Sense-VM Security Threat Analysis

Cyber threat analysis ref.

Introduction

A threat analysis is usually performed in relation to an *applicaiton*. In a way a virtual machine (VM) is an application, but as its indendent use is to host applications, further threat analysis must be performed on a per application basis. Sense-VM should provide a base-level of security that will be inherited by applications running on top of the VM as specified in (TODO: application-security-contract).

(TODO: Actually I think that the application-security-contract could be the result of doing this threat analysis rather than the input. We need to think about this.)

Scope

This threat analysis focuses on the virtual machine and the interfaces it provides to an application running on the VM. The VM also lives on top of a Hardware abstraction layer. The implementation of the HAL is not in scope for this threat analysis and must be analysed per HAL.

Goal

The goal is a set of mechanisms to build into the VM and the interfaces it provides that establishes a a set of security targets. (TODO: Formulate targets/goals).

Threat Modeling

Assets

What are the things that must be protected

ASST1 The applications running on the VM.

ASST2 The data owned and processed by the applications.

ASST3 The resources of the platform running the VM.

Explanations

ASST1: The service that the VM provides is hosting of applications. This service should not be interrupted or taken down.

ASST2: The VM vill be handling application data. This data should not leak out over channels that is not agreed upon in the contract between the VM and the applications (TODO: Formulate and specify this contract?).

ASST3: As an example, these may be battery powered deviceses and if someone manages to get some foreign code to run on the system for personal gain (even if it poses no threat to data or service in near time), that would use battery and compute cycles. These resources must be protected.

Security Breakdown and Profiling

The primary objective creating a security profile is to uncover each and every vulnerability in the system's design, configuration or implementation.

Risks

having the attackers goal in mind as well as know-how on the architecture and potential vulnerabilities of your system, distinctively identify the risks that could definitely affect the system or application.

Threat Classification

Logically document the threats in an organized manner – use a common threat template to capture the attributes specific to each and every threat.

Threat Rating

Rate the threat – arrange the threats in order of the potential damage that they are capable of causing to the system such that the most significant threats come first.