(2)

COMPUTER SECURITY POLICY ISSUES: FROM PAST TOWARD THE FUTURE

Willis H. Ware

December 1987

P-7402

The RAND Corporation, 1700 Main Street, P.O. Box 2138, Santa Monica, CA 90406-2138

NOTE ADDED IN PROOF

Subsequent to the presentation of the material in this paper but prior to its publication, the Senate passed H.R. 145 (Computer Security Act of 1987) on December 21, 1987. The House had previously passed the bill on June 22, 1987. The President signed it into public law (PL 100-235) on January 8, 1988.

The Act implements a major recommendation of this paper, that the Institute for Computer Sciences and Technology (of the National Bureau of Standards) have a greater role in computer security. The Act also makes various other provisions for accommodating computer security throughout the federal government.

This paper, however, makes a number of other suggestions designed to set an agenda for moving the country into an improved posture with regard to the overall security of computer systems within and outside the federal government. (KR)

COMPUTER SECURITY POLICY ISSUES: FROM PAST TOWARD THE FUTURE[1]

INTRODUCTION

It is a pleasure to be here with you this morning and to have such a splendid and choice audience. It is a cross section of people concerned with computer security with whom I rarely have an opportunity to intersect.

Since the National Computer Security Center (NCSC) at the National Security Agency (NSA) and its publications (each with a different colored cover) hold such a central position in the affairs and pursuit of computer security, a certain notoriety has gradually emerged within the "compusec" community for referencing the several documents by the color of the cover. Thus, in casting about for a title, it was tempting to select one that alluded to the well-known Orange Book[2] published by the National Computer Security Center.

I had thought of several phrases mentioning the color orange, or a nearby hue; but as it happens, a neutral grey title had already been selected for me by the meeting organizer so my scope of topic is quite unbounded.

Let's move on to the subject, but first let me say that I have not attended any of the sessions of the CSI annual meeting; and since my arrival here late last evening, I have not discussed the content of the various workshops with anyone. Thus any similarity between what I will say and what has been said must be considered purely coincidental; these are my own views and certainly reflect no coordination between me and others.

---

[1]Presented to the Ernst & Whinney sponsored Information Security Services breakfast meeting during the annual Computer Security Institute Conference at Anaheim, California, November 11, 1987. This is an enlarged and slightly edited version of the presented material.

[2]So-named because of the color of its cover. Its full and proper title is *Department of Defense Trusted Computer System Evaluation Criteria*, DoD Computer Security Center (now the National Computer Security Center), CSC-STD-001-83, 15 August 1983.

REVIEW OF THE BIDDING

Let's start by reviewing the bidding, see what can be learned from history, and understand how we got where we are. There is a bottom line to the review but by no means am I pointing fingers, simply looking for clues to the future.

In the spring of 1967 at the National Joint Computer Conference in Atlantic City, New Jersey, there was a special session which I had organized to introduce the topic of computer security to public discussion.[3] Security controls in computer systems had been a topic deep in the defense establishment before then, but computer practitioners and owners of systems in the world at large had really not heard about the topic in professional circles and meetings.

Soon after that came a Department of Defense (DoD) study, originally commissioned by the Advanced Research Projects Agency (now DARPA) but later transferred to the Defense Science Board (DSB). A classified report was published in February 1970. It was declassified and reissued in October 1979 as an unclassified publication, and is sometimes referred to as "the Ware report."[4]

The motivation for the DSB study was the emergence of resource-sharing computer systems and their alliance with communications, plus the fact that the DoD did not have adequate policy to address such systems. In addition, defense contractors had asked for guidance on using the same (then) mainframe systems for concurrently processing classified and unclassified material. The most extreme case was that of a system supporting the classified development of a tactical fighter aircraft plus some 1500 terminals for unclassified commercial accounts and located in unprotected areas.

---

[3]"Security and Privacy in Computer Systems," *AFIPS Conference Proceedings*, Vol. 30, 1967, pp. 279-300. "Practical Solutions to the Privacy Problem," pp. 301-304.

[4]Willis H. Ware (ed.), *Security Controls for Computer Systems*, Report of Defense Science Board Task Force on Computer Security, published for the Office of the Secretary of Defense by The RAND Corporation, Santa Monica, California, as a classified document February 1970; reissued by RAND as an unclassified publication R-609-1, October 1979.

The DSB study group came from the defense/intelligence establishment. Its members either were in government, or knew government and its defense agencies intimately; the commercial user world was not represented. The focus of the effort was any computer system (large mainframes at the time) that had to control access to defense classified information--be that system inside government or in a contractor facility.

There was an early recognition--wise I am convinced--that computer people, no matter how much they would prefer to, would never be able to force a restructuring of the classified scene as it had developed in a paper-oriented world. There was the accompanying appreciation that they should not even try. There was also recognition that a lot of people from the classified paper world would have to transfer to, work in, and feel comfortable with the computer world. Whatever could be done to ease the transition would be desirable.

Hence, the DSB study group made a fundamental decision to structure the access control situation within the computer in the image of the paper world as we collectively understood it at the time.

In a paper world of classified documents, there is little beyond access control. There are rudimentary audit trails in the form of logs and access lists, but there are no concepts of automated processes working in behalf of a user, or automated processing of the information within a document.

In view of this, the primary issue with which to be concerned at the time was:

- Limiting access to information and computer-system privileges to authorized recipients.

Since access in a paper environment is possession of a physical entity, physical protection and isolation of classified materials must also be present by implication.

Thus, it is not surprising that the DSB report primarily addresses access control; and, indeed, we spelled out in an appendix the complete set of Boolean logical equations that could implement the full intricate access control system of the classified DoD world as the rules were at the time.

The DSB group, because of its calendar timing and its tasking, did not address some things that a modern discussion would have to. On the other hand, we did point out that:

1. There are various kinds of vulnerabilities--accidental disclosure, active infiltration, passive subversion.
2. Security requires attention to all aspects--physical, personnel, administrative, procedural, hardware, software, communications.
3. A system must be responsive and adaptable to changing conditions, must be auditable, reliable and manageable, and assure its own configuration integrity.

We also talked about risk level and cost, and we introduced a set of definitions that provided new terms as required but also established a relationship between terms from the paper world and those of the computer environment.

We did not talk about threat--which was not within our tasking--but we did try to discuss vulnerabilities to some extent. We thought of them though as wiretaps, transmitting bugs in hardware, theft of magnetic tapes, and unauthorized actions of systems programmers and operators. In fact, the DSB report utilized a vulnerability chart that came from the Atlantic City session and has attained a certain prominence of its own through repeated usage in many other papers.[5]

The technical thinking within the computer security community had not progressed to the recognition of sophisticated software attacks through terminals; that came a few years later. The concepts of

[5] *AFIPS*, op. cit., p. 280.

software trapdoors, time bombs, and viruses had not yet entered the discussion, nor were the phrases even in use.

We stipulated the necessity for such specialized personnel as a responsible authority, a system administrator, a system certifier, a system security officer. We asked for transaction logging, receipting of output, system self-testing, and labeling of output. We called attention to the risk of user-to-user leakage. We described our view of the tests necessary for certification and when each should be performed.

Our treatment of software was thin, although we did call out a few features for the operating system, including minimizing the portion of it that runs in the privileged state, doing a security analysis of it, putting access controls in it, having an orderly startup.

We talked about terminals and protecting them and, even as now, passed the communications protection to the communications security community. We asked for audit trails and said what they should contain. We wanted the system to self-surveil, and to violate its own safeguards intentionally as a part of auto-testing. We noted several research areas, interestingly though not including software!

Finally, we spelled out our view of management and administrative controls.

Initially, because of its classified status, the report was necessarily limited in distribution; but even so, many hundred copies were distributed. Later, many hundred more copies of the unclassified edition were also distributed.

I have given this sketch of the DSB report to indicate the foundation of understanding and insight from which computer security has developed. The computer system security job in the classified environment was quite well-understood and appreciated by at least one set of 20 or so people in the the late 1960s. While we missed some technical points and our taxonomy of the problem was slightly different, one could still do a good security job by following the 1970 DSB report.

WHAT CAME NEXT

The DSB activity in turn begat a sequence of things. Through the early/mid 1970s, the DoD and intelligence communities wrote and rewrote policy documents, notably DoD Directive 5200.28 and its Manual. The Advanced Research Projects Agency (now DARPA) and the United States Air Force (USAF) kept the subject alive technically. ARPA funded penetration efforts, partly to support policy positions that the DoD needed to take, but also to demonstrate the weaknesses of the contemporary operating system software.

The ARPA- and USAF-sponsored work focussed on system specification and evaluation. There were several invitational workshops, the first by the Air Force in 1972. The common thread through everything of course was the software issue, in particular the operating system aspect, which was the dimension of the problem that had received least attention and the one with which we--the computer community--had minimal experience in a security context.

In 1977, the DoD launched its Computer Security Initiative to focus attention and action on the issue. In response to it during 1977 and 1978, the National Bureau of Standards sponsored two workshops addressing various aspects of secure systems, and the first of the Federal Information Processing Standard documents appeared along with some other special publications. Through the Air Force, in particular the Electronic Systems Division, The MITRE Corporation was brought into action and various technical issues came under analysis and study.

The concept of the kernel was invented and there were three efforts to build kernelized operating systems for mainframes popular at the time. A lot of effort went into trying to be analytic and mathematically formal about implementing software systems that would be secure, stay secure, and transition from state to state securely; and into criteria for evaluating them after the fact.

The concept of "trusted system" appeared along the way. Just to remind you of what the phrase means, a trusted system is one that enforces a security policy with extremely high confidence and integrity. One must immediately say that a "security policy" is the set of rules

governing who may access what information, and what each may do with it. "High confidence" is the design assurance aspect of knowing that the software security features are present and working properly. And finally, "integrity" is the ongoing assurance that the software protection features continue to be what they are expected to be.

The overall inference is that a trusted system can handle (i.e., process) information at various levels of classification (or sensitivity) concurrently, and hence maintain the necessary separation between various categories of it and limit access to each category and/or item of information as required by the security policy, all with initial assurance of security safeguards and with ongoing integrity.

By the end of the 1970s, there was a good awareness of what it meant to design a secure operating system; and there was a modest body of research achievements on which to build, including preliminary concepts for evaluating systems, and a number of relevant technical concepts for implementing secure software.

Concurrently in the commercial world there was little action other than a very slowly growing awareness that computer security indeed was a real thing, not something invented by the computer people to sell more hardware and software. However, vendors did not want to raise the subject lest the customer base conclude that computers were risky devices with the result that sales would be inhibited. There was a small amount of educational and guidance material available from a few sources, but not much.

Also of importance in the 1970s were activities in nondefense government, notably the various ones with respect to (what is called) personal privacy or informational privacy. The Secretary of the Department of Health, Education, and Welfare (now Health and Human Services) sponsored the Advisory Committee on Automated Personal Data Systems which reported in 1973. While the effort was launched by Secretary Elliot Richardson, because of personnel shifts the report was actually delivered to Secretary Caspar Weinberger. The report, also nicknamed "the Ware report," was the intellectual basis of the Federal Privacy Act of 1974. It in turn created the Privacy Protection Study Commission which submitted a major report with five appendices in 1977.

These privacy-related events called attention to the need for protecting personal information and for controlling access to it. The Privacy Act was also the signal to nondefense agencies of government that they should and could spend money on the security of their computer systems. Indeed, some views at the time believed that most of the money spent in behalf of privacy was in fact used to improve bad security situations. But that was, of itself, an important step toward improving information control.

THE 1980s

Each decade begets the next and by the 1980s, we--the computer specialists in security--understood that building a secure operating system was a technically tough and expensive job. There was also general agreement that it would require redoing the commercial products, in particular the operating system software; security could not be retrofitted.

The government was moving more and more into systems that demanded security controls, so the big question became:

- How could the government get secure software products?

An imaginative person in the DoD[6] decided that a deal could be arranged. If industry could be persuaded to invest its funds in designing and implementing secure software products, the government would test and certify them at no charge. Hence, industry would have the proper products to bid government RFPs that would ask for secure systems, and the government would get secure systems.

It looked like a winner all around. Industry would underwrite the bill for the software development; the government had the expertise (it felt) to test the software and would get products that it needed. A side payoff was that industry would have secure software systems for other customers as well.

---

[6]Stephen T. Walker, then of the Office of the Under Secretary of Defense for Research and Engineering, Department of Defense, and now president of Trusted Information Systems, Inc.

Certain collateral questions never came up, or were not a central part o_ the discussion at the time, or even may not have been anticipated:

- Would a vendor be allowed to sell his secure software products worldwide?
- Would secure systems good for the government also be good for the private sector, or even for civil government?
- How long would it take the government to test and certify a product versus its market lifetime?
- Was the commercial world's concerns about threat at all similar to those of the defense world?

From the government's point of view the issues were more global; namely, to get the whole show moving and on the road.

There was no natural place to give such a responsibility in behalf of the government. A new organization of some sort would be needed since the problem was much larger than communications security for which the National Security Agency already had the responsibility by law.

Clearly, a focal point within government was necessary to oversee the activity. The two and only reasonable candidates in government were the Institute for Computer Sciences and Technology (ICST) at the National Bureau of Standards (NBS) and the National Security Agency, which is a part of the Department of Defense.

There was much to-ing and fro-ing, not to mention jockeying for position. It was clear that Defense did not wish to trust the computer security issue to others; but it was equally clear that the National Security Agency--for good and understandable reasons--had not had the experience of dealing with the private sector in a large way and in an unclassified context. Yet NSA did have long-standing experience in and responsibility by law for communications security, and it had been concerned with computer security in its own behalf since the mid-1960s.

There was debate also about the possibility of two centers, and I along with others supported the view that the country could afford only one because it was felt that the job of building and testing secure software was so tough that we ought to concentrate all the intellectual assets we had in one place.

Ultimately, in the latter days of Admiral Bobby Inman's tenure as Director of the National Security Agency (DIRNSA), it was agreed with Dr. Gerald Dinneen, Office of the Secretary of Defense, that a center would be established and that NSA would be the executive agent for it in behalf of the government. From the beginning, the concern was for a center that could service all of government because it was recognized that civil government had the compusec problem also. I suspect, however, that it never occurred to anyone that the security problems of defense and civil government might be different in detail, not just in magnitude.

The Computer Security Evaluation Center (CSEC) itself was actually formed in January 1981 with an interim director, although its charter (DoD Directive 5215.1) was not issued until 25 October 1982.

The terms of the DoD Directive (in effect the Center's charter) specifies the scope of responsibility as the Office of the Secretary of Defense, the Military Departments, the Organization of the Joint Chiefs of Staff, the Unified and Specified [military] Commands and the Defense Agencies. It governs the "conduct of trusted computer system evaluation and technical research activities within the DoD in support of overall computer system evaluation."

The DoD Directive required the Director/NSA to "establish and operate the Computer Security Evaluation Center as a separate and unique entity within NSA." The Director/CSEC (among other things) is to:

- "Establish and maintain technical standards and criteria for the evaluation of trusted computer systems;"
- "Conduct evaluations;" and

- "Serve as the DoD principal technical point of contact on trusted computer systems with other government agencies, industry, foreign governments, and NATO."

The last is permissive, not mandatory. It simply identifies the CSEC as the technical point of contact if someone outside of the DoD decides to use or be interested in trusted systems. There is one place in the DoD Directive where the phrase "protection of sensitive and classified information" is used, but again it is in a permissive context.

In turn NSA created its own implementing directive, NSA/CSS Directive No. 21-1, *DoD Computer Security Center Operations*. Its words parallel those of the DoD Directive and are slightly different but convey the same intent as to scope, purpose, and assignments of responsibility, but the name of the Center was shortened to exclude "Evaluation."

The NSA Directive 21-1 states that the Computer Security Center (CSC) will support the "Office of the Secretary of Defense, the Military Departments, the Organization of the Joint Chiefs of Staff, Unified and Specified [military] Commands, and the Defense Agencies (hereafter referred to as the DoD Components), [and] those federal departments and agencies comprising the National Security Establishment for which the DIRNSA has responsibility for the protection of sensitive or classified information."

The NSA Directive 21-1 also clearly reflects the understanding that the DoDCSC would function as a separate entity under the stewardship of the Director/NSA who would be its advocate in budget and planning.

The DoDCSC is assigned [by 21-1] a variety of responsibilities, some in support of NSA internally, but including:

- "Establishing technical standards and criteria for the evaluation of trusted systems;"
- "Serving as the DoD focal point for technical matters concerning the use of trusted systems with non-DoD activities."

Importantly, the second item is still permissive, not mandatory; for example, if a non-DoD component should choose to use a trusted system, then the DoDCSC would be the focal point for technical matters. Finally, NSA Directive 21-1 identifies and specifies the interplay between the Computer Security Center and other relevant NSA elements, notably its R&D and COMSEC organizations.

The stage had been set for the creation of (what people refer to as) the various items of "colored literature." The Orange Book was about to be born from the groundwork that had been laid through the 1970s. Interestingly, though, a May 1982 draft of it did have a light blue cover.

The Orange Book (also referred to as the TCSEC or the Guidelines) was the first effort to structure a comprehensive set of evaluation criteria for computer systems that implement security controls and enforce a security policy. Even on simple things, much less complex things such as software security, it is rare to get everything right the first time. The Guidelines document has to be seen as a very good but nonetheless first cut at the computer security problem. It is neither demeaning nor critical to now ask: Given our understanding and insights after five years, do we think that we have the compusec issue structured properly, both technically and organizationally, at the national level?

On September 17, 1984, the President signed the National Security Decision Directive-145[7] which addressed itself to the security of telecommunications and automated information systems in the context of both classified and government-derived sensitive information. The latter was a new category of information seen as being threatened with inappropriate divulgence, and hence requiring protection. Without detailing the argument with quotations, let me just say that as far as the private sector is concerned, NSDD-145 uses only such words as "assist, support, advise, encourage and procure [equipment] for." No place is there any implication that the scope of the directive is mandatory to the private sector.

---

[7]*National Policy on Telecommunications and Automated Information Systems Security*, National Security Decision Directive-145, September 17, 1984.

However, the position in regard to civil government is clear; the directive applies. But to the extent that an impression has grown that it applies to the private sector, it has resulted from a series of administrative decisions and positions by bureaucrats interpreting the document.

It has been frequently observed in the privacy arena that if the country winds up in some unpleasant position relative to the infringement of personal privacy by information systems, it will not be because someone had a grand plan to steer the country there. Rather, it will be the culmination of a series of small decisions, each made probably with good intent, each looking like a good decision at the time in the context of circumstances at the time, each perhaps reflecting the enthusiasm, zeal, or unquestioned motives of an individual.

The same phenomenon had started to function with respect to the commercial sector and the new category of "unclassified but sensitive" information, but there has been a lot of backtracking. An unpleasant end-position, which probably would have evolved from the earlier activities, then would have had to be painfully undone and unraveled. The situation had clearly arisen from a series of suboptimization decisions and choices in the absence of a strategic overall plan to guide things.

AND HERE'S TODAY

Here we are today. The CSEC, later called the DoD Computer Security Center and now the National Computer Security Center, has been integrated into the structure of the National Security Agency, and parts of it have been shifted to other agency elements. The tie between communication security and computer security has properly become very close.

The National Center comes solely from a defense ancestry, from the DSB activity forward. Moreover, its defense orientation is that of the world that deals with classified information. The National Center's views, policies, and actions reflect its lineage.

Therefore, one would expect that the National Center's actions would automatically be to implement the standing requirements of the national security community for protecting and controlling access to the country's secrets--particularly those secrets which relate to our ability to counter, offset, circumvent or parry unpleasant things that an opponent can do to us. The National Center was bound to see the threat against computer systems as the traditional one that prevails in the operational and military planning side of the defense community--a threat from a well-funded, sophisticated, experienced, and persistent opponent.

There are other parts of the defense establishment that have not played a role in threat statements against their computers; namely, the so-called support systems, which include the logistic supply to military services; personnel services, which basically distribute entitlements; financial services; food services; and medical services. Such systems normally deal with unclassified information, although some of them handle sensitive personal information (e.g., medical records).

For them, the peacetime threat is not the national opponent; the threat is their own people who decide to misuse (rip off) a computer system somehow. The threat is the fraud, embezzlement, waste, and abuse combination of events, with the foreign opponent in second place. During wartime, of course, the foreign opponent becomes of increased importance. In fact, for such systems, it is not yet clear that they can be adequately secured with the controls set forth in the present rainbow of literature from the National Center.

Look at the two kinds of threats from a different point of view. The traditional threat from a foreign opponent is technically sophisticated, well-funded, intense, long-standing, persistent, focussed, and very explicitly targeted. The second, insider threat, is none of these but is an opportunistic one with mild overtones of focusing or targeting, is generally unsophisticated technically, and is often an isolated occurrence.

The second threat reflects the unauthorized actions of the authorized system user; the threat is from our side--our person, not theirs. It can change during wartime when personnel details, logistics movements, and a lot of other things can be of tactical value to an opponent, but during peace there are important differences between the classified and unclassified parts of defense systems.

The threat against the computer systems and networks of the business and industrial world is like tne second, not the first--at least as evidenced by the incidents we know about, the data we have been able to collect, and the views of the people concerned with the issue. When we successfully counter the insider threat against commercial systems, it may cause an evolution toward a more sophisticated variety; but such an event is downstream, probably a decade or more away.

But we ask: So what? So what, if the commercial threat is not the same as the one that drives the National Center, the Orange Book, and all related actions?

The answer lies in the genesis of the NCSC. While its thrust is to promote the use of trusted systems throughout government, the underlying hope from the beginning has been the quid pro quo arrangement between government and vendor.

It follows that:

- To solicit and maintain the interest and commitment of the vendors, it is essential that the NCSC transmit a consistent and unwavering signal to the vendor community, especially with respect to potential market and technical requirements.
- To do this, the general premises of the Orange Book must prevail because it represents the considered judgment of knowledgeable people with regard to endowing a computer system with safeguards that counter the perceived national threat against classified information
- Hence, the introduction of a different threat, which might require or be offset by a different or lesser set of safeguards, is a diversion that can be seen to threaten the goal that the National Center hopes to achieve.

The $64,000 question thus becomes:

- Can the objectives of the defense and commercial worlds be harmonized?
- Will the products that the NCSC seeks to have developed be acceptable to the commercial world? Or can they be made acceptable?

My snap answer to such questions is somewhere between "I don't know" and "maybe." The uncertainty arises from two parameters that the NCSC and the Orange Book community have not addressed, but neither do they have to for their clientele. They are:

- Performance--the impact of safeguards on throughput; and
- Cost, or better--the differential cost of having safeguards over not having them.

The defense community cares about cost, but it cannot measure very well the dollar consequence of a revelation or loss of some classified information, and thus it is not in a very good position to judge cost/benefit measures of security safeguards. On the other hand, the commercial/business community can very well measure dollar consequences in terms of inventory shrinkage, merchandise pilfered, or funds missing; and can compare them to safeguard costs.

Performance is really related to cost because, in principle, one can always offset performance impacts with a larger configuration.

In another dimension, assurance--the confidence with which one can expect the system to perform its security functions--is crucial to the defense community. The system has to withstand all manner of potential technically sophisticated intense attacks. Assurance is much less important to the commercial/business community--at least while the insider threat dominates, which will probably be for many years.

The basic issue remains: Can we harmonize the two communities? My more considered answer becomes: We must try; we have no choice.

There are several points to be made to support such a view:

- First, the "business side" of defense--logistics, personnel, finance--needs systems like the commercial community wants. At the moment it does not have them nor does it have a path to them. A big piece of the defense establishment will win from bringing defense and commercial interests together.
- Second, the vendors win because now they will see a consistent and solid signal.

  In the long run, the marketplace will have to offer a menu of safeguards from which to choose for each application. Some will be needed everywhere; what are they? Others are needed only by the classified establishment; what are they? Others, only by the business world or the nonclassified support side of the defense world; what are they?
- Third, assurance and choosing the suite of safeguards for any given situation should be independent choices. Assurance must be unbundled from the array of safeguards.

  Vendors will have to think this one over for a while because it is not immediately obvious how to proceed technically to achieve such a goal.
- Next, the government wins because it will have access to a wider variety of products suitable for all of its systems, not just products for classified systems.
- Finally, the private sector wins because it gets the advantage of the technical expertise within the government as it influences and guides the vendor community, and generally advances the state of the art.

HOW TO PROGRESS

How do we make this happen successfully? How do we make our way through the tar pits to achieve harmonization?

First, we need a good delineation of the threat as seen in the commercial sector. The Clark-Wilson paper[8] from the Oakland conference is an important start and the integrity conference[9] a few weeks ago is an equally important second step.

The unclassified support side of defense ought to get its story together also; what threat does it perceive? The Clark-Wilson paper describes functional requirements which exist in commercial systems, so I suspect that the unclassified defense world will find that the Clark-Wilson concepts have much relevance and application.

We are likely to need the analog of the Orange Book for the new commercial threat statements. However, we must acknowledge that the TCSEC safeguards have relevance to the commercial threat, so we cannot summarily throw them out and start all over. While there are views that say the Orange Book is totally relevant, there are other views that assert that it is an overkill and unnecessary. Yet some safeguards from it are clearly pertinent to the commercial sector (e.g., login procedures and audit trails, although the content of the last will probably be quite different).

Therefore, we should not summarily discard all the effort that the Guidelines document represents. We ought to start by assuming that all TCSEC safeguards are pertinent and then systematically examine each to ascertain its protection against the commercial threat before discarding it, to see what each can contribute, and to see how any might need to be modified. But we cannot stop there.

---

[8]D. D. Clark and D. R. Wilson, "A Comparison of Commercial and Military Computer Security Policies," *Proceedings of 1987 IEEE Symposium on Security and Privacy*, Oakland, California, August 27-29, 1987. Published by the IEEE Computer Society, Order No. 771, IEEE Catalog Number 87CH2416-6.

[9] Workshop on Integrity Policy in Computer Information Systems, Bentley College, Waltham, Massachusetts, October 27-29, 1987.

Next, we need to see what additional safeguards might be required for the commercial threat. There will probably be some. One that comes to mind is the "binding property" that the Clark-Wilson paper identifies: Only certain people are authorized to manipulate certain information with specified processes, and perhaps as well from specified terminal locations. The combination of events must be assured, not just each one individually because database integrity is the underlying motivation.

In a sense, a binding property is a higher-level security safeguard because it requires a combination of other controls to function in concert as well as individually, all in trusted fashion; and the combination as well as the individual controls must all be part of the trusted computing base. Access controls can obviously be a contributor to a binding safeguard, but I suspect that there is more to it. At least we need to examine the question.

One might argue that even the classified defense world has the requirement to bind the user to information and to processes. Indeed it does, but the users are cleared and thus become a part of the trusted process to bind user to information to process (or job assignment). Cleared users are, in effect, a de facto part of the trusted computing base. In the unclassified defense world and in the commercial world, users are commonly not cleared nor is trustworthiness established by other means. Thus, they cannot be considered a part of trusted activities which implies that additional safeguards are required within the system.

Defense systems, especially ones dealing with unclassified information, do many of the same activities as commercial systems (e.g., transaction posting, database updating). Database integrity is a much more important security policy issue for many defense systems than control of access to information. Defense users might find that a binding feature would be a very useful adjunct to other security controls now required in the Orange Book.

In regard to higher-order security controls, it would appear to be a significant R&D effort to work out the security primitives that all systems could have and from which higher-level security objectives can be assembled by securely locking primitives together. It is not obvious that the safeguards in the Orange Book are a complete set of primitives; nor is it clear that they are not. For example, it might be that binding could be implemented through a combination of access control and login procedures, but the two would have to function in a cooperative way, not as individual safeguards.

Having explicated the safeguard needs of the commercial systems and having harmonized the commercial and defense requirements, we then need to make sure that the vendor community understands exactly what has been done, and we must present a unified set of security requirements to it.

There are undoubtedly organizational interfaces within government that will need changing and some documents will need adjustment. Perhaps the present Orange Book will become one of several such documents and be applicable--possibly modified--only to classified systems. The NSDD-145 might need adjustment, as would various derivative documents.

The commercial/business world must be able to balance off performance consequences of safeguards against the risks and losses that derive from the threat. It is not technically obvious just how to make this possible, but the problem needs attention.

WHAT STEPS TO TAKE

What actions can move us forward? When the NCSC was a dream about to happen, there was an intense debate in regard to where it should be situated. The country decided to have just one center for the reasons already noted. Today, we are five years smarter and with a much broader technical base--thanks to the investments at the National Center and at the Institute for Computer Sciences and Technology.

I have had second thoughts about what we have done as a country. I am now wondering whether we may have asked something of an agency that it should never have been expected to deliver. In that regard, I am now

inclined to argue that it has been unfair and inappropriate--maybe even unwise--to demand of an agency wholly devoted to intelligence and defense matters that it deal with the broad commercial/business community in a largely wide-open unclassified fashion. On the other hand, we cannot and must not ignore the advances that the National Center and the National Security Agency have made, nor the expertise they have accumulated. Nor can we fail to take advantage of the extensive communication security experience and capability in NSA.

As I see it, we need to fit the National Center and NSA into the computer security picture in a better way than we have so far at the national level.

As I look for ways to progress, I conclude that it is time to put the NBS/ICST into the security business much more vigorously, much more visibly, and much more comprehensively. It has demonstrated a good track record with the security concerns of the financial community and with other computer security issues. The NBS/ICST is an asset that the country has not adequately supported or exploited. Moreover, the country can now afford, financially and intellectually, two centers addressing the computer security problem.

I hasten to add that such a suggestion is not an invitation to undermine or deny the goals that the National Center wishes to achieve. It has generated a lot of momentum with the vendor community that must be allowed to play out.

Clearly, we do not cast the present National Center aside and dismiss it with a "thanks, now get lost." It is much too valuable nationally to risk allowing it to pull into a shell and become an invisible player. Its activities and those of the ICST must be coordinated closely, but each must have a certain measure of independence because each will serve a clientele with different needs.

But both also serve a common set of goals in behalf of the government and country. First and foremost is the assurance that all government and business/commercial systems that require security safeguards will have commercially offered systems that include them, and second is a steady consistent signal to the marketplace and the vendor community about security needs.

I would also note that the presence of NBS/ICST could possibly help NSA interface the commercial and unclassified world more smoothly. The ICST can be interpreter, buffer, go-between, as well as a contributor in its own right.

Suppose we cannot achieve harmonization of the needs of defense and others? What is the alternative? There is one.

- The business/commercial community can go it alone.

It can get organized into communities of interest, each of which can get its act together and handle its own security requirements.

In the short run such an approach could work, but in the long run it will not because security requirements will transcend boundaries of communities of interest. We are inexorably moving ahead to a time of permanently interconnected systems for the regular exchange of information, and to systems that dial one another to exchange information on a demand basis. We can bet that in general not all such systems will ever be in the same community. Moreover, it is the nature of information affairs to be pervasive and to ignore organizational and jurisdictional boundaries.

Eventually, we will have to organize the solution of the computer security problem in much the same way that the several telephone companies got themselves organized in the early days of telephony. No matter who they are and what the details of any individual system might be, anybody must be able to connect to anybody and exchange data with assured security to both parties; and a guarantee that the behavior of one will not compromise the security safeguards of the other.

In the long run a uniformity and standardization of security approaches and safeguards will prove essential so we might as well get started in the right direction.

The standards organizations--Institute of Electrical and Electronics Engineers (IEEE), American National Standards Institute (ANSI), International Standards Organization (ISO)--will get there eventually but we will get there sooner with a fully cooperative effort

among the National Computer Security Center, the National Security Agency, and the Institute for Computer Sciences and Technology. The general conditions must be:

- Each attending its own scope of clientele;
- Building on the expertise of the NCSC, NSA, and the NBS/ICST jointly;
- Building together on the technical foundation that all have helped create.

That is my perception of things. It is time to have a marriage that, I hope, can be made a gracious one and not a shotgun affair.

Why don't the commercial and business interests go forth and make it happen? They have the influence and clout; they have the need for a solution; and they cannot adequately handle the computer and network security problem on a piecemeal basis.