SPONSORED BY THE

Federal Ministry
of Education
and Research

Simulation Environment (SE) for mobile Virtualized Security Appliances (VSA)

Prof. Dr. Kai-Oliver Detken,
DECOIT GmbH

VISA

Agenda

- Short introduction of DECOIT GmbH
- Introduction of the VISA project
- Platform architecture
- Platform requirements
- Mobile VSAs
- Conclusions
- Future works

Short introduction of DECOIT GmbH

.DECOIT

- Main focus:
  - Analysing of current trends of the technology market to help our customers to make the right decisions before starting new projects
  - Identifying of existing technology problems and provide innovative solutions by available products
  - Workshops and coaching for our customers
  - Software development to customise existing solutions and developing new innovative products
  - National and international research projects based on new technologies to increase own know-how and use the results for new product approaches
  - Vendor-independent cooperations

Introduction of the VISA project

Focus of the project

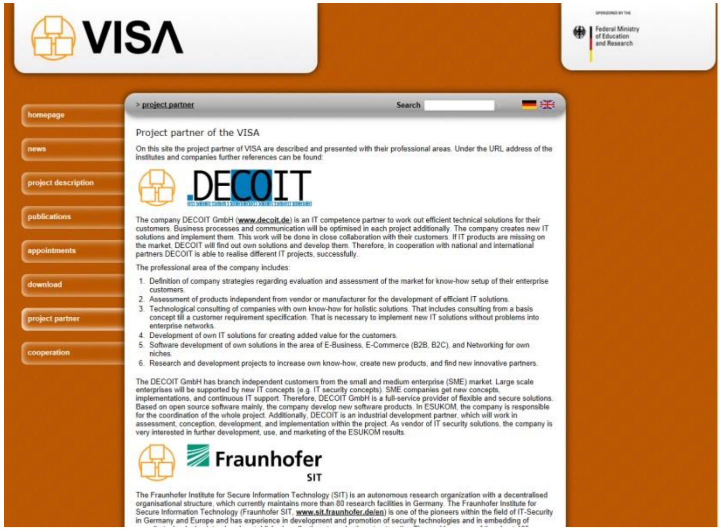
- In small and medium enterprises (SME), IT infrastructures have already become complex
- Security mechanisms such as firewalling, intrusion detection, and prevention systems become also complex and have deep impacts to the existing infrastructure
- Because SMEs can provide only limited personnel resources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

Two different main approaches

- VISA is based on two core technologies:
  - Simulation and evaluation of IT infrastructures 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 costs of their IT and enhance security

Overview of the VISA project

- Founded by the Federal Ministry of Education and Research (BMBF) of Germany (http://www.visa-project.de)
- VISA has been started in August 2011 and will end on July 2013
- Total budget of the project: 1,7 Mio. € (founded budget: 1,0 Mio. €)
- Partners of the project are:
  - DECOIT GmbH (leader of the project)
  - Fraunhofer SIT
  - University of Applied Sciences Dortmund
  - Collax GmbH
  - IT-Security@Work GmbH
  - National ICT Australia Limited



Project partner of the VISA

On this site the project partner of VISA are described and presented with their professional areas. Under the URL address of the institutes and companies further references can be found:

The company DECOIT GmbH (www.decoit.de) is an IT competence partner to work out efficient technical solutions for their customers. Business processes and communication will be optimised in each project additionally. The company creates new IT solutions and implement them. This work will be done in close collaboration with their customers. If IT products are missing on the market, DECOIT will find out own solutions and develop them. Therefore, in cooperation with national and international partners DECOIT is able to realise different IT projects, successfully.

The professional area of the company includes:

1. Definition of company strategies regarding evaluation and assessment of the market for know-how setup of their enterprise customers.
2. Assessment of products independent from vendor or manufacturer for the development of efficient IT solutions.
3. Technological consulting of companies with own know-how for holistic solutions. That includes consulting from a basis concept till a customer requirement specification. That is necessary to implement new IT solutions without problems into enterprise networks.
4. Development of own IT solutions for creating added value for the customers.
5. Software development of own solutions in the area of E-Business, E-Commerce (B2B, B2C), and Networking for own niches.
6. Research and development projects to increase own know-how, create new products, and find new innovative partners.

The DECOIT GmbH has branch independent customers from the small and medium enterprise (SME) market. Large scale enterprises will be supported by new IT concepts (e.g. IT security concepts). SME companies get new concepts, implementations, and continuous IT support. Therefore, DECOIT GmbH is a full-service provider of flexible and secure solutions. Based on open source software mainly, the company develop new software products. In ESUKOM, the company is responsible for the coordination of the whole project. Additionally, DECOIT is an industrial development partner, which will work in assessment, conception, development, and implementation within the project. As vendor of IT security solutions, the company is very interested in further development, use, and marketing of the ESUKOM results.

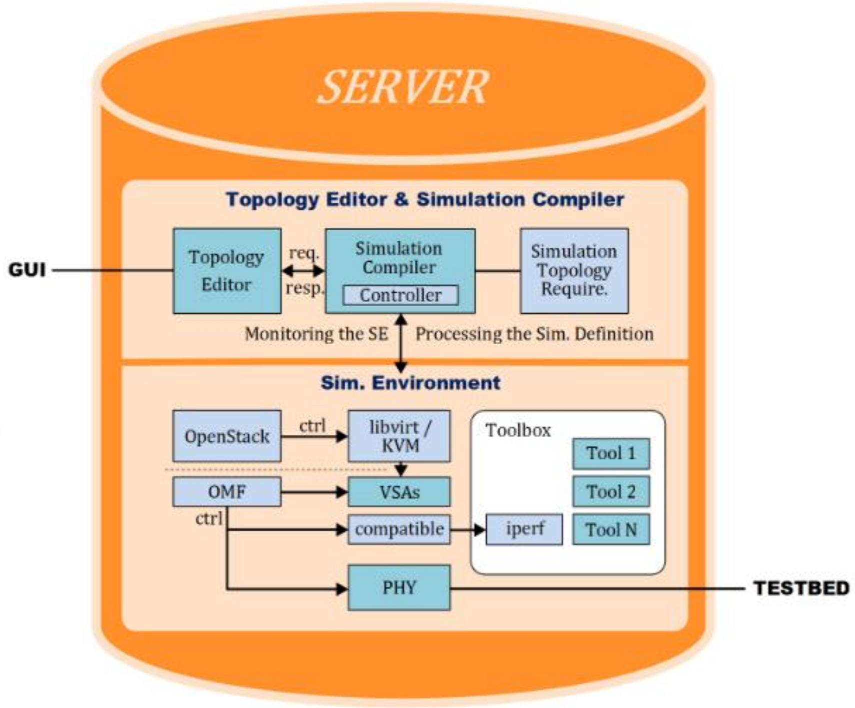
The Fraunhofer Institute for Secure Information Technology (SIT) is an autonomous research organization with a decentralised organisational structure, which currently maintains more than 80 research facilities in Germany. The Fraunhofer Institute for Secure Information Technology (Fraunhofer SIT, www.sit.fraunhofer.de/en) is one of the pioneers within the field of IT-Security in Germany and Europe and has experience in development and promotion of security technologies and in embedding of

www.visa-project.de

Architecture of the platform

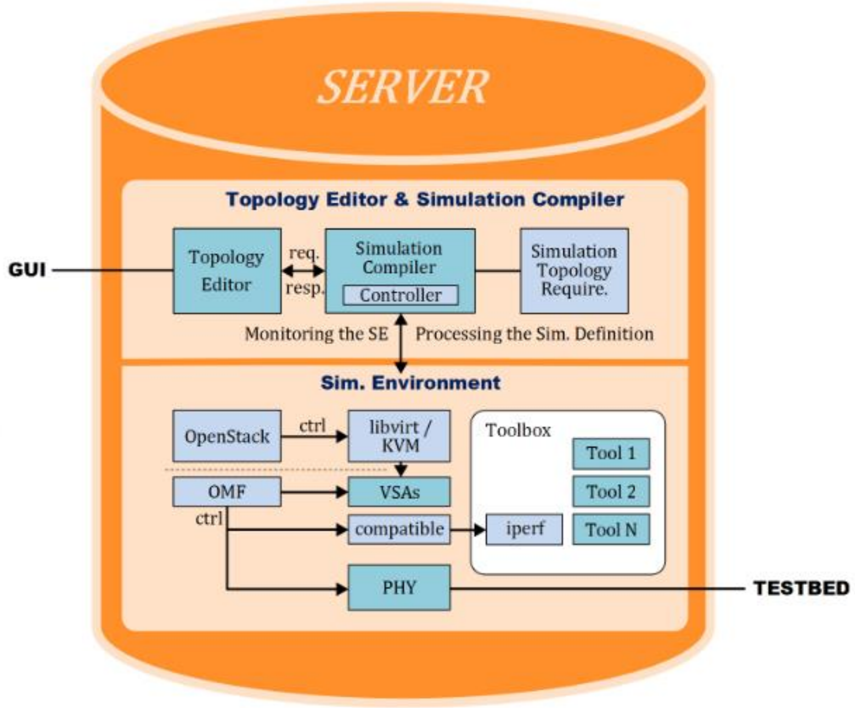
Components of the platform

- By the simulation system, testing of the functionality and availability is possible after introducing new features of the productive system
- The VISA Simulation Environment (VISA-SE) therefore offers the following components:
  - Topology Editor (TE)
  - Simulation Compiler (SC)
  - Simulation Environment (SE)



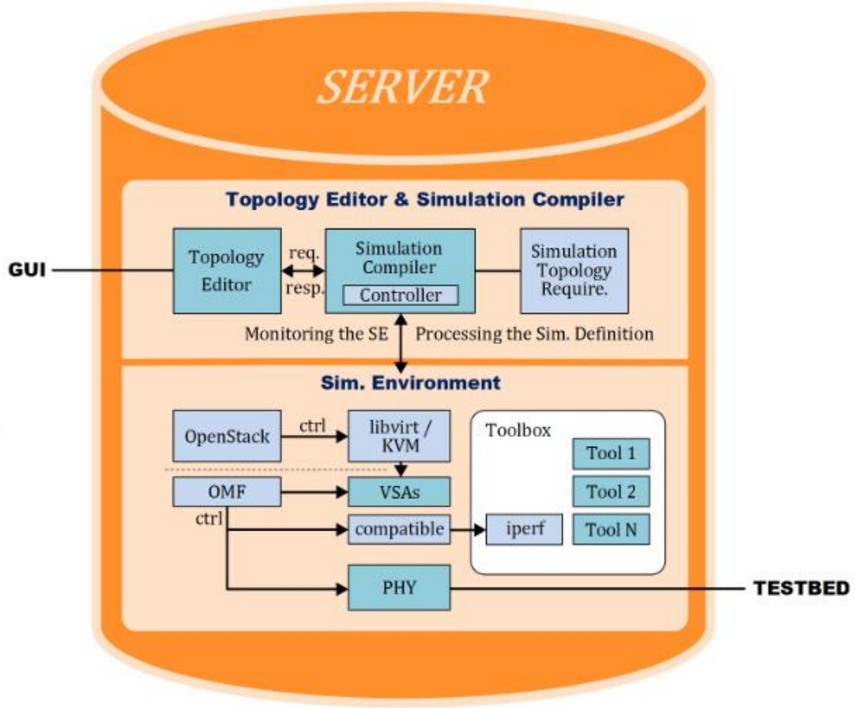
Topology Editor

- The *topology editor (TE)* offers the possibility to develop the model of the productive system, which has to be evaluated
- It is a graphical tool which defines the topology and offers additional functionalities such as
  - starting measurements
  - configuring properties for the simulation environment



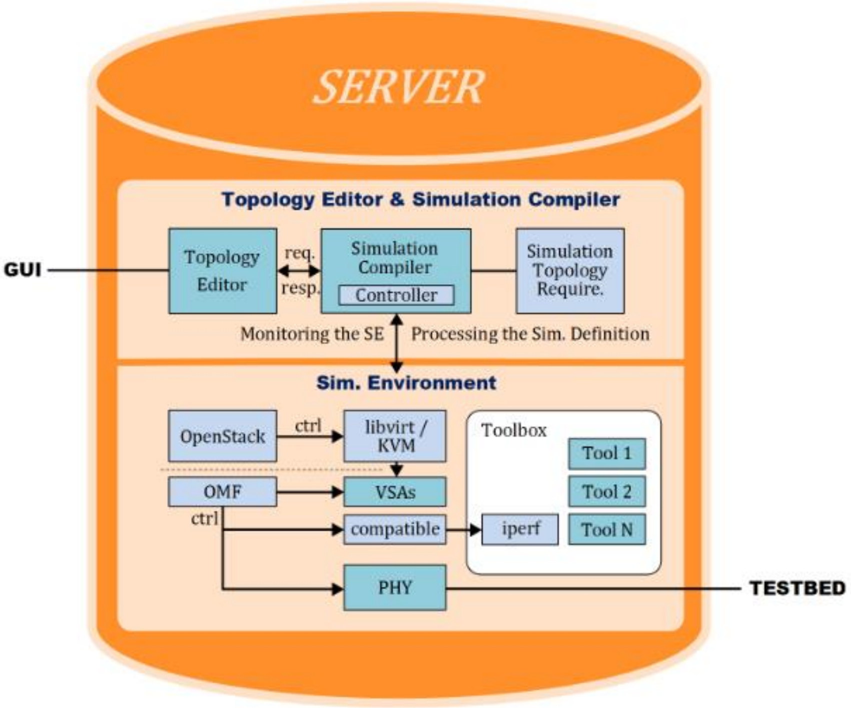
Simulation Compiler (SC)

- The *simulation compiler (SC)* translates the TE parameters into the simulation definition (e.g. the designed topology)
- The simulation definition may include
  - automated experiments
  - virtual images
  - requests to monitor the simulation
- A part of the simulation definition act as input for the *OMF framework*
- OMF is use for simulation environment deployments and services
- The SC passes the simulation definition to a controller to execute all actions by the given simulation definition (e.g. include starting OMF)
- The controller delivers the results back to the GUI



Simulation Environment (SE)

- The *simulation environment (SE)* executes the OMF controlled simulation and allows the SC's controller to directly access the SE
- The SE processes and executes parts of the simulation definition and also offers generic (OMF independent) scenarios
- The simulation facilitates measurements with respect to systems functionality
- The simulation uses virtual machine images



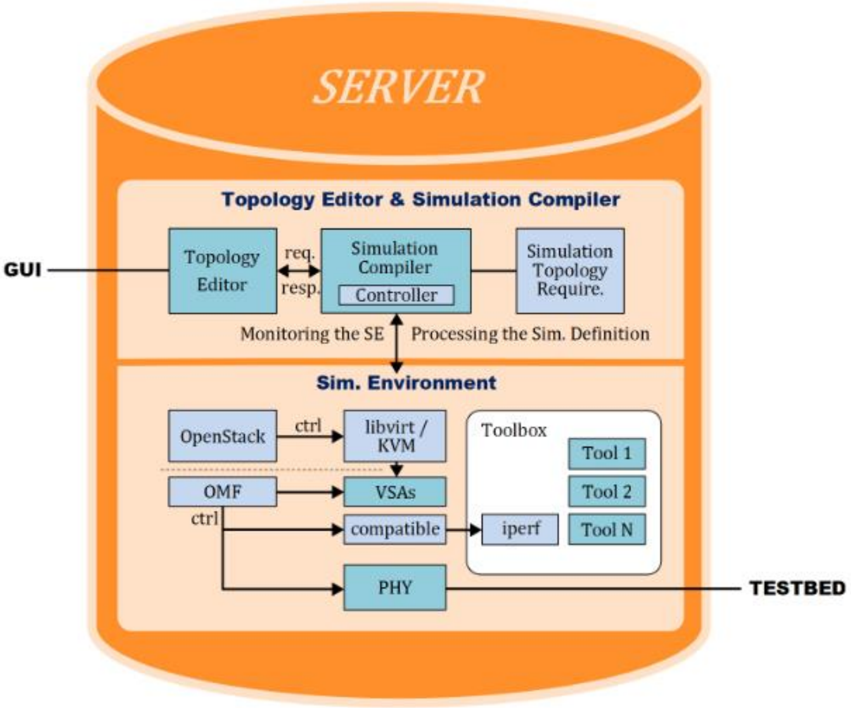
Platform Requirements

Components of the system model

- The VISA system needs to include the following components in its system model:
  - **Core functionality:** These components are used to model the IT system and incorporate systems such as e-mail servers and clients
  - **Security functionality:** One of VISA's goals is to evaluate security components with regard to their impact on the productive IT system's core functionality
  - **Network:** All core and security components are interconnected by networks
  - **Test data source:**
    - Data sources are required for core and security components (e.g. penetration tests) to simulate automated actors
    - Automated testing requires generator components

Workflow between TE, SC, and SE

- The *topology editor (TE)* allows the definition of models which represent productive environments
- Productive IT systems can be composed with servers, clients, and network connections
- After the user has defined the simulation description it is passed to the *simulation compiler (SC)*
- The *SC* has to be able to validate the topology definition given by the simulation description against defined and secured topology requirements
- In the *simulation environment (SE)* the different technologies are executed to load *Virtual Security Appliances (VSA)*, configure the network topology between the nodes, trigger events, and collect data



Mobile VSAs

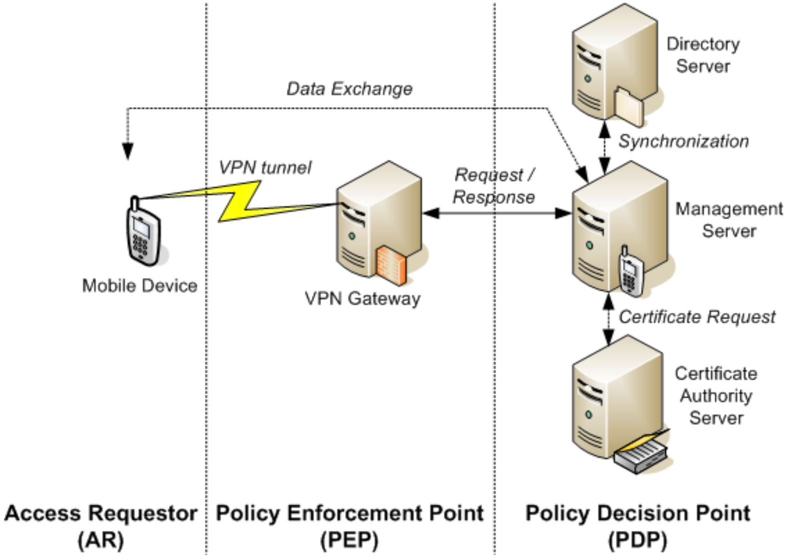
VISA

Definition of mobile VSAs

- The VISA project has been defined two mobile VSAs in order to address improved securing for smartphones (e.g. for Android OS):
  - **VSA-SRA** allows Android-based mobile devices to access different IT systems in a trustworthy manner (e.g. applications of enterprise networks) by the use of Trusted Computing (TC) technology to get hardware integrity.
  - **VSA-MAC** additionally use the IF-MAP protocol of the Trusted Computing Group (TCG). The IF-MAP specification currently defines a model for meta-data which addresses use-cases in the network security domain. With the correlation of other meta-data, the VSA is able to detect attacks which cannot be usually discovered by standalone security systems.

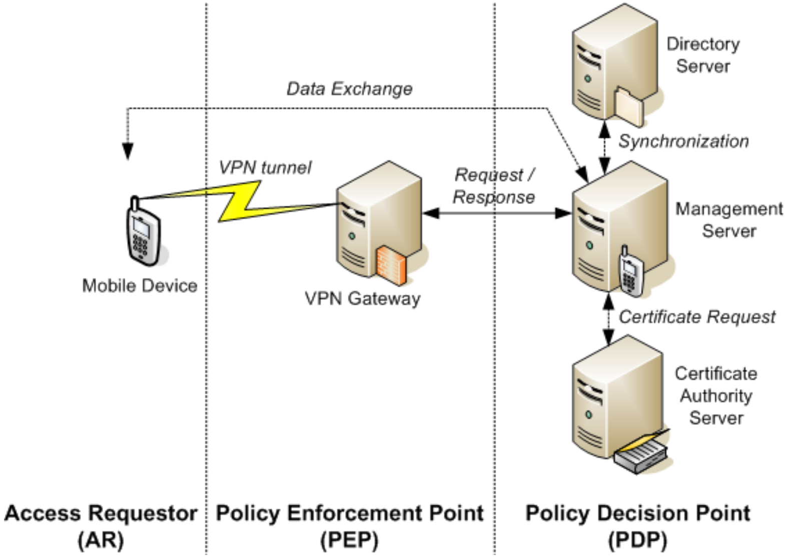
VSA-SRA (1)

- For *VSA-SRA* the core element of the platform is represented by the *VPN gateway*
- Additionally, management server (e.g. RADIUS), directory server (e.g. LDAP), and certification authority server are necessary
- In the first step, the user has to be identified accessing the VPN gateway
- All criteria are available on the directory server and assign the user to different profiles and user groups



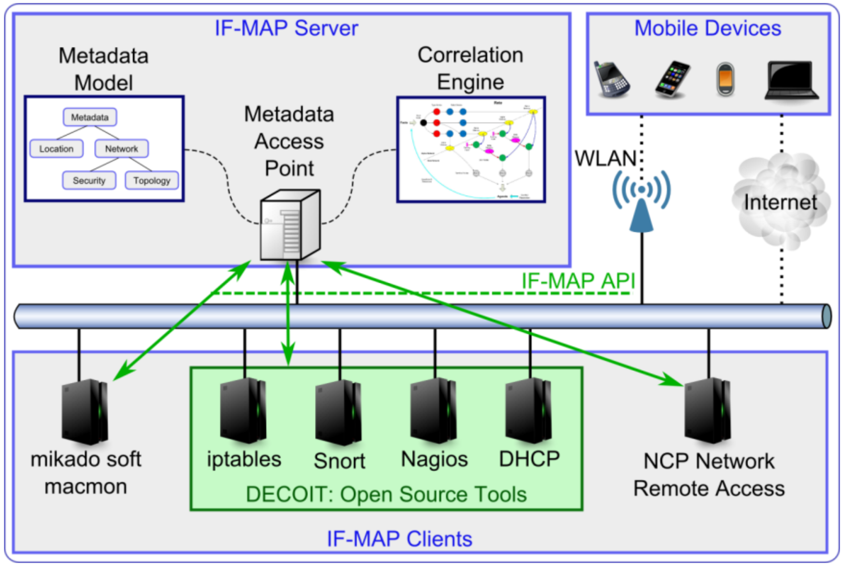
VSA-SRA (2)

- In companies each user group has different security policies for different access privileges
- The management system synchronises in intervals continuously user information with the directory server
- That includes that user from the directory server with VPN access privileges, if they are not yet available on the management server, will synchronize with all user group membership automatically after one interval
- As an option a public certification authority (CA) can be adapted



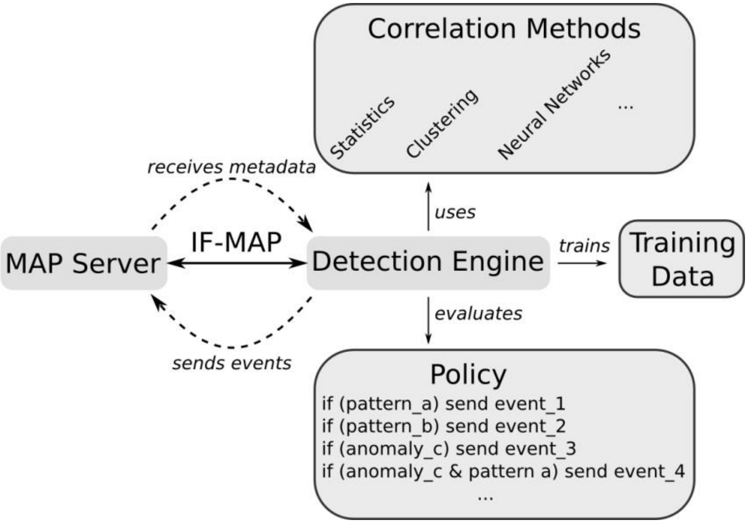
VSA-MAC (1)

- A further specification of the TCG is *IF-MAP*, a protocol for exchanging meta-data in a client-server based environment
- Its main purpose is to achieve interoperability for security related data exchange between components in a network
- So called *MAP clients (MAPC)* can publish new meta-data to a *MAP server (MAPS)* and also search for meta-data
- They also can subscribe to specific meta-data and provided with information when new meta-data are published



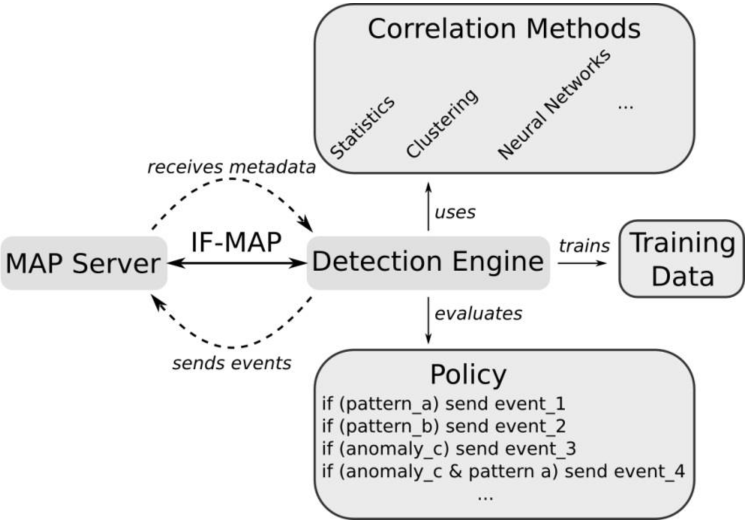
VSA-MAC (2)

- The *VSA-MAC* approach relies on the concept of trustworthy meta-data correlation based upon the IF-MAP protocol
- Any security relevant data, whether it stems from a smartphone or a service that is provided by the IT infrastructure (e.g. IDS, firewall, AAA service), is expressed according to a well-defined meta-data model
- In addition, a trust model has been defined that enables to reason about the trustworthiness of the meta-data instances
- Both the meta-data model and the trust model are based on the IF-MAP protocol



VSA-MAC (3)

- The extended meta-data graph forms the basis for any further correlation approaches
- By the use of the *detection engine* component, pattern and anomaly detection is possible for the VSA-MAC environment, based on real-time collected meta-data
- If the detection engine recognizes a pattern such as a signature or an unregistered app, an event will be sent to the MAP server
- This event can be analysed by other MAP clients, which can react (e.g. with a real-time enforcement) according to their policy definitions, if necessary
- The detection engine works as MAP client and is able to get any subscriptions from the MAP server directly



Correlation Methods

Statistics

Clustering

Neural Networks

...

receives metadata

uses

MAP Server

IF-MAP

Detection Engine

trains

Training Data

evaluates

sends events

Policy

if (pattern_a) send event_1
if (pattern_b) send event_2
if (anomaly_c) send event_3
if (anomaly_c & pattern a) send event_4
...

Conclusions

- The mobile VSAs consist of several security components
- All components work with each other and have to be configured
- The modelling framework developed in VISA allows security testing for IT systems more easily and efficiently
- This would be an important step in the direction of end-to-end security
- A further advantage of comprehensive IT infrastructure planning via the VISA framework is the tailor-made, simplified use of security applications based on VSA

Future works

- The architecture of the VSA platform is still in progress (e.g. the topology editor)
- Both mobile VSAs of VISA will be ready in the next weeks (October ‘12)
- Further VSAs are on preparation (e.g. VSA-AAA)
- Also the deployment process of the VSAs is in progress
- Implementation work will be done in November in Sydney, Australia at the partner NICTA
- The biggest challenge is to integrate the different approaches (KVM, libvirt, OpenStack, OpenVSwitch, Quantum, OMF, FreeIPA etc.) of the different partners into one prototype or demonstrator

Many thanks!

…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.

*Die in dieser Publikation enthaltenen Informationen stehen im Eigentum der folgenden Projektpartner des vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projektes „**VISA**“: DECOIT GmbH, Collax GmbH, IT-Security@Work GmbH, FH Dortmund, Fraunhofer SIT und NICTA. Für in diesem Dokument enthaltenen Information wird keine Garantie oder Gewährleistung dafür übernommen, dass die Informationen für einen bestimmten Zweck geeignet sind. Die genannten Projektpartner übernehmen keinerlei Haftung für Schäden jedweder Art, dies beinhaltet, ist jedoch nicht begrenzt auf direkte, indirekte, konkrete oder Folgeschäden, die aus dem Gebrauch dieser Materialien entstehen können und soweit dies nach anwendbarem Recht möglich ist.*