



HP ATTAINS COMMON CRITERIA SECURITY CERTIFICATION ON LINUX

Frequently Asked Questions

March 2006

Q: What is Common Criteria?

A: Common Criteria is an internationally recognized ISO standard (ISO/IEC 15408) for security in the technology industry. It is used by Government customers in the USA and the NATO community along with other organizations, particularly in the public sector, to determine the level of security and assurance of various technology products - in our case, Linux environments. Common Criteria stipulates the way security requirements are to be expressed and defines the criteria by which products should be evaluated.

Q: How did HP attain its Common Criteria certification?

A: HP's Linux offerings were evaluated by atsec information security company, one of the world's leading vendor-independent IT security consulting companies based in Europe and USA: The most recent certification was accredited by the National Information Assurance Partnership (NIAP).

Earlier certifications were accredited by the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik [BSI]) in Germany.

Q: What Linux configurations from HP are certified?

A: HP's Common Criteria Certification for CAPP at EAL 3+ spans HP Linux systems running Red Hat® Enterprise Linux 4 Update 2, including all HP Linux-supported ProLiant Systems (non-EM64T 32-bit Pentium/Xeon based servers, EM64T 64-bit extension Xeon based servers & single/dual core Opteron-based servers), and all HP Linux-supported Integrity2 systems (RX CX, & Superdome). Certification on Red Hat is also extended to the Intel Pentium 4/Xeon based xw series HP Workstation and the Intel Pentium 4 based HP Compaq dc series product line.

Red Hat® Enterprise Linux 3, Update 3, as well as Novell SUSE® LINUX Enterprise Server 8 with Service Pack 3 have also received EAL3+ Common Criteria certification for CAPP on all HP Linux-supported ProLiant Systems (x86 & Opteron-based), and all HP Linux-supported Integrity systems (RX & ZX on SUSE; RX, ZX, CX, & Superdome on Red Hat). Certification on Red Hat is also extended to HP Carrier Grade Systems (x86 [CC] and Itanium®-based [CX]), HP Workstations, and selected Linux-supporting desktops.

Q: Will HP be targeting LSPP, CAPP at EAL4, or enhanced security functionality in the future?

A: Yes. HP announced in October 2005 that we are again working with Red Hat toward securing an assurance level EAL4+ with LSPP, CAPP & RBACPP on Red Hat Enterprise Linux 5. And in April '06 HP and Red Hat announced official beginning of certification with NIAP again working with atsec as the evaluation lab.

Q: How does National Information Assurance Partnership (NIAP) - the collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) - explicitly define CAPP?

A: The Common Criteria (CC) Controlled Access Protection Profile, hereafter called CAPP, specifies a set of security functional and assurance requirements for Information Technology (IT) products. CAPP-conformant products support access controls that are capable of enforcing access limitations on individual users and data objects. CAPP-conformant products also provide an audit capability which records the security-relevant events which occur within the system.

CAPP provides for a level of protection which is appropriate for an assumed non-hostile and well-managed user community requiring protection against threats of inadvertent or casual attempts to breach the system security. The profile is not intended to be applicable to circumstances in which protection is required against determined attempts by hostile and well funded attackers to breach system security. The CAPP does not fully address the threats posed by malicious system development or administrative personnel. CAPP-conformant products are suitable for use in both commercial and government environments. CAPP is generally applicable to distributed systems but does not address the security requirements which arise specifically out of the need to distribute the resources within a network.

Q: From what was CAPP derived?

A: CAPP was derived from the requirements of the C2 class of the U.S. Department of Defense (DoD) Trusted Computer System Evaluation Criteria (TCSEC), dated December, 1985, and the material upon which those requirements are based. This protection profile provides security functions and assurances which are equivalent to those provided by the TCSEC and replaces the requirements used for C2 trusted product evaluations.

Q: For what level of risk is CAPP?

A: CAPP is for a generalized environment with a moderate level of risk to the assets. The assurance requirements and the minimum strength of function were chosen to be consistent with that level of risk. The assurance level is EAL 3 and the minimum strength of function is SOF-medium.

Q: What are CAPP and EAL?

A: CAPP stands for Controlled Access Protector Protocol, and it represents a level of security and a specific set of requirements set forth by the Common Criteria standard. EAL

stands for Evaluation Assurance Level, and it represents the degree of precision to which the CAPP level of security was attained and documented.

Q: How do CAPP and EAL apply to Linux from HP?

A: In our case, HP has received official Common Criteria Certification for a Controlled Access Protector Protocol (CAPP) at an Evaluation Assurance Level of 3+ (EAL 3+). Such certification has required expanded functionality, specifically an auditing subsystem, from the Linux distributions of our alliance partners, Red Hat and Novell, along with significant hardware and software testing and review. As stipulated by CAPP, our testing has verified the accuracy of critical event auditing and security functions that protect network transmitted data, all across specific software and hardware configurations.

Q: Against what features would Linux products be evaluated in Common Criteria?

A: Under Common Criteria, Linux software and hardware configurations would require scrutiny in terms of specific security functionality, the way security vulnerabilities are handled, documentation, testing paradigms, and the development environment, itself.

Q: Is HP's Common Criteria support unique in the industry?

A: HP is firmly committed to Common Criteria certification on Linux in order to meet our customers' increasing security needs. We are aware of other vendors like IBM who are active in this area but we have seen no other hardware vendor completing a Linux certification. Those vendors may be assuming, for example, that the certification applies merely to the Linux distribution and not to the specific hardware/software configuration. According to NIAP this is not correct and the hardware must be certified with the operating system. As Linux moves closer and closer to the datacenter, HP's track record of high security provisions within UNIX should be a clear signal of our similar direction with Linux.

Q: What about LSPP?

A: Labeled Security Protection Profile, LSPP, represents an additional level of security set forth by the Common Criteria standard. It is a superset of CAPP, adding mandatory access controls and labeling, thereby restricting or granting access to data only after verifying the clearance level of the user and comparing it to the security level of the data: LSPP is designed to support multiple levels of security on the same system. Labeling is required to identify and control access correctly for a multi-level security systems. LSPP certified systems are sometimes referred to as Multi-level Security or trusted systems.

Q: How does NIAP explicitly define LSPP?

A: The Common Criteria (CC) Labeled Security Protection Profile, hereafter called LSPP_V1.b, specifies a set of security functional and assurance requirements for Information Technology (IT) products. LSPP_V1.b-conformant products support access controls that are capable of enforcing access limitations on individual users and data objects. Specifically, two classes of access control mechanisms are provided: those that allow individual users to specify how resources (e.g., files, directories) under their control are to be shared; and those that enforce limitations on sharing among users. The latter is

implemented by the use of security markings (i.e., "labels"). LSPP_V1.b-conformant products also provide an audit capability which records the security-relevant events which occur within the system.

LSPP_V1.b provides for a level of protection which is appropriate for an assumed non-hostile and well-managed user community requiring protection against threats of inadvertent or casual attempts to breach the system security. The profile is not intended to be applicable to circumstances in which protection is required against determined attempts by hostile and well funded attackers to breach system security. LSPP_V1.b does not fully address the threats posed by malicious system development or administrative personnel. LSPP_V1.b-conformant products are suitable for use in both commercial and government environments. LSPP_V1.b is generally applicable to distributed systems but does not address the security requirements which arise specifically out of the need to distribute the resources within a network.

Q: From what was LSPP derived?

A: The LSPP_V1.b was derived from the requirements of the B1 class of the U.S. Department of Defense (DoD) Trusted Computer System Evaluation Criteria (TCSEC), dated December, 1985, and the material upon which those requirements are based. This protection profile provides security functions and assurances which are equivalent to those provided by the TCSEC and replaces the requirements used for B1 trusted product evaluations.

Q: For what level of risk is LSPP?

A: LSPP_V1.b is for a generalized environment with a moderate level of risk to the assets. The assurance requirements and the minimum strength of function were chosen to be consistent with that level of risk. The assurance level is EAL 3 augmented and the minimum strength of function is SOF-medium.

Q: Where can I get additional information?

A:

- o atsec web site, <http://www.atsec.com/01/index.php>
- o BSI web site, <http://www.bsi.de/english/index.htm>
- o NIAP CAPP overview, http://niap.nist.gov/cc-scheme/pp/PP_CAPP_V1.d.html,
- o CAPP requirements, http://niap.nist.gov/cc-scheme/pp/PP_CAPP_V1.d.pdf
- o LSPP overview, http://niap.nist.gov/cc-scheme/pp/PP_LSPP_V1.b.html
- o LSPP requirements http://niap.nist.gov/cc-scheme/pp/PP_LSPP_V1.b.pdf
- o RBAC requirements, <http://csrc.nist.gov/rbac/>
- o Common Criteria overview <http://niap.nist.gov/cc-scheme/index.html>
- o Acronyms and terms <http://niap.nist.gov/cc-scheme/terms.html>