Common Criteria®

Title: Network Device Fundamentals Essential Security Requirements
Maintained by: CCDB Work Group for Network Device Fundamentals
Version: 0.2
Date of issue: *2014-May-1*
Supersedes: *Version 0.2*

Status

The CCDB Working Group has been requested to develop an Essential Security Requirements (ESR) that captures the fundamental requirements for Network Devices. This initial draft contains material that was provided by the requestor, the United Kingdom, for a cPP.

Background and Purpose

This document describes the high-level fundamental security requirements expected of any Network Device. It is intended to provide a minimal, baseline set of requirements which can be built upon by future cPPs to provide an overall set of security solutions for an enterprise network.

A "network device" in the context of this document is a device which performs an infrastructure role in an enterprise network – and includes the hardware and software which comprise such a device. Examples of network devices include, but are not limited to, VPN Gateways, Firewalls, Switches and Routers. Examples of devices that connect to a network but are not suitable for consideration against this standard would include mobile devices and end-user workstations.

The intent of this document is to define the minimal set of common security functionality expected by all network devices, regardless of their ultimate security purpose. These include securing any remote management path, providing identification and authentication services for both local and remote logins, auditing security-related events, and offering some protection against common network-based attacks, such as Denial-of-service attacks. Devices must also be able to cryptographically validate the source of any updates to the device.

Use Case(s)

- The intent is that a device satisfying these requirements will "do no harm" on a network. Rather than providing any explicit security functionality, compliant devices simply ensure that they can be remotely managed in a secure manner, and that any updates are from a trusted source.

Resources to be protected

- Any network-facing management interfaces, including traffic to and from the device, including any critical data (e.g., audit data).
- Updates to the device.

Attacker access

- An attacker can send arbitrary packets to network interfaces.
- An attacker can intercept and arbitrarily modify or drop packets within existing traffic flows.

Attacker Resources

- An arbitrary amount of time to study traffic flows to/from a device
- Many sample devices to test and attack

Boundary of Device

- The hardware, firmware and software of the device define the physical boundary.
- All of the security functionality is contained and executed within the physical boundary of the device.

Essential Security Requirements

- The remote administration functions shall use cryptography to protect this communication path.
- The device shall be capable of auditing administrative actions, including any configuration changes and rebooting of the device.
- The device shall provide an authentication mechanism for local and remote administrators, as well as the device itself (e.g., the device maintains an authentication credential that can be used to authenticate it to an administrator's client) .
- The device shall provide a cryptographic means to validate the source of updates to be installed on the device.
- The device shall require any default passwords / other credentials to be changed.
- The device shall protect keys, key material, and authentication credentials from unauthorized disclosure.
- The device is robust against malformed network packets, including denial-of-service attacks.
- The device shall provide self-tests to ensure the security functions it implements are operating correctly.

Assumptions

- There are no general purpose computing or storage repository capabilities (e.g., compilers, debugging tools, editors, web servers, database servers or user applications) available on the device, unless they are directly related to the security functionality of the device (e.g., webserver to facilitate remote administration).
- The device is protected from physical attacks by the wider environment

Optional Extensions

Requirements captured in this section may already be realized in some products in this technology class, but this ESR is not mandating these capabilities exist in “baseline” level products.

- The device shall be able to assign which interface(s) remote administration may take place

Objective Requirements

Requirements specified here specify security-relevant behaviour that is not expected to be realized currently in products, but capabilities that may be mandated in future versions of the ESR and resulting cPPs.

- The device shall have internal security features to make the device more resilient to security breaches.
- The device shall provide two-factor authentication natively on the device (i.e., does not rely on a separate device to provide this capability).

Outside the Scope of Evaluation

- Additional security functionality that a security-enabled network device may employ (e.g., firewall, virtual private networking) is outside the scope, as these will be specified in other ESRs..
- Virus scanning, including email scanning.
- Intrusion detection/prevention capabilities
- Network Address Translation (NAT) as a security function..
- Virtualized network functions.