Running the CHIPSEC Framework in a Simics® Environment

Revision 1.00

September 12, 2019

Intel - PAR

Revision History

Date	Revision Number	Modifications
04/11/2019	0.10	Initial Revision
05/22/2019	0.50	Many updates and clarifications.
09/09/2019	0.90	Updated graphics.
09/10/2019	0.95	Sync with itp_user_guide.docx and review updates.
09/12/2019	1.00	Move to final release

Table of Contents

1. Introduction

1.1 Purpose and Scope

This document outlines the steps needed to get the CHIPSEC framework up and running within the Simics® simulated environment.

1.2 Warnings and Considerations

Simulated environments cannot simulate a platform completely. Consult the simulation software documentation for details on any limitations.

2. Setup

2.1 Simics

The CHIPSEC helper implementation was developed on and is known to work with Simics 5. The instructions here may require some modifications based on the version used. Refer to the appropriate Simics documentation for further details.

Follow the "**ItpII plugin for Eclipse. Installation Guide.**" section in the "**`Program Files\Simics\Simics <x>\ITPii scripting <ver>\doc\itp_user_guide.docx`**" for more details setting up and configuring the ITPII scripting module in Simics.

2.1.1 Simics Prerequisites:

Simics is properly installed and set up with the below minimum and recommended packages installed (along with any required platform packages):

- Simics Base package (#1000)
- Simics Eclipse package (#1001)
- Simics ITP II Scripting (#7033)

2.2 CHIPSEC

2.2.1 CHIPSEC Prerequisites:

The following software installed on a Windows host machine running Simics:

- Python 2.7.x (≥2.7.9 recommended)
  - This should already be setup as part of the Simics prerequisites, which is the predominate guidance for Python.
- PyWin32 installed on host
  - Known to work: **pywin32-219.win-xxx.msi**
- Additional details in the chipsec-manual.pdf

2.2.2 Install CHIPSEC support:

To install the CHIPSEC routines:

- From within a DOS box, navigate to the `\chipsec\` folder
- Install CHIPSEC using the command:

```
python setup.py install
```

2.2.3 Import and run CHIPSEC main

Run CHIPSEC modules from the Simics Itpii view, first import the `chipsec_main` module:

Import CHIPSEC main:

```
>>> import chipsec_main
```

Run standard CHIPSEC modules:

```
>>> chipsec_main.main()
```

Example command-lines:

Run a specific module:

```
>>> chipsec_main.main(['-m', 'common.bios_wp'])
```

NOTE: CHIPSEC may take longer than normal to run.

2.2.4 Import and run CHIPSEC util

Manual CHIPSEC testing from Simics Itpii view, first import the `chipsec_util` module:

Import CHIPSEC util:

```
>>> import chipsec_util
```

Run CHIPSEC util and list available commands:

```
>>> chipsec_util.main()
```

Example command-lines:

Read SPI info…

```
>>> chipsec_util.main(['spi', 'info'])
```

Read MSR…

```
>>> chipsec_util.main(['msr', '0x1f2'])
```

NOTE: The CHIPSEC log option (`-l`) may not work under normal Simics operation. Simics Eclipse may not have the permissions needed to create files (logs). A possible workaround is to either run Simics in Administrative Mode or manually copy-paste the desired output from the ItpII view port to a text file.

Disclaimers

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

This document contains information on products, services and/or processes in development. All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest forecast, schedule, specifications and roadmaps.

The products and services described may contain defects or errors known as errata which may cause deviations from published specifications. Current characterized errata are available on request. No product or component can be absolutely secure.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting www.intel.com/design/literature.htm.