Title: Some PP Name

Maintained by: NIAP and CESG

Unique Identifier: 42

Version: 1.0

Status: draft

Date of issue: 19 March 2015

Approved by:

Supersedes:

Background and Purpose

This section sets the context for not only the ESR, but what is expected of the resulting Protection Profile (PP). The intent is that the remaining sections provide succinct statements that highlight the relevant aspects to be addressed by the Technical Community (TC) constructing the PP. Here, the authors provide a narrative that introduces the reader to the problem being solved, and presents key aspects that support or guide the TC, and may elaborate on subtleties not apparent in the “bulleted” high level statements.

Use Cases

This section is intended to provide the initial scope/bound of the security problem by providing the reader with concise statements regarding the scenarios in which the technology is being used. The intended usage presented here should lay the groundwork for the identifying the resources to be protected, and what threats must be considered in the drafting of the Essential Security Requirements (ESR) and for the TC to consider when writing the PP.

Resources to be protected

This section is intended to provide the initial scope/bound of the security problem by providing the reader with concise statements regarding the scenarios in which the technology is being used. The intended usage presented here should lay the groundwork for the identifying the resources to be protected, and what threats must be considered in the drafting of the Essential Security Requirements (ESR) and for the TC to consider when writing the PP.

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 the product, its interaction with its platform, and the data it transmits over the network.
- An attacker is able to acquire their own copy of the target product and study its behavior on a platform that they control.

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 product and other endpoints.
- Network attack, in which an attacker may initiate malicious communications with the product or alter communications between the product and other endpoints.
- Local attack, in which an attacker has gained the ability to execute code on the system, which may be used to escalate privilege or access data without authorization.
- Limited physical access attack, in which an attacker may attempt to access data on the system by virtue of being physically present for a limited period of time. This limited physical access does not include attacks in which the attacker could disassemble the system to gain access to its storage media or manipulate the product's underlying hardware and firmware. Systems used for working remotely, such as laptops and tablets, for which an attacker could gain longer physical access to, should apply additional protections that are provided by products evaluated against other Protection Profiles (e.g. FDE cPP).
- Persistence, in which an attacker has already exploited the system and wishes to maintain presence on the system.

Essential Security Requirements

This is where the authors present an initial set of English requirements that specify security functionality, rather than design and/or implementation characteristics. These requirements will provide the foundation for which the detailed set of requirements is derived. It is important that the requirements captured here make an attempt to fully address the categories (e.g., access control, identification and authentication, management capabilities, roles of administration, secure communications, and audit). That's not to say the requirements are fully specified or detailed enough to simply translate to Common Criteria security functional requirements. The goal is that there is enough information contained here, as well as the other sections of this document, to provide the TC enough information to ensure they have an understanding of what is minimally required in breath.

Assumptions

Simply put, this section presents the aspects of the product and its intended environment that can be assumed to hold true. This will provide additional scope on the resulting PP. The following assumptions are made for the operating system product and its operational environment:

- The underlying platform is physically protected, to a large extent. The hardware that the product manages is secured by defensive measures that make physical attacks impractical for most attackers. At the same time, casual passersby might attempt to trivially access the system.
- The product implements some security-relevant functionality that does not require evaluation (e.g., network time synchronization, process scheduling, and virtual memory management including process separation).
- Depending on configuration and capability, the product may or may not be:
  - configuration-managed by the enterprise
  - bound to directory services to support multi-user login
- The product runs application software developed by a third-party. The applications are not intentionally developed to be malicious, but can contain inadvertent coding errors. These errors introduce risk that control of an application may be seized by a malicious entity. The product shall confine these applications within the originally designated operating environment.
- The platform is connected to a network. For purposes of sending/receiving data, to include software updates, the platform is connected to other entities. Other entities on the network are not inherently trustable.
- Administrators are not malicious in nature.
- Users are not malicious in nature, though they may inadvertently or intentionally engage in risky behavior.

Optional Extensions

Additional security functionality that may be appropriate for some use cases, and can be expressed in extensions to this document, includes:

-

Outside the TOE's Scope

The following list contains items that are explicitly out-of-scope for any evaluation against the product PP

- Malicious, Highly-Privileged Administrators - Highly-privileged administrators acting maliciously can disable most, if not all, security protections on the product. 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 product undergoing evaluation.
- Unofficial Versions - Non-vendor supplied install images often contain added functionality and may weaken the normal operating functionality of the product
- Platform - The product PP shall not address the hardware or firmware of its underlying platform to include the boot sequence before control is handed off to the product. That the platform itself is virtual or physical is irrelevant to any evaluations.
- Applications - The product PP shall not address applications that are not delivered as part of the product installation process.