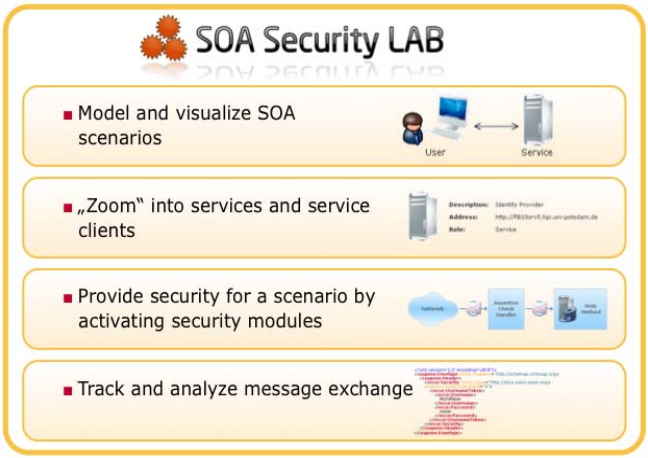
Ein Experimentierbaukasten für SOA – Entwicklung einer Experimentalplattform für die den sicheren Einsatz von SOA Technologien in der Praxis

Sicherheit in SOA

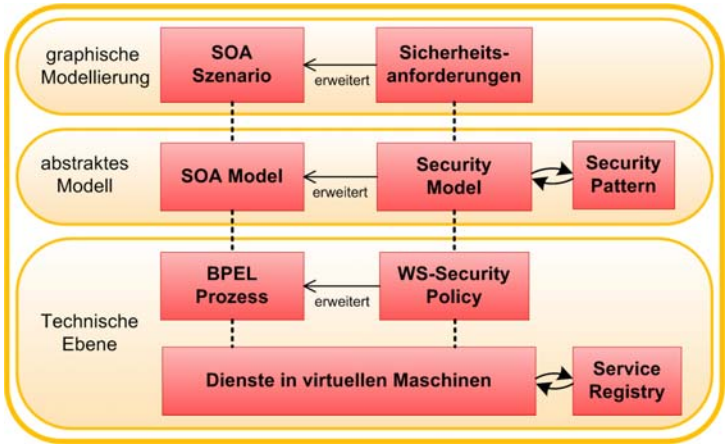
Service-orientierte Architekturen ermöglichen die Umsetzung von verteilten und lose-gekoppelten Systemen, in denen Funktionalität als Dienst angeboten wird. Dies ermöglicht die flexible Nutzung und Orchestrierung dieser Dienste zur Ausführung von Geschäftsprozessen – insbesondere auch über Unternehmensgenzen hinaus. Im Gegensatz zu traditionellen Architekturen stellt diese flexiblere Nutzung von Diensten allerdings auch umfassendere Anforderungen an die Sicherheit.



Die Absicherung von Service-orientierten Architekturen geht einher mit einer hohen Komplexität, die durch die große Anzahl an möglichen Ansätzen, Technologien und Standards bedingt ist. Dieses Projekt verfolgt das Ziel einen Experimentierbaukasten für SOA Technologien bereitzustellen, mit dem unter Vorgabe von Sicherheitszielen mögliche Sicherheitsmechanismen ausgewählt, erprobt und analysiert werden können. Als Grundlage soll das SOA Security Lab dienen, dass eine Plattform bietet um den Nachrichtenaustausch in SOA-Szenarien zu visualisieren.

Ein Experimentierbaukasten für sichere SOA-Technologien

Der Experimentierbaukasten für SOA soll eine webbasierte Plattform sein, der die graphische Modellierung eines SOA Szenarios und darauf aufbauender Anwendungsfälle ermöglicht. Während die grundlegende SOA-Infrastruktur durch die involvierten Teilnehmer in Form von Diensten und Clients bestimmt wird, stellt der Anwendungsfall konkrete Abläufe hinsichtlich der Verwendung dieser Dienste dar. Zudem bietet die Modellierungsebene eine adäquate Grundlage, um die Sicherheitsanforderungen für ein SOA-Szenario zu spezifizieren.



Basierend auf diesen Beschreibungen soll ein ausführbares Szenario konfiguriert werden, in dem

1) Dienste, die in virtuellen Maschinen vorkonfiguriert sind, für den Benutzer bereitgestellt werden und mittels BPEL orchestriert werden.
2) die in der Modellierung spezifizierten Sicherheitsanforderungen auf Sicherheitspolicies abgebildet werden, welche die Dienste in den virtuellen Maschinen konfigurieren und bestimmte Sicherheitsmechanismen wie bspw. Nachrichtenverschlüsselung vorgeben.

Der Benutzer kann dieses Szenario dann ausführen und anschließend über das SOA Security LAB die ausgetauschten Nachrichten und die verwendeten Protokolle graphisch nachvollziehen und analysieren.

Projektvorbereitung

Im Rahmen der Vorbereitungsphase werden die benötigten Technologien und Spezifikationen, deren Kenntnis für Umsetzung des Projektes erforderlich ist erarbeitet:

- Grundlagen der Webprogrammierung: Java und Grails
- Einarbeitung in Web Service Technologien and Spezifikationen (SOAP, WSDL, UDDI, WS-Policy, WS-Security, WS-Federation, WS-Trust, SAML …)
- Einarbeitung in SOA- und Sicherheitskonzepte
- Modellierung in FMC und UML

Aufgabenliste

- Konzeption und Umsetzung einer Webplattform zur Modellierung von SOA Szenarien, die eine SOA-Infrastruktursicht sowie eine Sicht der betrachteten Anwendungsfälle umfasst.
- Integration einer Sicht zur Spezifikation von Sicherheitsanforderungen.
- Konzeption und Bereitstellung von Webservices zur Verwaltung von virtuellen Maschinen, mittels denen die SOA-Szenarien ausgeführt werden.
- Integration einer SOA-Registry zur Verwaltung der Dienste.
- Konfiguration der Dienste in den virtuellen Maschinen basierend auf den modellierten Szenarien mittels BPEL und WS-Policy.
- Visualisierung des Nachrichtenaustausches.

Projektpartner

Bundesamt für Sicherheit in der Informationstechnik
Postfach 200363
53133 Bonn
Anspechpartner: Herr Holger Junker

Internet-Technologien und Systeme
Hasso-Plattner-Institut, 14440, Potsdam, Germany
Ansprechpartner: Prof. Dr. Christoph Meinel, Herr Michael Menzel