GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Design und Implementierung von Virtual Security Appliances (VSA)

Prof. Dr. Kai-Oliver Detken,
DECOIT GmbH

VISA

Agenda

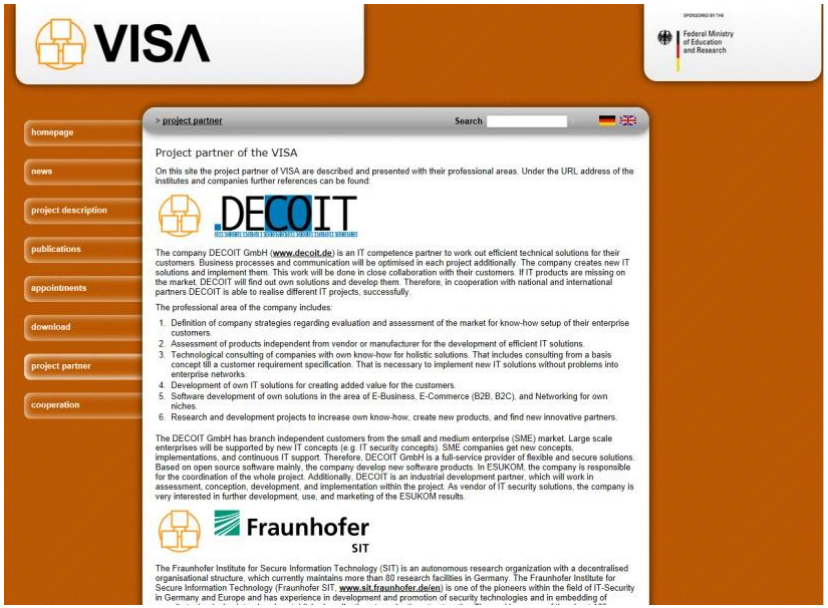
- Simulation von Server- und Netzwerkkomponenten
- Virtuelle Umgebungen analysieren und ausrollen
- Erheben einer bestehenden IT-Infrastruktur
- Experiment-Steuerung und Messung
- Automatisierte Konfiguration von VSAs
- Fazit und Ausblick

Simulation von Server- und Netzwerkkomponenten

VISA

Das VISA-Projekt

- Gefördert durch das BMBF
- Förderprogramm: KMU Innovativ
- VISA startete im August 2011 und endet im September 2013
- Das Gesamtbudget beträgt: 1,7 Mio. €
- Partners des Projektes sind:
  - DECOIT GmbH (Projektleitung)
  - Fraunhofer SIT
  - University of Applied Sciences Dortmund
  - Collax GmbH
  - IT-Security@Work GmbH
  - National ICT Australia Limited



www.visa-project.de

Projektziele

- Es ist das Ziel des VISA-Projektes, durch Nutzung von Virtualisierungstechnologien das Management von IT-Infrastrukturen, insbesondere der Sicherheits-komponenten, zu erleichtern und zu unterstützen
- Diese Unterstützung basiert auf drei Kernmerkmalen:
  - Simulation und Evaluierung der gesamten IT-Infrastruktur in virtuellen Umgebungen
  - Realisierung von Sicherheitsanwendungen als virtuelle Komponenten, sog. Virtual Security Appliances (VSA)
  - Vereinfachung und Nachweisbarkeit der Einhaltung von IT-Standards, IT-Security- und Compliance-Anforderungen durch geeignet entwickelte VSAs als fertig verwendbare IT-Bausteine

VSA-Entwicklung

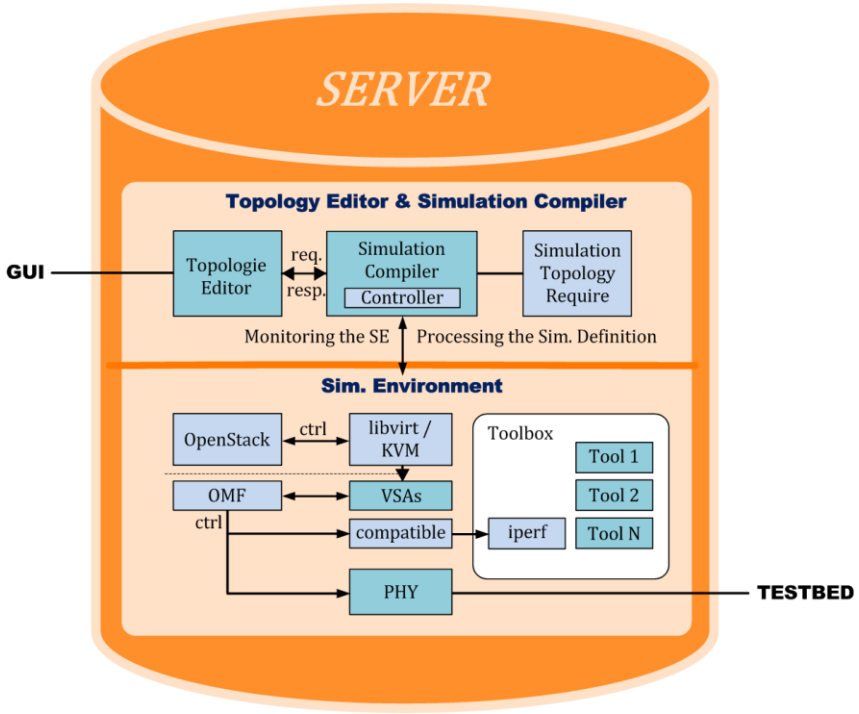
- Im VISA-Projekt wurden VSAs konzeptioniert, die vorrangig der Sicherheit dienen (von Netzwerksicherheit bis Anwendungssicherheit)
- Die VSAs bestehen im Wesentlichen aus virtualisierten IT-Security-Bausteinen (Modulen) und Services
- Sie haben das Ziel, unterschiedliche Bereiche der IT-Sicherheit in typischen KMU-Topologien abzudecken
- Folgende VSAs wurden im VISA-Projekt umgesetzt:
  - VSA-AAA (FH Dortmund)
  - VSA-SRC (DECOIT)
  - VSA-MAC (DECOIT)
  - VSA-DMZ (Collax)

Virtuelle Umgebungen analysieren und ausrollen

VISA

Simulationskomponenten

- Topologie Editor (TE)
  - GUI zur Verwaltung der Netz-/Servertopologie
  - Interworking zum SC
- Simulation Compiler (SC)
  - Simulationsbeschreibung und -definition mit Hilfe von Ontologien
  - Interworking zum TE
- Simulation Environment (SE)
  - Virtuelle Plattform auf Basis von OpenStack, libvirt und KVM
  - OpenStack dient zur Verwaltung der VMs
  - libvirt stellt einheitliche API zur Verfügung
  - KVM bietet die VMs an



Topologie Editor (TE)

- Der TE bietet dem Benutzer die Möglichkeit eine bereits bestehende Topologie zu bearbeiten und dieser neue Komponenten hinzuzufügen
- Es kann auch eine neue bzw. bestehende Topologie manuell modelliert werden
- Das Back-end besteht aus dem TE-, RDF- und HTTP-Modul

Netzwerkanalyse

- Es können vordefinierte Netzwerktests durch den TE angestoßen werden
- Die virtuelle IT-Infrastruktur kann dadurch auf u.a. Performance, Verfügbarkeit und Konfigurationsfehler getestet werden
- Die Tests lassen sich wie folgt unterteilen
  - Simulation von Angriffen
  - Messung der Auswirkungen
  - Emulation von Netzparametern
- Das cOntrol and Management Framework (OMF) ermöglicht es zudem skriptgesteuerte Programme in den VMs zu starten, um Angriffe simulieren zu können
- Die wichtigsten Analysetools, die direkt aus dem TE gestartet werden können, sind: Nmap, iperf, T-50, collectd, netem, Otg2

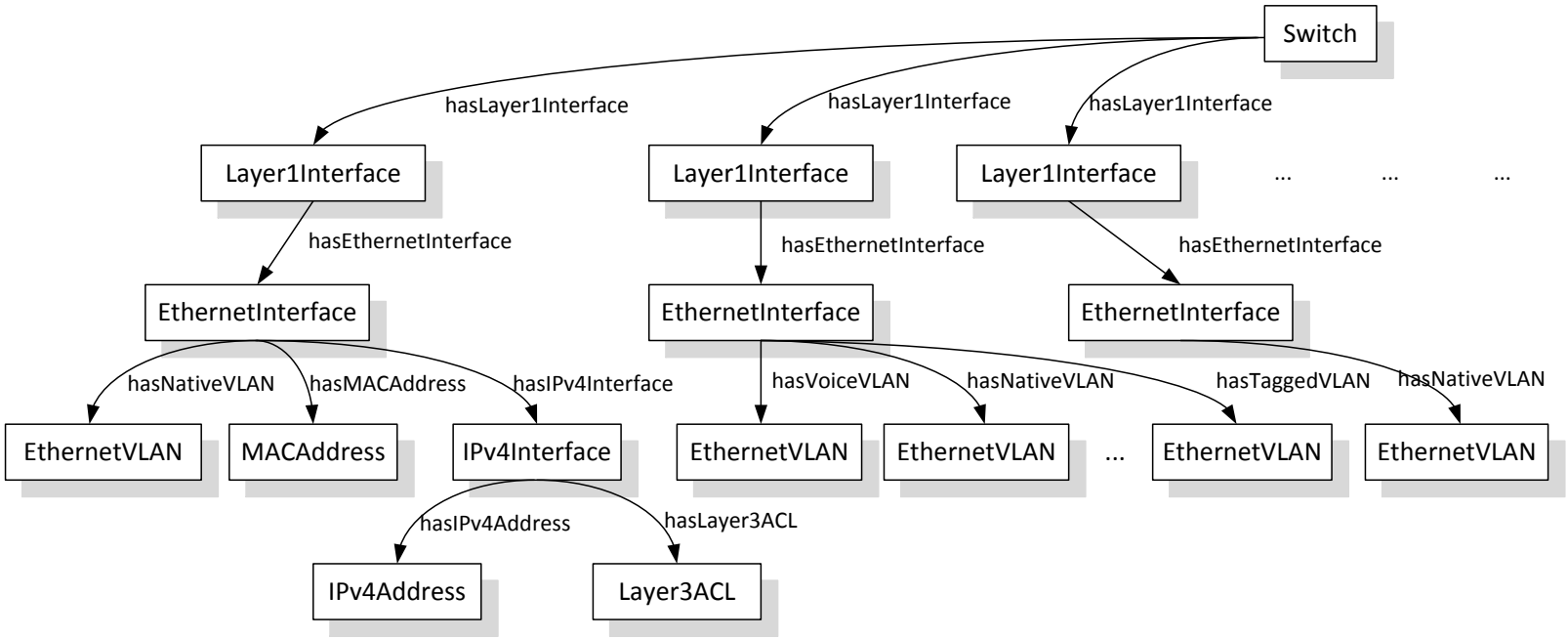
Erheben einer bestehenden IT-Infrastruktur

VISA

IO-Tool-Set

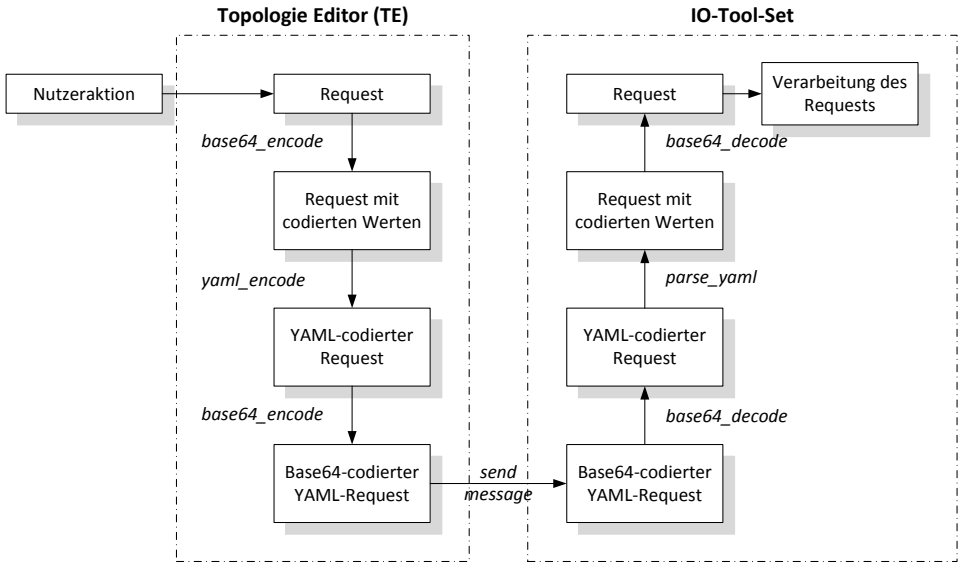
- Das IO-Tools-Set stellt Methoden zur Verfügung, den Ist-Zustand einer IT-Infrastruktur zu akquirieren, aufzubewahren und automatischen Weiterverarbeitungsprozessen zur Verfügung zu stellen
- Um die Anforderungen verschiedenartiger Verbraucher (z.B. dem TE) zu gewährleisten, werden IT-Asset-Informationen mit Hilfe einer ontologischen Repräsentation semantisch verknüpft und vorgehalten
- Die durch das IO-Tool-Set verwendete formale Repräsentation ist in der Lage komplexe und geschachtelte Netz-Topologien abzubilden, wie sie in Unternehmen typischerweise zu finden sind
- Als Datenformat für die Repräsentation der Ontologie kommt die Web Ontology Language (OWL) zum Einsatz

Ausschnitt eines IT-Assets



Kommunikation TE und IO-Tool-Set

- Die in der Ontologie hinterlegten IT-Asset-Informationen werden unter Verwendung von spezialisierten Query-Modulen in eine Simulationsdefinition konvertiert
- Das Query-Modul ermittelt dazu die Parameter, die zur Erstellung der virtuellen Umgebung in OpenStack notwendig sind und führt eine entsprechende Konfiguration der Virtualisierungsumgebung durch
- Änderungen an der in der Ontologie hinterlegten Netz-Topologie kann man mittels des TE vor der Erstellung einer virtuellen Umgebung vornehmen
- Die Kommunikation zwischen TE und IO-Tool-Set findet mit Hilfe textbasierte Nachrichten über eine TLS-Verbindung statt (IO-X)

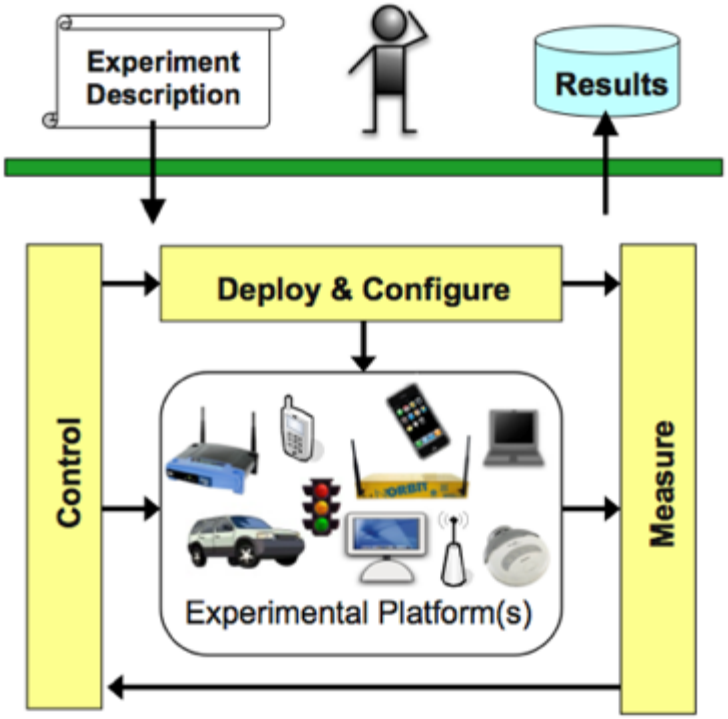


Experiment-Steuerung und Messung

VISA

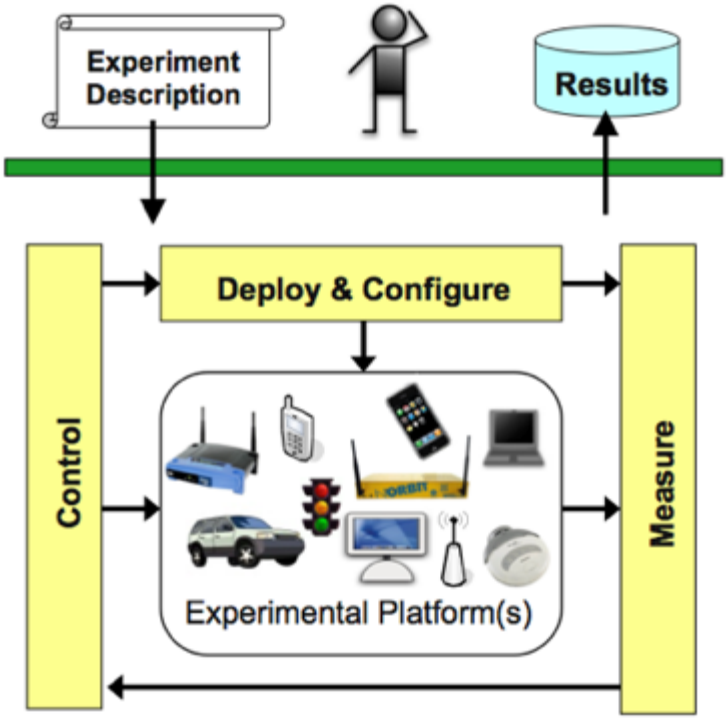
OMF-Framework (1)

- OMF ist ein Framework für die Durchführung von Experimenten auf einem Testbed
- Jeder am Experiment teilnehmende Knoten (Rechner/VM) führt dazu den OMF Resource Controller (RC) aus
- Dieser Dämon meldet sich an einem XMPP-Server an und wartet auf Befehle
- Der Experiment Controller (EC) ist die Software, die der Benutzer ausführt, um das Experiment zu steuern
- Dazu liest dieser ein vom Benutzer geschriebenes Skript ein, welches in der OEDL-Sprache (Ruby) verfasst ist
- Während des Experimentes sendet der EC die Befehle an verschiedene PubSub-Gruppen auf dem XMPP-Server, die wiederum von den RCs abonniert werden
- Die RCs senden ggf. Antworten, auf die der EC dann reagieren kann

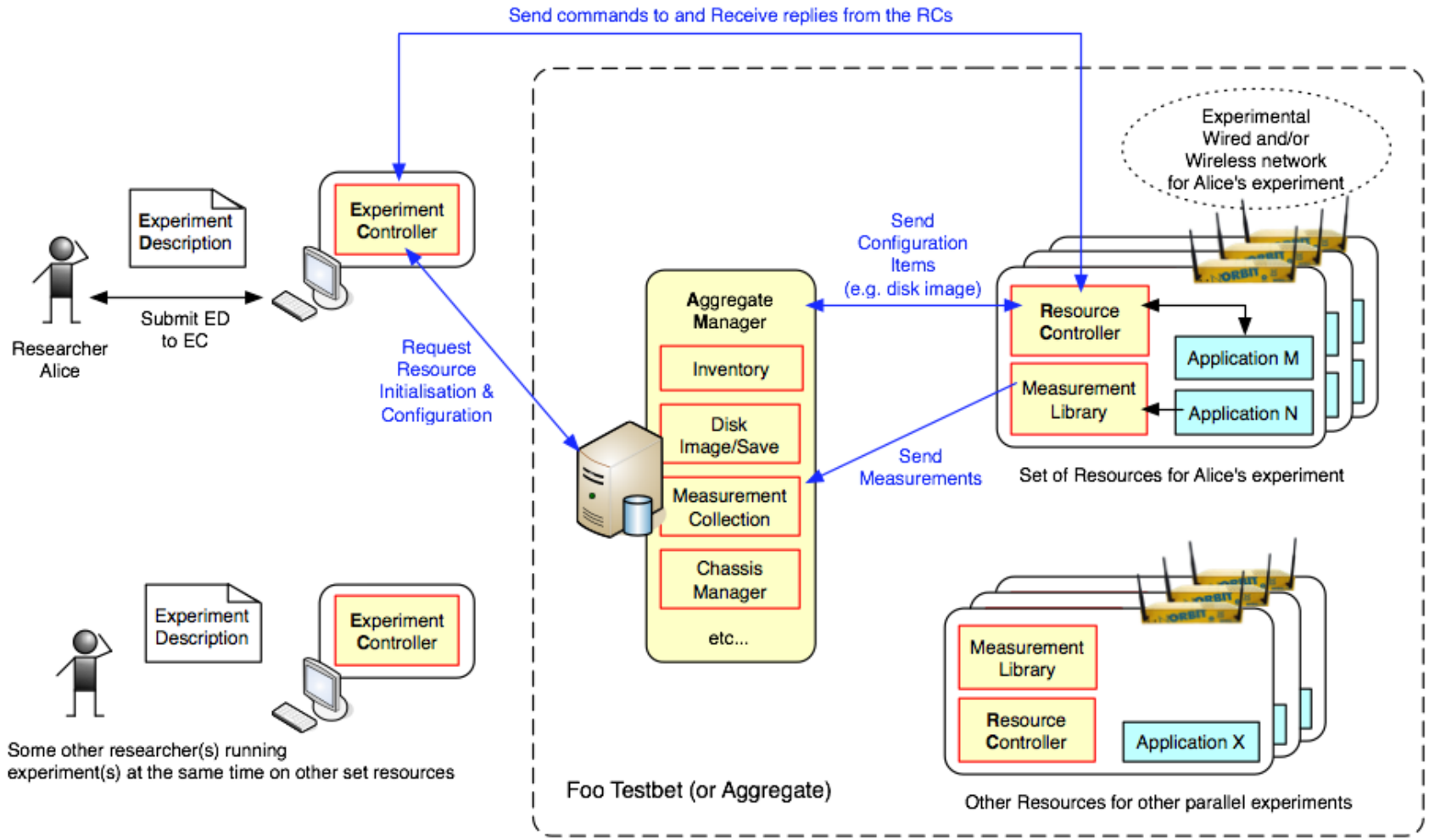


OMF-Framework (2)

- Eine weitere Komponente von OMF-Testbeds ist der Aggregate Manager (AM)
- Diese Komponente kann verschiedene Dienste im Testbed bereitstellen, z.B. die Dienste
  - Chassis Manager (CM): kann Knoten ein- und ausschalten
  - PXE-Dienst: kann Knoten über das Netzwerk booten
- VISA verwendet das OMF-Framework, um die Experimente in den VSAs zu steuern
  - Auf jeder VSA läuft der OMF Resource Controller (RC), der es dem Experimentator ermöglicht Programme zu starten und Messungen vorzunehmen
  - Der OEDL-Code für den OMF Experiment Controller (EC) wird vom VISA Simulation Compiler (SC) generiert



OMF-Systemarchitektur



Evaluierung von VSAs

- Um die Auswirkungen eines Experiments auf die VMs und Netzkomponenten zu messen, verwendet das VISA-Projekt die OML-Messbibliothek
- Diese C-Bibliothek kann man gegen existierende Programme verlinken, in deren Quellcode dann Messpunkte definiert werden können
- Zur Laufzeit lassen sich dann die Messpunkte an OML weitergereicht, woraufhin sie an einen OML-Server gesendet werden
- Dieser Server speichert dann alle eingehenden Messpunkte von den verschiedenen Knoten in einer Datenbank für das jeweilige Experiment, was die Analyse nach dem Experiment vereinfacht

Automatisierte Konfiguration von VSAs

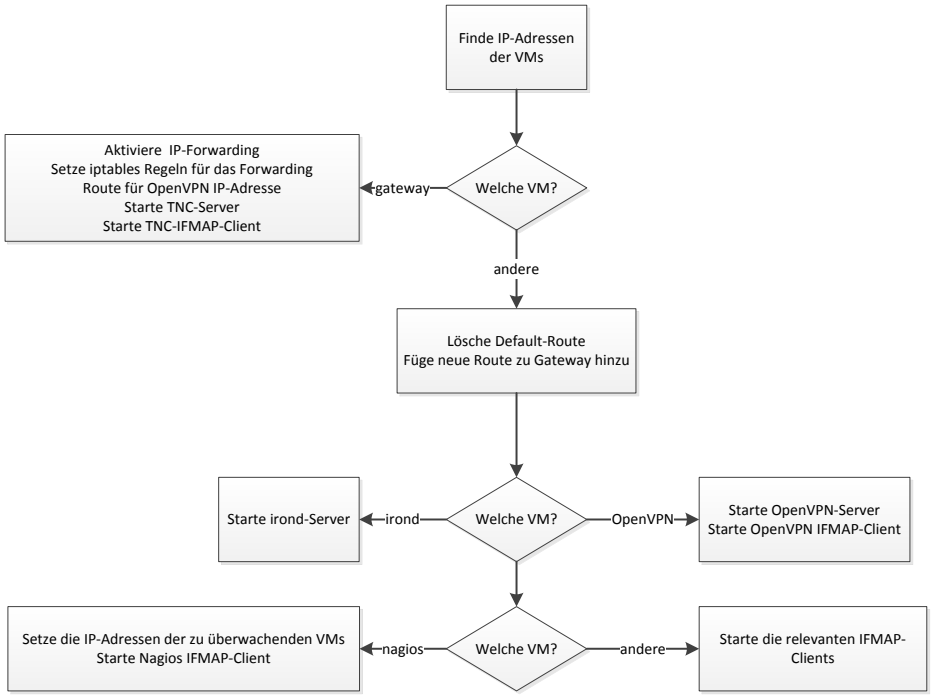
VISA

Autokonfiguration durch Puppet

- Ein weiteres Ziel des VISA-Projektes war es, dem Benutzer es auf einfache Art und Weise zu ermöglichen, den Sicherheitsstatus seines Netzes zu erhöhen
- Dafür wurden die VSAs entwickelt, die über den TE einer bestehenden IT-Infrastruktur hinzugefügt werden
- Aber auch die bereits vorkonfigurierten VSAs benötigen einige Informationen, die erst beim Instanziieren zur Verfügung stehen (z.B. IP-Adresse, Anpassen von Konfigurationsdateien)
- Um die einfache Einbindung gewährleisten zu können, müssen die VMs der VSA sich selbst konfigurieren
- Um dieses Ziel zu erreichen wurde im VISA-Projekt das Tool Puppet verwendet

Ablauf der automatischen Konfiguration

- Puppet ist ein Konfigurationsmanagement-Tool für Unix-basierte Betriebssysteme
- Hierbei werden auf einem zentralen Server die Konfigurationen der verschiedenen Computer angelegt und verwaltet
- Dazu werden am Anfang Templates deklariert, die einen bestimmten Zustand eines Systems beschreiben
- Dieser Zustand kann Pakete, Dienste, Dateien oder auch das Ausführen von Konsolenkommandos beinhalten
- Dabei eignet sich Puppet sowohl für einzelne Computer, als auch für Verbünde



Fazit und Ausblick

Fazit

- Die hier aufgezeigte VISA-Plattform ermöglicht
  - die Erhebung bestehender IT-Infrastrukturen
  - die Umsetzung in eine virtuelle Umgebung
  - die Emulation verschiedener Konfigurationen
  - das erneute Ausrollen der VSAs in eine reale Umgebung
- Dadurch erhält der IT-Administrator vorgefertigte IT-Bausteine, die er mittels Autokonfiguration relativ leicht in seine Umgebung einfügen und testen kann
- Neben dem Mehrwert der neuen Dienste erhält das Unternehmen somit auch gleichzeitig eine Möglichkeit an die Hand die Compliance seiner IT-Infrastruktur zu verbessern
- Dadurch wird das Sicherheitsniveau von Unternehmen letztendlich erhöht, ohne dass das entsprechende Spezialwissen vorgehalten werden muss

Ausblick

- Das VISA-Projekt endet im September 2013
- Es hat innerhalb der Projektlaufzeit seine Ziele erreicht
- So konnte u.a. ein gesamter Simulationskreislauf abgebildet werden
- Es gibt aber auch noch offene Fragestellungen, die evtl. in einem Nachfolgeprojekt zum tragen kommen:
  - Direkte TE-Anbindung an OpenStack
  - Direkte TE-Aufnahme von IT-Infrastrukturen
  - Compliance dokumentieren und Audit-gerecht bereitstellen
  - Erweiterte Fehlererkennung für falsch konfigurierte Netze

Vielen Dank!

…für die Aufmerksamkeit

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.