riscure

Inspector HPA

Changing the approach to side channel analysis testing

rev 1

The product

Context

Market

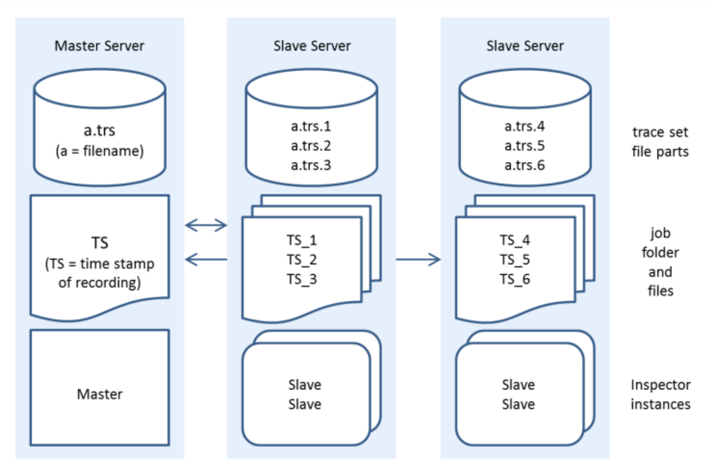
The number and complexity of SCA attack methods are constantly increasing. In addition to that high-end attacks on chips and embedded devices are starting to require very significant data processing time. As a result guaranteeing security takes more time and time and is delaying development- and certification processes.

Because of increasing market demands and always challenging timelines with the introduction of new chips it is important for manufacturers and test labs to have the most efficient ways to perform regression and exploratory tests.

Our approach

We introduce Inspector High Performance Analysis (HPA). A solution that can automate SCA test scenarios through record and playback features. In this way you can be sure that well though test scenarios are executed in exactly the same way. Over and over again. Inspector HPA can run on a server cluster to offer maximum scalability. This offers the performance that is needed to run large sets of automated tests. As it runs on a Linux operating system it also eases the integration into existing development environments.

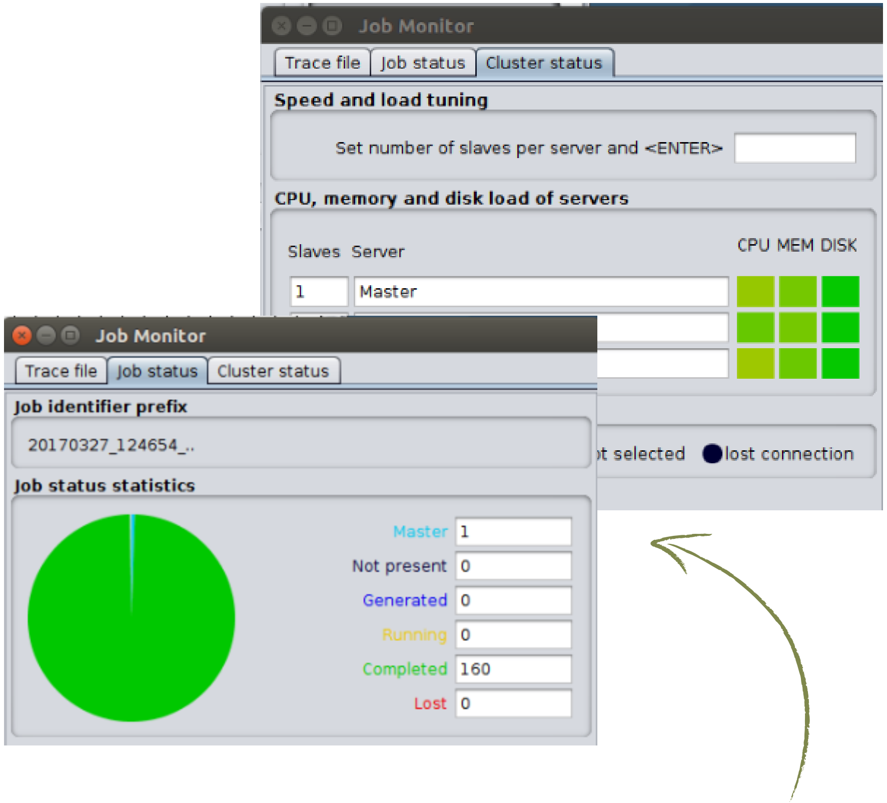
High performance scalable cluster



State of the art technology

- ✓ Optimized hardware package tuned for the best performance
- ✓ Create multiple test scenarios and play back when needed
- ✓ Reduce time needed for analysis from days to hours
- ✓ Add computing power for a fixed period of time

The challenge it solves



Speed and load tuning

Set number of slaves per server and <ENTER>

CPU, memory and disk load of servers

Slaves	Server	CPU	MEM	DISK
1	Master	🟩	🟩	🟩

t selected ● lost connection

Job identifier prefix

20170327_124654_..

Job status statistics

Master	1
Not present	0
Generated	0
Running	0
Completed	160
Lost	0

Life monitoring of all jobs, visibility of processor, disk and memory usage

- Regression testing
  Users of Inspector SCA have no automated way to repeat previous tests for regression testing / QA testing for new chip products

- Archiving is time consuming
  Archiving the test sequence followed takes a lot of time for the user since it is largely a manual process.

- Skipping tests due to time constraints
  In practice users take shortcuts in SCA testing because they manually execute each attack path, and are limited by the PC’s processing power.

- Windows OS not easy to integrate
  Inspector SCA runs on Windows O/S which for many users is hard to integrate into their existing testing environment.

- High-end attacks limited by processing power
  Attacks that require e.g. heavy trace alignment and advanced template analysis take too long for most users to execute because Inspector SCA’s scalability is limited to the PC workstation.

Unique features

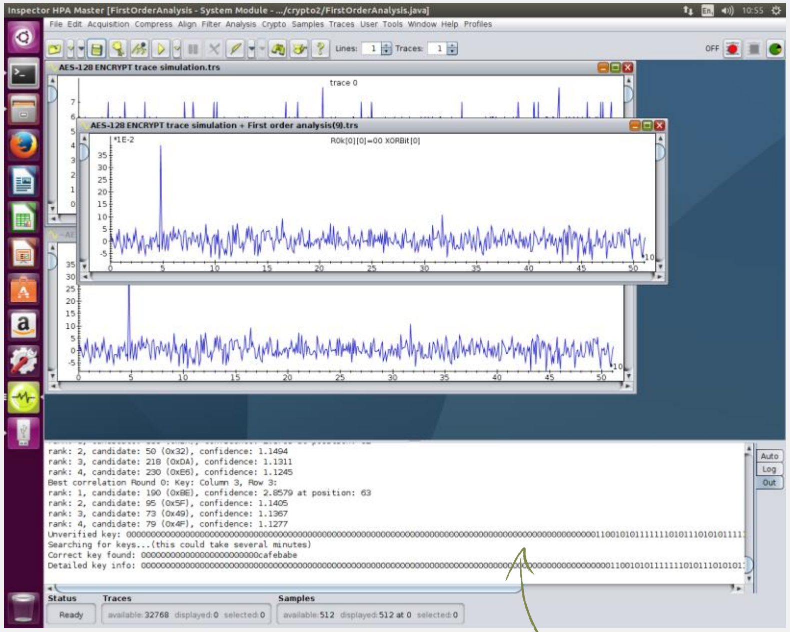
1. **Execute more analysis then before in a fraction of the time.** A scalable setup where multiple servers can be used gives optimal control over the computing power needed to be as fast a possible.

2. **Reduce manual work and work faster.** Record an playback features enables to create a test scenario once and run it multiple times without the need for repetitive actions

3. Automation features will allow you to better **guarantee constant quality** because test scenarios are always executed in exactly the same way

4. Opposed to Inspector SCA**, Inspector HPA** runs on **Linux** for **easy integration** in existing development and testing environments

Automation recording and cluster control


Inspector HPA Master [FirstOrderAnalysis - System Module - .../crypto2/FirstOrderAnalysis.java]
En
10:55
File Edit Acquisition Compress Align Filter Analysis Crypto Samples Traces User Tools Window Help Profiles
Lines: 1
Traces: 1
OFF
AES-128 ENCRYPT trace simulation.trs
trace 0
AES-128 ENCRYPT trace simulation + First order analysis(9).trs
*1E-2
R0k[0][0]=00 XORBit[0]
Auto
Log
Out
Status
Ready
Traces
available: 32768 displayed: 0 selected: 0
Samples
available: 512 displayed: 512 at 0 selected: 0

```
rank: 2, candidate: 50 (0x32), confidence: 1.1494
rank: 3, candidate: 218 (0xDA), confidence: 1.1311
rank: 4, candidate: 230 (0xE6), confidence: 1.1245
Best correlation Round 0: Key: Column 3, Row 3:
rank: 1, candidate: 190 (0xBE), confidence: 2.8579 at position: 63
rank: 2, candidate: 95 (0x5F), confidence: 1.1405
rank: 3, candidate: 73 (0x49), confidence: 1.1367
rank: 4, candidate: 79 (0x4F), confidence: 1.1277
Unverified key: 000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000110010101111111010111010101111
Searching for keys...(this could take several minutes)
Correct key found: 000000000000000000000000cafebabe
Detailed key info: 0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001100101011111110101110101011
```

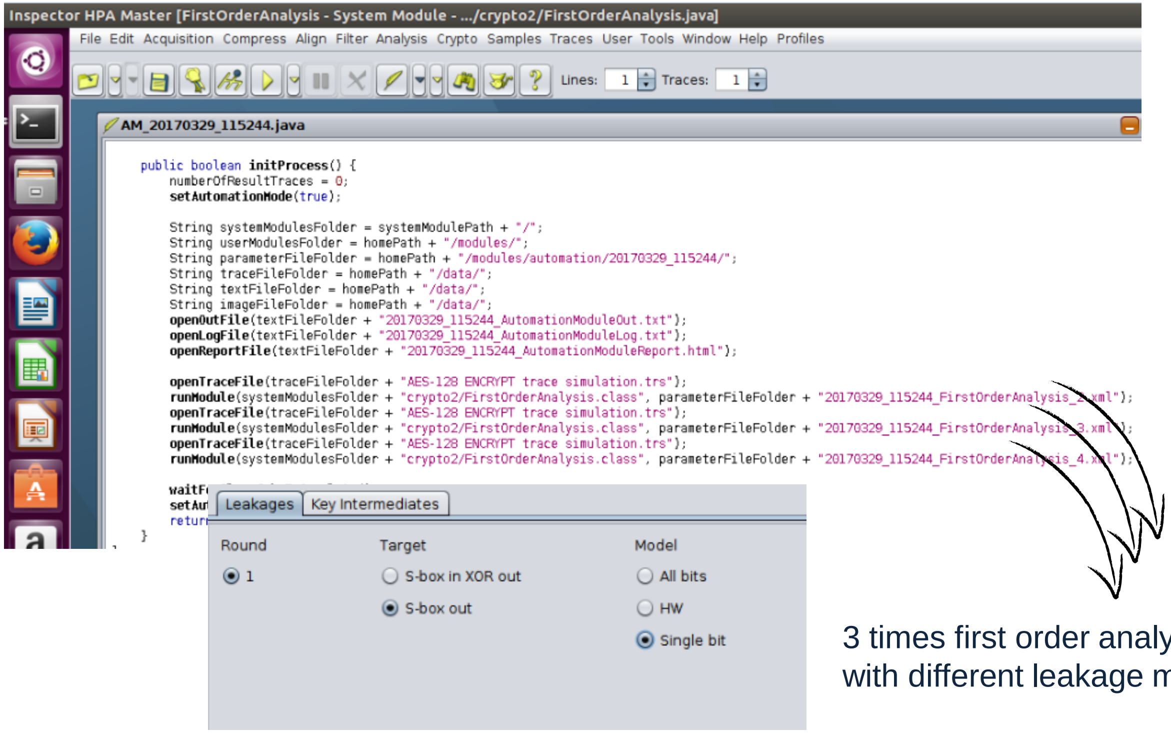
Runs on Linux

Inspector HPA is only used for analysis. Acquisition and pertubation is done with Inspector SCA or other tooling

Automation Example

Typical workflow

1. Use **record button** to start capturing your scenario
2. To make recording **fast**, just use a small part of the trace set
3. Stop recording to let Inspector **auto generate** a automation user module
4. Adapt the generated module programmatically when needed
5. Save the module and use it from **Inspector HPA**


Inspector HPA Master [FirstOrderAnalysis - System Module - .../crypto2/FirstOrderAnalysis.java]
File Edit Acquisition Compress Align Filter Analysis Crypto Samples Traces User Tools Window Help Profiles
Lines: 1
Traces: 1
AM_20170329_115244.java

```
public boolean initProcess() {
    numberOfResultTraces = 0;
    setAutomationMode(true);

    String systemModulesFolder = systemModulePath + "/";
    String userModulesFolder = homePath + "/modules/";
    String parameterFileFolder = homePath + "/modules/automation/20170329_115244/";
    String traceFileFolder = homePath + "/data/";
    String textFileFolder = homePath + "/data/";
    String imageFileFolder = homePath + "/data/";
    openOutFile(textFileFolder + "20170329_115244_AutomationModuleOut.txt");
    openLogFile(textFileFolder + "20170329_115244_AutomationModuleLog.txt");
    openReportFile(textFileFolder + "20170329_115244_AutomationModuleReport.html");

    openTraceFile(traceFileFolder + "AES-128 ENCRYPT trace simulation.trs");
    runModule(systemModulesFolder + "crypto2/FirstOrderAnalysis.class", parameterFileFolder + "20170329_115244_FirstOrderAnalysis_2.xml");
    openTraceFile(traceFileFolder + "AES-128 ENCRYPT trace simulation.trs");
    runModule(systemModulesFolder + "crypto2/FirstOrderAnalysis.class", parameterFileFolder + "20170329_115244_FirstOrderAnalysis_3.xml");
    openTraceFile(traceFileFolder + "AES-128 ENCRYPT trace simulation.trs");
    runModule(systemModulesFolder + "crypto2/FirstOrderAnalysis.class", parameterFileFolder + "20170329_115244_FirstOrderAnalysis_4.xml");

    waitF
    setAu
    retur
}
```

Round

● 1

Target

○ S-box in XOR out

● S-box out

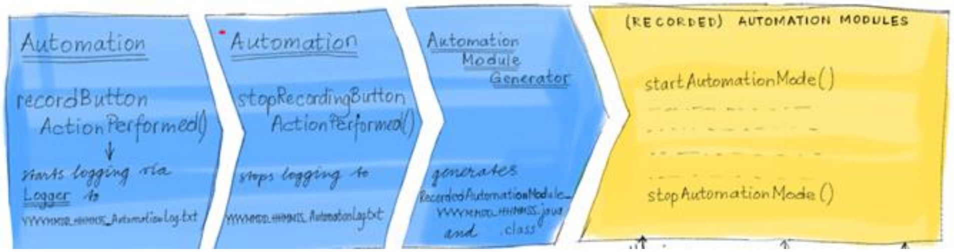
Model

○ All bits

○ HW

● Single bit

3 times first order analysis with different leakage model


Automation
recordButton ActionPerformed()
starts logging via Logger to
YYYYMMDD_HHMMSS_AutomationLog.txt
Automation
stopRecordingButton ActionPerformed()
stops logging to
YYYYMMDD_HHMMSS_AutomationLog.txt
Automation Module Generator
generates
RecordedAutomationModule_YYYYMMDD_HHMMSS.java and .class
(RECORDED) AUTOMATION MODULES
startAutomationMode()
stopAutomationMode()

HPA Server Specifications

PowerEdge FX2

Components

1	PowerEdge FX2 Chassis for up to 4 Half-Width Nodes
1	FX2S Chassis Configuration Label
1	PowerEdge FX2S Chassis Configuration with Flexible IO (up to 8 PCIe Slots)
2	FX2 Half-Width Node Filler Blank
1	2GB SD Card for CMC, Includes Flex Address Plus and CMC External Storage
1	Serial I/O Management Cable, for Ethernet Blade Switches
1	Power Supply, Redundancy Alerting Enabled Configuration
1	Module,Power Supply,2000W,Redundant,Delta Products
2	Jumper Cord, 230V,2.5M,C19/C20
1	Redundant Ethernet Switch Configuration
1	FX2 ReadyRails Sliding Rails

Software

1	No Systems Documentation, No OpenManage DVD Kit
1	CMC Enterprise for FX2

Service

1	Base Warranty
1	3Yr Basic Warranty - Next Business Day - Minimum Warranty
1	5Yr Basic Warranty - Next Business Day

Dell PowerEdge FN410T I/O Module, 8x Internal to 4x 10GBASE-T external ports, Factory Installed

Software

1	Software, Rights to use Full-Switch Mode, FN I/O Module

Service

1	Base Warranty
1	3Yr Basic Warranty - Next Business Day - Minimum Warranty
1	5Yr Basic Warranty - Next Business Day

PowerEdge FC630 Server Node

Components

1	PowerEdge FC630 Motherboard MLK
1	Intel Xeon E5-2630 v4 2.2GHz,25M Cache,8.0 GT/s QPI,Turbo,HT,10C/20T (85W) Max Mem 2133MHz
1	Intel Xeon E5-2630 v4 2.2GHz,25M Cache,8.0 GT/s QPI,Turbo,HT,10C/20T (85W) Max Mem 2133MHz
1	No Internal SD Module
1	MOD,INFO,ORD-ENTRY,2400,RDIMMS
1	Performance Optimized
8	16GB RDIMM, 2400MT/s, Dual Rank, x8 Data Width
1	DIMM Blanks for System with 2 Processors
1	iDRAC8 Enterprise, integrated Dell Remote Access Controller, Enterprise
1	120GB Solid State Drive SATA Value MLC 6Gbps 2.5in Hot-plug alue MLC 6Gbps 2.5in Hot-plug

Please contact Riscure for more information.

You can reach us by email : inforequest@riscure.com,

by phone : +31 15 251 4090   US: +1 650 646 9979

Or on the web: riscure.com.

riscure