Lumeta IPsonar 5.5C

The Significance of Common Criteria, Protection Profiles, and Lumeta IPsonar

The aim of the new Common Criteria is to ensure that commercial enterprise security products represent a good practice level of security, with a goal of secure-by default products suitable for emerging threats.

A publication of Lumeta Corporation
www.lumeta.com

Increased Cyber Threat Requires Increased Cyber Security

As the threat from cyber space increases to critical national infrastructures (e.g., power and water distribution, transport networks, food distribution, finance industry) and national economic wellbeing (loss of intellectual property rights, damage to business, theft from customers) as well as governments, there is an urgent need to greatly enhance cyber security not only in the public sector but also in commerce and industry.

Organizations are battling sophisticated cybercriminals on an increasingly global scale, and vendors need to demonstrate their dedication to constant improvement and an ability to stay ahead of today's complex security threat landscape.

Standards like Common Criteria help ensure that security products are effective and trustworthy across international borders. Common Criteria certification is significant because it provides independent, standards-based verification of the security functions delivered by IT products. Certification provides customers the highest level of confidence that the solutions deliver on their security promises and meet global security standards.

Common Criteria for IT Security Products

Common Criteria Evaluation and Validation Scheme (CCEVS) is a US Government program administered by the National Information Assurance Partnership (NIAP) to evaluate security functionality of information technology with conformance to the Common Criteria international standard. As the basis for the international standard ISO/IEC 15408, Common Criteria is a framework for information technology security certification.

Common Criteria standards institute worldwide criteria for evaluating information technology operational security. Information Technology developers, consumers, and evaluators who must implement or assess security within a system or product can use the Common Criteria to establish an internationally recognized baseline of security requirements and techniques.

Common Criteria certifications are recognized by all 26 nations of the international Common Criteria Recognition Arrangement (CCRA). CCRA carries a unified approach to the evaluations of information technology products and protection profiles for information assurance and security. This arrangement benefits member nation governments and other customers of IT products by creating more clarity in procurement decisions, more precision in evaluations, a better balance of security and features, and more rapid access to products from industry.

Common Criteria certification is a requirement for IT security products purchased by the US Government for national security systems. In addition, many federal directives and best practice guidelines prompt government agencies and enterprise customers to look for Common Criteria certification, even though not explicitly named as a requirement. Internationally, several countries promote Common Criteria validation as criteria for government purchase of new products. Also, Common Criteria is now a NATO standard.

> “Recognized by 26 nations as the evaluation standard for IT product security assurance, the Common Criteria certification is mandated for all IT solutions purchased by the US federal government, as well as several other countries, NATO … and is considered valuable by the private sector as well.”

What is Common Criteria and where does it fit in?

- International Standard for IT Product Security Assurance
- The basis for ISO/IEC 15408 and ISO/IEC 18045
- CCRA - Recognition Arrangement between 26 Nations
- Can provide a common foundation level for procurement
- Aim - Evaluate once, use in many countries.

The ‘New’ Common Criteria: Protection Profiles

Interpreting the product assurance certified under the Common Criteria Evaluation and Validation Scheme (CCEVMS) has, in the past, required a good level of understanding of the language, style and formats of Common Criteria documentation. However, following international agreements on changes to the Scheme, the assurance of security functions of products evaluated against ‘new style’ Common Criteria Protection Profiles[1] is more easily understood.

CCRA is changing to support a more IT industry driven use of Common Criteria. This should result in more effective and agile standards for IT products, and is better suited to the needs of cyber defence.

[1] E.g., Protection Profile for Network Devices Version 1.1 - https://www.niap-ccevs.org/pp/pp_nd_v1.1/

NIAP is transitioning to Protection Profile compliance and a move away from Evaluation Assurance Level (EAL) compliance. This strengthens evaluations by focusing on technology specific, tailored assurance requirements. Products are evaluated against a NIAP-approved Protection Profile which includes a collection of assurance activities tailored to the technology with no EAL assigned.

Protection Profiles define security functional and assurance requirements that government, military and other users expect products to meet. Vendors can then implement and make claims about the security attributes of their products, and testing laboratories evaluate the products to determine if they actually meet the claims.

These new style Common Criteria Protection Profiles are being developed and recognized initially nationally, but in the near future collaboratively between Common Criteria member nations as international knowledge sharing is an increasingly valued tool in the development of cyber security strategies and standards.   These Protection Profiles are designed to help end user organizations better meet the increasing threats from cyber space by making it easy for people procuring, deploying and using certified products to understand:

- what was and what was not evaluated,
- the applicability of the assured functionality to their requirements,
- the expected validity period,
- and how to effectively ensure the enduring security of their systems using the products.

The 'New' Common Criteria:

What is changing?

- Supporting wider standardisation via Collaborative Protection Profiles (cPPs)
- Greater industry involvement
- Via Common Criteria User Forum (CCUF)
- Via International Technical Communities (iTCs)
- Increased transparency, repeatability, effectiveness
- Supporting stronger links to procurement and users/specifiers

How is it changing?

- Supporting wider standardisation via Collaborative Protection Profiles (cPPs)
- New Recognition Arrangement (CCRA) drafted
- Encourages use of cPPs and iTCs
- Close working with Common Criteria User Forum (CCUF)
- Collaborative Protection Profile process
- Supporting stronger links to procurement and use

The changes to the way in which Common Criteria Protection Profiles are developed together with other improvements to the scheme (e.g., faster certification and lower costs) have taken into account the need for the assurance scheme to add value to cyber security solutions beyond just government and public sector systems.

Nations have begun to endorse the new Protection Profiles. In February 2014, Australia, Canada, UK and US – participants in the Common Criteria Recognition Arrangement – issued a statement endorsing an initial set of new-style Protection Profiles, including that for Network Devices (Version 1.1). The complete Joint Endorsement Statement can be found on the CESG website: https://www.cesg.gov.uk/servicecatalogue/ccitsec/Pages/CCITSEC.aspx

Lumeta IPsonar for Network Discovery & Awareness

Lumeta IPsonar is in the vanguard of new national and international good practice standards for security products. The Common Criteria Certificate issued for Lumeta IPsonar v5.5C (CCEVS-VR-VID10506-2013) was evaluated using the new style of Protection Profile[1].

These Protection Profiles are designed to encourage a wider spectrum of security products to be certified to increase the assurance levels of complete security solutions. Most well designed Network Security Operations Centers (NSOCs) will deploy Common Criteria certified firewalls but would not expect to find certified products for other security functions. Lumeta is among the first companies to have the vision to address this. The Lumeta IPsonar network situational awareness product provides functions in the network discovery and analysis space that have been independently assured by a Common Criteria test house and evaluation body.

Lumeta IPsonar targets the network situational awareness challenges impacting its customers; it thoroughly identifies the routed infrastructure of a network and fills any knowledge gaps. Common Criteria certification means that IPsonar has been evaluated by a neutral third party and meets Lumeta's claims for security features and capabilities. The certification provides Lumeta's customers with high confidence in the strength of the security mechanisms within IPsonar.

[1] Protection Profile for Network Devices Version 1.1

Lumeta has worked with the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) to deliver a certified product that adds value and assurance in all market sectors, within the USA and internationally.

The complete Lumeta IPsonar Security Target and Validation Report can be found at https://www.niap-ccevs.org/st/vid10506/. It is a critically important read for anyone carrying the heavy responsibility of defending their organisation against cyber threats.

The following summarizes the product functionality and assured security functions[1]:
(N.B. A glossary of abbreviations is provided at the end of the paper.)

Product Description
In the context of this evaluation, the Target of Evaluation (TOE) – Lumeta IPsonar – is a network device that provides a secure base for its other operational functions, primarily involving auditing, cryptographic support (for network communication and update integrity), user identification and authentication, secure management, and secure product updates.

The product is designed to plug into a network and to actively examine and discover the network infrastructure. To that end it can identify and examine network connected assets such as hosts and other network devices in order to create a view of the routed infrastructure associated with the attached network. It primary functions include:

- **Network Discovery** – Identifies all network address spaces, routing devices and connectivity flows across the network (including "stealth" assets, that is hidden devices that do not respond to queries) utilising advanced multi-protocol discovery technology, and creates a comprehensive route-based topology that identifies a network's true perimeter. Host Topology Visualisation / Layer 2: An optional product module supports layer 2 topology mapping, stealthy device identification, guest network and extranet security, VLAN compliance and Virtual Machine identification. The TOE can be operated with or without this module present.

- **Host Discovery** – Detects all known and previously unknown network devices by conducting a census of IP addresses across protocols. Flags devices unrecognized by official network inventories for remediation.

- **Leak Discovery** – Reveals unauthorised connections between a network and another network, sub-net, or the Internet, and determines whether access is outbound, inbound or both. Leak discovery highlights unknown connections into other organizations (e.g., legacy divestiture connectivity) or to the Internet.

[1] Excerpted from https://www.niap-ccevs.org/st/vid10506/

- **Device Discovery** – Identifies web services, wireless access points and IP applications active on hosts and devices – including those not owned by the client or its employees – pinpointing resources for which tested ports are active. Additionally, Layer 2 discovery matches a device's unique MAC address with its assigned IP address, providing crucial information for asset management and diagnostics.

Note that while these are the primary functions of the product, the evaluation does not specifically address these capabilities. Rather, the evaluation (and hence this security target) focuses on the security of the device as a network infrastructure component as required in Protection Profile for Network Devices[1].

Security Functions

The evaluation of the Lumeta IPsonar 5.5C TOE provides assurance that the security functions implemented by the TOE satisfy the security functional requirements specified in Lumeta IPsonar Security Target and the guidance documentation describes how to use the TOE in a secure fashion. Assurance was achieved by the performance of the assurance activities specified in Protection Profile for Network Devices. Lumeta IPsonar 5.5C implements the following security functions:

- **Security audit** – The TOE is designed to be able to generate logs for a wide range of security relevant events. The TOE uses FreeBSD-based auditing features that can be configured to store the logs locally so they can be accessed by an administrator and also sent to a remote log server using syslog-ng in order to protect the exported records using TLS.

- **Cryptographic support** – The TOE includes the FIPS-certified OpenSSL FIPS Object Module (FIPS 140-2 Cert. #1051) (valid on compatible operating systems along with CAVP algorithm testing specific to IPsonar 5.5) that provides key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher level cryptographic protocols including SSH and TLS/HTTPS.[2]

- **User data protection** – The TOE performs a variety of network infrastructure detection functions, but as a rule does not pass data among network entities. The exception is that data is passed among distributed TOE appliances. Otherwise, it collects data from the network and attached components and ultimately forwards information to TOE administrators. Regardless, the TOE is designed to ensure that memory and other storage resources are reused properly to mitigate potential data corruption or repetition.

[1] https://www.niap-ccevs.org/pp/pp_nd_v1.1/

[2] The Heartbleed security bug in OpenSSL allows anyone on the Internet to read the memory of systems protected by OpenSSL software **versions 1.0.1 through 1.0.1f and 1.0.2 – beta.** Lumeta IPsonar is **NOT** impacted by the affected OpenSSL versions. OpenSSL 0.9.8y is in use in IPsonar version 5.5F and earlier supported versions of IPsonar..

- **Identification and authentication** – The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE. It provides the ability to both assign attributes (user names, passwords and roles/privilege levels) and to authenticate users against these attributes. Users can optionally be configured with public certificates so that PKI-based authentication can be used.

- **Security management** – The TOE provides menu-driven console (Console) commands and a Web-based Graphical User Interface (Web GUI) to access the wide range of security management functions to manage its security policies. Security management commands are limited to authorised users (i.e., administrators) only after they have provided acceptable user identification and authentication data to the TOE. The security management functions are controlled through the use of privileges associated with roles that can be assigned to TOE users.

- **Protection of the TOE Security Function** – The TOE implements a number of features design to protect itself to ensure the reliability and integrity of its security features. It protects particularly sensitive data such as stored passwords and private cryptographic keys so that they are not accessible even by an administrator. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability). Note that the TOE is a single appliance or an associated collection of appliances acting together. The communication between associated appliances is protected using TLS. The TOE includes functions to perform self-tests so that it might detect when it is failing. It also includes mechanisms so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

- **TOE access** – The TOE can be configured to display an informative banner when an administrator establishes an interactive session and subsequently will enforce an administrator-defined inactivity timeout value after which the inactive session (local or remote) will be terminated.

- **Trusted path/channels** – The TOE protects interactive communication with administrators using SSHv2 for Console access or TLS/HTTPS for Web graphical user interface access. In each case, both integrity and disclosure protection are ensured. If the negotiation of an encrypted session fails or if the user does not have authorisation for remote administration, an attempted connection will not be established. The TOE protects communication with an audit log server using TLS connections as part of a syslog-ng implementation to prevent unintended disclosure or modification of logs.

Implementation of Secure Systems

This summary provides an overview to inform secure system designers and system security management teams of the functionality and assured security attributes of the Lumeta IPsonar product. More detailed information is provided in the Common Criteria Security Target (https://www.niap-ccevs.org/st/st_vid10506-st.pdf) and Validation Report (https://www.niap-ccevs.org/st/st_vid10506-vr.pdf). Using products that have been assured in this manner greatly eases the complexity and cost of achieving independent assurance for the system as a whole (e.g. ISO27001 compliance) and meeting the requirements of governance and regulatory bodies.

With this internationally recognized certification, Lumeta demonstrates the company's commitment to providing the highest level of independently verified security and information assurance to its US government, international government and commercial enterprise customers, as well as its partner community.

Glossary:

Term	Expansion	Description
TLS	Transport Layer Security	A cryptographic protocol to provide communication security
FIPS	Federal Information Processing Standard	US Government standards for use on computer systems
SSL	Secure Sockets Layer	A cryptographic protocol to provide communication security
SSH	Secure Shell	A cryptographic protocol to provide secure network services
HTTPS	Hypertext Transfer Protocol Secure	A protocol to provide a secure connection to a browser
PKI	Public Key Infrastructure	A system for delivering / validating secure public key certificates