Joshua Main-Smith
November 29, 2020

Evaluation

1. (10 points) When you review the list of products evaluated against the Common Criteria, such as that found on the Common Criteria Portal website, very few products are evaluated to the higher EAL 6 and EAL 7 assurance levels. Indicate why the requirements of these levels limit the type and complexity of products that can be evaluated to them. Do you believe that a general-purpose operating system, or database management system, could be evaluated to these levels?

A product with EAL 6 has been semiformally verified, designed and tested. A product with EAL 7 has been formally verified, designed and tested. It's easier to evaluate specialized products that have very little tasks to the degree of EAL 6 and 7 than it does for general purpose products. This is because the level of depth required in studying products grows rapidly with an increase in complexity. Smart cards are an example of products that are easier to study in-depth, containing a minimal task-set. General purpose operating systems, on the other hand, are so complex that it may be difficult to even understand its entirety on a fundamental level, let alone to the degree of security design.

As for if it's possible for a general use operating system, database management system, etc. to reach EAL 6 or 7: it's possible, but the cost of reaching such levels would be economically infeasible for any business in reaching such a feat. An operating system very likely contains tens of millions of lines of code. For this reason, it could take several years for a security vulnerability involving an operating system to be discovered (by the good guys). An example of this is the Dirty COW exploit that first appeared in 2007 and wasn't discovered until 2016.

2. (10 points) Assume you work for a government agency and need to purchase a network firewall device that has been evaluated to CC assurance level EAL 4 or better. Using the Common Criteria website , select some products that meet this requirement. Examine their certification reports. Then suggest some criteria that you could use to choose among these products. https://www.commoncriteriaportal.org/

The highest level for any product under the *Network and Network-Related Devices and Systems* is EAL 4+. There were six firewall devices I found with an EAL rating of 4 or higher (two of them written in French). A few of these products are the Sophos Firewall OS Version 17.0 from Sophos Ltd., the genugate 9.0 Firewall Software from genua gmbh, the F5 Networks BIG-IP® Application Delivery Firewall (ADF-Base), version 11.5.1 HF10 by F5 Networks, Inc., Eudemon1000E-N (USG6600) Series Firewall by HUAWEI Technologies Co., Ltd., and Eudemon200E-N (USG6300&6500) Series Firewall by HUAWEI Technologies Co., Ltd.

One thing to consider from the start is the last two technologies are from companies that have been in the news somewhat recently regarding allegations of espionage, fraud, and IP theft. Whether these allegations have any merit would be up to the government agency to take into consideration. Another thing to take into consideration is the certificate expiration date, as an expiration date soon would be a risk for the agency if the company decides to not re-certify. The product with the latest expiration date is the Sophos Firewall, expiring in 2025-02-18.

Further, one should consider the TOE security functionality of each product and how these functionalities would be the best fit for the functionality of the agency. Some of the functionality from Sophos is security audit, user data protection, identification and authentication. Genugate offers security audits, data flow control, identification and authentication. The F5 Network offers a wide range of security functionality from such topics as device management, traffic management, cryptographic mechanisms, TSF protection and support functions. Both of the Eudemon Firewall Series offers authentication, access control, communication security, and flow control policies. It may be useful to also read the product testing section to see if there is third party verification in product quality.