A RETROSPECTIVE ON THE CRITERIA MOVEMENT

Willis H. Ware

P-7949

Published 1995 by RAND
1700 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138

A RETROSPECTIVE ON THE CRITERIA MOVEMENT[1]

Willis H. Ware
RAND
Santa Monica, California

INTRODUCTION

The intent of this paper is to review the chronology and evolution of various "criteria efforts" and suggest where they fit into the overall scheme of secure systems. I want to be clear that my comments are not critical ones, but rather observations based on history as I have observed it.[2]

HISTORY

First the history. Remote access systems were entering the operational inventory during the late 1960s, and a major aircraft manufacturer wanted to commingle 250 commercial accounts with a classified aircraft project in the same machine. The DoD realized that it had no policy in place for the security of such an operational environment; and in addition to sponsoring penetration efforts that were successful, it organized a study group to examine the issue and make recommendations.

This committee worked for about two years and from it came the well-known so-called "Defense Science Board report."[3] As might be anticipated, the report said little about software, although it did raise the issue of (what we would call today) trusted distribution.

At that time, except for one defense project,[4] no one had really examined the software issue in regard to security safeguards, nor had the R&D community addressed it. Other aspects

---

[1] This paper was presented at the 18th National Information Systems Security Conference (formerly the National Computer Security Conference), October 10-13, 1995, Baltimore, Maryland.

[2] During the preparation of this material, which originally occurred in April 1995, the author had not remembered an earlier paper which provided a technical critique of the shortfalls of criteria. I was reminded of it during a conversation with its author after I had finished this retrospective. Now there are at least two data points in this conference series, separated by five years, that look at the criteria movement and ask about its historical importance and effect.

Peter G. Neumann, "Rainbows and Arrows: How the Security Criteria Address Computer Misuse," *Proceedings of the 13th National Computer Security Conference*, NIST/NCSC, Washington, DC, October 1990, pp. 414-422.

[3] Willis H. Ware, ed., *Security Controls for Computer Systems*, Report of the Defense Science Board Task Force on Computer Security, R-609-1. Published for the Department of Defense by RAND, Santa Monica, CA, February 1970 as a classified document and republished as an unclassified document in October 1979.

[4] Bernard Peters, "Security Considerations in a Multi-programmed Computer System," *AFIPS Conference Proceedings*, Vol. 30, 1965, pp. 283 ff.

now well understood to be a part of the comprehensive computer security treatment were covered though: the comsec, administrative, management oversight, personnel, and physical dimensions. Hardware, to this day, has of course not ever been addressed. The report also reflected the environment of the time: pre-LAN, pre-explosion of microcircuits, pre-small computers, pre-intense networking, pre-Internet.

Subsequently, the DoD (USAF/ARPA) sponsored research throughout the 1970s, including three major efforts to build secure versions of then popular operating systems.[5]

Toward the end of the 1970s, the government had realized its dilemma. Industry was not producing secure software, and was not likely to make the investment to do so because no commercial demand for them was perceived. The government believed that if it wanted secure system software, it would have to pay for it under special development projects, which it felt that it could not afford.[6]

So a deal was culminated in late 1980. Industry was asked to invest its funds to develop secure operating systems; and in return, the government would test, examine, and evaluate the resultant products at no cost. Products that successfully passed evaluation could be sold to the government without further qualification.

And an organization was created to preside over this effort; namely, the DoD Computer Security Center.[7]

THE TECHNICAL COMPUTER SYSTEM EVALUATION CRITERIA (TCSEC)

The implication of the arrangement was that some specification had to be established against which vendors could design and build. There had to be a common target for such efforts; and in addition, there had to be a common understanding between government and industry as to what performance features the government would test to.

---

[5]These were known by the acronyms KSOS, PSOS, and KVM.

[6]As the DoD moved ahead in its computer security thrust, Stephen T. Walker (founder and president of Trusted Information Systems) played a prominent role. First at ARPA and later in the Office of the Secretary of Defense, he convened some of the early discussion groups, sponsored the writing of earliest drafts of a criteria document, sponsored workshops which included the earliest discussions with industry, and formulated a program that later became known as the Computer Security Initiative. He later brokered the discussion that led to the formation of the DoD Computer Security Center at the National Security Agency. He is credited with introducing the phrases "trusted computer system" and "trusted computer system evaluation criteria."

[7]This was done under the authority of DoD Directive 5215.1, *Computer Security Evaluation Center*, October 25, 1982.

Thus, a series of workshops were convened to create the document which eventually became known as a "Criteria"; and with it, the "criteria movement" was born and acquired public awareness.

The people involved in the workshops had some or all of these characteristics: generally defense oriented, researchers that had been funded by the DoD during the 1970s, people who knew the historical defense threat and defense operations, computer scientists. In particular, there was essentially no representation from nondefense government or from the commercial-user sector.

The *Technical Computer System Evaluation Criteria* —later nicknamed the Orange Book— was first published 15 August 1983.[8] It was a very difficult document to read because its language, its constructs, and the attempt to make it very general combined to present a very alien technical discussion even to well-informed technical people. As it gained visibility, there developed a belief that it would apply not only to the defense part of government, but in fact to all of government and to the extra-government sector as well.

Later, there was published additional items in the "Rainbow Series" of literature:

Yellow book — a guide for applying the TCSEC, but strictly in terms of defense constructs. June 1985[9]

Puce book — Database Management Systems. April 1991[10]

Red book — Trusted Networks. By the time of its appearance, wide area networks, the Arpanet, and similar approaches had become the contemporary technology, but only an appendix addressed them. Most of the book spoke to the older mainframe-oriented network serving its own community of users. July 1987[11]

---

[8]Department of Defense *Trusted Computer System Evaluation Criteria,* DoD Computer Security Center, National Security Agency, CSC-STD-001-83, 15 August 1983.

While the document is characterized in its preface as "a uniform set of requirements and basic evaluation classes," the TCSEC really filled the role of a standard and was later adopted as a DoD standard.

[9]*Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments,* DoD Computer Security Center, National Security Agency, CSC-STD-003-85, 23 June 1985.

[10]*Trusted Database Management System Interpretation,* National Computer Security Center, National Security Agency, NCSC-TG-021, April 1991.

[11]*Trusted Network Interpretation,* National Computer Security Center, National Security Agency, NCSC-TG-005, 31 July 1987.

Some of these documents were called "interpretations" which implied that they were ministerial treatments derived from the Orange Bible. They did not address an issue de novo, but simply related the constructs and content of the Orange Book to the issue at hand.

TCSEC Ancestry

Thus, looking back over history, we can conclude that the ancestry of the Orange Book and related documents reflected the following heritage:

- It was defense driven ab initio;
- The defense threat was the implicit focus of concern;
- A defense concept of operations was implicitly assumed;
- The defense personnel environment was implicitly assumed—cleared personnel;
- The defense operational environment was implicitly assumed—usually secure;
- Mainframe oriented, reflecting the calendar time;
- Oriented to stand-alone systems—they were the environment of the time; and
- Little treatment of networks—in particular LANs, WANs, Internets, client-servers, and modern architectures were not addressed.

Other Criteria Efforts

The TCSEC begat a number of other efforts.

The author suggested in the National Computer Security Conference of 1989 that a "civil sector orange book" was needed, and proposed that two years might be needed to produce it.[12]

There followed:

- The Minimum Federal Security Requirements

  Started in early 1991; a final draft appeared August 1992.
- The Federal Criteria Working Group

  Agreement to create it was signed December 1990; first meeting took place January 1992; final document was released January 1993.

[12]Brief remarks by the author upon receipt of the National Computer System Security Award, 12th National Computer Security Conference, October 11, 1989

There were concurrent efforts in other countries:

- The Canadian Trusted Computer Product Evaluation Criteria

  Begun August 1988; version 1.0 appeared in May 1989;version 3.0e was published in January 1993.

- The UK Security Evaluation and Certification Scheme

  The decision to undertake it was announced December 1989; the first document, version 1.0, appeared 1 March 1991; Issue 2, UKSP 01 was published April 1994.

- The Information Technology Security Evaluation Criteria

  A joint effort of four ITSEC countries:
  UK/Germany/France/Netherlands. The Provisional Harmonized Criteria, version 1.2, appeared 28 June 1991.

- The Common Criteria

  The most recent and current effort; a world-wide effort of prior players in the criteria movement: ITSEC group plus Canada and the United States. The agreement to undertake it was signed February 1993. The final draft is expected to be out for wide comment, late first or early second quarter of 1996. It is an enormous volume, approximately 800 pages.

It should be noted that, like the TCSEC itself, most of the people involved in other criteria efforts came from, or were closely related to, the various national defense establishments. Moreover, the group was formally called an "Editorial Group" and clearly stated that its mission was only to harmonize the content of the input documents. Specifically, the group was not chartered to deal with new substantive concepts, to add new kinds of safeguards, etc.

FEATURES AND ASSURANCE

All criteria have (what are called) Features and Assurance.[13] Just to remind the reader: features are the security safeguards expected of the system or software; and assurance is a measure of the confidence with which one knows that the features are present, work as intended, are themselves safe from circumvention or modification, and ideally do not introduce a new basis

[13]Assurance is also referred to as "quality" and "correctness" in some documents.

for a penetration attack. Indirectly, assurance also implies that the system (in a security sense) does not do what it is not supposed to do.

It is well understood now that assurance is and has been the big stumbling block, although it is unlikely that its true difficulty was not foreseen in the earliest days. The process of establishing assurance—called evaluation—has proved to be so long that the time to complete it has often exceeded the market lifetime of the product. It has proved to be costly for the vendor to prepare for it.

(Un)bundling

The TCSEC bundled these two aspects; certain levels of assurance were bound to certain sets of features. Knowing of the experience with the TCSEC, the European efforts opted for unbundling.

The Common Criteria has followed the unbundling decision and has emerged as a very complex document, one with many different sets of features, many different levels of assurance, and allowing them in principle to be pairwise coupled as a product vendor sees fit.

The Common Criteria, as structured, allows anyone to propose a product, affiliate his choice of features and assurance level with it, indicate its intended use, get it evaluated, and offer it to the market. The Common Criteria, in fact, even includes a claims language which the vendor is to use in describing his product and making security assertions about it.

One has to wonder about the possibility that its ultimate generality might detract from its utility. If vendors exploit its flexibility widely, end-users might be faced with building systems from components which do not have much in common; certainly with regard to assurance and maybe with regard to features also. Conversely, if an end-user wishes all components to have a common level of assurance, he might not have enough choice in regard to features.

DEFENSE vs. OTHER ENVIRONMENTS

Such is the history and current status of the Criteria Movement. Let's now consider the differences between the defense and other environments, notably the private sector. In particular, why has the Criteria Movement not had more consequence for civil government and for the private commercial sector?

There is a dominant observation of course; namely, the awareness of and the need for computer and network security has been understood in the defense environment since the mid-1960s. Conversely, this insight was slow to emerge in civil government and the commercial sector, probably 20 years later in a large-scale way.

But evaluated products have been around, as have criteria. Evaluated products are being used of course and to that extent, so are criteria. However, there must be other characteristics inherent in criteria that are collectively of importance. Consider these:

- The defense heritage stresses the wrong paradigm; namely, protect the system and data at any cost vs. the commercial view of protecting the system and data at acceptable cost. It's the matter of risk avoidance vs. risk management.

- Criteria are based on the wrong threat. They assume the well- funded, diligent, persistent, technically smart foreign opponent vs. the commercial threat of the insider, the cracker, daily operational mistakes, or employee misbehavior.

- Criteria by ancestry assume the defense operational environment and the defense personnel environment implicitly. They expect the physically protected and possibly classified enclave populated by either cleared people or ones under military discipline. By contrast, the private sector environment is one of commercial machine rooms populated by people of unknown trustedness, functioning under civilian law and sometimes hired in response to national social policies.

- Criteria, with its defense heritage, anticipates different management motivations: the rules/regulations/laws for defense managers, whereas cost/losses/P&L statements drive the commercial manager.

CURRENT VIEWS ON CRITERIA

There are extreme views about the impact and relevance of some fifteen years of the criteria movement. At one end is the assertion that military installations are no more secure because of the TCSEC-related activity, and another that it has yielded a brain-dead idea as a major focus.

I submit that there is a more balanced view that is appropriate. Among other things, I think that the Criteria Movement, the TCSEC in particular,

- has and will improve software quality in operating systems and in other major software packages;

- helped to drive the evolution and adoption of good software development environments;

- indirectly sparked attention to computer security as an issue, instituted an important annual national conference, provided forums for discussion;

- has been a guiding model for people putting security safeguards into products;

- produced a moderate number of evaluated products of potential usefulness in systems; and

- has really been a forcing function to help maturation of the field.

Components vs. Systems

At best, any criteria can only produce components with known safeguards and defined levels of assurance. Except for the simplest systems, it cannot produce secure ones in general. The criteria as they exist today are not intended to address those collateral aspects of security which arise on a daily basis from operational glitches, mistakes, and anomalous situations. Yet such things are of high importance to commercial installations, and they are regarded within the scope of security. They seemingly should also be of importance to defense support systems which are usually unclassified and have many of the attributes of the commercial world.

Integrity

Even more importantly, criteria do not address the integrity issue satisfactorily, although there was an abortive attempt in the beginning to do so. Considering "integrity" as "meeting expectations" or "freedom from surprise," the business enterprise is currently concerned with integrity of components, of people, of systems, of networks, of software processes, and of the overall business processes inherent in the information systems. This is a far more general scope of concern than ever was envisioned in the TCSEC.

Heritage

Whatever else can be said about the TCSEC and for the follow-on efforts in the United States, there has been little participation from the commercial sector, little representation from people who ever had responsibility for running the daily operations of a big system, and very

little representation from people who had ever designed, implemented, and installed a big commercial system.

The very word "security" is used differently in defense vs. business. To the defense establishment, it means protecting the data and making sure that it is disseminated only to authorized individuals; the classes defined in the TCSEC and other criteria reflect that view. It has excluded such things as daily mistakes, glitches, and other anomalous events, and has generally ignored the insider threat.

In contrast, to the private sector, the computer system is understood to be the life-blood infrastructure for the organization and must be protected from that point of view. Hence, the metric for expending funds for security controls is a business decision, not a doctrinal one; namely, for a threat that might exploit an identified vulnerability, what are the consequent probable losses compared to the cost of the safeguards that would have fended off the loss?

The many reasons that I have just suggested are collectively why I suspect that criteria efforts have had so little consequence for the business world, other than the collateral payoffs previously noted.

REALITY

The commercial end-user must be responsible for the design, implementation, and operation of a secure system. The commercial end-user must establish his view of the threat and do a system design with security safeguards as appropriate. The commercial end-user has to be concerned with other dimensions of security that the defense people have generally ignored, although they seemingly should be of importance in all defense systems. The end-user must do a design balanced between expected loss and cost of security. The commercial end-user simply cannot give such responsibilities away.

How, then, will the Common Criteria likely fit into security activities in the nondefense applications?

Timing

The Common Criteria final comment-draft is scheduled for release in January 1996 to the drafting group. Release to the sponsors (the participating countries) is scheduled for three to four months thereafter; that brings us to the spring of 1996. It is anticipated that the sponsors will adopt it and presumably replace national criteria with the common version. At the time, the document will be released for general comment. We are probably now into the Fall of 1996.

No one can forecast how much comment will be received. No one can predict what response the Common Criteria drafting team or its sponsors will take. In the best of all worlds, it

will get prompt and wide acceptance; but even if it does, how fast can the vendors respond? How fast can products be brought to market in accord with the Common Criteria? Again, no one really can know. It is likely to be at least a year for some products, and probably two to three or more years for new products not now even available.

Putting all the uncertainty together, it seems that it will be rather close to the year 2000 before the Common Criteria will have major consequence on the security of information systems. That date happens to have been my unspoken belief for several years; I see no reason to change it.

Products

To date, vendors have participated in the evaluation process partly through persuasion, but also partly to be assured of being able to compete for government business. To the extent that a commercially viable product did achieve success, then it replaced the prior product and found its way into systems of the commercial and nondefense sectors.

With the sweeping flexibility of the Common Criteria, what are vendors likely to do? They might do business as usual and follow the past, considering the Common Criteria to be simply a generalized extrapolation of extant criteria. But there is a new option; namely, to target products especially at the security needs of the private sector business base. It is often argued that the classes of the TCSEC and similar criteria overkill some aspects of the risks as perceived by industry and business, and do not address others that are important to them. To the extent that vendors can guess at or define or anticipate what industry really wants as evaluated products, the Common Criteria will have opened an important new direction.

Such an argument, though, implies new products with different sets of safeguards and different approaches to assurance, and would support the belief that year 2000 is the earliest that the Common Criteria will have much impact.

Overall

If these projections are more or less correct, it will be 30 years since computer security was first flagged as an important policy issue at the DoD level. It will be 17 years since the first criteria was published. It will be six years since the criteria community was nudged at this conference for a document pertinent to the nondefense user.

But maybe that isn't so bad in hindsight! The computer and network security problem is, after all, technically intricate in many ways. While the threats have lead to local problems, annoyances, and frustrations, there have not been national catastrophes or disasters. Commercial losses have generally been accepted as a risk of business. Losses to business have evidently been judged as less than the costs of installing security and/or they have been passed along to

consumers. Computer system vulnerabilities and risks have been lumped into the other risks inherent in doing business.

On balance, there has been little motivation in the commercial world to really move ahead on computer and/or network security in a big way. Within government, funding shortages have been a persistent impediment.

THE FUTURE

What does the future hold? Are we poised for a big advance in computer and network security? Or will we have another half-decade or more of continued slow progress, acceptance of risks, and hoping for the best?

It is not at all clear how things will go, but what are some of the forces that might influence things?

- Many countries are building what the United States calls a "national information infrastructure." It is a "new kid on the block" and wields new influence.

- The cracker threat is emerging as one of growing sophistication, with more directed, less casual attacks and a higher level of activity.

- There is the steady spread of computer-based systems into ever more diverse applications and organizations.

- Electronic commerce seems poised to vigorously move forward.

- Networking and automatic connections among systems are becoming common.

- There are new technical opportunities for malicious actions; for example, software that is apparently benign but has an awareness of the local environment and able to affect it.

- While the cold war is over for defense, the new "visible enemy" has become Information Warfare whose true dimensions have yet to be accurately judged.

- Finally, let us not forget that institutions and governments have enormous inertia.

Collectively, maybe all such influences will drive things more rapidly, but I am not sanguine enough to bet on it. Forced to bet, though, I will opt for slow continued progress, a continuation of the past. I cannot identify a "grand event" that will drive large-scale progress in computer and network security.

It does look as though the ball is in the court on the vendors' side. It may well prove that their innovation in exploiting the flexibility of the Common Criteria, their imagination, their cleverness, their understanding of commercial-system security—coupled to the ability of commercial users to convey a cohesive statement of their needs—will collectively become the mover-and-shaker influence in security for the next five or more years. It remains to be seen.

Finally, there is a collateral observation. To the extent that US vendors do not perceive the opportunity that I have suggested for the Common Criteria but those of other countries do, then US industry is going to fall behind in developing the market for security-related components and systems, and fail to capture its share of it. As a result of inattention, we can easily lose another part of our industrial base to offshore interests.

Moreover, if the exploitation of the Common Criteria by vendors and end-users in concert does not occur as suggested, then we must be prepared to ask whether the Criteria Movement has been overtaken by events and has become an evolutionary dead end. We must be prepared to conclude that a criteria-based approach has had its chance but not succeeded, and that further pursuit of it is inappropriate.

But what then? What would the successor approach be? What should be the next evolutionary step? Perhaps it is time to begin thinking again about fundamentals, and about mechanisms that will assure systems secure and stalwart enough to support an information-intensive future.