Common Criteria

Common Criteria Evaluation and Validation Scheme

National Information Assurance Partnership (NIAP)

Title: Extended Package for SSH Server and Client Functionality

Maintained by: National Information Assurance Partnership

Unique Identifier: 42

Version: 1.0

Status: draft

Date of issue: 9 November 2015

Approved by:

Supersedes:

Background and Purpose

Secure Shell (SSH) is an encrypted network protocol for initiating shell sessions between a client and a server. An SSH session allows a user to interact with the remote system via a text-based shell. Typically SSH is used to perform privileged tasks on remote machines.

This essential security requirements (ESR) document outlines the high-level security requirements for an SSH Client or Server, which will be expressed in a Common Criteria Extended Package (EP). These requirements address threats within a scope established by use cases and environment assumptions.

The security functionality must be realistic and achievable by commercially available products. The resulting EP will also include objective and repeatable evaluation activities, so that evaluations can be executed in a timely manner.

With regard to evaluation scope, the SSH Client or Server is composed of the software that is delivered to the end user. This Extended Package is envisioned for combination with base PPs in the following ways:

- A standalone SSH product would be covered by this EP extending the Application Software Protection Profile.
- SSH Client or Server software included as part of an Operating System or Mobile Device would be covered by this EP extending the General Purpose Operating System PP or Mobile Device Fundamentals PP, respectively.

Use Cases

SSH enables encrypted network communications for activities such as

- remote, interactive system access
- remote systems management (interactive or through management system)

Resources to be protected

- Sensitive data transmitted over the network.

Attacker access

The following assumptions are made about attackers' ability to develop attacks:

- An attacker has an arbitrary amount of time to analyze the behavior of SSH client or server software, including the data it transmits over the network.

The attacker is expected to engage in the following general classes of attack:

- Network eavesdropping, in which an attacker may monitor and gain access to data exchanged between the SSH Client and SSH Server.
- Network attack, in which an attacker may initiate malicious communications with an SSH Client or Server or alter communications between the SSH Client and Server.

Essential Security Requirements

The following are the essential security requirements expected to be implemented by an SSH Client or

Server within the established scope:

- SSH software shall implement the SSH protocol that complies with RFCs.
- SSH transport implementation uses the following encryption algorithms:
  - aes128-cbc
  - aes256-cbc
- SSH connection be rekeyed after no more than 2^28packets have been transmitted.
- Provide a trusted update mechanism to update itself.
- Provide strong authentication mechanisms.
  - Support authentication methods as described in RFC 4252: public key-based, password-based.

Assumptions

The following assumptions are made for the SSH Client or Server product and its operational environment:

- Administrators are not malicious in nature.
- Users are not malicious in nature.

Optional Extensions

None

Outside the TOE's Scope

The following list contains items that are explicitly out-of-scope for any evaluation against an SSH Client or Server

- Malicious, Highly-Privileged Administrators - Highly-privileged administrators acting maliciously can disable most, if not all, security protections. Additionally procedural controls that are out of scope of this document should be considered to help highlight administrator accounts acting suspiciously.
- Zero Days - The disclosure of recently published vulnerabilities (Zero Days) should not be used as a reason to fail an SSH Client or Server undergoing evaluation.
- Unofficial Versions - Non-vendor supplied install images often contain added functionality and may weaken the normal operating functionality of the SSH Client or Server.