GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Design and implementation of Virtual Security Appliances (VSA) for SME

Prof. Dr. Kai-Oliver Detken, DECOIT GmbH (Germany)

Christoph Dwertmann, NICTA (Australia)

VISA

Table of contents

Short introduction of DECOIT GmbH

- Analyse current trends on the technology market to help our customers make the right decisions before starting new projects
- Identify existing technology problems and provide innovative solutions through available products
- Workshops and coaching for our customers
- Software development to customise existing solutions and making new innovative products
- National and international research projects based on new technologies to increase our own know-how, then use the results for new product approaches
- Vendor-independent cooperations

Short introduction of NICTA

NICTA

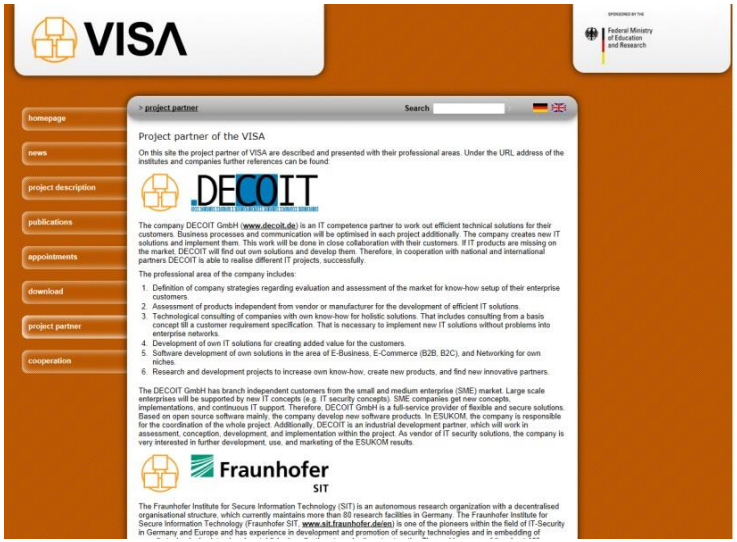
- NICTA is Australia's Information Communications Technology (ICT) Research Centre of Excellence and the nation's largest organisation dedicated to ICT research
- NICTA's primary goal is to pursue high-impact research excellence and, through application of this research, to create national benefit and wealth for Australia
- NICTA's research addresses the technology challenges facing industry, the community and the whole nation
- We seek to improve the international competitiveness of both academic ICT research and industry innovation by tightly linking the two to achieve greater economic and social impact

Introduction of the research project

VISA

Overview of the VISA project

- Funded by the German Federal Ministry of Education and Research (BMBF)
- VISA started in August 2011 and will end in September 2013
- Total budget: 1,7 Mio. €
- Partners of the project are:
  - DECOIT GmbH (project leader)
  - Fraunhofer SIT
  - University of Applied Sciences Dortmund
  - Collax GmbH
  - IT-Security@Work GmbH
  - National ICT Australia Limited



www.visa-project.de

Focus of the project

- In small and medium enterprises (SME), IT infrastructures have already become complex
- Security mechanisms such as firewalling, intrusion detection, and prevention systems have also become complex and have deep impacts to the existing infrastructure
- Because SMEs can provide only limited personnel resources and know-how for operative IT management, IT management has to be made easy
- The goal of VISA is to simplify and support management of IT infrastructures, especially security components, by using virtualization technology

Two different main approaches

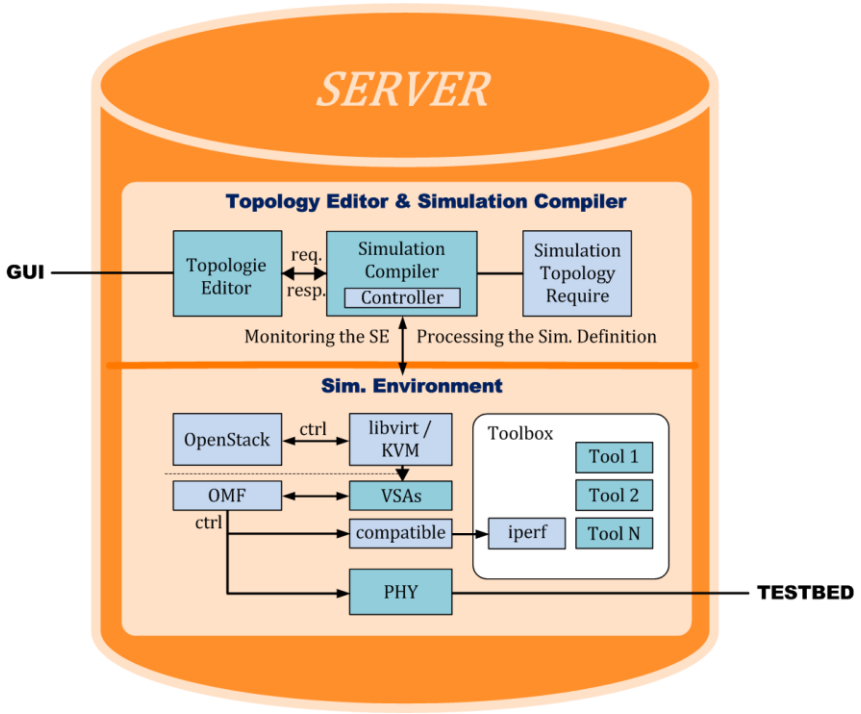
- VISA is based on two core technologies:
  - Simulation and evaluation of IT infrastructure in virtual environments
  - Realization of security applications as virtual components, so-called virtual security appliances (VSAs)
- The VISA framework simplifies the usage of security components based on VSAs, which can be directly integrated into an existing IT infrastructure
- By combining virtual and real infrastructure components, this approach will help SMEs to estimate the costs of their IT and enhance security

Simulation architecture of components

VISA

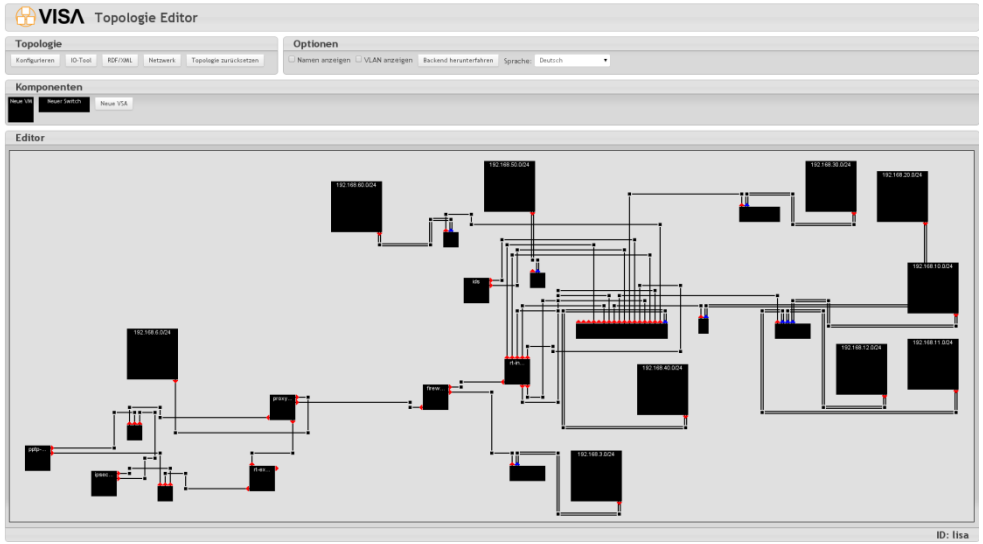
Simulation components

- Topology Editor (TE)
  - GUI for managing the network and server topologies
  - Measurements starting point
  - Configuration of the simulation environment
  - Interworking to the SC
- Simulation Compiler (SC)
  - Simulation description and definition with help of ontologies
  - OMF is used for deployments
  - Interworking to the TE
- Simulation Environment (SE)
  - Virtual platform based on OpenStack, libvirt, and KVM
  - OpenStack manages the VMs
  - libvirt offers a universal API
  - KVM offers virtual machines (VMs) for the infrastructure



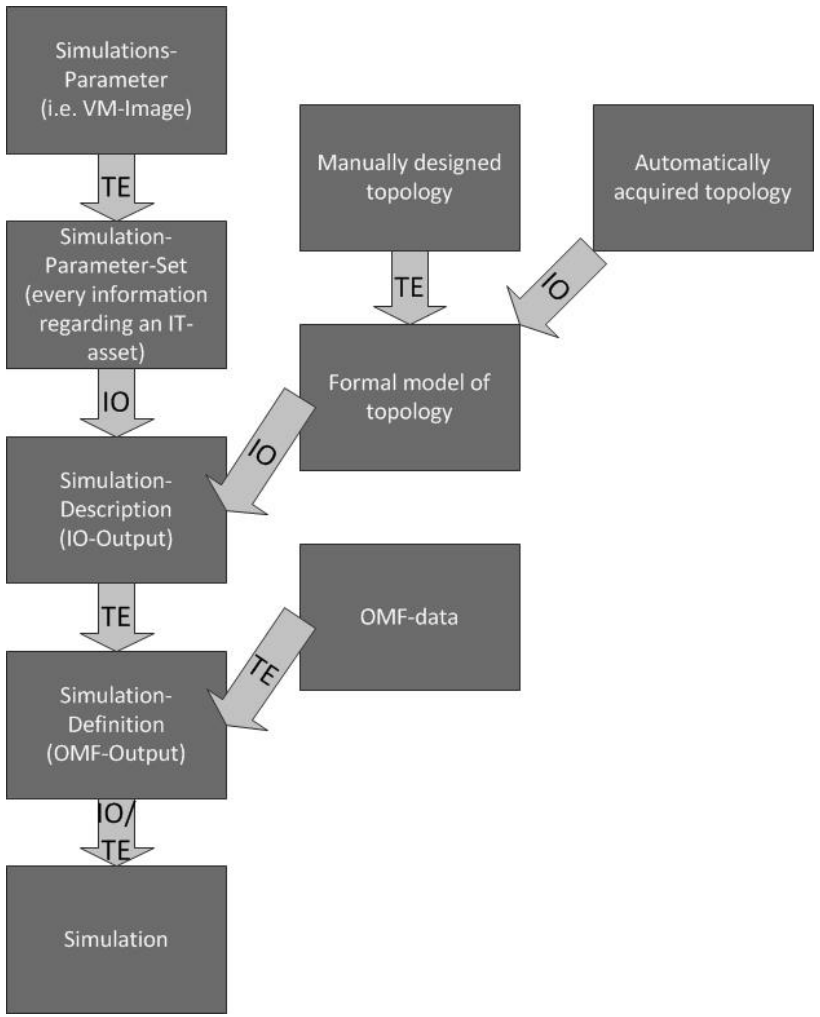
VISA Topology Editor (V-TE)

- The V-TE lets the user work on an existing topology and add new components
- Additionally, a new or existing topology can be changed manually
- Infrastructure components can be:
  - Hosts
  - Network Interfaces
  - Switches
  - VLAN-IDs
- The formal representation processed by the V-TE is stored in the Interconnected-asset Ontology (IO toolset)



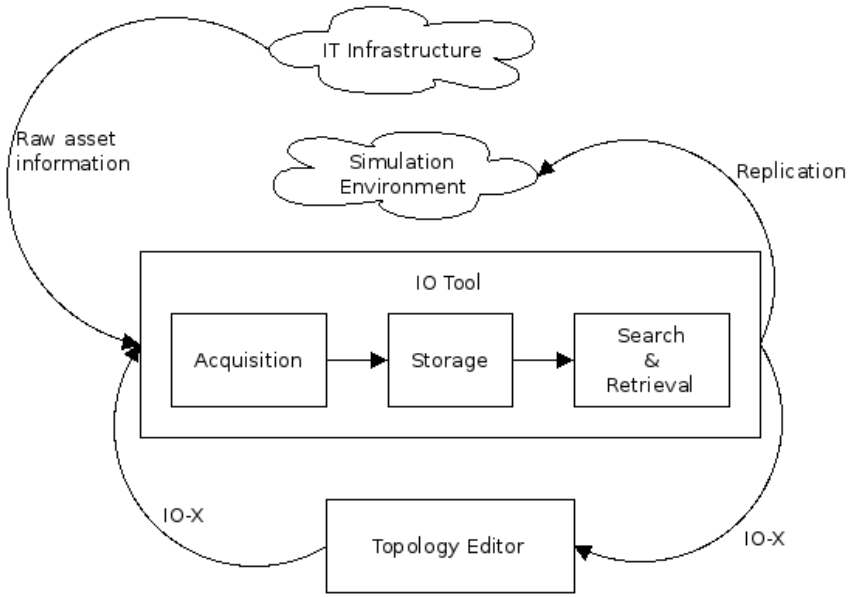
Workflow of the VISA architecture

- The workflow between the simulation components starts with the V-TE
- The user defines or modifies the formal representation of the simulation topology
- Based on a set of existing virtualised machines, additional IT-assets can be added to the model of the productive infrastructure
- Within the model represented in the V-TE, it is also possible to define certain behaviours of the IT-assets involved
- For example, in the case of a mail server, a specific simulation description could define a data source with an automated process sending e-mails to the simulated server



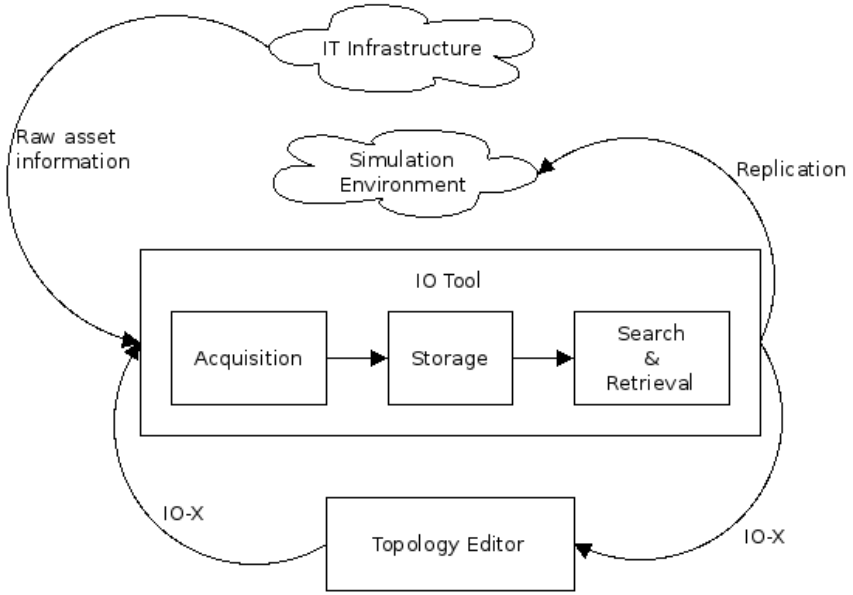
IO tool-set (1)

- The IO tool-set aggregates heterogeneous infrastructure information and meta-data in an ontological representation with a high level of detail
- This includes
  - Static IT-asset information (e.g. manually assigned address configuration, vendor IDs, serial numbers)
  - Volatile information (e.g. dynamic address configuration, neighbourhood relationships)
- All data that can be extracted from managed network components (e.g. network equipment or network endpoints) can be processed by the IO tool-set



IO tool-set (2)

- The figure shows two corresponding data flows regarding the IO tool-set
  - Acquisition of IT-asset information from productive IT-infrastructure and utilization of the resulting formal representation by the Simulation Compiler (SC)
  - Processing of a manually composed infrastructure topology saved and loaded by the Topology Editor (V-TE) via IO-X
- IO-X functions as a platform independent exchange protocol that is based on RDF
- Optionally OWL can be used if more complexity is required by consumers or producers of information

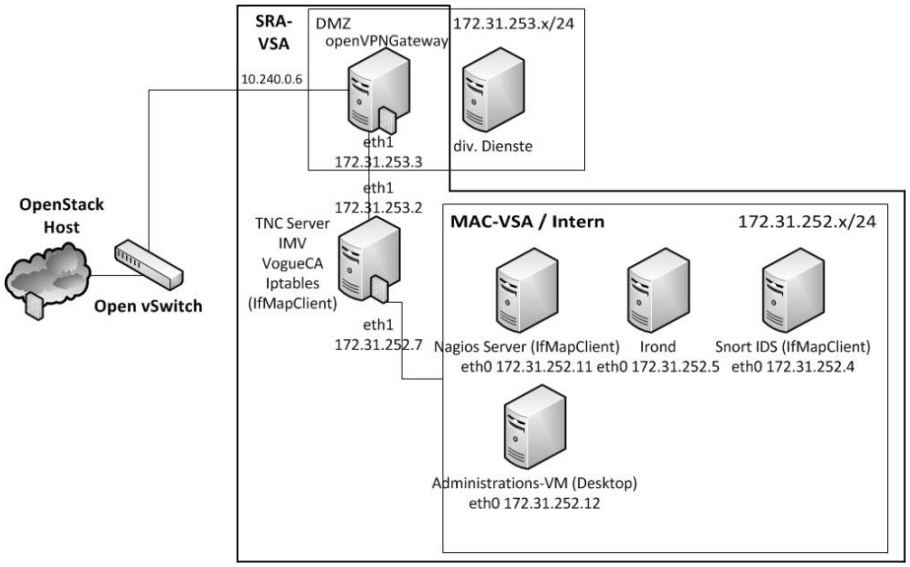


Virtual Security Appliances (VSA)

- A virtual security appliance (VSA) can be a single virtual machine (VM) or a combination of multiple VMs
- A VSA is able to offer different services within IT infrastructures, especially regarding IT security
- The VSA of VISA consists of virtual IT security modules and services
- The goal is to improve IT security of a typical SME network topology
- Two examples of VSAs of the project are:
  - VSA-MAC (Virtual Security Appliance – Meta-data Access Control)
  - VSA-SRA (Virtual Security Appliance – Secure Remote Access)

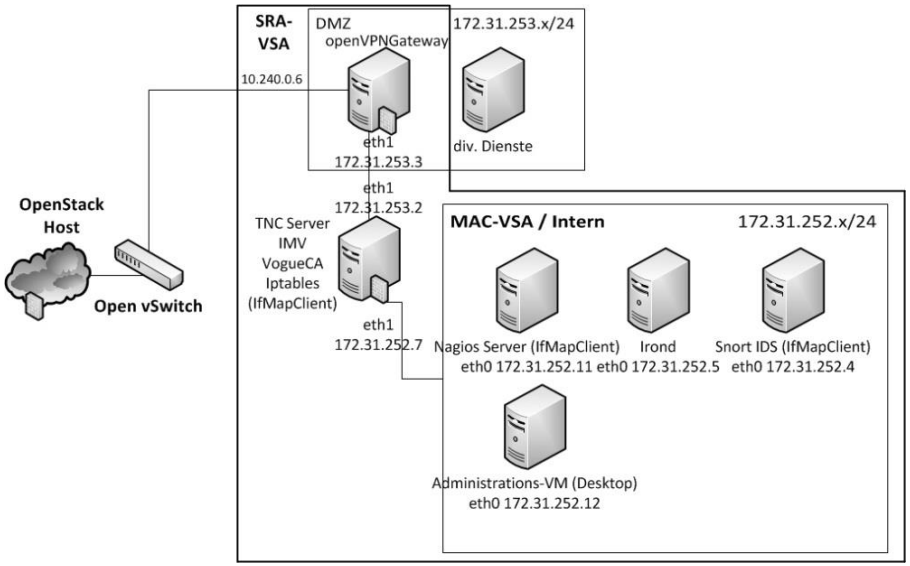
VSA-MAC

- The *VSA-MAC* is based on the components IF-MAP server and IF-MAP clients for Android, Snort, iptables and Nagios
- IF-MAP is an open and vendor-independent client/server protocol to exchange meta-data
- The central component is the IF-MAP-server, which stores the collected meta-data from the clients and also provides the data for the clients
- With the help of the collected meta-data, anomalies can be detected easily through correlation of all information
- An important specification of the VSA-MAC is IF-MAP for exchanging meta-data in a client/server based environment



VSA-SRC

- The *VSA-SRA* allows a secure dial-in to a SME network via an Android-based mobile phone
- The VSA contains an Android client, TNC server, and VPN gateway
- The mobile phone connects to the SME-network through the VPN gateway
- But the mobile phone isn't trustworthy, because only the user credentials have been used and the software and hardware haven’t been checked
- Therefore, to reach a higher security level, it is necessary to send additional meta-data from the Android mobile phone as well
- The metrics include the installed application, version number and policies that are applied to the mobile phone
- The TNC server compares the metrics with those in its database
- If all policies are fulfilled, the mobile phone is granted access to the internal resources, if not, it is rejected



Automatic configuration

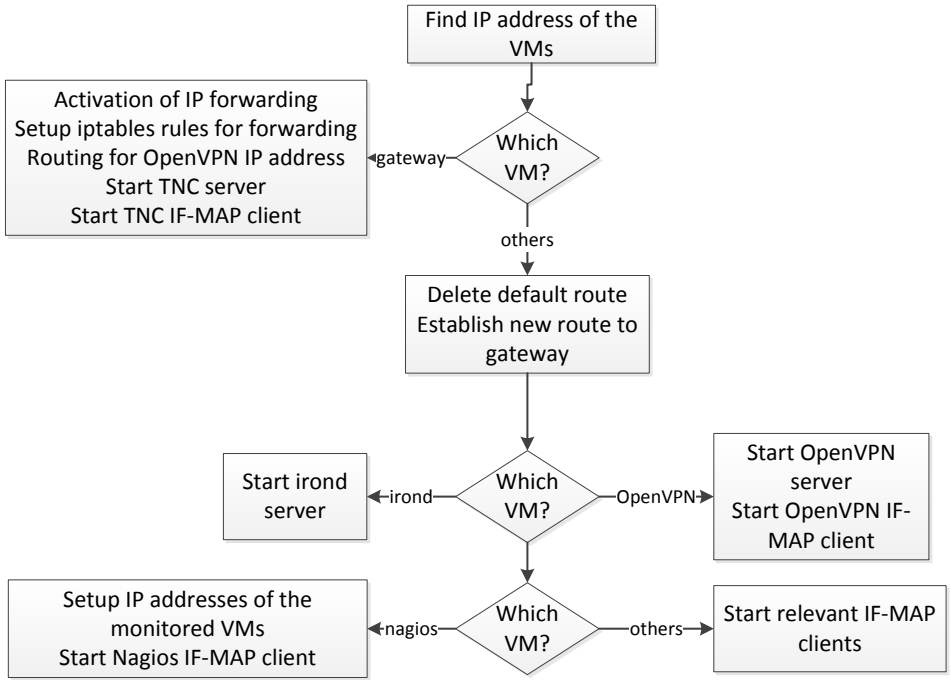
VISA

Delivering of the VSAs

- The VSAs of VISA will be delivered into an existing IT infrastructure with a basic configuration
- Therefore, an automatic configuration of the VSA components is necessary
- However not all configuration parameters are available when the VSA will be established, such as:
  - IP address of the default gateway
  - IP address of the irond server
  - IP address of the OpenVPN server
  - Nagios server needs IP addresses of the monitored virtual machines
- Additionally, some services have to be started manually if the configuration changes
- To avoid this, the VISA project uses the configuration management tool puppet (http://puppetlabs.com)

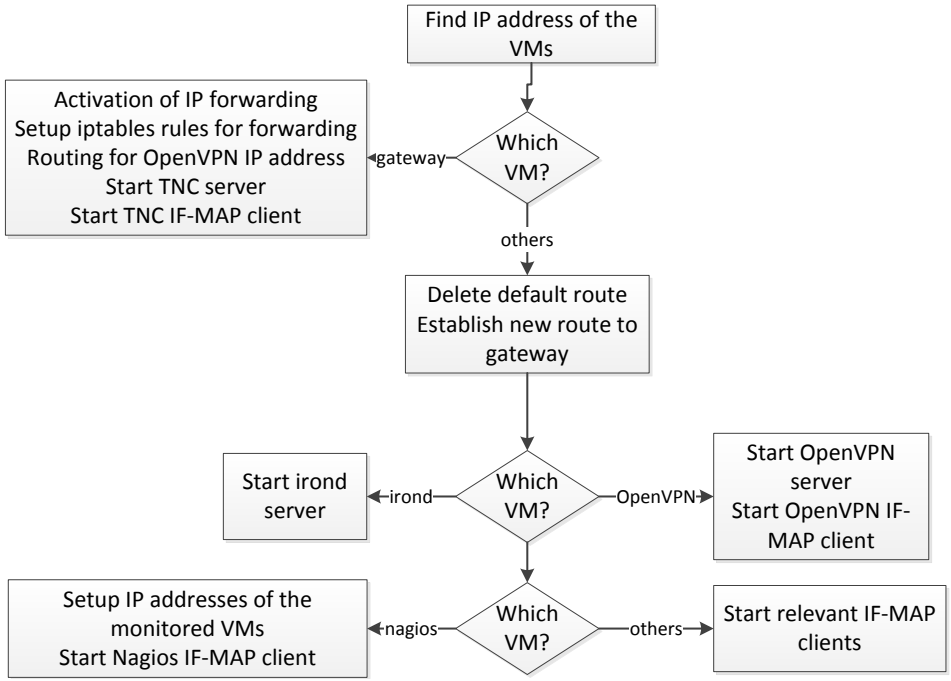
Use of puppet

- Within VISA a client-/server model is used
- This includes a puppet server on the OpenStack host and a puppet client on every virtual machine (VM) instantiated from the VSAs
- To reserve an IP address range in real-time, an additional script was written and is used on the OpenStack host
- These IP addresses can be used for the puppet templates
- Next, the new default gateways will be set and the IF-MAP clients and the server start
- The gateway VM activates the IP forwarding and loads the iptables policies
- Also the TNC server and client start up



Workflow

- When a VSA has been started, the VMs try to reach the puppet server and ask it for the configuration
- The VMs are identified by their fully qualified domain names (FQDN)
- If a configuration for a client exists, the puppet server transfers the necessary content (files, commands, etc.) to the client
- The puppet client compares the existing configuration with the required one
- If there is a difference, the new configuration is applied
- The puppet clients are configured to ask the server for the configuration every five minutes
- The communication between the puppet server and the clients is encrypted with SSL

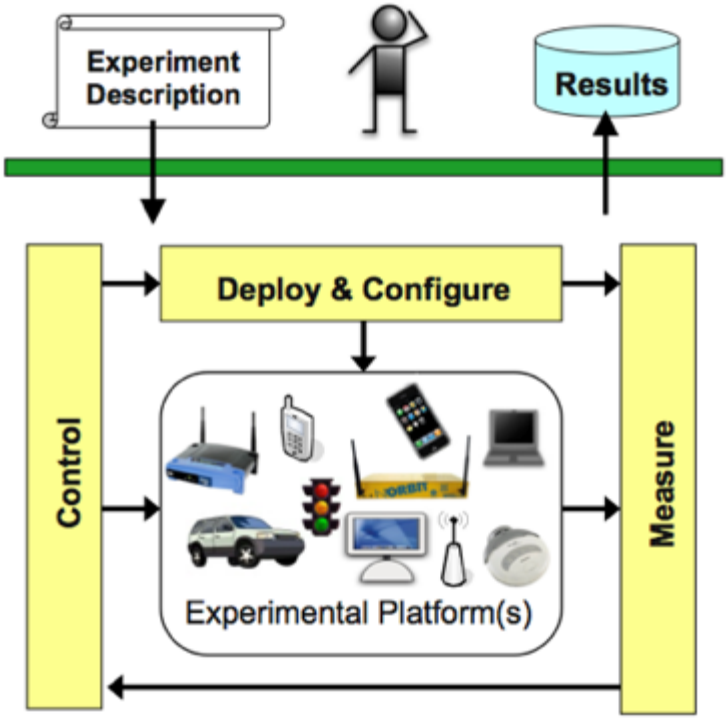


Orchestration & Measurement

VISA

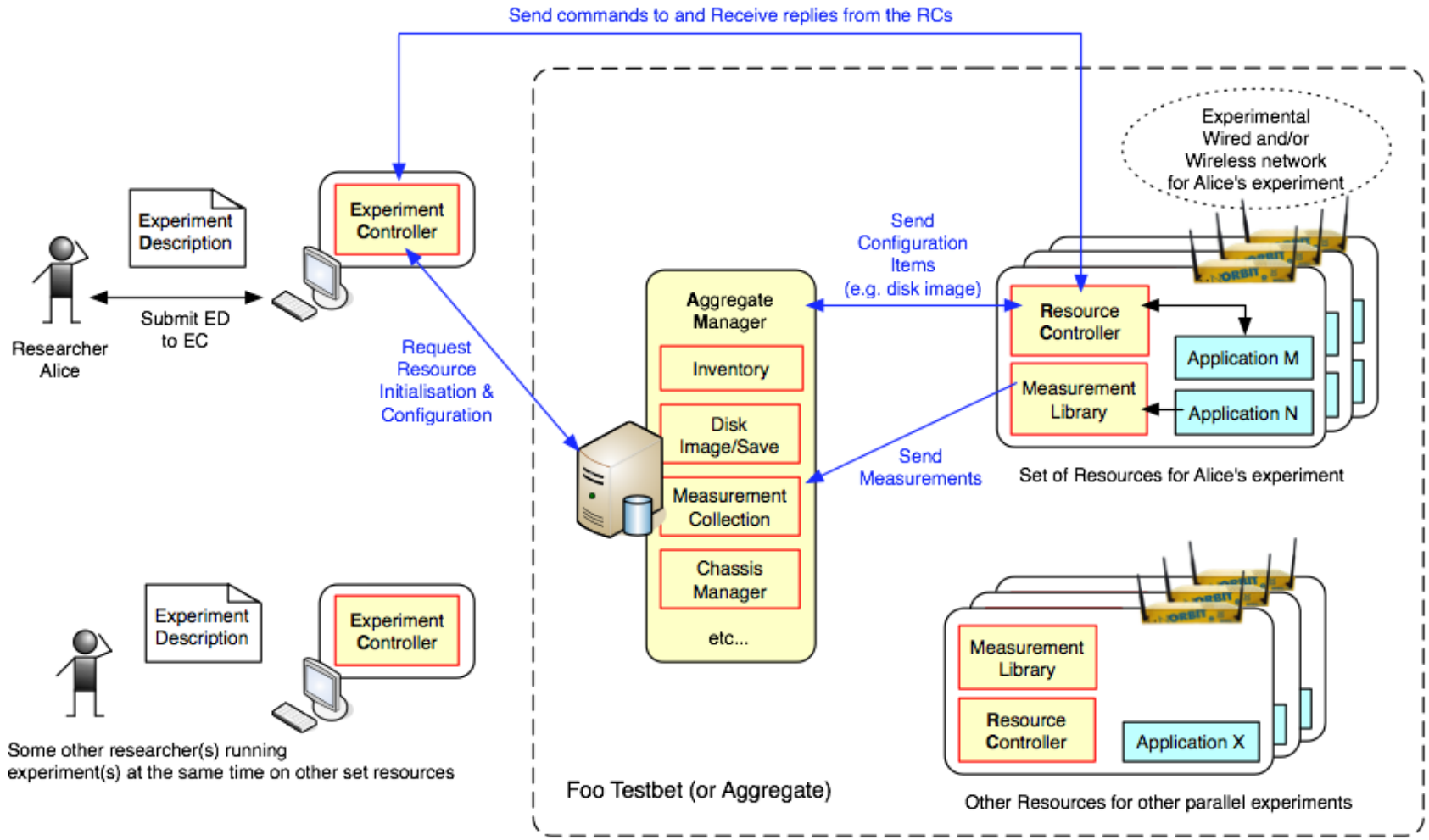
OMF - http://omf.mytestbed.net

- OMF is a NICTA-developed control and management framework for experiments in networking test-beds
- From the experimenter's point of view, OMF provides a set of tools to describe and instrument an experiment, execute it and collect its results
- From the test-bed operator's point of view, OMF provides a set of services to efficiently manage and operate the test-bed resources (e.g. resetting nodes, retrieving their status information, installing new OS image)



omf.mytestbed.net

OMF system architecture



Evaluation of the VSAs (1)

- VISA uses the OMF Framework to control the flow of experiments inside the VSA
- Each VSA runs an OMF Resource Controller (RC), which allows a remote experimenter to execute instructions, e.g. starting programs or setting up measurements
- The experimenter's tool is the OMF Experiment Controller (EC), which steers the experiment through an experiment description file
- The file format is OEDL (OMF Experiment Description Language), which generated by the VISA simulation compiler
- All OMF components communicate via XMPP protocol
- OMF entities can be in different networks and behind NAT or firewalls, but can still communicate as long as they can all reach an XMPP server
- To measure the impact of a security experiment on the VMs and network components, VISA uses the OML measurement framework

Evaluation of the VSAs (2)

- A common scenario in VISA is to deploy a couple of VSA that mimic a SME and then introduce an “attacker” VSA to the network
- OMF is used to start up applications (e.g. a mail server) on the SME VSA and run the attack on the “attacker” VSA
- OMF also runs OML-instrumented measurement tools to monitor network throughput (e.g. iperf) and system load (e.g. nmetrics) during the attack
- OML data is stored in a database for live graphing and post-attack analysis
- After examining the data and securing the VSAs, the exact same attack can be repeated by OMF and measured by OML to check whether the security measures taken were successful in closing the hole

Conclusions

VISA

Conclusions

- The goal of VISA is to establish more security mechanisms in SME infrastructures
- That also means making the configuration itself more secure, which is a difficult task in general
- Through the VISA project, it is now possible to setup a virtual IT infrastructure with different security components and automatic configuration mechanisms without extensive knowledge about the individual VMs
- It is feasible to simulate the infrastructure and the configuration of the VMs and analyse the security afterwards (by using the visualization tools of OMF)
- Using the topology editor, an administrator can design and re-design the IT infrastructure in a simple-to-use graphical tool
- The existing infrastructure can be analysed and simulated on this virtual platform

Outlook

- The project VISA ends in September 2013
- Within the project lifecycle, all goals have been reached
- A complete simulation cycle can be established, which helps to institute more security in SME environments
- Future tasks are still left open:
  - Direct TE connection to OpenStack
  - Direct recording of existing IT infrastructures in the TE
  - Compliance documentation with an Audit-compatible format
  - Extended bug recognition regarding incorrectly configured networks

Thank you!

…for your attention.

Copyright 2011-2013

Das dem Projekt zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen „01BY1160“ gefördert. Die Verantwortung für den Inhalt liegt bei den Autoren.