Global Information Assurance Certification Paper

GIAC Certification Practical Assignment Submission for:

Francis L Mayer

Assignment Version 1.2e

Considerations for Using Independently Certified or Evaluated Products

Wednesday, October 10, 2001

Part of the task of engineering a secure system is to ensure that the products integrated into the system are securely configured. The secure integration and configuration of products is a significant part of the overall security engineering effort supporting system development and deployment. The challenge is to determine exactly how to securely configure and integrate a product into a system because there are numerous sources of guidance. The sources include those that have been developed by both government and civilian organizations such as Department of Defense (DoD), National Institute of Standards (NIST), Computer Emergency Response Team (CERT) organizations, and System Administration, Networking, and Security (SANS) Institute. This guidance is in addition to the guidance provided by the vendor of the product and the configuration specified in a product's independent evaluation. This paper will outline the secure configuration considerations that security professionals need to address when integrating evaluated products into the systems they support.

Background:

- The benefit of using an evaluated product is that it has undergone an independent assessment that verifies it meets the criteria for the rating that it has achieved (TPEP FAQ, 1999). Stated another way, security evaluations provide customers with an independent, expert evaluation of vendor claims (Abramowitz & Connolly, 1995). This can reduce performance, cost, and schedule risks because the security functionality of the product has already been independently verified.
- Product evaluations are based on a specified system environment and configuration. When the product is not employed in a manner consistent with the configuration and environment in which it was evaluated, the evaluation can not be considered valid. Therefore, the validity of an independent evaluation of a trusted product is based on the configuration as evaluated and documented in the Final Evaluation Report (FER) or Common Criteria Certification Report. Changes to a system's configuration can have an impact on the system's security posture.
- Part of the engineering effort in certifying a system as part of its accreditation effort is verifying that evaluated products are being used for their intended purpose (DITSCAP, 1997) (NIACAP, April 2000) and that they are correctly integrated into the overall system they support.
- In addition to vendor produced documentation outlining how to securely configure a system and the guidance provided in an evaluated products test report there are numerous other "authoritative" guidelines have been produced by many organizations. Among these types of guides are the SANS Step-by-Step Guides, Center for Internet Security, CIS Benchmark and Scoring Tools, National Security Agency (NSA) Guides, and Defense Information System Agency (DISA) guides. This plethora of guidance is both helpful and overwhelming. Furthermore, these guides often only address the technical configuration of a product such as an Operating System (OS), not the overall hardware and software configuration of the system.

- The security engineer should consider not only the configuration guidance outlined in the aforementioned sources but all the existing policies, regulations, and standards that are binding on the organization or organizations that will develop, deploy, and operate the system (IATF, 2000).

Discussion:

The selection of products that will be employed in a particular system is driven by many factors such as cost, performance, and schedule as well as security considerations. The security professional may not have control over which products are chosen or how they are employed because business and mission needs may override to some extent other considerations such as information security. Nevertheless, the security engineer must formulate and implement an approach that will provide good security and mission functionality. For example, interoperability with and connections to other systems are business requirements that at times are at odds with security. The challenge is to take advantage of the capability various products offer and to avoid inherent pitfalls in these products. Accomplishing this tasks requires an understanding of what product evaluations, such as those performed under the internationally recognized Common Criteria, provide and how to securely integrate these products without sacrificing required system functionality.

The first step is to obtain the certification or evaluation report for the products used in the system being developed, integrated, and deployed. Among the sources for these evaluations are (note: URLs for these sources are listed at the end of this paper):

- Trust Technology Assessment Program Commercial Product Evaluations
- INFOSEC Assurance and Certification Services (IACS) Management Office, Certified Products
- Library of TCSEC Final Evaluation Reports
- National Information Assurance Partnership (NIAP) Validated Products List
- Vendor web sites that point back to the organization performing the evaluation

The next step is to study the configuration and environment outlined in the report to determine the limits of the evaluation. The certification report will outline how the system was configured for the evaluation and what is considered outside the evaluations. Several examples that illustrate the types of considerations that come out of this analysis are as follows:

- The Evaluation Technical Report for Check Point Software Technologies LTD Firewall-1 Version 4.0 reveals that the client authentication, session authentication, account management, Interaction with Operational Security (OPSEC) products, content filtering, Network Address Translation, Remote Administration, Fire Wall-1

Virtual Private Networking, and Windows NT 4.0 features not used in the evaluation, are all considered outside the scope of the evaluation. The configuration for this evaluation was Windows NT 4.0 with Service Pack 4.

- The Windows NT 4.0 Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) C2 evaluation which stipulates that POSIX and OS/2 Subsystems, Streams, and RAS, Dynamic Host Configuration Protocol (DHCP), NetBEUI, Appletalk, and IXP protocols are not part of the evaluated configuration. The Windows NT evaluation requires Service Pak 6.a, with the C2 Update, and an OS configuration consistent with the C2 Administrator's and User's Security Guide provided by the vendor, Microsoft.

- The Common Criteria Certification Report No. P148, Sun Solaris Version 8 with AdminSuite Version 3.0.1, outlines the evaluated configuration and patches applied to the system and also refers readers to the associated Security Target and Solaris 8.0 Security Release Notes. The Release Notes contain secure configuration guidance that the system administrator must implement to place the system in the evaluated configuration. The configuration settings include things such as configuring the boot device for both the SPARC and Intel type systems and setting the file creation mode to umask-022. The Security Target lists functionality not supported in the evaluated configuration such as the DHCP protocol and Smartcard authentication. In this case, understanding the evaluated configuration requires a study of all three documents.

The above examples are only illustrate some of the issues that can be encountered when studying the evaluated configuration and its applicability to the configuration that will be used in the system being developed. Hardware, Software, and firmware configuration guidance must be reviewed to get a clear picture of the configuration used to evaluate the product.

The next step is to consider the existing policies, regulations, and standards that are binding on the organization. For example, engineers working on Department of Defense (DoD) systems that are required to be compliant with the Defense Information Infrastructure (DII) Common Operating Environment (COE) need to consider the secure configuration requirements outlined in the DII COE Integration and Runtime Specification (I&RTS) as well as service regulations and local security policies. In addition security engineers may need to consider other organizational level policies unique to their systems such as OS specific secure configuration policies and higher level organizational policy requirements that will require specific configuration settings. An example of this is an audit requirement that outlines a particular set of security events that must be captured. The evaluated configuration may outline one set of events and local policy may outline a different set. The local policy may also outline a requirement for audit retention that will require configuration settings that may or may not be consistent with the evaluated configuration. An obvious approach may be to implement the more stringent configuration. However, operational concerns may complicate this approach. For example, the level of audit may become such that the

system and the system administrators are overwhelmed with audit data to the point where the value of the audit data collected actually starts to diminish. Another example is where required interoperability that exists with other systems and networks is made to fail because of too restrictive settings. In this case the restrictive settings cause a denial of service that poses a threat to the organization's mission. A more balanced approach may be to step back and examine the value of a particular setting and then to determine the best setting for a particular situation that poses the least overall risk to the security of the system and the mission. Then this solution should be documented in a risk assessment that is approved by the manager having the authority to accept the risk such as the Designated Approving Authority (DAA) in the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) or National Information Assurance Certification and Accreditation Process (NIACAP).

Consideration must then be given to the environment in which the system will be used. For example, some evaluated configurations do not make provisions for remote security management, as noted in one of the examples above. However, the system being developed may be deployed over a wide area with numerous devices that need to be securely managed. In this situation it may not be practical or desirable to manage each device locally instead of centrally. Therefore, a security solution will need to be developed to permit secure management of system components or like systems over a wide area even though the evaluated configuration made no allowance for this situation.

Required system functionality may come into conflict with secure configuration guidance. For example, certain protocols may be outside the evaluated configuration such as the Dynamic Host Configuration Protocol (DHCP), as noted in the examples above. Overriding mission and business needs may dictate that DHCP be used to provide services essential for a dynamic network. In this case the security professional can not realistically approach the problem by simply asking the system architects to come up with another protocol to meet the need. The approach required is one that will develop appropriate solutions with associated countermeasures supporting the required system functionality.

Another problem that the security engineer may encounter is situations where the evaluation was performed in the past and in the intervening time inadequacies in the evaluated product have been discovered. The vendor may have developed patches and procedures to address these problems that are not captured in the trusted product's evaluation. For example, as noted in the examples above, the firewall was evaluated with Windows NT 4.0 Service Pack 4, however, the later evaluation of the OS requires Service Pack 6.a and a C2 Update. Additionally, since the evaluation of the OS additional fixes have been published that need to be implemented. It may appear to be a straightforward process to simply apply the latest fixes to solve this problem but updates may adversely affect mission critical applications or performance, cost, and schedule of a system under development. A better solution may be to evaluate each fix to determine what the impact is if it is not implemented versus what the impact is if it is implemented. This risk analysis may determine that for a particular environment a particular vendor security patch does not need to be added to the system or a countermeasure may exist that can more easily be implemented and that will avoid

unknown changes that have the potential to put critical business or mission applications at risk. Since it is likely that systems will be put into operation before all available security fixes are applied, this type of approach will probably be more effective that frantically applying all security patches, as they become available. This is especially true since security fixes are published on an almost daily basis in some cases.

The security professional should not discount the value of using other sources of secure configuration guidance such as the SANS Step-by-Step Guides and Center for Internet Security, CIS Benchmark and Scoring Tools, which although may not be required by policy, may provide useful solutions to problems like some of those just presented. These sources often provide insights into the 'why' or rationale behind certain secure configuration settings. Armed with this knowledge, the security engineer can develop solutions to conflicting guidance or conflicts between interoperability, mission functionality, and system security. There are also instances where these types of guides are the only place where information is provided on how to configure a particular setting.

Once the secure configuration settings have been determined they need to be documented so that the work in deriving them is not lost and so that developers, system administrators, and maintainers may implement them. Part of this effort should include documenting the secure configuration settings as requirements that test personnel can verify. In the DITSCP and NICAP processes this can be done by adding secure configuration requirements to the system's Security Requirements Traceability Matrix (SRTM). This effort should also include ensuring secure configuration procedures are added to the system administrator's guide or the portion of the system's standing operating procedures used by privileged users. Ideally this is done before the system's overall certification test so that the testers can verify that the system can be securely installed and configured using the guidance in the documentation developed for the system. The system administrators will then need to be trained so that they understand and can apply the secure configuration procedures unique to this system.

After all the products are integrated into the system and the configuration of the system is set to comply with the secure configuration settings derived from the process outlined above, the system should be tested to ensure that the overall security functionality works as intended and that mission and business related functionality works properly. Part of the evaluation should include both penetration type testing and use of a vulnerability scanner run against the system to determine the systems overall security posture. Like the system administrators, the certification testing personnel will need to be trained on the secure configuration procedures and implementation unique to a particular system so that the evaluation can be both effective and efficient. This training should also preclude 'false' failures caused by misunderstanding of the system's intended configuration. The need for this step may raise the question: "Why use evaluated products if I am going to have to do security testing anyway?" The answer is that if the components that are used to build a system are evaluated by an independent authority before the system developer integrates them, then the risk that they will create a problem or not provide the basic security functionality required is greatly reduced.

Another benefit is that much of the low level testing against an evaluated component has already been accomplished, such as limit testing and error checking, and this reduces the level of effort required in subsequent system level testing. Another advantage is that system level certification testers can use the information in the product's certification report to reduce the level of effort required to understand a system component and the best way to test it in an integrated system.

Conclusion:

The assurance of an individual product does not guarantee system assurance or overall system security. Complementary controls are needed, such as sound operating procedures, adequate training, comprehensive policies, sound security architectures, system testing, and a risk management program (NIST SP 800-23, August 2000). The security professional needs to understand what the evaluated product provides and what it does not provide. The ability to reconcile the evaluated configuration against the system architecture that it will be integrated into as well as the ability to perform a risk analysis is critical to the successful integration of an evaluated product.

References

Communications-Electronics Security Group (CESG), INFOSEC Assurance and Certification Services (IACS) Management Office, Certified Products (2001)
URL: http://www.cesg.gov.uk/assurance/iacs/itsec/cpl/index.asp

Common Criteria Certification Report No. P148, Sun Solaris Version 8 with AdminSuite Version 3.0.1, UK IT Security Evaluation and Certification Scheme Certification Body, Issue 1.0 (November, 2000)

Connolly, Julie L. & Abramowitz, Beth S. (1995). "The Trust Technology Assessment Program and the Benefits to U.S. Evaluations"
URL: http://www.radium.ncsc.mil/tpep/ttap/TTAPpaper.html

Department of Defense Instruction (DoDI) 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP) (December 30, 1997)
URL: http://mattche.iiie.disa.mil/ditscap/DitscapFrame.html

DoD 8510.1-M, DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Document (July 31, 2000)
URL: http://mattche.iiie.disa.mil/ditscap/appjuly00.pdf

Defense Information Systems Agency (DISA), DII COE Integration & Runtime Specifications Version 4.1 (October 3, 2000)
URL: https://dod-ead.mont.disa.mil/cm/general.html

Information Assurance Technical Framework (IATF), Release 3.0 (September 2000)
http://www.nsff.org/framework_docs/version-3_0/index.cfm

Information Assurance Technical Framework Forum, Controlled Access Protection Profile, Version 1.d, 8 October 1999
http://www.iatf.net/protection_profiles/profiles.cfm

Library of TCSEC Final Evaluation Reports (September 21, 2000)
http://www.radium.ncsc.mil/tpep/library/fers/tcsec_fers.html

Lodge, David, Solaris 8 Security Target, Issue 1.0 (July 28, 2000)
URL: http://www.sun.com/software/solaris/securitycert/STarg.pdf

Microsoft Corporation, Windows NT C2 Evaluations (December 2, 1999)
URL: http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/news/c2summ.asp

Microsoft Corporation, Windows NT 4.0, The C2 Administrator's and User's Security Guide (1999)
URL: http://www.microsoft.com/technet/treeview/default.asp?url=

/technet/security/tools/c2config.asp

NIST Special Publication 800-23, Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products (Edward A. Roback, August 2000).

National Information Assurance Partnership (NIAP) Validated Products List (August 14, 2001)
http://niap.nist.gov/cc-scheme/ValidatedProducts.html

National Security Agency (NSA), Security Recommendation Guides (October 5, 2001)
URL: http://nsa1.www.conxion.com/

National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 1000, National Information Assurance Certification and Accreditation Process (NIACAP), (April 2000)
URL: http://www.nstissc.gov/Assets/pdf/nstissi_1000.pdf

SANS Step-by-Step Consensus Guides
http://www.sansstore.org/

Solaris 8 Release Notes Common Criteria Certification (January 9, 2001)
URL: http://www.sun.com/software/solaris/securitycert/SRN_1.0.pdf

The Center for Internet Security, CIS Benchmark and Scoring Tools for Solaris (V1.0.1b) (July 2001)
URL: http://www.cisecurity.org/

The Computer Security Evaluation Frequently Asked Questions (V3), Trusted Product Evaluation Program, (August 16, 1999)
URL: http://www.radium.ncsc.mil/tpep/process/faq-sect6.html#Q1

Trust Technology Assessment Program Commercial Product Evaluations (August 16, 2000)
URL: http://www.radium.ncsc.mil/tpep/

Trust Technology Assessment Program Evaluation Technical Report for Check Point Software Technologies LTD Firewall-1 Version 4.0, CSC (October, 1999)

Final Evaluation Report Microsoft Windows NT Workstation and Server Version 4.0 with C2 Update, SAIC (December 15, 1999)