Twenty years of evaluation criteria and commercial technology

Conference Paper · February 1999

DOI: 10.1109/SECPRI.1999.766905 · Source: IEEE Xplore

1 author:

Steve Lipner
SAFECode
34 PUBLICATIONS **1,155** CITATIONS

SEE PROFILE

Twenty Years of Evaluation Criteria and Commercial Technology

Steve Lipner
Mitretek Systems
McLean, Virginia

Abstract

The major source of progress in computer security products during the last twenty years has been the Internet revolution of the mid-nineties. Evaluation criteria and processes have provided users with some characterization of the security attributes of operating system products. The newly developed Common Criteria show promise of offering more timely and relevant evaluation results. However, there is little sign of progress in products that can deal with hostile code or in meeting needs for high assurance.

1. Twenty Years of Progress?

Perhaps a suitable test for the last twenty years is "Are your systems and networks more secure now than they were twenty years ago?" And a follow-up question, given the role of commercial products in the security of our systems and networks is "What is the role of product evaluation in the changed security status of your systems and networks?" This brief paper addresses these two questions.

Progress in computer security technology must be measured against the broader backdrop of progress in computer and networking technology. The computer technology of 1980 was composed of mainframes and minicomputers used for batch processing, time-sharing, and transaction processing. Some systems were connected to networks that supported remote login, file transfer and email services. Vendors' proprietary network protocols were the norm although the ARPAnet was a significant facility for academics and researchers. Widespread use of network encryption was a dream of researchers and security specialists.

While security was not a major factor in the software products of 1980, it was by no means totally absent. Mainframe security products were widely used in commercial installations. Minicomputer operating systems, including Unix and various proprietary offerings, included user identification and authentication mechanisms as well as basic access controls.

2. The Orange Book

The U. S. Government implemented the Trusted Product Evaluation Program (TPEP) so that it would be able to buy commercial computer systems that would have sufficient security to meet government's needs. The Orange Book was intended to communicate security requirements to vendors, evaluators, and purchasers of computer systems. At its inception, the TPEP was very successful. Every major vendor of computer systems sought C2 evaluation, and almost all started projects aimed at meeting the requirements of the higher evaluation classes.

As the TPEP process evolved, however, it became obvious that evaluation was not going to be "a walk in the park." The developers of the Orange Book had expected that C2 evaluations would put a seal of approval on existing products around whose attributes the C2 class was designed. B1 products were intended to add labels to the discretionary security mechanisms in C2 products. In fact, obtaining C2 evaluation proved to be a time-consuming process that required more development and documentation effort than vendors had expected. Development of products beyond C2 or B1 proved to be extraordinarily costly and time-consuming.

The difficulty of building evaluated products coincided with vendors' discovery that the demand for such products was very limited. While C2 security became a least common denominator for government (and some commercial) procurements, vendors discovered that evaluation of any version allowed them to sell all succeeding versions as though evaluated. Government users found only limited use for the mandatory security features in B1 systems, and no commercial market at all developed. Demand for the few systems beyond B1 was minimal, while vendors reported great disappointment with demand for B1 and CMW products. Both vendors and government product evaluators discovered that end users sought modern software features such as windowing, advanced networking, and current applications, even at the expense of evaluated security.

3. The Growth of Security Products

By the early nineties, the populations of evaluated systems and systems under evaluation had dropped to the hardy survivors at C2 and occasionally B1 plus a handful at B2 and above. It would have been easy to write security off as a requirement of the past.

Instead, the market for security products "took off." Major vendors developed new offerings while startup niche vendors grew out of garages around the world to go public at sometimes absurd valuations. These vendors were not developing secure operating systems (evaluated or otherwise). Instead, they offered firewalls, intrusion detection systems, authentication tokens, security management products, and encryption packages to deal with the "growing threat from organizational access to the Internet." While organizations might have been as exposed to attack through dialup lines as through the Internet, the perception of vulnerability was much greater, probably as a result of the wide publicity given to the Internet Worm, the "Wily Hacker," and other incidents.

It is easy to conclude that Internet security products such as firewalls and encryption packages meet all the requirements of enterprises that plan to connect to the Internet. Most, in fact, counter real vulnerabilities. For example, firewalls prevent Internet-based attacks on ill-managed systems on an organization's internal network. However, it is equally easy to conclude that Internet security products offer only the appearance of security and can easily be defeated by attacks that were demonstrated in the early seventies. For example, Internet security products are ineffective against Trojan Horse attacks that have become easy to deploy through mechanisms such as documents that contain macros (programs).

4. Evolving Evaluation

In the late 1980s and early 1990s, several European countries developed an alternative to the Orange Book. This scheme, known as the ITSEC, allowed the evaluation of specialized security components (more likely to be produced in Europe) as well as operating systems. Since European customers appeared to take security evaluation more seriously than customers in the U.S., U.S. as well as European vendors began to seek European evaluations. The appeal of the ITSEC was enhanced because ITSEC evaluations were conducted by commercial laboratories paid by the vendors rather than the Government, and thus more likely to respond to vendors' schedules and priorities. (The U.S. began evaluations by commercial laboratories in the mid-nineties under the Trust Technology Assessment Program.) In addition, component evaluations under the ITSEC were much more easily adapted than Orange Book evaluations to the emerging Internet security products.

From the early nineties, the U.S. and European agencies responsible for product evaluations sought a basis for mutual recognition of product evaluations. This quest ended in late 1998 with the adoption of the international Common Criteria (CC) and an agreement for mutual recognition of evaluation results. The CC, like the earlier ITSEC, allows for the evaluation of products with arbitrary security functions. As with the ITSEC and TTAP, commercial laboratories conduct CC product evaluations.

The prospects for the CC are largely positive. Evaluations conducted by commercial laboratories have been fast and cost-effective, and the ITSEC and CC have shown themselves to be adaptable to the wide range of security products that appear in a modern networked organization. Vendors are committing to CC evaluations in growing numbers.

The major drawback of the CC process results from one of its assets. By supporting evaluation of many types of security products, the CC leaves to the products' users much of the task of understanding the worth of the products' security functions and of integrating individual evaluated products into a secure system. By comparison, it is relatively simple for the user of an operating system evaluated under the Orange Book to understand the more limited utility of the product and the import of the evaluation.

5. Whither Products and Evaluation?

With the evolution of the CC, and the availability of security products driven by organizations' use of the Internet, it is easy to conclude that commercial demand will "solve the security problem." However, two caveats should serve as challenges to vendors, evaluators, and researchers. (1) Modern security products still do not effectively address the problems posed by hostile code (Trojan Horses) and our software systems are only increasing the power of hostile code to do harm and the ease of distributing such code to its targets. (2) Modern products fail to meet the needs of those organizations that require high assurance of security to protect extremely sensitive data.

In answer to the questions that began this note, it seems that new security products and features have at best compensated for the increased security exposure that results from the growth of networks and connectivity. Product evaluations have probably led to modest enhancements in the quality and completeness of those products that have been subject to evaluation. However, major needs for assurance and for the ability of products to contain hostile code remain unmet.

1081-6011/99 $10.00 (c) 1999 IEEE