to as the "Orange Book" because of its orange cover. This document is part of what has become known as the "rainbow series" of computer security publications printed by NCSC. These criteria defined graded levels of trust with A as the highest level. These grades are further subdivided and indicated numerically (A1, B3, B2, B1, C1, C2). Additionally, the criteria were written in general terms so that they would not drive or limit hardware and software design. As such, the criteria are not self-applying meaning that someone would have to determine if a particular design satisfies the criteria—much like hiring a lawyer to interpret the law.

Evaluation Process

The trusted computer evaluation process is the method by which companies get their commercial systems evaluated according to the standard. Obviously, having a product with approved security features and assurances speeds up the implementation of a program demanding secure processing and/or multilevel processing. These evaluated systems would be the systems of choice for military users with such requirements. Thus,

it is to a company's advantage to have evaluated systems if it wants to be competitive in this market.

The evaluation process consists of (1) initial contact phase, (2) developmental phase, and (3) evaluation phase. In the initial contact phase, a company submits a proposal describing the system to NCSC which determines if it has a reasonable chance of completing the evaluation.[8] This review is necessary as the evaluation process is very expensive and time-consuming. Once the proposal is accepted for evaluation, NCSC and the company sign a memorandum of agreement that addresses the formal aspects of the product and the accompanying responsibilities of both parties.

The next step in the evaluation process is the trusted product development phase. Basically, this phase is a design and documentation check. The evaluators become familiar with the design of the system and its security features and ensure it is ready for evaluation (without delays for additional development or more extensive documentation). The company benefits from NCSC involvement as it is much easier to make changes to a system in the development phase than during production.[9] In this phase there is little or no hands-on use of the system. The development process is over when the vendor's system is ready for production and all necessary documentation is complete. NCSC produces an interim report on the system that serves as the basis for the decision to proceed to the evaluation phase. Both parties sign another memorandum of agreement, and the system enters the evaluation phase.[10]

The draft "NCSC Trusted Product Evaluations: A Guide for Vendors" describes the evaluation phase as a "detailed analysis of the hardware and software components of the system, all system documentation, and a mapping of the security features and assurances to the Orange Book. The analysis performed during this phase requires 'hands on' testing."[11]

As stated previously, the evaluation criteria are not self-applying. Thus a person must completely understand the functionality and interfaces of the system being evaluated in order to determine if it meets the intent of the criteria. In fact, this educational process is a critical element in the evaluation phase management plan used by the NCSC Evaluation Division.[12]

Once the evaluators are knowledgeable about the system under evaluation, they analyze all of its documentation and source-code information. The purpose of this analysis is to ensure the system and security features actually perform as advertised.[13]

Once testing is complete, the evaluators prepare a final report and assign a rating. The system then goes on the evaluated products list (EPL), a listing of computer systems that have been evaluated and assigned a level of trust according to the Orange Book. It was established to allow users to purchase an off-the-shelf system without having to design and develop the security features. Acquiring an evaluated system greatly simplifies the certification process.

Certification Process

The certification process is a site-dependent activity. The designated approving authority (DAA) has the ultimate responsibility to accredit a system for processing classified information. A system must undergo a certification process before the DAA can approve it.[14] Certification is "the technical evaluation of an automated information system's security features and other safeguards, made in support of the accreditation process, which establishes the extent that a particular automated information system design and implementation meet a set of specified security requirements."[15] Although DOD directives and Air Force regulations specify the need for certification, the process itself is not described beyond the definition stated above.

The certification process is much like the evaluation process. When a system has unique design and development requirements, the security features must be specified and tested. And system development testing is costly. Unfortunately, because of budget cuts, the certification process is often shortchanged.[16] An extensive certification program provides few, if any, immediate tangible payoffs. Moreover, most people complain about a lack of security only after an incident has occurred; and these problems are unlikely to surface during the developmental stage. Even if there were no budget cuts in the certification area, it is unlikely that the process would be as rigorous as the evaluation process described. In fact, this is where the real beauty of acquiring an evaluated system starts to show. If NCSC has already evaluated the system, then much of the certification process has been accomplished. The only remaining requirement would be to examine the unique security features implemented for the system's environment. In essence, acquiring an evaluated computer system means less-expensive certification costs and a greater assurance that it will be properly certified—because NCSC conducts a rigorous system evaluation.

Summary

The two distinct processes involved in getting a trusted computer system approved for the user are evaluation and certification. NCSC conducts the evaluation process on a general-purpose system. The result of the evaluation is that the system is placed on the evaluated products list, allowing users to acquire the system knowing it has the needed security features and that it has been evaluated to a given level of trust according to the Orange Book criteria. The certification process is accomplished on every system before its accreditation. Certainly, the level of difficulty in accomplishing the certification process can be greatly reduced by acquiring a system on the EPL. Therefore, it seems logical that people would be flocking to acquire evaluated systems. And they are! However, these EPL

products are in very short supply. Chapter 2 explains the reason for this shortage.

Notes

1. Roger R. Schell, *Computer Security: The Achilles Heel of the Electronic Air Force?*, AWC report no. 468 (Maxwell AFB, Ala.: Air War College, 1978), 3.
2. David Germian, "Student Suspected in Virus," *Montgomery Advertiser and Alabama Journal*, 6 November 1988, A-3.
3. Carole E. Ludwig, *An Analysis of the Air Force Computer Security Program*, AU-ARI-87-4 (Maxwell AFB, Ala.: Air University Press, December 1987), 37.
4. Quoted in ibid., 38.
5. DOD Directive (DODD) 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria*, December 1985, 114.
6. Ludwig, 6.
7. Government Printing Office, *National Computer Security Center*, information pamphlet #1986-623-957/00642, 1.
8. "Trusted Product Evaluations: A Guide for Vendors," NCSC-TG-002, version 1, draft (Fort Meade, Md.: National Computer Security Center, 1 March 1988), 11.
9. Ibid.
10. Ibid., 13.
11. Ibid.
12. D. B. Baker, *Trusted Computer System Evaluation Management Plan*, TOR-0086(6777-25)-1 (El Segundo, Calif.: Aerospace Corporation, 1986), 1–81.
13. Ibid., 1–79.
14. DODD 5200.28, *Security Requirements for Automated Information Systems*, 21 March 1988, 5.
15. Ibid., 2–2.
16. David J. Lanenga, "Security Evaluations of Computer Systems," in the 10th National Computer Security Conference Proceedings (Fort Meade, Md.: National Computer Security Center, 21–24 September 1987), 274.

Chapter 2

Problems in Evaluating/Certifying Trusted Computer Systems

An organization faces many problems in trying to acquire a trusted computer system or in developing and certifying a system with needed security features. In this chapter I discuss some of these problem areas: (1) lack of user understanding of the processes, (2) the evaluation process, (3) the certification process, (4) reorganization and guidance problems, and (5) the lack of education, materials, and training.

Lack of User Understanding

In the computer security field, the military user outside of the Washington, D.C., area received little information about the DOD criteria contained in DODD 5200.28-STD (Orange Book) and little about the National Computer Security Center evaluation program. In fact, users found out about the Orange Book only after it was delivered to them in 1985. After reviewing the book, their general comment was, "What is this?" Users thought this book was going to be a general reference manual on computer security and trusted systems. The organizations acquiring computer systems understood the need for computer security and expected to see a method of specifying needed security features for their systems. The Orange Book, however, was not designed for this purpose.

The task of translating these criteria into usable requirements was beyond the capabilities of the major command (MAJCOM) staffs. Basically, requests for help sent through the chain of command usually found a dearth of usable assistance.[1] Thus, frustration was the order of the day for the user and the computer security staff officer. The appearance of high-level guidance directing all systems that processed classified or unclassified but sensitive information have a C2 level of security by 1992[2] only added to their frustration, as most users did not know what C2 meant.

Evaluation Process

The evaluation process itself has been a problem. Initially, NCSC had more interested vendors than it could handle. Most of them wanted to develop, or at least find out how to develop, a secure system. Although most

vendors wanted to work on some kind of trusted system, very few had any kind of expertise in the trusted system methodology, and as a result, they needed a great deal of guidance from NCSC. For the most part the user was unaware of the problems the vendors were having. In fact, the problem did not surface for the user until the organization went to the evaluated products list (EPL).

Lack of Evaluated Systems

Imagine the frustration of the user agency who, after finally determining its requirements in terms of the Orange Book criteria, goes to the EPL only to find out that no system meets those requirements. After hearing NCSC claims about the benefits of acquiring an evaluated system, the user realizes that very few systems are on the list (table 1).

TABLE 1

April 1988 Evaluated Products List

Security Class	*Evaluated Systems*
A1	1
B3	0
B2	1
B1	0
C2	5

Source: 1988 Evaluated Products List [electronic data base] (Fort Meade, Md.: National Security Agency, 1988).

Procurement policies requiring vendor competition pose another problem. Since the EPL shows there is only one A1 or B2 system available, competitive contracting is impossible. Until the EPL has a number of systems in each security class, it remains a useless tool for the military user.

Additionally, software development is constantly changing. System ratings on the EPL are for one particular version of the system. Thus, the rating does not apply to subsequent versions of the system. NCSC has recognized this problem and is developing a program to address this issue. Chapter 4 discusses this solution.

Vendor Interaction

When NCSC first started conducting evaluations, they had no systematic approach for dealing with the vendors. Often, vendors would not know whom to contact about the status of their product or proposal, or even if it was under evaluation. NCSC addressed this problem by publishing a guide that outlines the trusted product evaluation process.[3] This guide lists the steps of the evaluation and states how the formal process works with memoranda of understanding signed by both parties. Vendors, interviewed

during my research, indicated they were more satisfied with the new system and had a greater understanding of the evaluation process.

Even with this new guidance, some vendors still experience frustrations in dealing with NCSC during the evaluation process. In particular, during the developmental stage, NCSC inputs to the vendor have been less than helpful. For example, Matt Hecht, a software engineer on the IBM Secure Xenix program, commented that an evaluator said, "I have a bad feeling about a particular area."[4] However, when pressed for more specific information about the problem, the NCSC evaluator could not provide a specific response. Obviously, developmental guidance must be specific enough to provide clear direction for the vendors to evaluate and correct the problem. C. S. Chandersekaran, chief of the IBM Secure Xenix program, feels that this kind of response stems from a lack of confidence and experience on the part of NCSC evaluators to make decisive judgments in the area they are looking at.[5]

NCSC evaluators and vendors cite lack of responsiveness during the evaluation phase as a problem.[6] NCSC, in order to deal with its manpower shortage, developed a matrix-type work schedule, requiring the evaluators to work on many evaluations at the same time. According to NCSC, this allows the evaluators to be fully utilized as the vendors do not usually respond immediately to evaluator inquiries. This kind of work schedule creates an input-wait-response-wait-input cycle that slows the evaluation process. Some vendors have not found this to be a real problem, as their personnel are also working on many other projects at the same time.

Chandersekaran suggests, however, that NCSC should examine the amount of effort given by the vendor and devote evaluation resources appropriately. For example, he has about 200 people working full time on the Secure Xenix program, thus they respond quickly to evaluator inputs. However, their team experiences delays because they must wait for the evaluators to get back to them. After citing this example, I believe Chandersekaran's suggestion warrants consideration, as it would significantly speed up the evaluation process.

Time to Complete Evaluation

Vendors feel that NCSC is in no hurry to complete evaluations. The NCSC *Trusted Computer System Evaluation Management Plan* allows approximately two years for the evaluation of a B1 to C1 level system with no time limit for the technical support cycle in the developmental evaluation phase. Having a cycle within a phase that has no time limit eliminates the validity of the time line as a forecasting tool for evaluation completion. This timetable lengthens to approximately two and one-half years for an A1 to B3 evaluation.[7] NCSC does not seem to live by any real-time constraints. Chris Inglis, head of the NCSC Evaluation Division stated that he is primarily concerned with getting a properly evaluated system out the door.[8] I would not argue with this approach except that there should be a balance

between getting a perfectly evaluated system and living with some reasonable constraints. If NCSC developed a more rigorous timetable and forced both the vendors and itself to comply with it, both parties would benefit. It would serve their goal of populating the EPL and shortening the evaluation process.

Lack of Trained Evaluators

The NCSC evaluation section operates with a critical manpower shortage and faces a large backlog of work. Currently, NCSC has 45 evaluators in the evaluation section, with no current plans to increase this number.[9] Even if they could double their current staff levels, this section would still have products waiting to be evaluated. Additionally, over the years, NCSC has suffered a tremendous exodus of its evaluators to the private sector. In fact, Inglis stated that virtually 25 percent of the section's evaluation expertise lies with one evaluator who has been with NCSC for several years.[10]

Trusted computer system evaluation is a very specialized field, and there is no ready supply of trained evaluators. Therefore, NCSC must train its own. It takes approximately six months for a new evaluator to be reasonably conversant on a particular system, and about a year to be ready to perform an evaluation without supervision. Like a pilot who has just learned to solo, the evaluator is not yet completely knowledgeable of the process. It usually takes the evaluator another year to develop a significant level of expertise. The individual may stay with NCSC for only a year or two more before moving to the private sector.[11] NCSC will continue to experience a shortage of evaluators in the foreseeable future.

Certification Process

The requirement for users to certify their computer systems before processing classified information has been in force for almost 10 years.[12] Yet in all that time, there has been a complete lack of information to the field on how to develop a certification plan for an acquired system or how to perform the certification process. In short, users have been tasked with completing a process for which they have no guidance. Thus, users have developed their own certification plans based on their experience and expertise.

Since there are virtually no trusted systems available, military users needing security features for their systems have to specify and develop these features and their own certification plans from scratch. For a while NCSC provided developmental guidance to DOD agencies developing such systems. For instance, NCSC had a computer security team help with the development of the IS/A AMPE program. However, NCSC no longer provides such guidance, leaving the user on their own again.

Like the civilian community, the Air Force lacks computer security expertise. The Air Force agency responsible for developing trusted computer system guidance and for providing user education is the Air Force Cryptological Support Center Computer Security Office (AFCSC/SR). In the last few months, AFCSC/SR has started acquiring the resources and developing the materials needed for the user. From 1978 to 1987, however, the user could find virtually no materials or assistance. The primary reason for this was the constant reorganization of what used to be called the Air Force Communications-Computer Security Management Office.

Reorganization and Guidance

Since its beginning, the Air Force Communications-Computer Security Management Office, now AFCSC/SR, has been in a constant state of turmoil. It has experienced numerous name and office symbol changes. In fact, the name Air Force Communications-Computer Security Management Office in the draft copy of AFR 205-16, *Computer Security Policy*, is no longer used. From 1978 to 1985, the office had a total staff of nine people including administrative personnel. Its organizational mission is to:

a. Perform computer security related studies, analyses, and RDT&E as directed.

b. Advise MAJCOMs on procedures, techniques, and standards for managing computer security programs.

c. Respond to MAJCOM requests for:

(1) Technical interpretation of and implementation guidance on HQ USAF/SCT security policy.

(2) Assistance in establishing, implementing, and reviewing command computer security programs.

(3) Recommendations related to hardware, software, and procedural safeguards.

(4) Technical assistance to acquisition and development activities.

(5) Penetration testing and on-site assistance in conducting risk analyses and certifying computer systems to process classified or sensitive unclassified information.

d. Maintain technical computer security reference material to provide Air Force activities a centralized source for technical information and guidance on computer security requirements and related issues.

e. Establish and direct special studies and research and development directed at computer security technology.

f. Manage the Air Force computer security technical vulnerability reporting program (Report Control Symbol (RCS)HAFSCT(AR)8702) according to guidance in chapter 17 (AFR 205-16).

g. Establish special program and provide guidance for computer security education, training, and awareness: chair the Computer Security Education and Training Working Group (CSETWG); and coordinate training requirements with HQ Air Training Command (ATC) as necessary.

h. Establish and maintain reporting criteria for the Air Force Computer Security Program.

i. Direct and manage the development, testing, and documentation of new or improved computer security procedures, tools, techniques, hardware, and software.

j. Maintain currency in computer security technology.

k. Manage the Air Force Reporting Criteria for the Computer Security Evaluation and Assistance Program data call according to attachment 5. [Note: this program is no longer in existence.][13]

Clearly this office was not staffed to handle a mission of this scope—providing computer system security support to all systems in the Air Force. In 1985 the office was moved from Gunter AFB, Alabama, to Kelly AFB, Texas. Only three of the original staff transferred with the move.[14] Since the relocation, the office has grown considerably and is beginning to provide the support listed in its mission statement, nearly 10 years since its inception.

In addition to the problems caused by constant reorganization, the user has had to deal with conflicting Air Force guidance. The regulations governing computer security and certification are so complex and contradictory that unit communications-computer system security officers (CSSO) are extremely frustrated. A 1986 survey of CSSOs substantiates that statement.[15] Additionally, since 1986, AFR 205–16 has been under revision. Unfortunately, this lack of guidance on computer security issues only serves to increase user frustration.

Lack of Education, Materials, and Training

The lack of available educational materials on the Orange Book criteria and the certification process has contributed significantly to the lack of progress in developing trusted computer systems. As stated previously, there is no ready pool of trained computer security experts. Thus, educational material is critically needed to train current computer system security officers.

Until recently, the only educational materials available to unit CSSOs were the "rainbow series" documents published by NCSC. These publications are useful for those involved in computer security. Unfortunately, Air Force regulations do not make it clear whether these materials are authoritative guidelines for action.

In terms of training, the Air Force conducts one security course for unit CSSOs. This course provides a basic overview of computer security and teaches very little on trusted computer systems as described in the Orange Book.[16] Approximately 500 people attend each year. The course is a positive step toward addressing the education issue, but it does not go far enough. I feel that it is critical for CSSOs at all levels to understand the essence of trusted systems. TSgt Michael Bishop, a course instructor, says that the school had problems matching the course curriculum to the needs of the units because, until recently, higher headquarters provided little direction as to course content. He feels AFCSC/SR's reformation of the

Computer System Security Education and Training Working Group will go a long way toward matching course content with unit CSSO needs.[17] In fact, with the fielding of trusted computer systems, training about these systems is a must for unit CSSOs.

Summary

The Orange Book criteria and methodology have received a high degree of acceptance among experts in the computer security field. NCSC has been successful in stimulating an interest in trusted systems and in improving its image among system vendors. Despite this change of attitude, the number of trusted systems available on the market today is unacceptably small.

The evaluation process has been problematic, especially in the area of vendor interaction. Although the procedures have been refined, the evaluation process is still unacceptably long. The problem of extending the evaluation results to subsequent revisions of the system, already addressed, will be discussed in the next chapter. NCSC's shortage of trained evaluators likely will continue for some time to come.

The certification process needs to be further defined. The user needs to be educated on the "how to" of the process and have an agency available to provide certification expertise. Currently, AFCSC/SR is responsible for providing that expertise. The need for AFCSC/SR to provide support to the user is even more critical today since NCSC no longer provides developmental guidance.

The lack of educational materials and training for CSSOs throughout the Air Force, particularly those who are involved in acquiring trusted computer systems, has been one of the major impediments toward progress in this area. Also, the lack of clear direction from the Air Staff and the various iterations of the Air Force Computer Security Management Office have adversely affected the development of adequate certification programs. The lack of leadership in the computer security field has caused a tremendous impetus to avoid computer security issues.

However, in the last year significant developments and changes in computer security have taken place. Chapter 3 discusses some of these new developments.

Notes

1. Timothy R. Gernert, Communications, Computer Systems Security Officer, Headquarters MAC, interview with author, 5 January 1989.

2. DOD Directive 5200.28, *Security Requirements for Automated Information Systems*, 21 March 1988, 4.

3. "Trusted Product Evaluations: A Guide for Vendors," NCSC-TG-002, version 1, draft (Fort Meade, Md.: National Computer Security Center, 1 March 1988).

4. Matthew Hecht, systems developer, Secure Xenix Program, IBM Corporation, interview with author, 20 October 1988.

5. C. S. Chandersekaran, chief, Secure Xenix Program, IBM Corporation, interview with author, 20 October 1988.

6. Ibid.; Chris Inglis, director, Product Evaluation Division, NCSC, interview with author, 20 July 1988; Susan Passmore, staff security analyst, Tandem Corporation, interview with author, 26 July 1988.

7. D. B. Baker, *Trusted Computer System Evaluation Management Plan*, TOR-0086(6777-25)-1 (El Segundo, Calif.: Aerospace Corporation, 1986), 1-12, 1-29, 1-51, 1-67, 1-79, 1-107, 1-123.

8. Inglis interview.

9. Ibid.

10. Ibid.

11. Ibid.

12. Robert Pierce, staff officer, AFCSC/SR, interview with author, 8 February 1989.

13. AFR 205-16, *Computer Security Policy*, 28 April 1989, 8.

14. Pierce interview.

15. Carole E. Ludwig, *An Analysis of the Air Force Computer Security Program*, AU-ARI-87-4 (Maxwell AFB, Ala.: Air University Press, December 1987), 112-17.

16. TSgt Michael Bishop, USAF, computer security course instructor, 3390th TTHTG, Keesler AFB, Miss., interview with author, 27 March 1989.

17. Ibid.

Chapter 3

Changes, Initiatives, and Activities in Trusted Computer Systems

In the last 10 years the development of trusted computer systems has been sporadic with few useful results from the user's standpoint. However, in 1988 more changes and initiatives took place than ever before. The National Computer Security Center made some positive changes. And for the Air Force user, the Air Force Cryptological Support Center Computer Security Office (AFCSC/SR) developed a viable program that addressed long-standing grievances in the development and acquisition of trusted systems. In this chapter, I discuss these changes and other activities that directly affect the trusted system area.

National Computer Security Center Changes

As stated previously, NCSC had focused its efforts on dealing with vendors and the evaluation process, neglecting the needs of the DOD community which provides the majority of NCSC's funding.[1] In 1988, however, NCSC began to make some significant changes in assessing DOD needs, developmental guidance, evaluated system software updates, education, and the evaluated products list.

Assessing Department of Defense Needs

To determine the trusted computer system needs of the war-fighting commanders, senior management directed the formation of a management team to travel to the joint command staffs to conduct this assessment. This action will allow NCSC to focus its limited resources on research and the stimulation of development of the computer systems that the war-fighting commanders need.

In addition, this team will brief flag officers on their findings, which should stimulate active support for the development and acquisition of trusted systems. In an era of austere budgets, I believe flag officer support will prove to be crucial to the fielding of these needed systems.

Developmental Guidance

NCSC has reinstituted a developmental guidance group to provide DOD agencies with the needed expertise for developing trusted systems.[2] Its focus is to build multilevel secure (MLS) systems at DOD operational sites. At this time, the group is collecting information on DOD needs and formulating a strategy for meeting those needs. However, the manpower crunch is still on and the demand for the group's services is likely to increase. Properly allocating these limited resources will remain a major problem.

Evaluated System Software Updates

NCSC instituted the ratings and maintenance program (RAMP) to address the problem of software updates to evaluated systems.[3] Under this program, a vendor with an evaluated product sends one of its employees to NCSC to receive training on evaluating updated software and to ensure that these changes have not compromised its current rating. Within limits, this individual's validation of software updates and completes the recertification effort without the need for a new evaluation by NCSC personnel.

Although the benefits of the program are obvious, it has some significant limitations. First, there appears to be a limited number of slots. Susan Passmore from Tandem Corporation stated that her company had been trying for some time to get an individual into the program and still had not received a class date.[4] Second, RAMP applies only to evaluated products at the B1 level or lower. I see this stipulation as a significant limitation because usually the more complex systems require more frequent software changes or upgrades. Thus, this program needs to be expanded to include all levels of trust.

Education

In an attempt to address the critical need for education of those involved with the acquisition of trusted systems, NCSC developed a course for acquisition managers. The first course went very well, with about 27 people in attendance from various DOD agencies. Recently, however, NCSC has turned over course administration to the Army Logistics Management College (ALMC). ALMC revised the materials and started teaching the course in July 1989. Additionally, ALMC is sending instructors to various sites to teach the course.[5]

Evaluated Products List

Finally, the evaluated products list shows signs of developing new life. As of July 1989 NCSC has added seven new products to the EPL (table 2).

TABLE 2

July 1989 Evaluated Products List

Security Class	*Evaluated Systems*
A1	1
B3	0
B2	1
B1	2
C2	10

Source: 1989 Evaluated Products List [electronic data base] (Fort Meade, Md.: National Security Agency, 1990).

These numbers include subsystems which can be added to an existing system and that provide C2-type security features to trusted systems. This infusion of products will provide DOD agencies with some options to pursue in meeting the requirement for a C2 level of trust by 1992.

Air Force Cryptological Support Center Computer Security Office Initiatives

In informal discussions with members of the other services, it appears that, even with the problems highlighted, the Air Force is well ahead of the other services in coming to grips with computer security issues. The initiatives AFCSC/SR has taken in the last year show great promise of accelerating Air Force efforts to comply with DOD directives and obtain trusted systems.

Project Firestarter

To ensure a centralized approach to Air Force research and development in the computer security area, AFCSC/SR established Project Firestarter. This program will determine Air Force needs and focus all research under a single statement of need developed by AFCSC. A program objective memorandum (POM) of the Electronic Security Command (ESC) provides funding. (ESC is the parent command of AFCSC.) Firestarter will coordinate all research and funding efforts and provide a program that will be responsive to Air Force needs. Additionally, ESC will advocate the POM. This will ensure these vital programs will not loose visibility in local MAJCOM funding decisions. This support will become critical when budget cuts are called for. Also, this program will provide a focal point for lessons learned in research and development of secure systems.[6]

Contract Specifications

To address the problem of specifying security features and assurances in contractual terms, AFCSC/SR has developed a set of standard contract data requirements lists (CDRL) and data item descriptions (DID), which specify Orange Book security features and assurances in the appropriate contrac-

tual language.[7] These CDRLs and DIDs are currently under review by the acquisition commands and will be included in the Air Force Systems Command's master CDRL file. These specifications will lay the groundwork for the development of a solid certification plan. With clear specifications, the task of writing a certification plan—to ensure the security features operate as specified—becomes much easier.

Product Evaluation Resource Center

In February 1988 AFCSC/SR established a Product Evaluation Resource Center (PERC) to assess microcomputer security subsystems. These subsystems will provide microcomputers with the hardware and software necessary to implement security features equivalent to a machine with a given level of trust (e.g., C2). The assessment process the PERC team uses is very similar to NCSC's evaluation process. To avoid any misunderstanding, however, PERC does not use the term *evaluation*, as NCSC is the only agency that performs evaluations. When the assessment is complete, the subsystem is placed on the assessed products list. This list will aid Air Force users in acquiring these subsystems for their microcomputers. Another goal of PERC is to perform assessments of mainframe systems; however, they currently do not have the resources to do so.[8]

Like NCSC, PERC faces a shortage of trained evaluators. Hence, the center will not become truly productive for a couple of years. However, once it is firmly established, the Air Force will have a unique capability—to perform assessments on mainframes, which would significantly aid the Air Force in its efforts to acquire trusted systems.

Regulations and Specialized Publications

Another initiative at AFCSC/SR is the development of new regulations and specialized publications to address user needs in acquiring and certifying trusted computer systems. Unlike previous publications, they will be newly developed and will provide coherent, nonconflicting guidance. Of particular interest will be AFR 56–31, "Security Policy and Requirements in the Acquisition and Development of Computer Systems" (currently in draft). It will "support the general requirement to incorporate security requirements into the acquisition process. It is supported by detailed how-to specialized publications."[9]

AFCSC/SR has completed drafts of such specialized publications as *Security Requirements for Computer Systems Acquisition and Development*, *Security Methodologies, Tools, and Techniques for Computer Systems Acquisition and Development*, and *Accreditation and Certification*.[10] However, before they are ready for publication, these documents must undergo MAJCOM review. Unfortunately, this means that the field will not see these documents until the early 1990s. Despite this delay, when the publications hit the field, they will provide unit CSSOs and others with needed educational materials on trusted systems.

Other Agency Activities

In the trusted computer system area, the activities of other DOD agencies deserve comment. The first program I want to highlight is the multilevel secure program spearheaded by Headquarters Military Airlift Command (MAC). This program is an outgrowth of the model command center program, which MAC designed to procure and test state-of-the-art equipment and integrate it into a working command center as a model for DOD command and control centers. This program bypassed many of the usual long lead time acquisition procedures, allowing MAC to purchase state-of-the-art equipment and determine its functionality.[11]

In August 1988 Headquarters MAC drew up a memorandum of understanding for the DOD MLS prototype. The program has two goals: "First, it will provide Multi-Level secure (MLS) systems and technological lessons applicable DOD wide; second, it will furnish Military Airlift Command (MAC) an incrementally developed operational command and control MLS capability."[12] MAC's approach of "exploring unproven technology through non-traditional methods"[13] has aroused the ire of those who must work through traditional channels. However, since the memorandum of understanding was signed by the secretary of the Air Force (SAF), CINCMAC, AFCSC/CC, and the Defense Communications Agency Director, this program has received more high-level support than normal.

Many of the products acquired under this program are currently under evaluation at NCSC.[14] The goal of the MLS prototype program is to take these products and evaluate how well they can be used in a command and control environment. As stated previously, one of the functions of a trusted system is to provide an MLS capability. The use of these products in an integrated fashion could fill the gap left by the lack of a single computer system with an MLS capability.

Compartmented Mode Workstation

One real problem is the proliferation of workstations for different systems in a work area. Each system requires its own terminal, which can clutter up a work area quite rapidly. There is a real need for a single "smart terminal" that can replace all the "dumb terminals" in the work area. Connecting these terminals to trusted systems further complicates the problem. This means that the "smart" terminal must have trusted features that will not compromise the system to which it is connected. This is the goal of the compartmented mode workstation (CMW). In fact, the Defense Intelligence Agency (DIA) has been working with MITRE Corporation to develop specifications for a compartmented mode workstation.[15] This workstation will enable a user to access several systems simultaneously from one workstation. In addition, the user will be able to integrate his or her activities, creating new files from different systems. The CMW will allow

MLS activity, automatically resolving the level of classifications of files generated at the CMW.

Not all experts agree with the way the developers have applied the Orange Book criteria to the CMW design. Roger Schell, a leading computer security expert and one of the authors of the Orange Book, feels the method of handling classification labels violates the integrity of the Orange Book criteria.[16] However, DIA continues to try to find a workable solution to this problem.

In 1987 DIA contracted with five corporations to develop a working model of the CMW.[17] The agency expects to see the machines in early 1990. DIA will, in conjunction with NCSC, evaluate the systems to determine suitability and compliance with the Orange Book criteria. By 1991 DIA expects to start fielding a CMW.

Headquarters System Replacement Program

The headquarters system replacement program (HSRP), a system designed to give multilevel capabilities to users within the Pentagon, replaces their current dual systems (one classified, one unclassified).[18] Users will now be able to process both unclassified and secret information from the same terminal. Additionally, other cleared users will be able to process secret and top secret information at the same terminal.

Since there was no single machine that provided this capability, the Grumman Data Systems Corporation developed a multilayered system that uses different machines for each level of classification and is connected by a communications control module.[19] In addition, Grumman Data Systems developed a software evaluation methodology which minimizes the amount of software that needs to be modified to meet trusted criteria.[20] This design will allow for easy migration of the system to higher levels of trust.

This system is significant as it is a way to have a trusted data-base capability without a trusted data-base system—none exist at this time. Like the CMW, it provides another real-life application of the Orange Book criteria and will provide valuable insights into practical applications of trusted systems.

Summary

It is encouraging to see the significant progress that has occurred in the trusted computer system area over the past year. NCSC is now focusing its efforts on DOD requirements. This resulted in flag officer support of trusted computer system acquisition, developmental guidance, programs such as RAMP to address the problems of updated systems, the education of acquisition managers, and the expansion of the EPL. In the Air Force, AFCSC/SR has moved forward with many initiatives in the trusted computer system security area: Project Firestarter, standard contract specifications (CDRLs and DIDs), PERC, and regulations and specialized

publications. These efforts will meet critical user needs and will focus primarily on Air Force computer security issues.

The contributions of other DOD agencies in this area are also important. Such programs as the MLS prototype, the compartmented mode workstation, and the HSRP provide innovative, practical applications that fulfill trusted computer requirements. In fact, these programs have generated high-level visibility and interest in computer security. This kind of activity will help us "over the hump" and provide answers to current problems. What can the Air Force do to support and enhance these efforts? Chapter 4 provides some suggestions.

Notes

1. Nicolas Pantiuk, military and intelligence operations staff officer, NCSC, interview with author, 20 July 1988.
2. Chris Inglis, director, Product Evaluation Division, NCSC, E-Mail message, subject: Evaluated Products, 31 March 1989.
3. Chris Inglis, director, Product Evaluation Division, NCSC, interview with author, 20 July 1988.
4. Susan Passmore, staff security analyst, Tandem Corporation, interview with author, 26 July 1988.
5. Debora M. Clawson, security officer, NCSC, E-Mail message, subject: Program Manager's Course, 26 March 1989. Point of contact for course is Stephan Ball, ALMC, Fort Lee, Virginia 23801, DSN 687-3851.
6. Air Force Cryptological Support Center (AFCSC), "Project Firestarter" (Point paper, Air Force Cryptological Support Center, San Antonio, Tex., 16 March 1989).
7. Robert Pierce, staff officer, AFCSC/SR, interview with author, 8 February 1989.
8. Dick Mason, point of contact for PERC team, AFCSC/SR, telephone interview with author, 29 March 1989.
9. "Air Force Communications-Computer Systems Security," briefing handout, Communications Computer Systems Executive Seminar, Maxwell AFB, Ala., October 1988.
10. Ibid., 24.
11. Steven Dyer, staff officer, Headquarters MAC/SX, telephone interview with author, 13 January 1989.
12. *Memorandum of Understanding for the DOD Multi-Level Security Prototype*, Headquarters Military Airlift Command, 31 August 1988, 1.
13. Ibid.
14. Dyer interview.
15. Defense Intelligence Agency, *Security Requirements for System High and Compartmented Mode Workstations*, DRS-2600-5502-86 (Washington, D.C.: Defense Intelligence Agency, May 1986).
16. Roger R. Schell, vice president for engineering, Gemini Computers Incorporated, telephone interview with author, 21 December 1988.
17. Gary Huber, compartmented mode workstation program manager, Defense Intelligence Agency, telephone interview with author, 30 March 1989.
18. Dan Gambel and S. Walter, "Retrofitting and Developing Applications for a Trusted Computing Base," in the 11th National Computer Security Conference *Proceedings* (Fort Meade, Md.: National Computer Security Center, 17–20 October 1988), 344.
19. Ibid., 345.
20. Ibid.

Chapter 4

Comments and Recommendations

The recent efforts to develop practical trusted system applications are encouraging. Interest in computer security is much higher, thanks to the media attention over the last year. Industry interest appears higher as attendance at the 1988 NCSC Computer Security Conference has climbed significantly.[1] At this time, however, there are more promises than real systems. What does this interest mean for trusted systems? And what can the Air Force do to support development of these systems? This final chapter addresses these important questions.

Comments

Trusted systems development remains primarily a DOD phenomenon. Although vendors appear much more interested in trusted computer systems than ever before, it seems that the only real market for them is in the federal government. In most cases, federal systems comprise only about 10 percent of a major company's total sales.[2] Congressman Tom McMillen, who has been involved in computer security legislation, feels we are at a critical juncture for trusted systems. If DOD waffles in its commitment to procure trusted systems, current progress could stop.[3] This progress could halt anyway if future budgets are cut. If, however, DOD can continue its efforts, trusted systems can become widespread in both markets. For instance, in the case of data encryption—now widely used in banking systems—it took the military to demonstrate its effectiveness in order to get industry acceptance.[4] The same could happen for trusted systems. In fact, the method of systematically designing trusted security features into operating systems is a more effective strategy than the current one of adding the features at a later date.

In both DOD and civilian markets, computer security fights an uphill battle because there is no bottom-line dollar return. In designing a system, security considerations are often fifth or sixth on the priority list.[5] Yet, systems with high levels of trust require integration of security features into the core of their design.[6] The current media attention given to computer viruses has highlighted the vulnerabilities of our current systems. This publicity will likely raise interest in computer security and spur the development of trusted systems.

Flag-officer support and sponsorship of such programs as the multilevel secure (MLS) prototype and the Pentagon's headquarters system replacement program (HSRP) are critical to developing momentum in this field. However, until recently, computer security did not receive much support from the Air Force. The lack of manpower and funds dedicated to the issue clearly attested to that fact. The increases in support for Air Force Cryptological Support Center Computer Security Office (AFCSC/SR) and the manpower authorization for a base computer security officer indicate a welcome change of attitude Air Force-wide.

Recommendations

Since NCSC is working toward solving its problems, I will address only actions the Air Force may take to enhance and support NCSC efforts.

1. *Provide new regulations and specialized publications on computer security to the field as soon as possible.* By publishing clear program guidance, the Air Force can significantly help users direct their efforts. This action would resolve the current nightmare of conflicting and ambiguous regulations. For example, AFR 205–16, *Computer Security Policy*, has been under revision for over three years. Failure to complete and publish this guidance has contributed to the sense of a lack of leadership in this field.

AFCSC/SR has started revamping and streamlining regulations.[7] AFCC, as the implementing agency for computer security, needs to work closely with AFCSC/SR to ensure that publications and documents meet the users' requirements, to hold AFCSC/SR to the due-out date, and to aggressively distribute the publications once published. Until these regulations are available to give clear direction to the people in the field, personnel will avoid any efforts to develop a workable computer security program. Forthright and visible leadership in the form of strong and clear written guidance is the key element in maintaining momentum in Air Force computer security and trusted systems development.

2. *Provide user education and training on trusted systems.* The people involved in computer system acquisition must be educated on trusted systems and the tools available to aid in acquiring such systems. AFCC needs to identify the acquisition personnel in the command, from headquarters down to the communications division level who are acquiring computer systems. These people need to attend the Acquisition Manager's Course taught by the Army Logistics Management College (ALMC), whether in residence or at one of the classes taught by the ALMC field instructors.

Although the acquisition personnel are the key people to be educated, all Air Force personnel need to have a basic understanding of computer security and trusted systems. The materials under development by AFCSC/SR will help in this effort. AFCSC/SR is also preparing to field it's education and training awareness program (ETAP) as an ancillary training program that will ensure individuals entering the Air Force receive training

in computer security and their responsibilities.[8] Additionally, all Air Force personnel will receive refresher training upon a permanent change of station, much like our current social actions training. However, personnel involved in classified computer processing will receive more in-depth annual training. Though this training will help raise general awareness, more effort should be expended to educate the individuals with direct computer security responsibilities. Because these people must implement Air Force and higher-level policy, they need to be schooled to understand the policy and to be able to articulate it to their agencies.

3. *Ensure that system requirements specify the need for trusted systems.* Program managers often say they need trusted systems but do not list these requirements in the requests for proposal (RFP). Often, a contractor may discourage a program manager from specifying a trusted system by saying it would be too difficult to accomplish, or that the specifications would be too difficult to prepare. The result is a watered-down proposal, and a system that does not provide the multilevel security needs of the user.

Roger Schell, a computer security expert and former Air Force officer, feels this problem is pervasive and will stymie the fielding of trusted systems.[9] My experience at MAC headquarters confirms his conclusions. The Air Force must educate its program managers. An educated program manager will be able to accurately discern the risks and costs of developing a trusted system and will not be as subject to being intimidated by others.

A consistent demand for trusted systems will increase the availability of these systems. This demand will be another catalyst in maintaining the momentum gained over the last year.

4. *Identify a flagship system to demonstrate the utility of trusted systems.* In the trusted computer system area, there are few real success stories. I agree with Roger Schell who believes that we need a flagship system that can demonstrate the practicality of trusted systems and the usefulness of the MLS capability.[10] The HSRP seems to be a likely candidate for such a demonstration. Representing "65% of the computing power available to OSD, OJCS, and HQ USAF,"[11] its successful implementation can only serve to encourage other efforts within the Air Force and DOD and will be another way of maintaining interest in trusted systems.

5. *Establish an information network for Air Force computer security personnel.* For the Air Force the critical need is for people involved in computer security to talk with one another. This exchange is essential in getting everyone headed in the right direction. Obviously, the lack of clear guidance has severely hampered computer security activities in the Air Force, including those in the trusted systems area. Those involved in computer security need to know what is going on in the field, how others have successfully acquired trusted systems, and many other important concerns.

What I propose is the creation of a bulletin board system (BBS) that all Air Force computer security personnel could access. Such a BBS would have several positive effects. First, it would be a fast way to get information

to the field. Second, it would also provide a valuable forum for getting a rapid corporate response to a proposed direction or idea and could rapidly disperse and implement good ideas. Finally, it could serve as an invaluable information resource for new unit communications, computer system security officers.

Bulletin board systems are not new, but their usefulness is obvious. For example, colleges have interconnected their computer systems across the country. These systems have forums where information about a particular subject is sent to a moderator who then distributes it to addressees on an electronic mailing list. This technique is a very useful method of exploiting communications and computer technology, because it allows the gathering of current information in a short period of time.

NCSC has such a system—called Dockmaster—for their evaluation projects. Using Dockmaster, they establish individual projects for each system under evaluation. This means that they can pass information rapidly to people all over the country who are working on that particular evaluation. At this time, NCSC is willing to set up an Air Force project for those who are involved in computer security. Air Force personnel could access the system throughout the world through the Dockmaster's computer link with the Defense Data Network. Since the system is already in place, Air Force computer security personnel could apply to get on the system in a relatively short period of time.

I recommend AFCSC/SR set up an inquiry response office to administrate the Air Force project on the Dockmaster system. This office would handle overall project administration, authorizing users, setting up the discussion forums, enlisting forum chairpersons, and encouraging active involvement by security personnel at all levels. Since NCSC runs the system, this office would not be bogged down with the routine of operating the computer system, distributing the system documentation, signing up users, and so forth. Rather they would be free to concentrate on the dynamic of monitoring and encouraging this electronic community.

Additionally, since AFCC knows where the computer security personnel are, the command needs to send a message to all applicable personnel to get them to register on the Dockmaster system. I recommend, as a minimum, all computer security personnel at AFCSC/SR, the Air Staff, AFCC headquarters, and the communications divisions be registered initially. Also, the personnel manning the recently created base-level computer security positions need to be registered. My ultimate goal would be to have everyone who is involved in computer security Air Force-wide on the system.

The system would not replace regulations or written guidance, but it would help fill the present documentation gap. In addition, it could help increase the usefulness of written information and guidance, as one would now have the capability to receive a rapid and useful response from the field.

6. *Continue developing senior officer interest and involvement.* The old adage "The squeaky wheel gets the grease" remains true today. As discussed previously, there has been some flag officer interest developed over the last couple of years. I feel, however, that computer security and trusted systems need to remain in the forefront as much as possible to ensure the senior officer support. I first recommend briefing the communication division commanders on the status of computer security to date. The involvement of these commanders is key to getting the staff the support they need to ensure computer security is treated as something other than an annoyance. Computer security needs to be a mainline part of AFCC activities, and people need to think about computer security in all that they do. It should be as pervasive as the influence of safety is in military flight operations today. That safety emphasis came about only because senior officers articulated, and continue to articulate, its importance to flight operations. The same thing has to happen in computer security. This can only happen by getting senior officers throughout the Air Force to understand and appreciate the importance of computer security and to express their support for computer security to everyone else.

7. *Actively manage computer security expertise within the Air Force.* There are few experts in computer security and the Air Force needs to carefully manage the resources they have. I propose an Air Force specialty code shredout that would identify those individuals who have computer security expertise. Those people trained at NCSC need to have the opportunity to use the training they gained from that assignment. Though computer security may be too narrow a specialty to make a career field out of at this time, the Air Force should keep track of computer security expertise to allow assignments in that specialty as openings occur.

Summary

Trusted system development and computer security is at a crossroad. If DOD loses momentum because of budget cuts, it may take years to get back to where we are today. As a result, vital command, control, and communication systems will continue to be vulnerable. AFCC as the implementing agency for computer security will be the command who takes the heat for any serious compromise that should occur. Additionally, AFCC is in a unique position to reach people throughout the Air Force and raise interest in all aspects of computer security. Education, networking computer security expertise, and senior officer involvement and support are the keys to continuing the momentum gained in this field over the last year. The threat continues to grow and we must be willing to work to counter that threat before a serious compromise occurs.

Notes

1. Roger R. Schell, vice president for engineering, Gemini Computers Incorporated, telephone interview with author, 21 December 1988.

2. Susan Passmore, staff security analyst, Tandem Corporation, interview with author, 26 July 1988.

3. Congressman Tom McMillen, Maryland, keynote speech given at 11th National Computer Security Conference, 18 October 1988.

4. Schell interview.

5. Morrie Gasser, *Building a Secure Computer System* (New York: Van Nostrand Reinhold Co., Inc., 1988), 10.

6. Ibid., 39.

7. "Air Force Communications-Computer Systems Security," briefing handout, Communications Computer Systems Executive Seminar, Maxwell AFB, Ala., October 1988.

8. Don Hanson, education officer, AFCSC/SR, "Background Paper on Air Force Communications-Computer Systems Security Education, Training and Awareness Program" (Unpublished paper, Air Force Cryptological Support Center, 15 March 1989).

9. Timothy R. Gernert, computer security staff officer, Headquarters MAC, telephone interview with author, 5 January 1989.

10. Schell interview.

11. Phillip W. Henning, 7th Communications Group, "Security for Headquarters System Replacement Program," point paper, Washington, D.C., 2 March 1989.

Glossary

AFCSC	Air Force Cryptological Support Center
AFCSC/SR	Air Force Cryptological Support Center Computer Security Office (formerly called the Air Force Communications- Computer Security Management Office)
ALMC	Army Logistics Management College
BBS	bulletin board system
CDRL	contract data requirements list
CMW	compartmented mode workstation
CSSO	computer system security officer
DAA	designated approving authority
DIA	Defense Intelligence Agency
DID	data item description
EPL	evaluated products list
ESC	Electronic Security Command
ETAP	education and training awareness program
HSRP	headquarters system replacement program
IS/A AMPE	interservice agency automated message processing exchange
MLS	multilevel secure
MOU	memorandum of understanding
NCSC	National Computer Security Center (formerly called the Department of Defense Computer Security Center)
PERC	Product Evaluation Resource Center
POM	program objective memorandum
RAMP	ratings and maintenance program
RFP	request for proposal

AU GAFB, AL (910812) 1000