GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Statustreffen der Forschungsvorhaben der IT-Sicherheitsforschung

Das VISA-Projekt

am 17.-18.09.13 in Darmstadt

Dr. Carsten Rudolph, Fraunhofer SIT

Prof. Dr. Kai-Oliver Detken, DECOIT GmbH

VISA

Agenda

- Projekteinführung
- Schaffung virtueller Infrastrukturen
- Virtual Security Appliance (VSA)
- Fazit und Ausblick

Projekteinführung

Projektumfang, -ziele und Konsortium

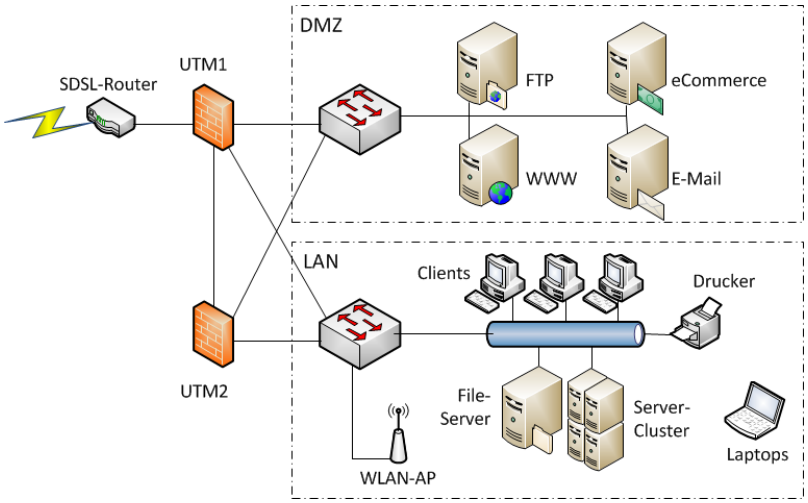
VISA

Projektübersicht

- Das VISA-Projekt (www.visa-project.de) startete im August 2011 und endet im September 2013
- Es handelt sich um ein BMBF-gefördertes Projekt aus dem Arbeitsprogramm „KMU Innovativ“, mit einem Gesamtvolumen von 1,7 Mio. Euro
- Projektpartner sind:
  - DECOIT (Konsortialführer) in Bremen
  - Collax GmbH in München
  - Fraunhofer SIT in Darmstadt
  - Fachhochschule Dortmund in Dortmund
  - IT-Security@Work in Mainz
  - NICTA in Sydney, Australien

Hintergrund des Projektes

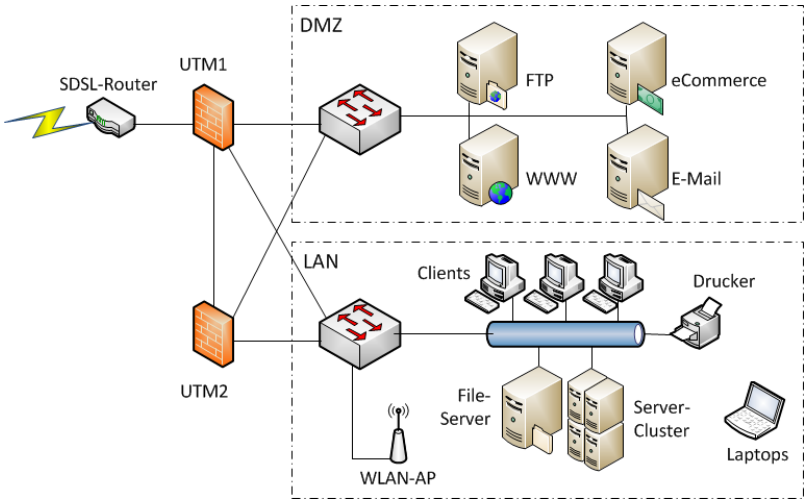
- IT-Infrastrukturen sind mittlerweile auch schon in kleinen und mittelgroßen Unternehmen (KMU) sehr komplex
- Die Auswirkungen von Änderungen an solchen Infrastrukturen sind oft erst im Echtbetrieb zu erkennen
- Die Integration neuer Sicherheitskomponenten erfordert oft die Integration neuer Hardware und den Umbau der Netztopologie
- Hierbei fehlt oft das entsprechende Wissen in KMUs, so dass Umsetzungen oft ohne eine genaue Kenntnis der Auswirkungen vorgenommen wird



Typische KMU-Netzumgebung

Projektziele (1)

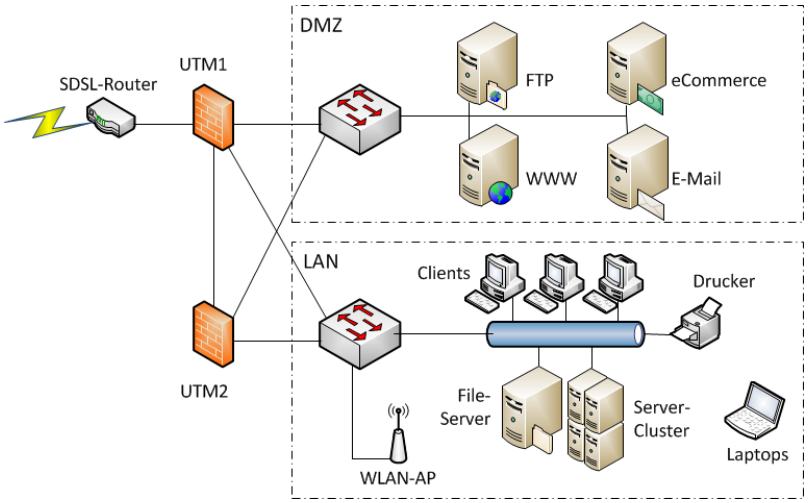
- Daher muss für Klein- und Mittelständische Unternehmen (KMUs) der Umgang mit IT-Infrastrukturen vereinfacht werden
- Dies kann erreicht werden durch:
  - Einsatz von Virtualisierung und Simulation von IT-Infrastruktur
  - Realisierung KMU-gerechter Darstellung und Bedienbarkeit der resultierenden Sicherheitsfunktionalität
- Es war daher das Ziel des Projektes VISA, durch Nutzung von Virtualisierungstechnologien das Management von IT-Infrastrukturen, insbesondere der Sicherheitskomponenten zu erleichtern und zu unterstützen



Typische KMU-Netzumgebung

Projektziele (2)

- Die Unterstützung basiert auf zwei Kerntechnologien:
  - Simulation und Evaluierung der gesamten IT-Infrastruktur in virtuellen Umgebungen
  - Realisierung von Sicherheitsanwendungen als virtuelle Komponenten, sog. Virtual Security Appliances (VSA)
- Durch das VISA-Rahmenwerk wird der passgenaue und vereinfachte Einsatz von Sicherheitsanwendungen auf Basis von Virtual Security Appliances (VSA) ermöglicht
- Durch die umfassende Emulation der IT-Infrastrukturen können die betriebsrelevanten Parameter und die Integrationspunkte der VSAs bereits in der virtuellen Umgebung identifiziert und der Einsatz erprobt werden
- Dadurch ergibt sich eine Vereinfachung und Nachweisbarkeit der Einhaltung von IT-Standards, IT-Sicherheits- und Compliance-Anforderungen



Typische KMU-Netzumgebung

Projektkonsortium

- DECOIT
  - Projektmanagement
  - Entwicklung von zwei VSAs
  - Entwicklung eines Topologie Editors
  - Einbettung der Analysewerkzeuge
- Collax
  - Weiterentwicklung der eigenen Produkte
  - Entwicklung einer eigenen VSA
  - Entwicklung eines Topologie-Editors für eigene Umgebung
- Fraunhofer SIT
  - Technische Projektbegleitung
  - Entwicklung einer Attacker VM
  - Entwicklung eines Ontologie-Toolsets
- IT-Security@Work
  - Definition und Kontrolle der Compliance-Anforderungen
  - Evaluierung der Compliance der VSAs
- Fachhochschule Dortmund
  - Entwicklung einer eigenen VSA
  - Entwicklung eines Topologie Editors für LISA-Umgebung
- NICTA
  - Bereitstellung und Weiterentwicklung des OMF-Rahmenwerks

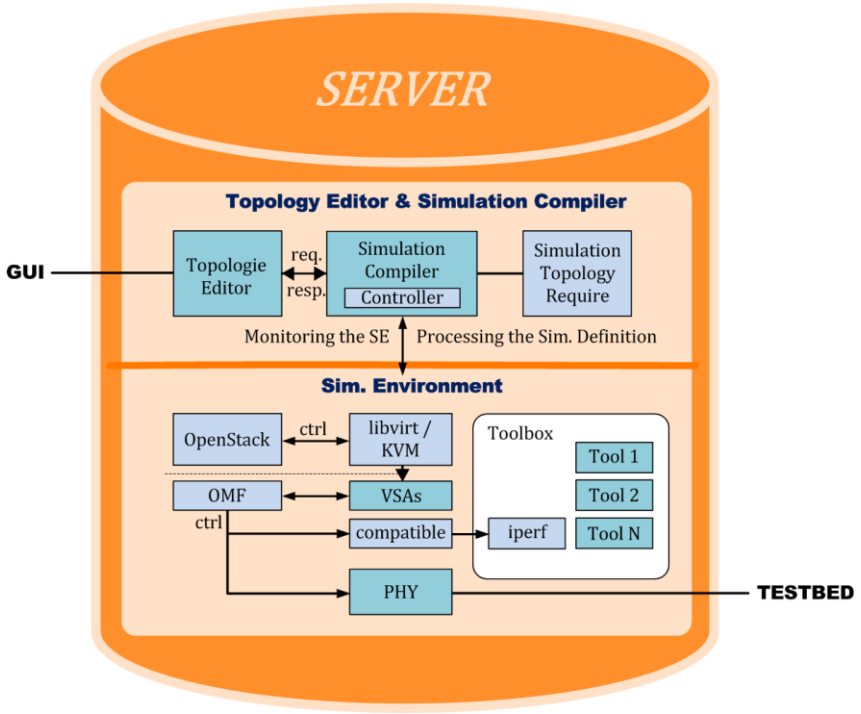
Schaffung virtueller Infrastrukturen

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
  - libvrt stellt einheitliche API zur Verfügung
  - KVM bietet die VMs an



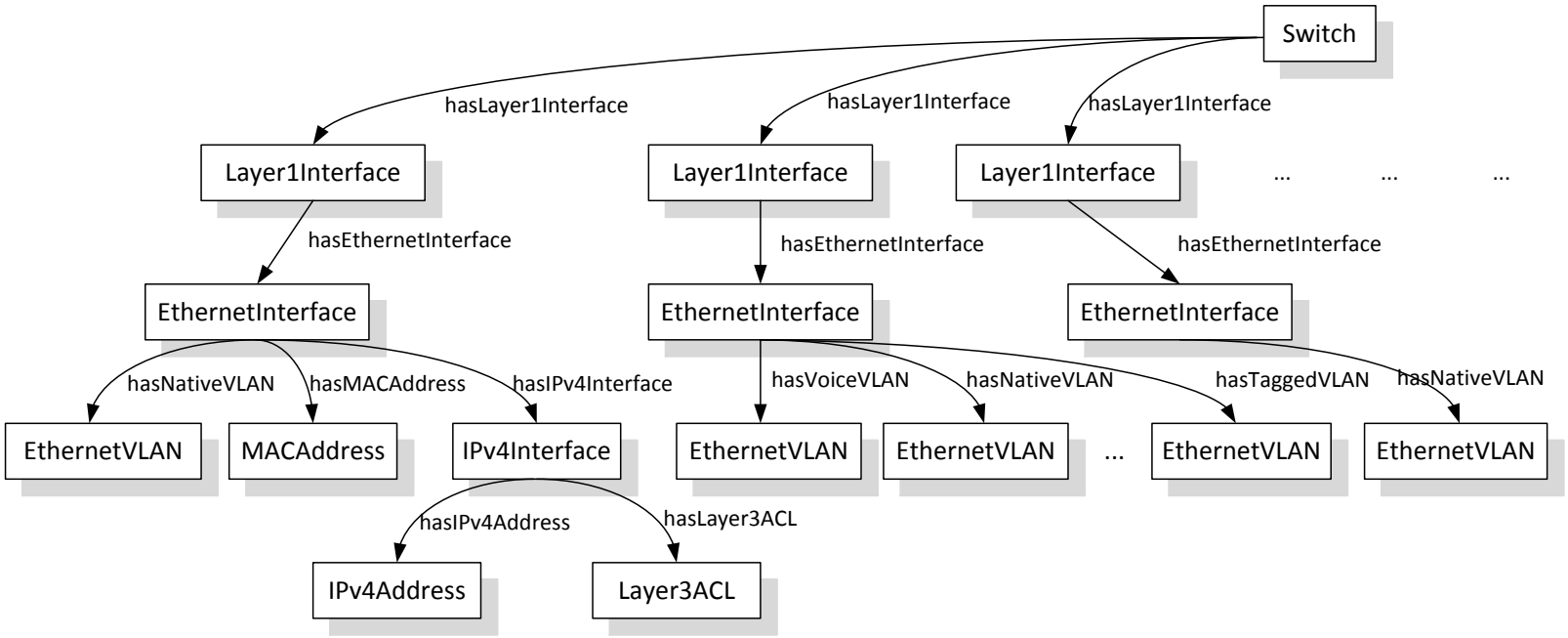
Topologie Editor (TE)

- 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

IO-Tool-Set

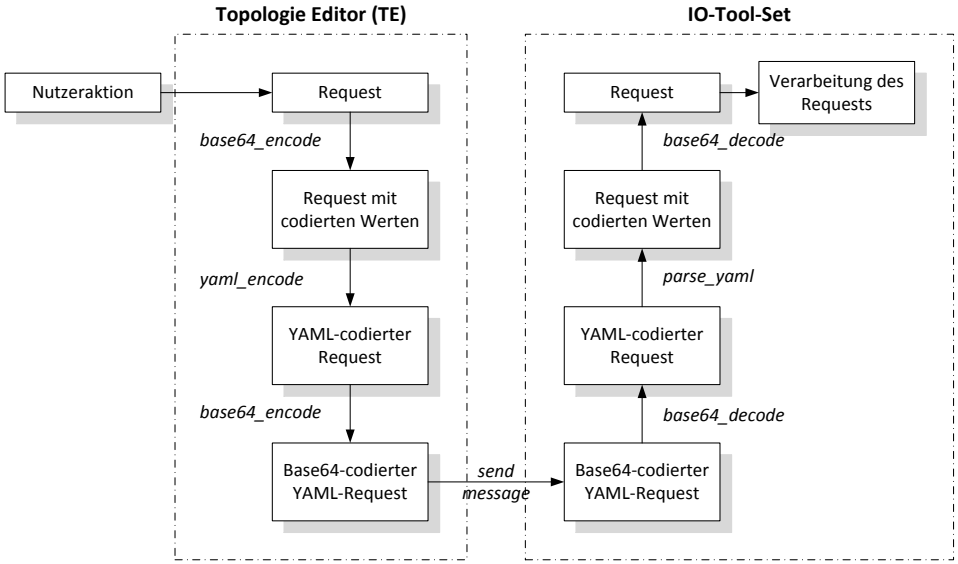
- Das IO-Tools-Set stellt Methoden zur Verfügung, den Ist-Zustand einer IT-Infrastruktur zu akquirieren, aufzubewahren und automatischen Weiterverarbeitungsprozessen zur Verfügung zu stellen
- Um die Anforderungen verschiedenartiger Verbraucher (z.B. dem TE) zu gewährleisten, werden IT-Asset-Informationen 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

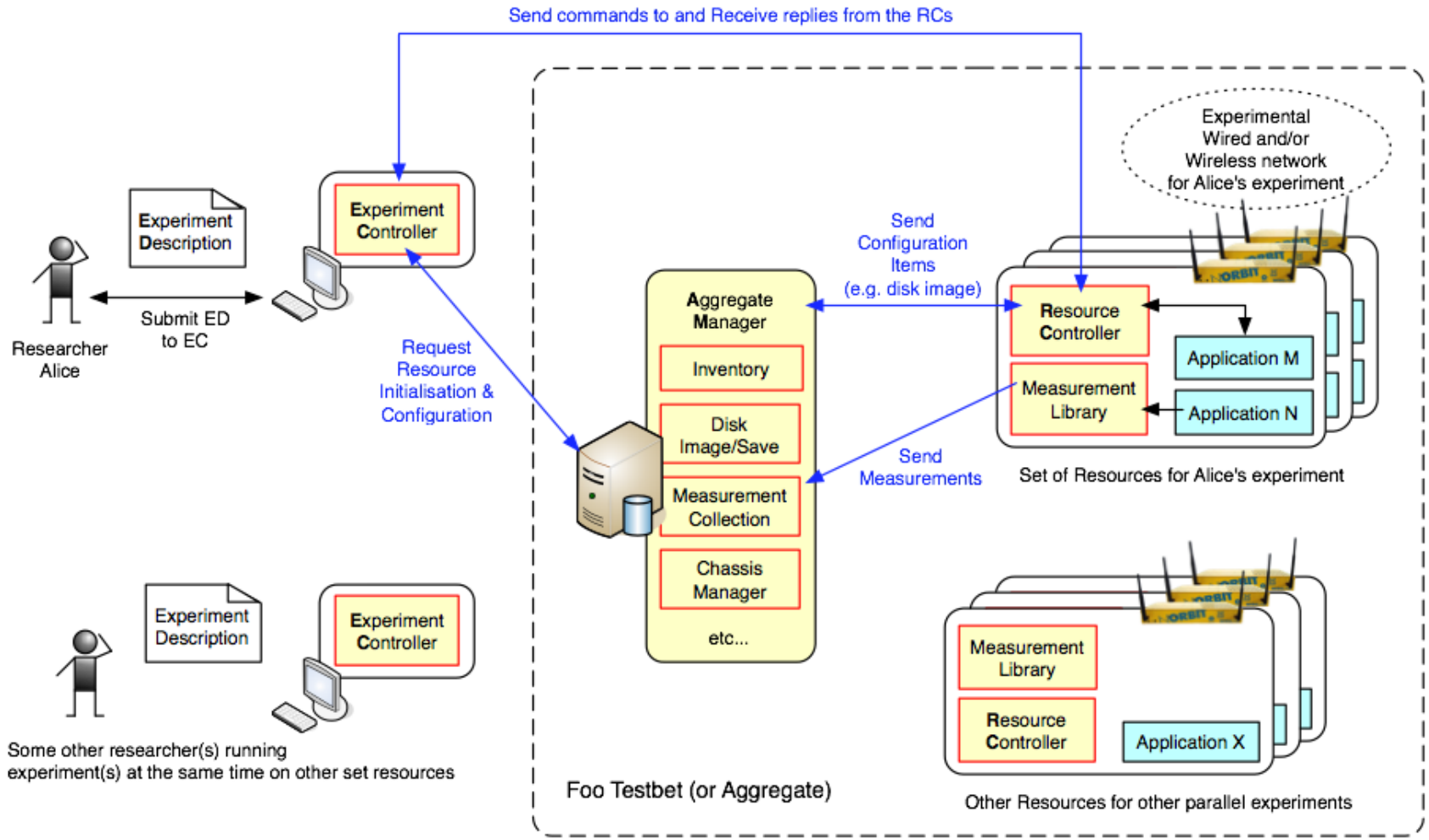
- Die in der Ontologie hinterlegten IT-Asset-Informationen werden unter Verwendung von spezialisierten Query-Modulen in eine Simulationsdefinition konvertiert
- Das Query-Modul ermittelt dazu die Parameter, die zur Erstellung der virtuellen Umgebung in OpenStack notwendig sind und führt eine entsprechende 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)



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

OMF-Systemarchitektur



Virtual Security Appliance (VSA)

Zwei VSA-Beispiele:
VSA-SRA und VSA-MAC

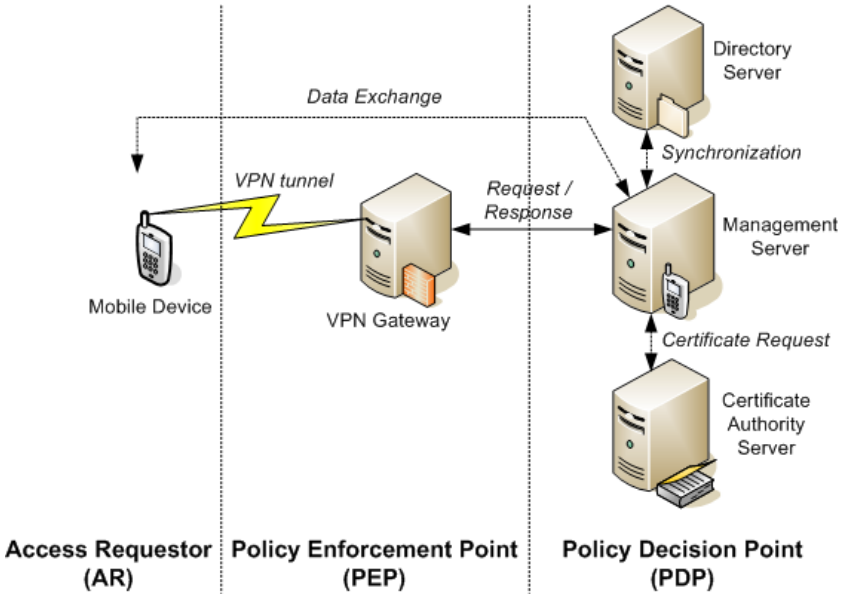
VISA

VSA-Entwicklung

- Es wurden im VISA-Projekt die 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)

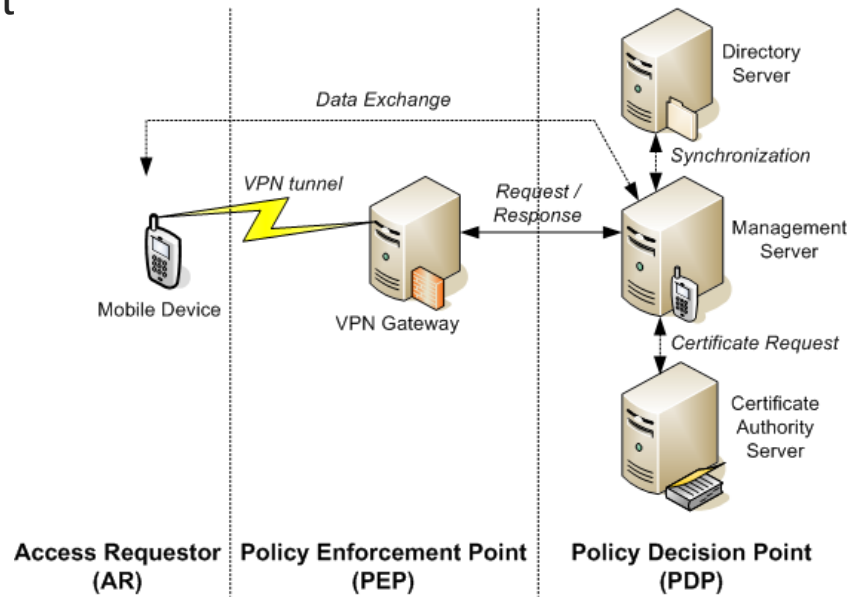
VSA-SRA (1)

- Die *VSA-SRA* ermöglicht das sichere Einwählen in ein Firmennetz mittels eines Android-Smartphones
- Dies beinhaltet die Komponenten Android-Client, FreeRADIUS-Server, TNC-Server und VPN-Gateway
- Das Smartphone verbindet sich durch das VPN-Gateway mit dem Unternehmensnetz
- Dadurch ist aber noch nicht sichergestellt, ob das Smartphone als vertrauenswürdig eingestuft werden kann, da nur die Teilnehmerdaten abgefragt werden
- Dies wird erst durch das Senden gesammelter Metriken des Android-Smartphones vom TNC-Client an den TNC-Server ermöglicht
- Die Metriken enthalten die installierte Applikationsbasis, Versionsnummern und Richtlinien, die für das Smartphone gelten



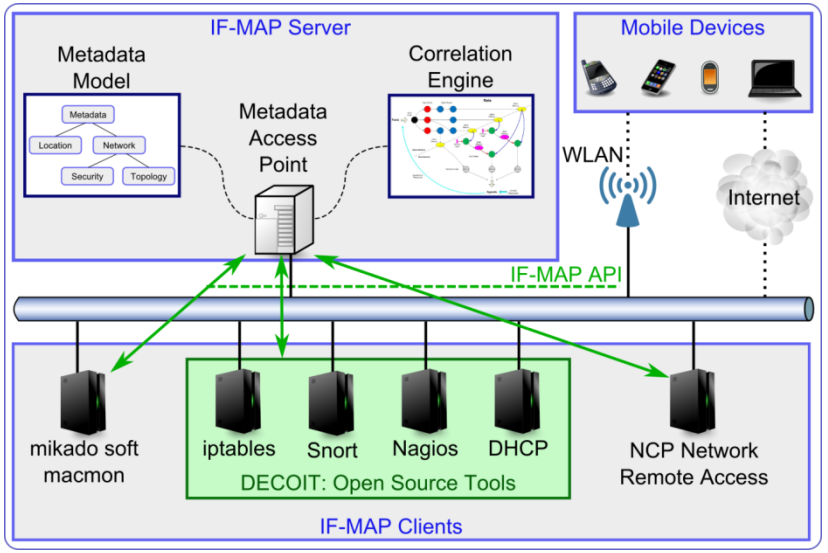
VSA-SRA (2)

- Der TNC-Server vergleicht anschließend die gesendeten Metriken mit denen in seiner Datenbank
- Sind Applikationen installiert, die er nicht kennt oder die auf seiner Blacklist enthalten sind, wird dem Smartphone der Zugang verweigert bzw. das Smartphone wird in ein Quarantänenetz isoliert
- Innerhalb des Quarantänenetzes kann das Endgerät mithilfe einer Softwareverteilungslösung auf den geforderten aktuellen Stand gebracht werden
- Anschließend kann das Gerät gemäß den TNC-Spezifikationen eine erneute Attestierung anfordern
- Sind alle Voraussetzungen erfüllt, erhält der Teilnehmer des mobilen Endgeräts Zugriff auf die gewünschte Zielapplikation und somit auf die gewünschten Zielressourcen



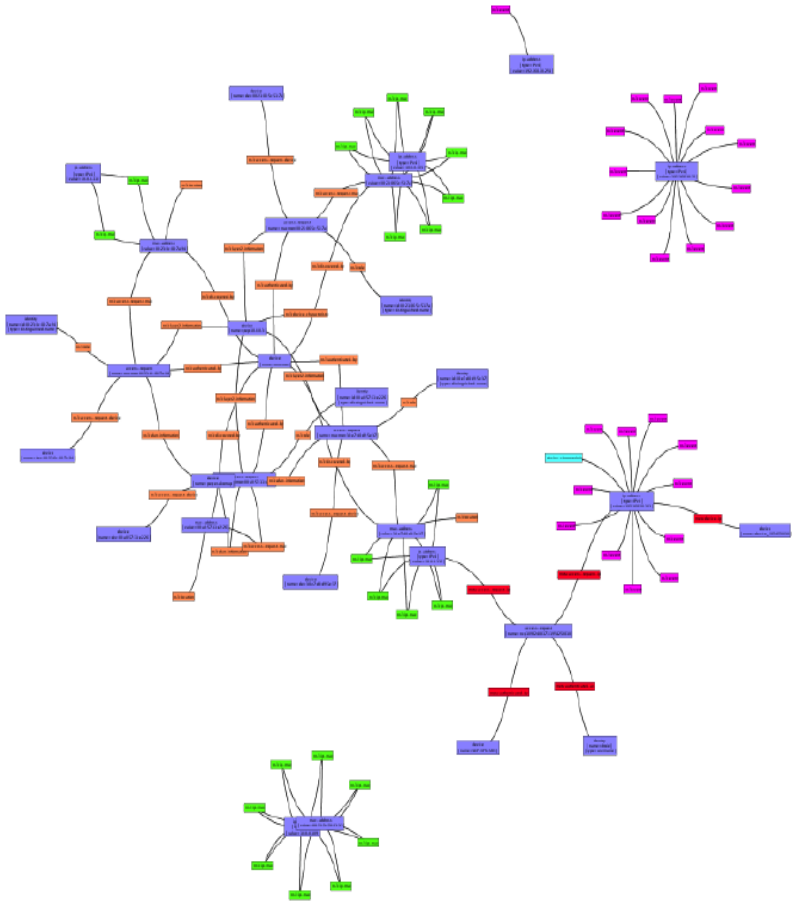
VSA-MAC (1)

- Die *VSA-MAC* besteht hingegen aus den Komponenten IF-MAP-Server und den IF-MAP-Clients für Android, Snort, iptables, FreeRADIUS und Nagios
- Bei IF-MAP handelt es sich um ein offenes, herstellerunabhängiges Client-Server-Netzprotokoll zum Austausch von beliebigen, in XML codierten Metadaten
- Dabei stellt der IF-MAP-Server die zentrale Komponente dar, indem die Daten von allen IF-MAP-Clients gesammelt und durch einen Graphen zur Verfügung gestellt werden
- Weiterhin stellt er die gesammelten Daten auch den IF-MAP-Komponenten zur Verfügung



VSA-MAC (2)

- Die Stärke von IF-MAP gegenüber einer reinen IDS-basierten Anomalie-Erkennung liegt dabei in der Diversität der Daten
- Durch die gesammelte Datenbasis lassen sich Korrelationen durchführen und Anomalien leichter erkennen bzw. Angriffen entgegenwirken
- Beispiele hierfür sind u.a. die Blockierung des Datenstroms durch eine Firewall, Sperren des Zugriffes in Form eines Switches oder eines VPN-Gateways, Isolierung des Endgerätes in eine Quarantänezone etc.
- Auf Grundlage der gesammelten Informationen können die Details protokolliert und entsprechende Meldungen an die verantwortlichen Systemadministratoren generiert werden



Fazit und Ausblick

Erreichte Ziele und offene Aufgaben

VISA

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 alle erreicht
- So konnte u.a. ein gesamter Simulationskreislauf abgebildet werden
- Es gibt aber auch noch offene Fragestellungen:
  - Direkte TE-Anbindung an OpenStack
  - Direkte TE-Aufnahme von IT-Infrastrukturen
  - Verbesserte Autokonfiguration
  - Compliance dokumentieren und Audit-gerecht bereitstellen
  - Erweiterte Fehlererkennung für falsch konfigurierte Netze

Vielen Dank

für Ihre 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.