SOA-Security 2010

Symposium für Sicherheit in Service-orientierten Architekturen

28. / 29.Oktober 2010 am Hasso-Plattner-Institut

HPI Hasso Plattner Institut
IT Systems Engineering | Universität Potsdam

INHALTSVERZEICHNIS

GRUSSWORT

HPI Hasso Plattner Institut
IT Systems Engineering | Universität Potsdam

Sehr geehrte Damen und Herren,

liebe Teilnehmer des SOA Security Symposiums,

zu unserem SOA Security Symposium heiße ich Sie zum nunmehr zweiten Male ganz herzlich am Hasso-Plattner-Institut willkommen. Ich freue mich sehr auf hoch interessante Vorträge der Experten und Fachleute aus Forschung und Industrie, die unserer Einladung nach Potsdam gefolgt sind, und denen ich hiermit nochmals ein besonderes Willkommen aussprechen möchte.

Die Sicherheit von Service-orientierten Architekturen stellt nach wie vor ein schwieriges und herausforderndes Feld für IT Unternehmen dar. Der Wunsch nach Kostenersparnissen und höherer Effizienz lässt viele Unternehmen ihre Daten und Prozesse aus der eigenen Sicherheitsdomäne in die Welt des Internets verlagern.

Während service-orientierte Architekturen den technologischen Schlüssel dafür bereitstellen, sind insbesondere Sicherheitsfragestellungen oftmals noch unzureichend geklärt. Gerade im Hinblick auf die neue Offenheit der Systeme, müssen Risiken analysiert und durch adäquate Sicherheitskonzepte adressiert werden.

Dieses Symposium soll einen Einblick in die aktuelle Entwicklung von SOA-Sicherheitslösungen geben sowie offene Probleme aufzeigen und zur Diskussion stellen.

Ich wünsche Ihnen allen zwei spannende, lehrreiche und interessante Tage mit anregenden Vorträgen und fruchtbaren Gesprächen bei uns am Hasso-Plattner-Institut.

Mit freundlichen Grüßen

Prof. Dr. Christoph Meinel

(Institutsdirektor und Geschäftsführer HPI,

Leiter des Lehrstuhls Internet-Technologien und Systeme)

PROGRAMM

Hasso Plattner Institut
IT Systems Engineering | Universität Potsdam

DONNERSTAG, 28. OKTOBER 2010

ab 12:00 Registrierung der Teilnehmer

12:30 – 14:00 **BEGRÜßUNG UND ERÖFFNUNG DES SYMPOSIUMS**

Prof. Dr. Christoph Meinel, Institutsdirektor und Geschäftsführer Hasso-Plattner-Institut

KEYNOTE: SOA SECURITY HEUTE UND MORGEN

Holger Junker, Bundesamt für Sicherheit in der Informationstechnik (BSI)

Kaffeepause und Get Together

14:30 – 16:00 **SESSION 1: ENTWURF UND MODELLIERUNG VON SICHERHEIT IN SERVICE-ORIENTIERTEN ARCHITEKTUREN**

Chair: Martin Raepple, SAP AG

- A Security Modelling Approach for Web-Service-Based Business Processes
  Prof. Dr. Jörg Schwenk, Ruhr-Universität Bochum
- SOA Security in der Praxis - Entwurfsmuster für eine sichere Umsetzung
  Arbeitsgruppe "SOA Security" des TeleTrust Deutschland e.V.
- Modellierung und Umsetzung von Sicherheitsanforderungen im SOA Security Lab (1. Platz IEEE Service Cup 2010)
  Dipl. Inf. Michael Menzel, Hasso-Plattner-Institut

Kaffeepause und Get Together

16:30 – 17:30 **SESSION 2: SICHERE DIGITALE IDENTITÄTEN**

Chair: Prof. Dr. Jörg Schwenk, Ruhr-Universität Bochum

- Facets of Secure Identification
  Prof. Dr. Volker Roth, Freie Universität Berlin
- Managing Reliable Digital Identities
  Ivonne Thomas, Hasso-Plattner-Institut

19:00 Konferenzdinner

PROGRAMM

Hasso Plattner Institut
IT Systems Engineering | Universität Potsdam

FREITAG, 29. OKTOBER 2010

9:00 – 9:45 **KEYNOTE: SOA SECURITY IN DEN ZEITEN DES CLOUD COMPUTING**
Jan Peters, IBM Deutschland

Kaffeepause und Get Together

10:00-11:00 **SESSION 3: SOA SICHERHEIT IM UNTERNEHMEN**

Chair: Dr. Bruno Quint, CORISECIO GmbH

- SSO mit SOA: Neue Herausforderungen an die Einmal-anmeldung im Unternehmen
  Martin Raepple, SAP AG
- IT Security Governance & Messbarkeit
  Dr. Thomas Störtkuhl, Secaron AG

Kaffeepause und Get Together

11:30 – 13:00 **SESSION 4: AKTUELLE SOA SECURITY PROJEKTE**

Chair: Holger Junker, BSI

- secRT - Das OpenSource Security Framework des BSI
  Dr. Bruno Quint, CORISECIO GmbH
- Open Source Identity und Access Management
  Michael Kleinhenz, tarent GmbH
- Einbruchserkennung in SOA
  Daniel Wagner, SHE Informationstechnologie GmbH

13:00 Ende und Ausklang der Veranstaltung

SICHERHEITSFORSCHUNG AM HASSO-PLATTNER-INSTITUT

PROF. DR. CHRISTOPH MEINEL

Direktor und Geschäftsführer des Hasso-Plattner-Instituts,
Leiter des Lehrstuhls Internet-Technologien und Systeme

Christoph Meinel ist Institutsdirektor und Geschäftsführer des Hasso-Plattner-Instituts für Softwaresystemtechnik GmbH (HPI) an der Universität Potsdam und ist dort Ordinarius für Internet-Technologien und –systeme. Er ist Teacher an der HPI School of Design Thinking und zusammen mit Larry Leifer von der Stanford-University Initiator und Programmdirektor des 2008 gestarteten HPI-Stanford Design Thinking Research Programs. Zusammen mit Hasso Plattner war er 2006 Gastgeber des von Bundeskanzlerin Dr. Merkel in Potsdam veranstalteten Ersten Nationalen IT-Gipfels.

Christoph Meinel ist Autor bzw. Co-Autor von 10 Büchern, Inhaber internationaler Patente und hat mehr als 350 wissenschaftliche Publikationen veröffentlicht. In seinen aktuellen Forschungen entwickelt Christoph Meinel zukünftige Internet-Technologien – vornehmlich für mehr Sicherheit und das Web 3.0 (Social, Semantic, Service Web) – sowie innovative Internet-Anwendungen in den Bereichen E-Learning und Telemedizin. Auch im Bereich der Innovationsforschung ist er aktiv und leitet als Programmdirektor das HPI-Stanford Design Thinking Research Program. In der Vergangenheit hat er erfolgreich auf dem Gebiet der Komplexitätstheorie gearbeitet und (BDD-basierte) Datenstrukturen und effiziente Algorithmen für das Chip-Design untersucht und entworfen.

Christoph Meinel studierte von 1974 bis 1979 Mathematik und Informatik an der Humboldt-Universität Berlin, promovierte dort 1981 zu Fragen der Komplexitätstheorie und habilitierte sich 1988 mit der Schrift "Modified branching programs and their computational power". Von 1992 bis 2004 war Christoph Meinel Professor für Theoretische Konzepte und neue Anwendungen der Informatik an der Universität Trier. Neben seiner Tätigkeit als Universitätsprofessor war Christoph Meinel von 1996 bis 2002 Gründungsdirektor des Instituts für Telematik e.V. in Trier, das unter Betreuung der Fraunhofer Gesellschaft mit Fragestellungen aus dem Gebiet der Internet- und Web-Technologien befasst war. 1995 bis 2007 gehörte er dem wissenschaftlichen Direktorium des Internationalen Begegnungs- und Forschungszentrums für Informatik Schloß Dagstuhl an. Christoph Meinel ist Gastprofessor an der Universität Luxemburg und an der Technischen Universität von Peking (China), wohin

seine Vorlesungen zur Internetsicherheit im HPI mittels der von seinem Team entwickelten tele-TASK-Technologie übertragen werden. Darüber hinaus leitet er das Steering Committee des HPI Future SOC Labs und ist in verschiedenen internationalen Programmkomitees und Aufsichtsräten aktiv.

ABSTRACT

Service Orientierte Architekturen werden schon heute in einer Vielzahl von Unternehmen eingesetzt und werden als eine mögliche Technologie zur Umsetzung von Cloud Computing weiter an Bedeutung gewinnen. Die Ausdehnung von einstmals isolierten Softwaresystemen zu unternehmensweiten oder gar Unternehmensgrenzen sprengenden offenen Systemen wirft eine große Zahl hochinteressanter Fragestellungen im Sicherheitsbereich auf, geht doch die alte Vorstellung vom Schutz der Systeme allein an ihren Außengrenzen verloren. Gerade deshalb müssen Risiken neu analysiert und adäquate Sicherheitskonzepte entwickelt werden.

Mit diesem Einführungsvortrag soll ein Überblick über die Forschungsaktiväten und Projekte im Sicherheitsbereich am Hasso-Plattner-Institut gegeben werden. Diese umfassen insbesondere den Lock-Keeper aus dem Bereich Netzwerksicherheit, das SOA Security Lab und den HPI Identity Provider aus dem Bereich SOA Security und das Tele-Lab, welches eine Lernplattform zur Erhöhung des Sicherheitsbewußtseins bei Anwendern bereitstellt.

HPI Hasso Plattner Institut

IT Systems Engineering | Universität Potsdam

Herzlich Willkommen zum SOA Security Symposium 2010

Prof. Dr. Christoph Meinel
Chair "Internet Technologies and Systems"
Hasso-Plattner-Institute
University of Potsdam, Germany

Herzlich Willkommen!

- Zweite Symposium in dieser Reihe
- 2 Tage aktuelle Vorträge aus dem universitären und industriellen Umfeld, neue Projekte, Ideen, Erfahrungsaustausch … und
- Kennenlernen neuer Entwicklungen und Technologien
- Knüpfen neuer Kontakte

Programm heute

12:30 – 14:00 **Begrüßung und Eröffnung des Symposiums**
Prof. Dr. Christoph Meinel, Institutsdirektor und Geschäftsführer
Keynote: SOA Security heute und morgen
Holger Junker, Bundesamt für Sicherheit in der Informationstechnik (BSI)

14:00 – 14:30 Kaffeepause und Get Together

14:30 – 16:00 **Session 1: Entwurf und Modellierung von Sicherheit in Service-orientierten Architekturen**

- *A Security Modeling Approach for Web-Service-based Business Processes*
  Prof. Jörg Schwenk, Ruhr-Universität Bochum
- *SOA Security in der Praxis – Entwurfsmuster für eine sichere Umsetzung*
  TeleTrust SOA Security Arbeitsgruppe
- *Modellierung und Umsetzung von Sicherheitsanforderungen im SOA Security Lab (1. Platz IEEE Service Cup 2010)*
  Michael Menzel, Hasso-Plattner-Institut

Programm heute

16:00 – 16:30 Kaffeepause und Get Together

16:30 – 17:30 **Session 2: Sichere Identitäten**

- *Facets of Secure Identification*
  Prof. Volker Roth, Freie Universität Berlin
- *Managing Reliable Digital Identities*
  Ivonne Thomas, Hasso-Plattner-Institut

19:00 **Konferenzdinner**

Programm morgen

09:00 – 09:45 **Keynote: SOA Security in den Zeiten des Cloud Computing**
Jan Peters, IBM Deutschland

09:45 – 10:00 Kaffeepause und Get Together

10:00 – 11:00 **Session 3: SOA Sicherheit im Unternehmen**

- *SSO mit SOA: Neue Herausforderungen an die Einmalanmeldung im Unternehmen*
  Martin Raepple, SAP AG
- *Messbarkeit & IT Security Governance*
  Dr. Thomas Störtkuhl, Secaron AG

11:00 – 11:30 Kaffeepause und Get Together

Programm morgen

11:30 – 13:00 **Session 4: Aktuelle SOA Security Projekte**

- *secRT - Das OpenSource Security Framework des BSI*
  Dr. Bruno Quint, CORISECIO GmbH
- *Open Source Identity- und Access Management*
  Michael Kleinhenz, tarent GmbH
- *Einbruchserkennung in SOA*
  Daniel Wagner, SHE Informationstechnologie AG

13:00 **Ende und Ausklang der Veranstaltung**

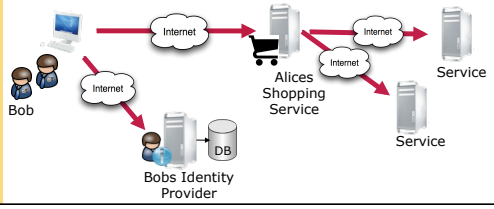
Womit befaßt sich SOA-Security ? Motivierendes Szenario

7

Bob bestellt Waren bei Alice

- Verschiedene Sicherheitsaspekte
  1. Sicheres Netzwerk

- Abwesenheit von Schwachstellen
- Konsequenter Einsatz und korrekte Konfiguration von Sicherheitssystemen (Firewall, ID Systeme)



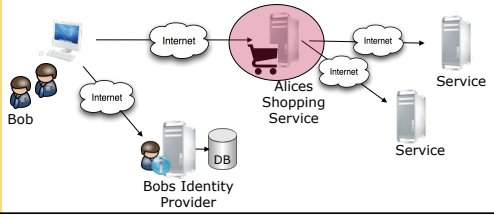
Womit befaßt sich SOA-Security ? Motivierendes Szenario

8

Bob bestellt Waren bei Alice

- Verschiedene Sicherheitsaspekte
  1. Sicheres Netzwerk
  2. Anforderungen und Policies

- Was sind die sicherheitstechnischen Anforderungen eines Services?
- Welche Sicherheitsmechanismen, techniken und -token werden zur Nutzung des Services benötigt?



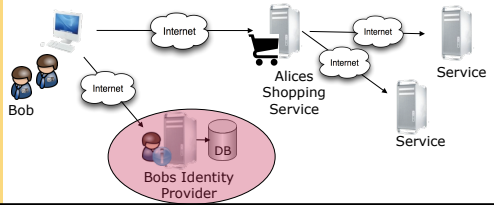
Womit befaßt sich SOA-Security ? Motivierendes Szenario

9

Bob bestellt Waren bei Alice

- Verschiedene Sicherheitsaspekte
  1. Sicheres Netzwerk
  2. Anforderungen und Policies
  3. Vertrauen und Reputation

- Verschiedene Domänen (Bob, Alice) erfordern Etablierung einer Vertrauensbeziehung
- Vertrauen als Grundlage für die Akzeptanz von Sicherheitstoken
- Reputation als Hilfsmittel zur Auswahl eines Serviceanbieters



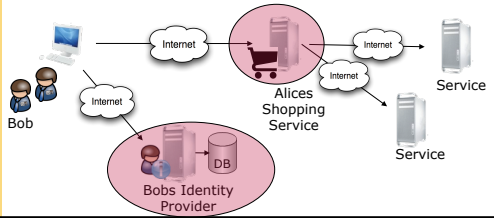
Womit befaßt sich SOA-Security ? Motivierendes Szenario

10

Bob bestellt Waren bei Alice

- Verschiedene Sicherheitsaspekte
  1. Sicheres Netzwerk
  2. Anforderungen und Policies
  3. Vertrauen und Reputation
  4. Identifizierung und Authentifizierung

- Verwaltung von Bob's Identität kann durch dritte Partei (Identity Provider) erfolgen
- Alice vertraut auf die Authentifizierung durch den Identity Provider



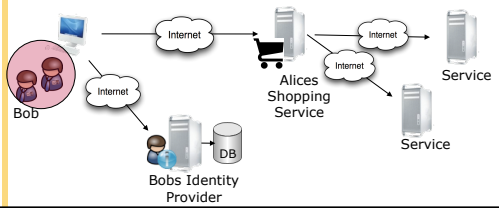
Womit befaßt sich SOA-Security ? Motivierendes Szenario

11

Bob bestellt Waren bei Alice

- Verschiedene Sicherheitsaspekte
  1. Sicheres Netzwerk
  2. Anforderungen und Policies
  3. Vertrauen und Reputation
  4. Identifizierung und Authentifizierung
  5. Sicherheitsverständnis beim Nutzer

- Fehlendes Sicherheitsverständnis beim Nutzer führt zu Fahrlässigkeit in sicherheitskritischen Situationen, z.B. zu schwach gewählten Passwörtern, und PINs, fehlender Trojanerschutz, etc



Welcome at Hasso-Plattner-Institute ...

12

... for IT-Systems Engineering

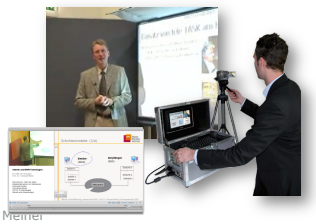
Fact Sheet:

- Full professors and chairs: 10
- Lecturers, Assistant Professors, Scientific Co-workers: 100
- PhD-Students: 120 – 100 internal, 20 external ones
- Bachelor and Master Students: 450
- **Top rank** among all German speaking Computer Science Departments

Lehrstuhl Prof. Dr. Christoph Meinel „Internet Technologien und Systeme“

13

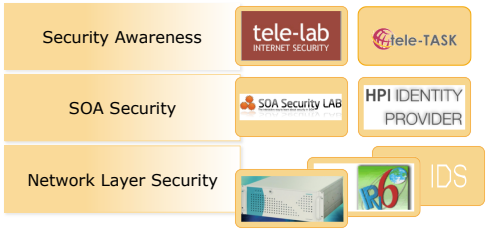
- **Future Internet Technologies** mit besonderem Fokus auf
  → Security Engineering und
  → Web 3.0 (Semantic, Service, Social Web)
- **Next-Generation Internet-Anwendungen** für
  → Web-University, z.B. tele-TASK …
  → Telemedizin
- **Design Thinking Research**
  → d-tools, z.B. tele-Board …



Sicherheit-Forschung am Lehrstuhl Internettechnologien und -systeme

14

Sicherheit auf allen Ebenen:

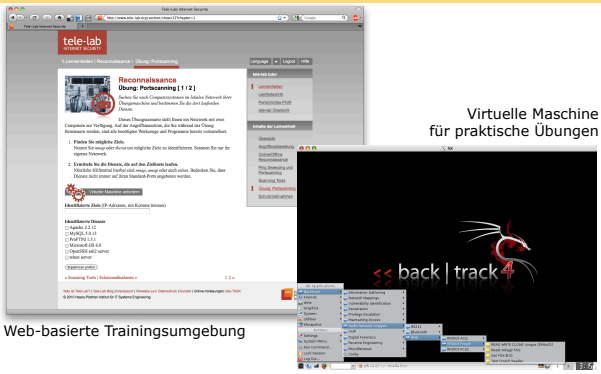


Sicherheit-Forschung am Lehrstuhl Internettechnologien und -systeme

15

Tele-Lab – unser Online-Labor für IT Security Training

16



Virtuelle Maschine für praktische Übungen

Web-basierte Trainingsumgebung

Tele-Lab – Features

17

IT Security Training im Web

- Tele-Lab stellt realistische, praktische Übungen zur Verfügung
- System kann über das Internet überall und jederzeit genutzt werden, lediglich ein Browser mit Java-Plugin werden benötigt

Einsatzgebiete

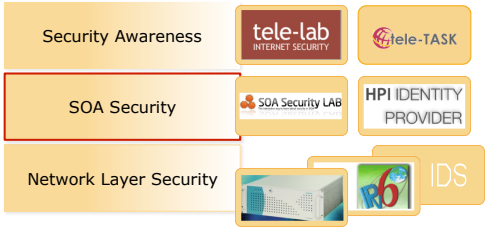
- Sicherheitsausbildung für IT Professionals (z.B. an der Universität)
- Awareness Raising für Jedermann (z.B. Mitarbeiter in Unternehmen)

Viele unterschiedliche Lerneinheiten:

- Passwortsicherheit, Portscanning, Remote Exploitation, sichere E-mail, Man-in-the-Middle Angriffe, WLAN-Sicherheit, etc.

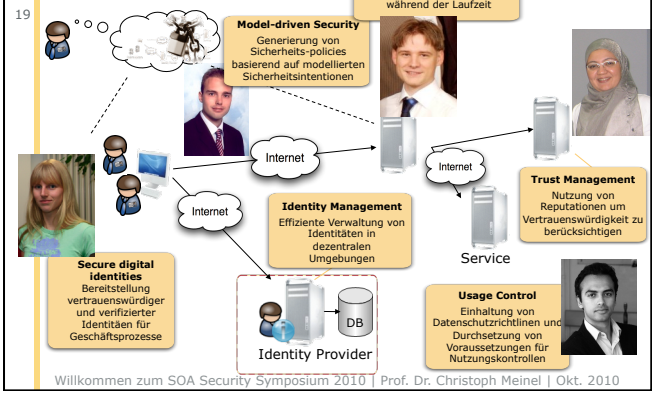
Sicherheit am Lehrstuhl Internettechnologien und -systeme

18



SOA-Security Team und Forschungsfelder

19



SOA-Security – Unsere Projekte und Aktivitäten

20

Bundesamt für Sicherheit in der Informationstechnik

SOA Security Kompendium 2.0 (veröffentlicht: Q4 2009)

Messbarkeit von Sicherheit in SOA

SOA Security LAB
The interactive way to learn about security in SOA

- Lerne den Umgang mit SOA Sicherheit in einer Web-basierten Plattform

HPI Identity Provider

- Verwalte digitale Identitäten und nutze sie mit OpenID und Information Cards

Board Activities

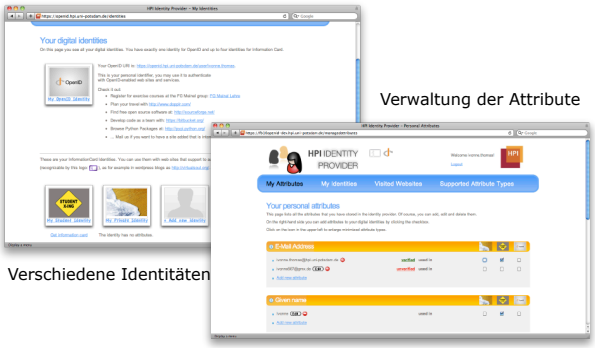
Information Card DACH-Initiative

TeleTrusT Pioneers in IT security. 1989 20Jahre 2009

- HPI ist Mitbegründer des deutschen Verbands der globalen Information Card Initiative
- HPI war in der TeleTrust SOA Security Arbeitsgruppe aktiv

HPI Identity Provider – Wege aus dem Passwortdilemma

21



HPI Identity Provider - Features

22

- Verwaltet digitale Identitäten von Studenten und HPI Mitarbeitern
- Bietet SSO für verschiedene Anwendungen am HPI, z.B. Einschreibung in Übungen, Tutorien, tele-TASK-Account
- Integration verschiedener Technologien
  - OpenID
  - Information Card
  - Web Service Schnittestelle (WS-Trust)
- Möglichkeit der Verifizierung von Attributen (z.B. eMail per Zertifikat)

HPI IDENTITY PROVIDER

SOA Security Lab

23

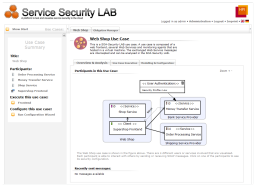
SOA Security LAB
The interactive way to learn about security in SOA

1. Place
IEEE Service Cup

Plattform zur Generierung, Ausführung und Analyse von abgesicherten Webservice-basierten Webapplikationen

Modellierung von Webservice-Szenarien:

- Web-basiertes Modellierungswerkzeug
- Automatisierte Erzeugung von Systemkonfigurationen
- Modell-getriebene Absicherung durch Entwurfsmuster für SOA Sicherheit



SOA Security Lab

24

SOA Security LAB
The interactive way to learn about security in SOA

Ausführung und Analyse:

- Instanziierung in einer virtuellen Maschine
- Monitoring der nachrichten-basierten Kommunikation
- Werkzeuge zur Analyse der Nachrichtenstruktur

www.soa-security-lab.de

Sicherheit am Lehrstuhl Internettechnologien und -systeme

25

- Sicherheit auf verschiedenen Ebenen

Lock-Keeper High-Level Security mittels PS (1)

26

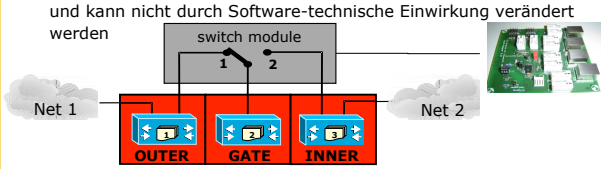
- Neue Herausforderungen für IT-Security
  - Angriffe auf private Netzwerke sind ein bekanntes Problem
    - Online Angriffe und Offline Angriffe
    - Bekannte Angriffe und unbekannte Angriffe
    - Interne Angriffe und externe Angriffe
  - Falls Verbindung zu einem Netzwerk hergestellt ist besteht immer die Gefahr eines Angriffs
  - Die ultimative Methode ein Netzwerk abzusichern ist die Entkopplung der Verbindung – Physical Separation (PS).
- Lock-Keeper ist eine Implementierung des Konzeptes Physical Separation, welches Security und Usability gleichzeitig unterstützt.

Lock-Keeper High-Level Security mittels PS (2)

27

Der Lock-Keeper besteht aus folgenden Komponenten
(1) Drei unabhängige aktive Computer: **INNER, GATE, und OUTER**
(2) Ein patentiertes Switch-Modul: Switch-PCB

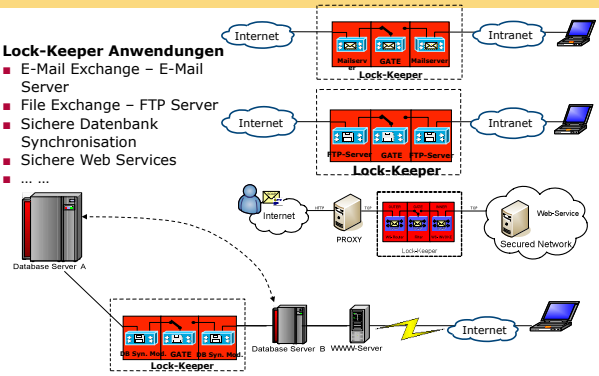
- Das Switch-Module kontrolliert die internen Verbindungen vollständig
- Funktion und Timing des Switch-Moduls ist vollständig autonom und kann nicht durch Software-technische Einwirkung verändert werden



Lock-Keeper High-Level Security mittels PS (3)

28

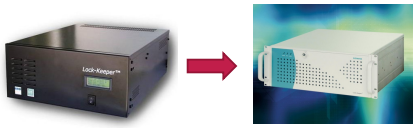
Lock-Keeper Anwendungen
- E-Mail Exchange – E-Mail Server
- File Exchange – FTP Server
- Sichere Datenbank Synchronisation
- Sichere Web Services
- ... ...



Lock-Keeper High-Level Security mittels PS (4)

29

- Patentiert in 10 Ländern und Regionen
- Publikation mehrere wissenschaftlicher Arbeiten
- 2002 Lock-Keeper wird von der Investitions- und Strukturbank Rheinland-Pfalz (ISB) als beste Erfindung ausgezeichnet
- Juli 2005 Lizensierung der Lock-Keeper Technologie durch Siemens Schweiz AG und Start gemeinsamer R&D Kooperationsprojekte
- 2006 Erster Lock-Keeper wird verkauft
- 2007 Lock-Keeper gewinnt Deutschen "IT Security Award" (in der "Kategorie Web/Internet Security")



Unsere Aktivitäten im Bereich IPv6 und IPv6 Security

30

- IPv4 Adressraum ist erschöpft
  - Neue IPv4 Adressen sind schwer verfügbar (ca. 5% verfügbar)
  - IPv4 Adressen nicht ausreichend für Vielzahl an Mobile Devices
- IPv6 soll IPv4 ersetzen
  - IPv6 schon heute standardmäßig eingeschaltet für viele OS
- IPv6 als Grundlage für weiteres Wachstum des Internet
- IPv6 bietet neue Features
  - Vereinfachte Header
  - Security
  - Mobility
  - Erweiterbarkeit, ...
- Neue Security-Fragestellungen kommen auf
  - Problematische Features wie Auto-Configuration oder Co-Existenz-Mechanismen (Dual-Stack, Tunneling)

Unsere Aktivitäten im Bereich IPv6 und IPv6 Security

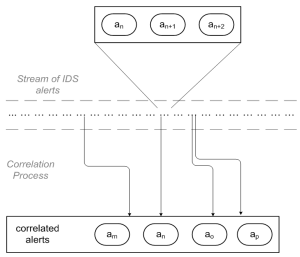
31

- Ipv6 Deployment und Management
  - IPSec - Fragestellungen zum Thema Management und Re-Keying von Internet Key Exchange (IKE) Sessions
  - Neighbor Discovery Protocol (SEND), Cryptographically Generated addresses (CGA) – Fragestellungen zur Performance und Sicherheit
  - Interoperabilität von IPSec, SEND und CGA
- Sicherheitsuntersuchungen des IPv6 Protokolls
  - IPv6 Schwachstellen: Auto-Configuration, Tunneling, Dual-Stack, Routing, Mobility, etc.
- Praktische IPv6 Angriffe
  - Testbed für Experimente und Angriffe: Scanning, Sniffing, Spoofing, Fake Router Advertisement, …
  - Suche nach neuen Angriffsmethoden
- Integration von IPv6 mit anderen Sicherheitslösungen (Lock-Keeper)

Unsere Forschungen im Bereich IDS und IDS Correlation

32

- Verteilte IDS-Sensoren und Logging-Systeme erzeugen eine Vielzahl von Security-Events
- IDS Correlation identifiziert durchgeführte Angriffsszenarios in einem Stream von Security-Events



IDS Correlation mittels Alternativ-Storage und Multi-Core

33

- Alternative Storage-Konzepte zur Durchführung der IDS Korrelation
  - Spalten-orientierte Datenbank (MonetDB)
  - In-Memory Datenbank
- Multi-core Algorithmen für IDS Correlation
  - Map-Reduce-basierte Ansätze
  - CUDA Implementierungen

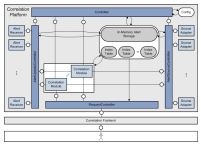
Technische Basis – HPI Future SOC Lab

- Moderne Systeme bieten riesige Kapazität an Hauptspeicher
  - Fujitsu RX600 S5 (CPU: 4x Xeon, RAM: 1024 GB)
- Moderne Systeme arbeiten mit Multi-Core & verteilten Ansätzen
  - Intel's Single-chip Cloud Computer (SCC) – 48 Kerne
  - CUDA ermöglicht beliebige Berechnungen mittels GPU (NVIDIA Graphics)

Correlation Platform - Forschung

34

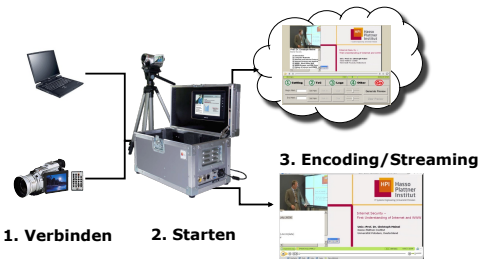
- Entwicklung einer flexiblen und effizienten IDS Correlation Platform
- Storage-Konzepte in Anwendung und Kombination
- Multi-Core und verteilte Algorithmen für IDS Correlation
- Attack-Graph-basierte Korrelation
- Visualisierung von Korrelationsergebnissen
- Collaboration für IDS Correlation



One more thing… **tele-TASK**

35

Aufnahme der Veranstaltung mit unserem tele-TASK System



HPI Hasso Plattner Institut

IT Systems Engineering | Universität Potsdam

Ich wünsche uns allen eine gute Tagung mit fruchtbaren Gedankenaustausch

Univ.-Prof. Dr. Christoph Meinel
Hasso-Plattner-Institut Potsdam

KEYNOTE: SOA SECURITY HEUTE UND MORGEN

HOLGER JUNKER

Regierungsrat, Bundesamt für Sicherheit in der Informationstechnik (BSI)

Holger Junker ist Diplom Informatiker mit den Schwerpunkten Sicherheit in verteilten Architekturen und Java. Nach dem Studium an der Uni (TH) Karlsruhe begann er im Bundesamt für Sicherheit in der Informationstechnik (BSI) im Bereich „Kommunikationssicherheit in Geschäftsprozessen" mit der Analyse und Optimierung der Sicherheit von Softwarekomponenten für das E-Government. Seit mehreren Jahren liegt der Arbeitsschwerpunkt im Bereich SOA und verteilten Architekturen allgemein.

Neben der Tätigkeit am BSI ist Herr Junker als freier Dozent tätig und verfasst regelmäßig Artikel in verschiedenen Fachzeitschriften.

ABSTRACT

Zunächst erfolgt eine Betrachtung von aktuellen Lösungen zur Gewährleistung der Sicherheit in Service-orientierten Architekturen. Hierbei werden insbesondere die Aktivitäten und Produkte des BSI dargestellt. Neben dem Grundlagenwerk „SOA Security Kompendium" sowie weiteren Studien werden hierbei insbesondere Softwarekomponenten für die Absicherung der Kommunikation, dem Identity & Access Management sowie der Einbruchserkennung in SOA vorgestellt, die das BSI unter freier Lizenz zur Verfügung stellt.

Anschließend werden aktuelle Herausforderungen und zukünftige Tätigkeitsfelder skizziert. Während technische Probleme der SOA Security weitgehend gelöst sind, betrifft dies in erster Linie organisatorische Aspekte der Sicherheit.

So ist es beispielsweise in einer verteilten Architektur wie einer SOA mitunter sehr anspruchsvoll, eine Sicherheitsanalyse durchzuführen oder SLAs zu definieren und durchzusetzen.

Darüber hinaus gilt es, die Brücke von einer sicheren SOA hin zu einer sicheren Cloud zu bilden und diese beiden Ansätze gewinnbringend miteinander zu kombinieren.

SOA-Security heute und morgen

Holger Junker

Bundesamt für Sicherheit in der Informationstechnik

SOA Security Symposium 2010

Agenda

1. SOA in der Bundesverwaltung
2. SOA Security heute – Produkte des BSI
3. SOA Security morgen – aktuelle Herausforderungen
4. Von der SOA zur Cloud
5. Zusammenfassung

Agenda

1. SOA in der Bundesverwaltung
2. SOA Security heute – Produkte des BSI
3. SOA Security morgen – aktuelle Herausforderungen
4. Von der SOA zur Cloud
5. Zusammenfassung

SOA in der Bundesverwaltung

Die Beauftragte der Bundesregierung für Informationstechnik

- *„Professionelle IT-Leistungen für die Bundesverwaltung [...] sind eine wesentliche Zielmarke der neuen IT-Steuerung des Bundes. Zentrale IT-Angebote des Bundes werden daher schrittweise in leistungsstarken IT-Dienstleistungszentren gebündelt.“*
  - → Dienstleistungszentren IT
  - → Rahmenarchitektur IT-Steuerung Bund
  - → SAGA berücksichtigt in Version 4.0 SOA

SOA in der Bundesverwaltung: BAMF

Bundesamt für Migration und Flüchtlinge

- Mehrere tausend unterschiedlichste Partnerbehörden führen zu einer hybriden IT-Landschaft
- Schnelle Reaktion auf Gesetzesänderungen u.ä.:
  „Wenn sich herausstellt, dass eine Straße zu schnell befahren wird, lässt sich an einer Straßenecke auch kurzfristig eine Ampel aufstellen.“
  K. Munsi, Leiter Software-Entwicklung BAMF
- Erhöhte Anforderungen an Sicherheit und Datenschutz

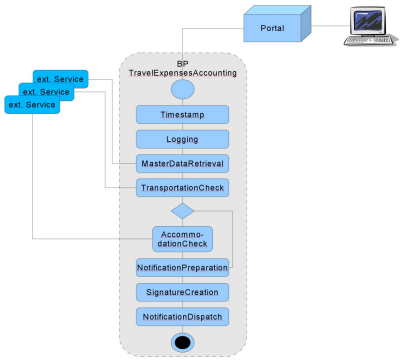
SOA im Kontext erhöhter Sicherheitsanforderungen

- Vorgangsbearbeitung im VS-Kontext
- Arzneimittelzulassung
- Geoinformationsdienste
- Nationales Waffenregister
- Virtuelle Poststelle des Bundes & OSCI-Kommunikation (insbes. Gerichtswesen)

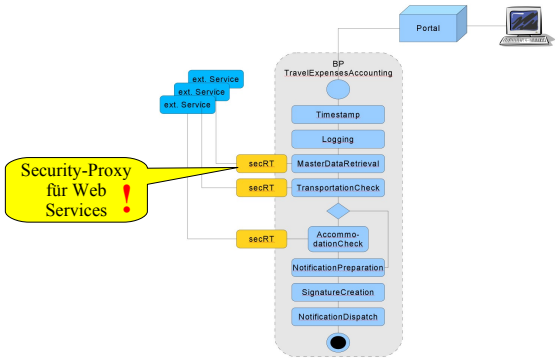
Agenda

1. SOA in der Bundesverwaltung
2. SOA Security heute – Produkte des BSI
3. SOA Security morgen – aktuelle Herausforderungen
4. Von der SOA zur Cloud
5. Zusammenfassung

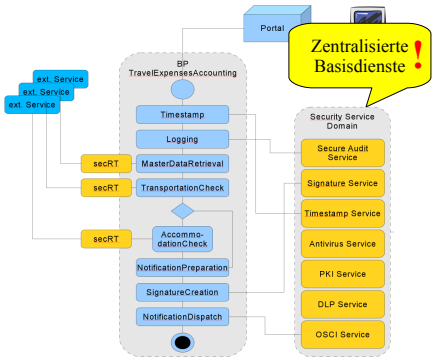
Geschäftsprozesse in SOA



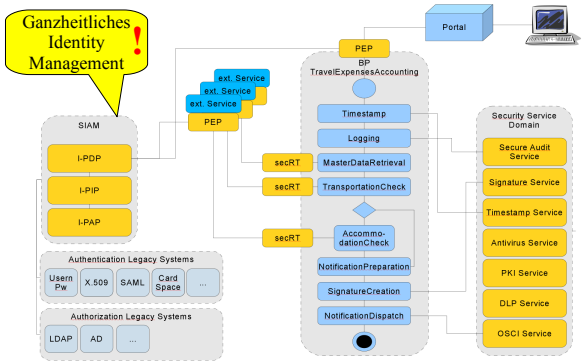
Sichere Geschäftsprozesse in SOA



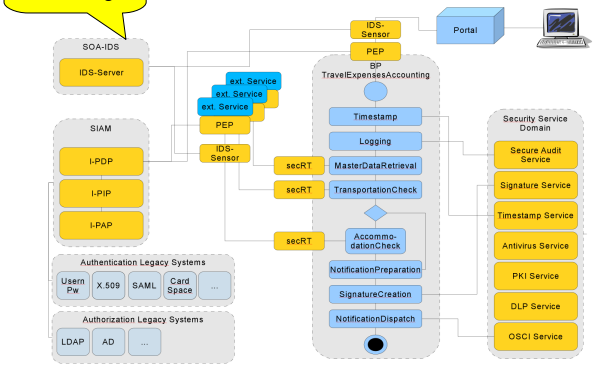
Sichere Geschäftsprozesse in SOA



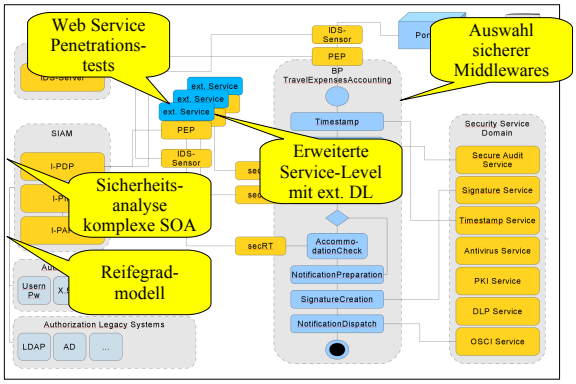
Sichere Geschäftsprozesse in SOA



Sichere Geschäftsprozesse in SOA



Sichere Geschäftsprozesse in SOA



Agenda

Technische & akademische Herausforderungen

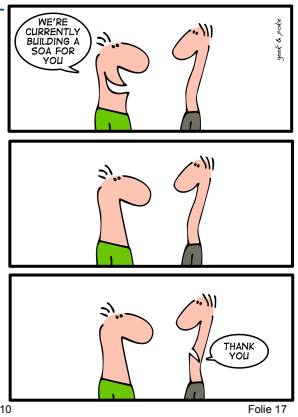
- Sicheres Parsen von XML / SOAP
- Sicherheit von XML-Signaturen
- Standardisierte Sicherheit für REST
- Model-driven Security
- Optimierung Policy-basierter Sicherheit
- ...

Sicherheit als Ausgangspunkt für eine SOA-Einführung?!

- Start small – think big
- Häufig werden abgegrenzte Fachdomänen für eine SOA-Einführung ausgewählt, ohne dabei Security zu berücksichtigen
- Sicherheit als möglicher Ausgangspunkt für eine SOA-Einführung, z.B.
  - Identity & Access Management
  - Security as a Service
- Vorteile einer SOA-Einführung können leicht aufgezeigt werden
  - Wiederverwendbarkeit
  - Return of Invest

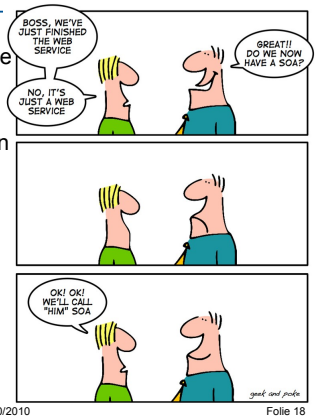
Erfolgsfaktoren für SOA: kulturelles Umdenken

- SOA als gemeinsame Herausforderung von Business & IT



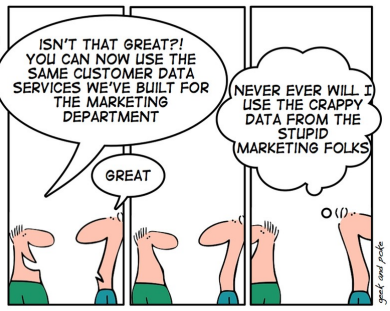
Erfolgsfaktoren für SOA: kulturelles Umdenken

- SOA Strategie geeignet in die jew. Hierarchieebenen kommunizieren
- Erwartungshaltungen steuern



Erfolgsfaktoren für SOA: kulturelles Umdenken

- Wiederverwendbarkeit fördern
- „Not invented here“-Syndrom bekämpfen

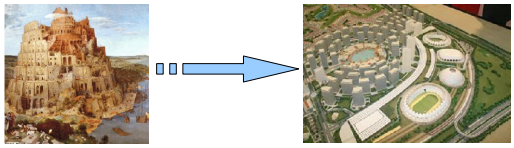


Sicherheitsspezifische Erfolgsfaktoren – SOA als Chance für IT-Sicherheit?!

- SOA erzwingt eine strukturierte Vorgehensweise für Aufbau und Organisation
  - Enterprise Architecture Management (EAM)
  - Governance, Risk & Compliance
  - IT- und Business Continuity & Disaster Recovery
  - Sicherheitsanalyse

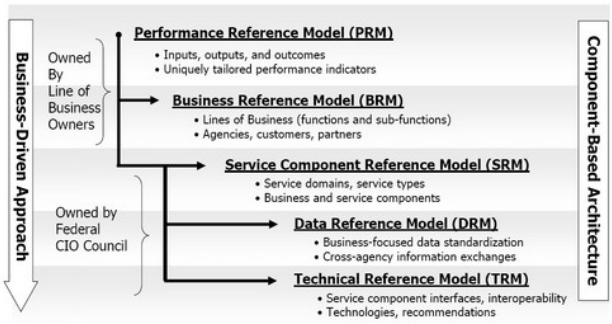
→ Diese nicht-technischen Aspekte sind kritische Erfolgsfaktoren für eine sichere SOA

Enterprise Architecture Management

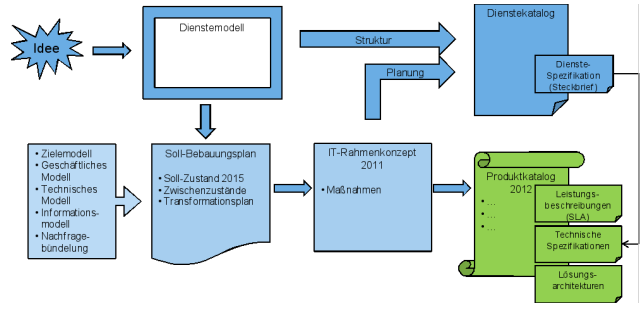


- Ausrichtung der IT an den Geschäftsprozessen
- Beherrschbarkeit der Komplexität von (Teil-)Architekturen und deren Zusammenhängen
- Nachhaltigkeit von IT-Investitionen

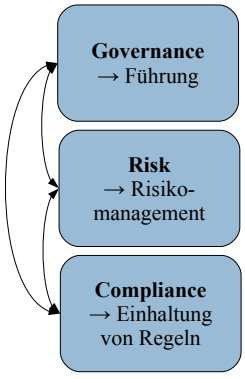
EAM mit dem FEA-Framework



Enterprise Architecture Management



Governance, Risk, Compliance



- Ziele
- Methodik zur Umsetzung
- Richtlinien, Policies & Abläufe

- Analyse
- Bewertung
- Minimierung
- Controlling / Monitoring

- Interne & externe Normen
- Zugriffsregelung für Daten
- Verwendung von Daten
- Controlling / Monitoring

Governance, Risk, Compliance

- GRC erhöht die Möglichkeiten für Organisationen
  - strategische Entscheidungen auf Basis einer Risikoorientierung zu treffen,
  - Vorschriften jeglicher Art einzuhalten und
  - Aktivitäten zur Verbesserung der SOA selber zu steuern.
- SOA-Security muss als Teil von GRC verstanden werden
- Ohne eine etablierte Governance wird eine SOA schnell unbeherrschbar

Notfallvorsorge

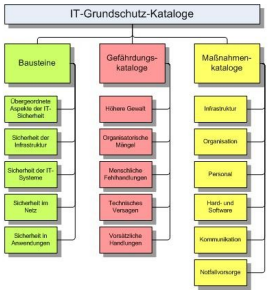
- BSI 100-4 Notfallmanagement
- IT-Grundschutz Maßnahmenkatalog M6 Notfallvorsorge
  - 6.1 Erstellung einer Übersicht über Verfügbarkeitsanforderungen
  - 6.60 Festlegung von Meldewegen für Sicherheitsvorfälle
  - 6.50 Archivierung von Datenbeständen
  - 6.83 Notfallvorsorge beim Outsourcing
  - 6.112 Aufbau einer geeigneten Organisationsstruktur für das Notfallmanagement
  - 6.114 Erstellung eines Notfallkonzepts
  - 6.117 Tests und Notfallübungen
  - 6.134 Dokumentation von Sicherheitsvorfällen

Notfallvorsorge

- *[Auszug aus M 6.83 Notfallvorsorge beim Outsourcing]*
  Im Notfallvorsorgekonzept müssen diese Vorgaben genau spezifiziert und im Detail beschrieben werden:
  - Zuständigkeiten, Ansprechpartner und Abläufe müssen klar geregelt und vollständig dokumentiert werden.
  - Detaillierte Arbeitsanweisungen mit konkreten Anordnungen für bestimmte Fehlersituationen sind zu erstellen.
  - Ein Konzept für Notfallübungen, die regelmäßig durchgeführt werden müssen, muss erarbeitet werden.
- Bislang meist praktiziert für interne Verfahren oder Outsourcing, aber nicht für Geschäftsprozesse mit einer Vielzahl von Akteuren

SOA Sicherheitsanalyse

- Testen der einzelnen Web Service Schnittstellen ist nur ein Aspekt von vielen bei der Realisierung einer sicheren SOA
- Weitere Aspekte:
  - Sicherheitskonzept nach IT-Grundschutz
  - IS-Revision (nach IT-Grundschutz)



Agenda

1. SOA in der Bundesverwaltung
2. SOA Security heute – Produkte des BSI
3. SOA Security morgen – aktuelle Herausforderungen
4. Von der SOA zur Cloud
5. Zusammenfassung

Schwerpunkte von SOA und Cloud Computing

- SOA
  - Fokus: Geschäftsprozesse
  - Wiederverwendbarkeit
  - Austauschbarkeit
  - Governance
- Cloud
  - Fokus: Ressourcen (I/P/SaaS)
  - Skalierbarkeit
  - Nutzung bei Bedarf

SOA und Cloud-Computing

- Konvergenz zur Cloud-based SOA
  - Vorteile, z.B. bzgl. Business Continuity & Disaster Recovery
  - Nachteile, z.B. höhere Komplexität bzgl. GRC
- Adaption von Konzepten
  - Ansätze für GRC, Sicherheitsanalyse, etc. können von SOA auf die Cloud übertragen werden

Agenda

1. SOA in der Bundesverwaltung
2. SOA Security heute – Produkte des BSI
3. SOA Security morgen – Zukünftige Herausforderungen
4. Von der SOA zur Cloud
5. Zusammenfassung

Zusammenfassung

- Security kann sowohl Einstiegspunkt als auch Showstopper bei der Einführung einer SOA sein
- Für viele der sicherheitsspezifischen Herausforderungen im SOA-Kontext gibt es Lösungen
- Kritische Erfolgsfaktoren einer (sicheren) SOA-Einführung sind meist nicht-technischer Natur
- SOA-Einführung kann Chance und Motivation sein, Sicherheit auf technischer und organisatorischer Ebene zu optimieren

Kontakt

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Holger Junker
Godesberger Allee 185
53175 Bonn

Tel: +49 (0)22899-9582-5599
Fax: +49 (0)22899-10-9582-5599

holger.junker@bsi.bund.de
soa@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de

A SECURITY MODELING APPROACH FOR WEB-SERVICE-BASED BUSINESS PROCESSES

PROF. DR. JÖRG SCHWENK

Lehrstuhl für Netz- und Datensicherheit, Horst Görtz Institut für IT-Sicherheit, Ruhr-Universität Bochum

The rising need for security in SOA applications requires better support for management of non-functional properties in web-based business processes. Here, the model-driven approach may provide valuable benefits in terms of maintainability and deployment. Apart from modeling the pure functionality of a process, the consideration of security properties at the level of a process model is a promising approach.

In this talk, we present an extension to the ARIS SOA Architect that is capable of modeling security requirements as a separate security model view. Further, we provide a transformation that automatically derives WS-SecurityPolicy-conformant security policies from the process model, which in conjunction with the generated WS-BPEL processes and WSDL documents provides the ability to deploy and run the complete security-enhanced process based on Web Services technology.

ABSTRACT

Prof. Dr. Jörg Schwenk has the chair for Network and Data Security at the Horst Görtz Institute for IT Security at RUB since 2003. From 1993-2001 he worked in the security department of Deutsche Telekom on different projects. He has written more than 60 patents, and more than 50 scientific publications. His research interests include cryptographic protocols (especially multi-party protocols), XML and Web Service security and internet security (especially protection against real world challenges such as pharming or WWW-based attacks).

SOA-Security 2010

A Security Modeling Approach for Web-Service-based Business Processes

Jörg Schwenk, Meiko Jensen, Sven Feja, Andreas Speck

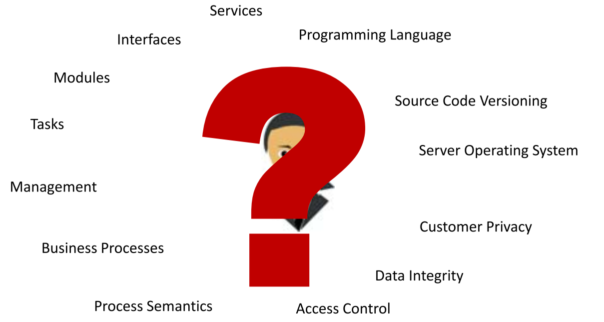
Horst Görtz Institute for IT-Security, Ruhr-University Bochum

Computer Science Department, Christian-Albrechts-University of Kiel

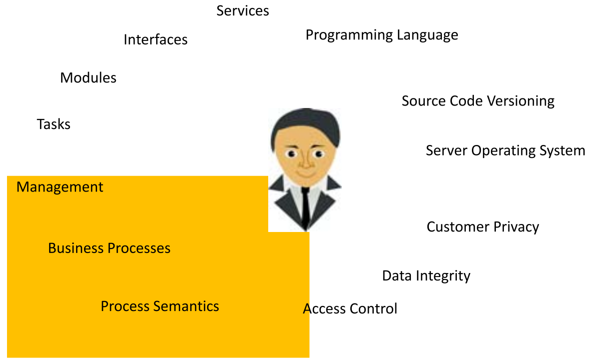
Overview

- Model-Driven Software Development
- Modeling Requirements
- Model-Driven Security
  - The Approach
  - The Model
  - The Transformation
- Conclusion and Future Work

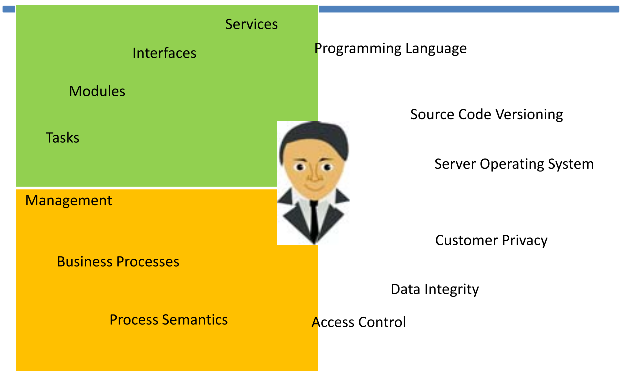
Model-Driven Software Development



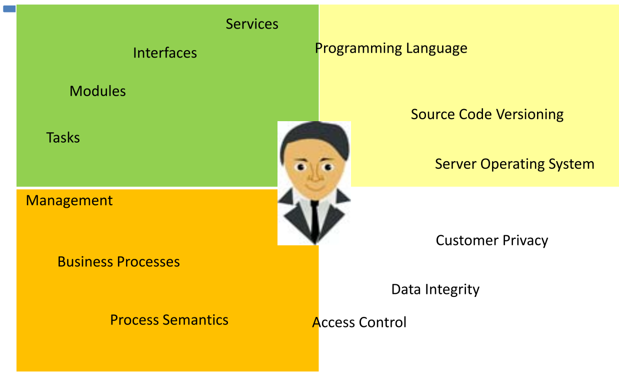
Model-Driven Software Development



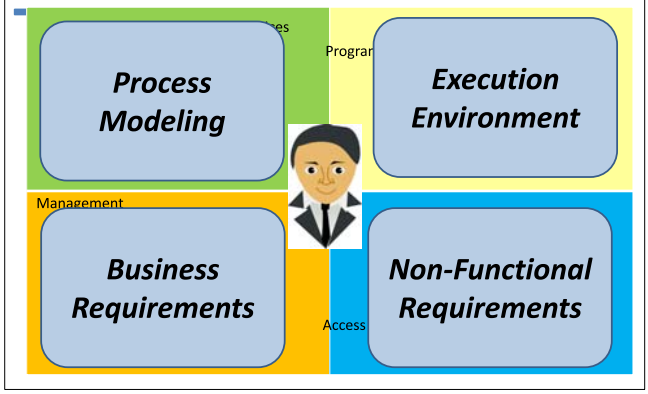
Model-Driven Software Development

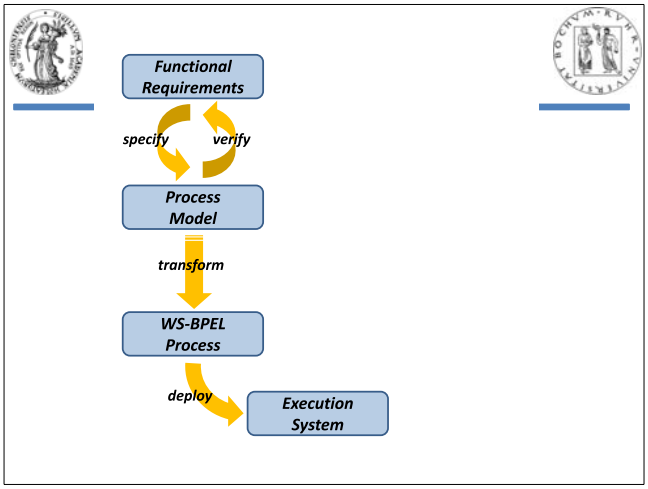


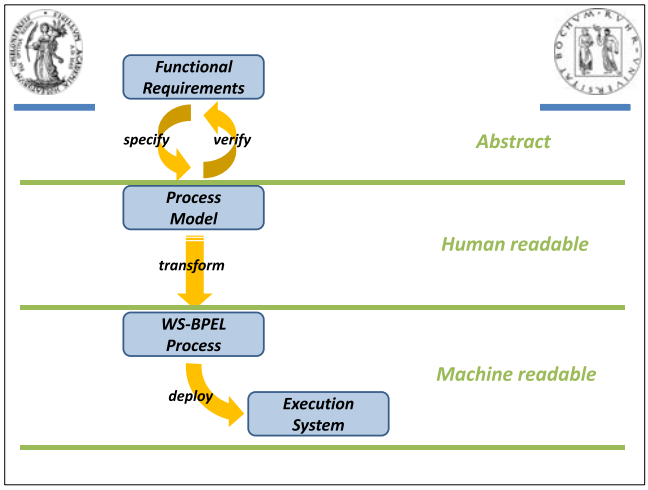
Model-Driven Software Development

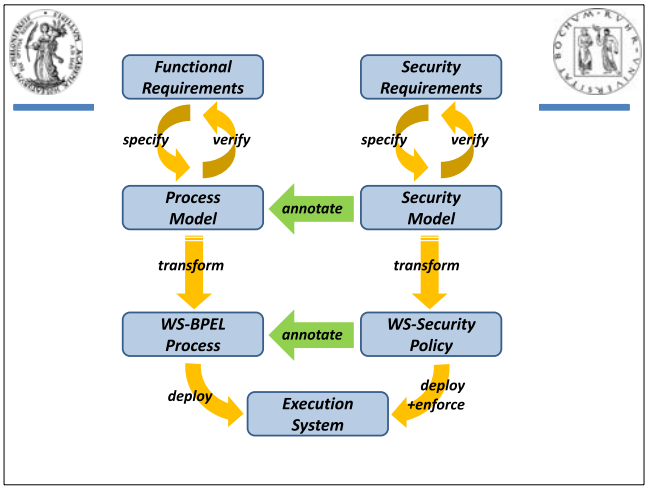


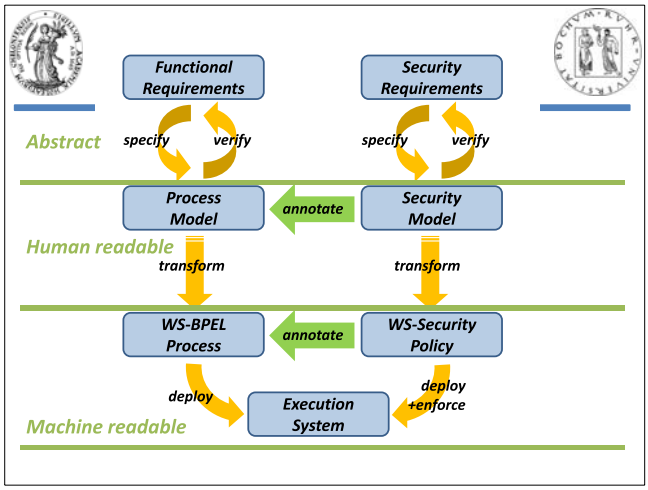
Model-Driven Software Development

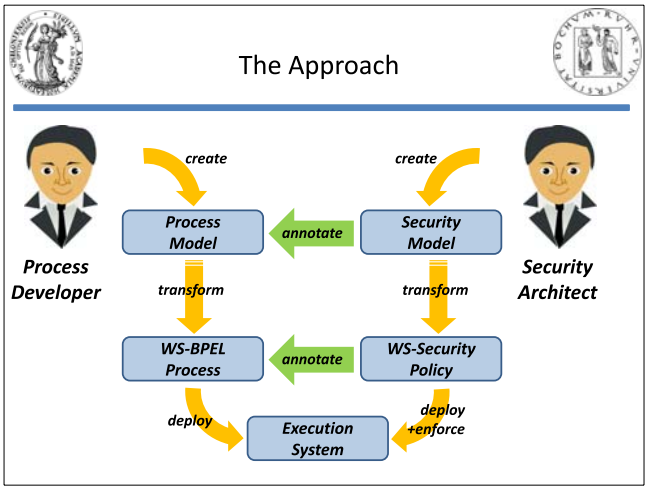




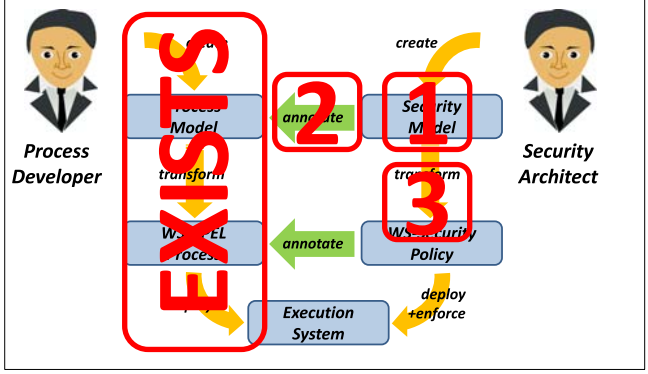




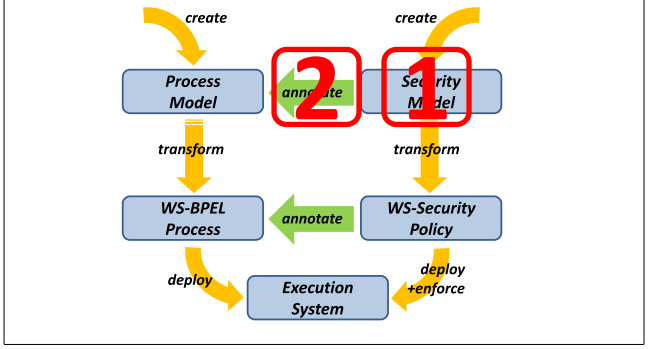




The Approach



The Model



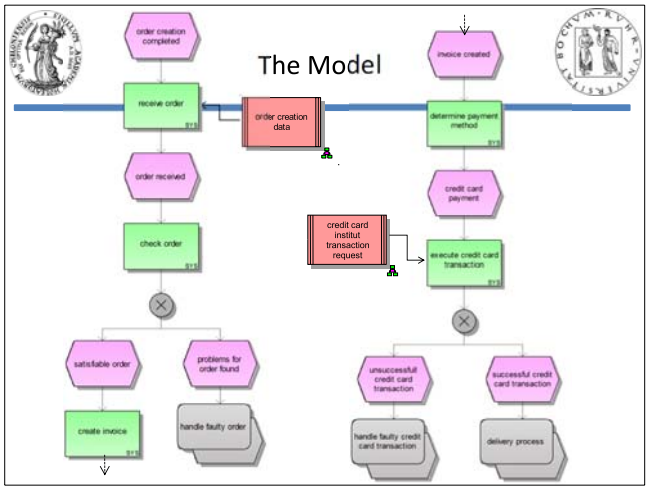
The Model

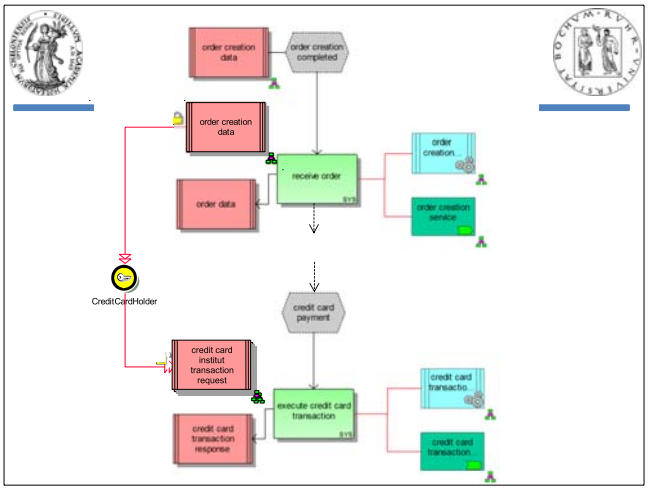
- A common security model…
  - …annotates the process model
  - …represents all security-related aspects of the underlying process model
  - …enables separation of responsibilities

The Model

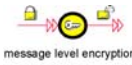
- A „cool“ security model…
  - …can be automatically transformed into appropriate applications of cryptographic algorithms
  - …can be used as a basis for security auditing and verification
  - …is not bound to a single process modeling language

The Model





The Model



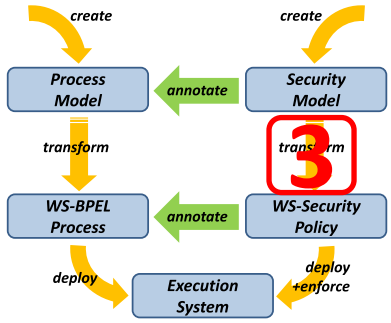
Encryption at the SOAP message level

Encryption at the XML data level

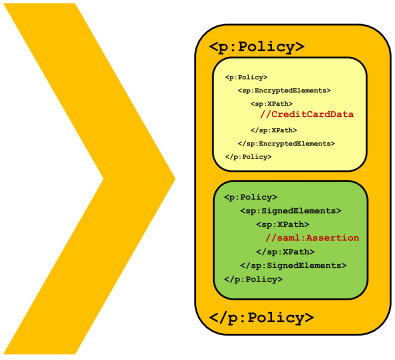
Digital Signature at the XML data level

Authentication Token required
at the SOAP message level

The Transformation



The Transformation



The Transformation

```
<p:Policy>
   <sp:SymmetricBinding>
      <p:Policy>
         <sp:ProtectionToken>
            [...]
         </sp:ProtectionToken>
         <sp:AlgorithmSuite>
            <p:Policy>
               ?????
            </p:Policy>
         </sp:AlgorithmSuite>
      </p:Policy>
   </sp:SymmetricBinding>
   <sp:EncryptedElements>
      <sp:XPath>
         ?????
      </sp:XPath>
   </sp:EncryptedElements>
</p:Policy>
```

The Transformation

```
<p:Policy>
   <sp:SymmetricBinding>
      <p:Policy>
         <sp:ProtectionToken>
            [...]
         </sp:ProtectionToken>
         <sp:AlgorithmSuite>
            <p:Policy>
               ?????
            </p:Policy>
         </sp:AlgorithmSuite>
      </p:Policy>
   </sp:SymmetricBinding>
   <sp:EncryptedElements>
      <sp:XPath>
         /Envelope/Body/order/CreditCardData
      </sp:XPath>
   </sp:EncryptedElements>
</p:Policy>
```

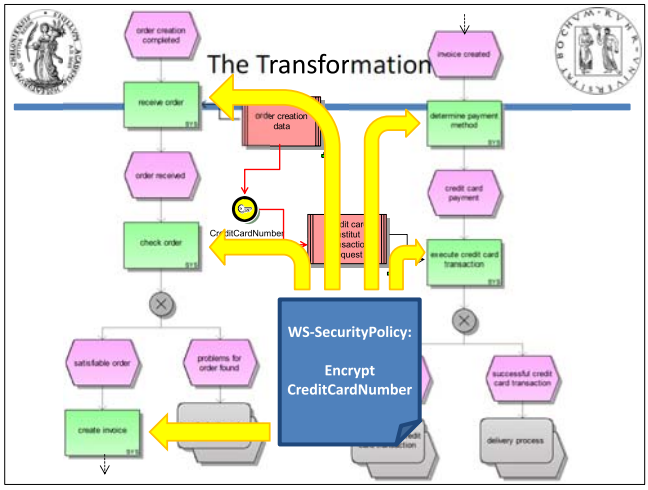
What is to be encrypted?

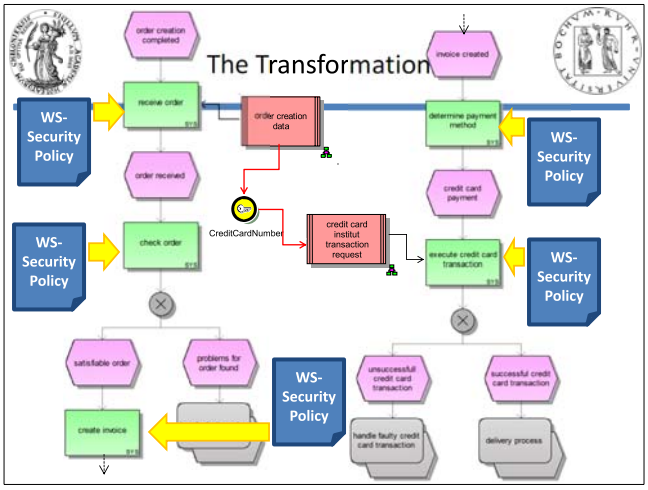
The Transformation

```
<p:Policy>
   <sp:SymmetricBinding>
      <p:Policy>
         <sp:ProtectionToken>
            [...]
         </sp:ProtectionToken>
         <sp:AlgorithmSuite>
            <p:Policy>
               <sp:TripleDesRsa15/>
            </p:Policy>
         </sp:AlgorithmSuite>
      </p:Policy>
   </sp:SymmetricBinding>
   <sp:EncryptedElements>
      <sp:XPath>
         /Envelope/Body/order/CreditCardData
      </sp:XPath>
   </sp:EncryptedElements>
</p:Policy>
```

How is it to be encrypted?

What is to be encrypted?





Conclusion

- Model-Driven Security Development
  - Model Basis: Process Model
  - Model Tool: Security Model
  - Model Transformation: WS-SecurityPolicy
- Support security development process
- Automate what can be automated
- Encapsulate cryptologic details

Future Work

- Include more security properties (e.g. SSL)
- Define End-to-End Security in WS-SecurityPolicy
- Make more features of WS-SecurityPolicy available in the security model
- Use the security-annotated model to prove privacy properties or compliance
- Required: Secure generation of XML Security data formats from WS-Policy

Thank you!

Questions?

Jörg Schwenk (joerg.schwenk@rub.de)
Meiko Jensen (Meiko.Jensen@ruhr-uni-bochum.de)
Sven Feja (svfe@informatik.uni-kiel.de)

SOA SECURITY IN DER PRAXIS
ENTWURFSMUSTER FÜR EINE SICHERE UMSETZUNG

SOA Security Arbeitsgruppe des Teletrust e.V

Der IT-Sicherheitsverband TeleTrusT Deutschland wurde im Jahr 1989 gegründet, um verlässliche Rahmenbedingungen für den vertrauenswürdigen Einsatz von Informations- und Kommunikationstechnik zu schaffen.

TeleTrusT entwickelte sich rasch zu einem bekannten Kompetenznetzwerk für IT-Sicherheit, dessen Stimme in Deutschland und Europa gehört wird.

Heute vertritt TeleTrusT mehr als 100 Mitglieder aus Industrie, Wissenschaft und Forschung sowie öffentlichen Institutionen.

In Projektgruppen zu aktuellen Fragestellungen der IT-Sicherheit und des Sicherheitsmanagements tauschen die Mitglieder ihr Know-how aus. So wird die TeleTrusT "European Bridge CA" betreut, nach deren Standards für sichere E-Mail-Kommunikation im Internet über 700.000 sog. Public-Key-Zertifikate bestehen. Das Personenzertifizierungsprogramm "TeleTrusT Information Security Professional" (T.I.S.P.) qualifiziert Experten für IT-Sicherheit.

Quelle: http://www.teletrust.de/ueber-teletrust/ziele-und-nutzen/

ABSTRACT

Service-orientierte Systeme gehen aufgrund ihrer dezentralen und verteilten Natur mit SOA-spezifischen Sicherheitsrisiken einher. Diese Risiken müssen zusammen mit den Risiken, die auch für monolithische Systeme gelten, berücksichtigt werden. Zur Umsetzung von Sicherheit existiert allerdings eine Vielzahl von unterschiedlichen Sicherheitsmechanismen und Protokollen.

Hier setzt dieser Beitrag an. Er greift all die unterschiedlichen Ansätze, Technologien und Methoden im Bereich der Service-orientierten Architekturen auf, um sie in einem Pattern- oder zu Deutsch Entwurfsmusterkatalog zusammenzufassen, welcher es Entwicklern und Sicherheitsverantwortlichen einfacher macht, Alternativen und Möglichkeiten für die Umsetzung von Sicherheit in allgegenwärtigen SOA Sicherheitsszenarien zu finden. So wird ein Modell eines Best Practice Ansatzes für die Sicherheit von SOA einwickelt. Aufbauend auf den im SOA Security Kompendium definierten Schutzzielen Authentizität, Integrität, Vertraulichkeit, Nichtabstreitbarkeit und Autorisierung werden verschiedene Entwurfsmuster vorgestellt und mit Anwendungsfällen, Architekturen und verwendbaren Technologien beschrieben.

TeleTrusT-Studie "SOA Security"

Dr. Bruno Quint, Michael Menzel,
Ivonne Thomas, Eva Saar, Dr. Thomas Störtkuhl

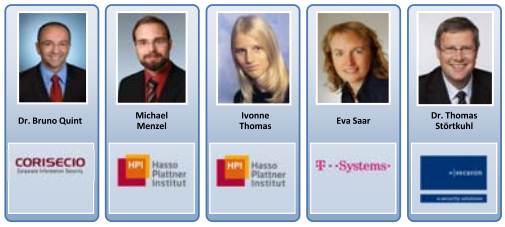
© TeleTrusT Deutschland e.V.

TeleTrusT Deutschland e.V.

- IT-Sicherheitsverband
- 1989 gegründet, für verlässliche Rahmenbedingungen und vertrauenswürdigen Einsatz von IKT
- über 110 Mitglieder aus Industrie, Behörden, Forschung sowie assoziierte Vereine und Verbände
- Arbeitsgruppen zu aktuellen IT-Sicherheitsthemen
- verbandspolitische Stellungnahmen, Pressearbeit, Publikationen, Messe- und Konferenzbeteiligungen
- European Bridge CA (PKI-Infrastruktur)
- T.I.S.P. (IT-Personalzertifizierungsprogramm)

© TeleTrusT Deutschland e.V.

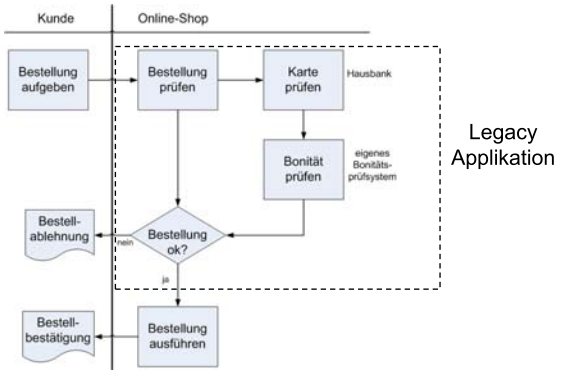
Autoren der Studie



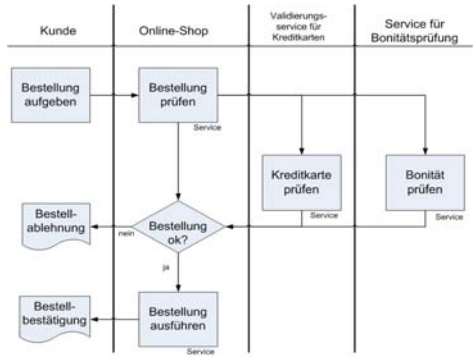
© TeleTrusT Deutschland e.V.

- **Motivation**
- **Vorgehensmodell**
- **Anwendung**

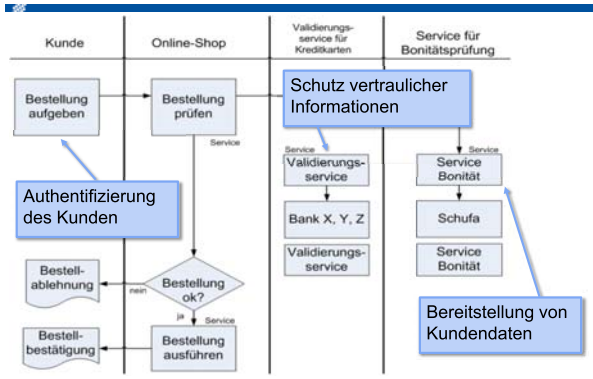
© TeleTrusT Deutschland e.V.



© TeleTrusT Deutschland e.V.



© TeleTrusT Deutschland e.V.



© TeleTrusT Deutschland e.V.

Problemstellung

- Wie können die Sicherheitsanforderungen umgesetzt werden?
- Welche Sicherheitskonzepte sind anwendbar?
- Welche Technologien und Standards sind nutzbar?

Ziele

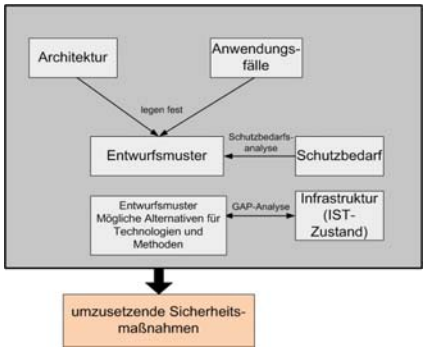
- Entwicklung eines Best Practise Ansatzes
- Beschreibung der bewährten Verfahren mittels Entwurfsmustern
- einfaches Vorgehen mit definierten Elementen

© TeleTrusT Deutschland e.V.

- **Motivation**
- **Vorgehensmodell**
- **Anwendung**

© TeleTrusT Deutschland e.V.

Elemente und Vorgehen

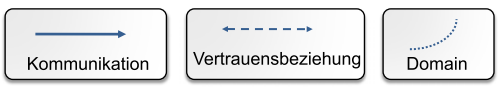


© TeleTrusT Deutschland e.V.

Architektur

- Bausteine

- Beziehungen

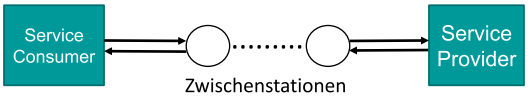


© TeleTrusT Deutschland e.V.

Architektur

- Nachrichtenaustausch
  - Direkter Service Request ohne Antwort
  - Direkter Service Request mit Antwort
  - Direkter Service Request mit Antwort und Bestätigung
  - Indirekter Service Request mit Antwort über Zwischenstationen
- Vertrauensbeziehungen
  - Direktes Vertrauensverhältnis
  - Indirektes Vertrauensverhältnis mittels Security Provider

Beispiel: Indirekter Service Request mit Response über Zwischenstationen



© TeleTrusT Deutschland e.V.

Anwendungsfälle

- Spezifizieren Zielstellung und Rahmenbedingungen
- Vorgabe der Sicherheitsziele
- Definiert für
  - **Authentizität**
  - **Autorisierung**
  - **Integrität**
  - **Vertraulichkeit**
  - **Nichtabstreitbarkeit**

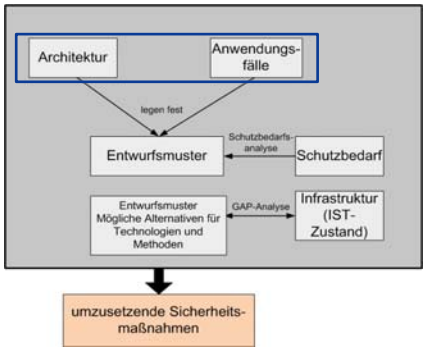
© TeleTrusT Deutschland e.V.

Beispiel eines Anwendungsfalls

Authentifizierung – Wie sind die Benutzer einem Service bekannt? / Wer soll einen Service benutzen dürfen?	
Anmelden eines Service Consumers bei einem Service Provider (Authentifizierung bei einem Web Service)	**Auth_U2**

© TeleTrusT Deutschland e.V.

Elemente und Vorgehen



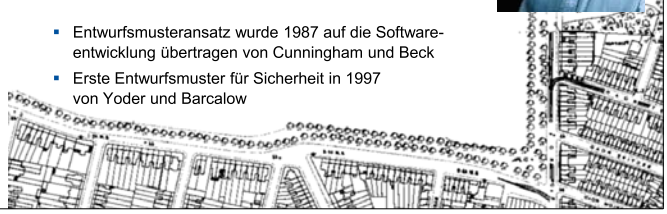
© TeleTrusT Deutschland e.V.

Entwurfsmuster

„Each pattern describes a problem which occurs over and over again in our environment, and then describes the core of the solution to that pattern…"

Christopher Alexander, „A Pattern Language", 1977

- Entwurfsmusteransatz wurde 1987 auf die Software-entwicklung übertragen von Cunningham und Beck
- Erste Entwurfsmuster für Sicherheit in 1997 von Yoder und Barcalow



© TeleTrusT Deutschland e.V.

Struktur eines Entwurfsmusters

Name	Bezeichnung des Musters
Context	Beschreibung der Umgebung *(hier: Architekturbeschreibung)*
Problem	Beschreibung eines nicht-trivialen Problems *(hier: Anwendungsfall)*
Forces	Bedingungen *(hier: Entwurfsmusterauswahl)*
Solution	Lösungsansatz des Problems

© TeleTrusT Deutschland e.V.

Auswahl eines Entwurfsmusters

Architektur

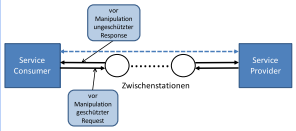
	(A2) mit (A5) Direkte Kommunikation beidseitige Vertrauensbeziehung	**(A4) mit (A5)** Indirekte Kommunikation beidseitige Vertrauensbeziehung
(DS_U1) Daten-übermittlung	→ **(P4)** Integrität des Kommunikationskanals gewährleistet	→ **(P1)** Integrität des Request gewährleistet → **(P2)** Integrität der Response gewährleistet → **(P3)** Integrität des Requests und der Response gewährleistet

Anwendungsfall

Verweis zu den Sicherheitspattern

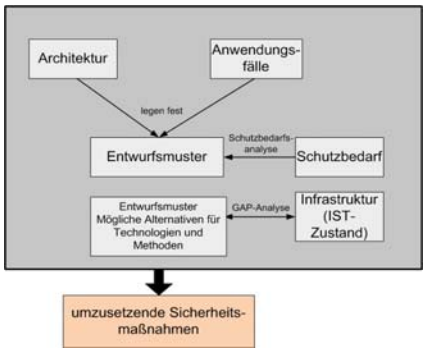
© TeleTrusT Deutschland e.V.

Beispiel Entwurfsmuster

Muster P3: Integrität des Request und der Response gewährleistet	
Beschreibung	
Beispielszenarien	…
Beispiele für Technologien	Schutzziel: Schutz der Integrität des Requests Technologie: digital signierte Message (XML-Signature)

© TeleTrusT Deutschland e.V.

Weiteres Vorgehen

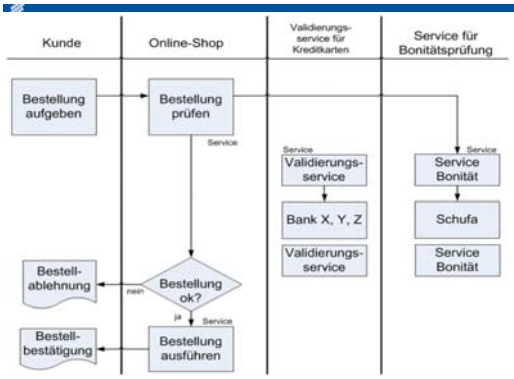


umzusetzende Sicherheits-maßnahmen

© TeleTrusT Deutschland e.V.

- **Motivation**
- **Vorgehensmodell**
- **Anwendung**

© TeleTrusT Deutschland e.V.



© TeleTrusT Deutschland e.V.

Anwendungsschritte

1. Identifizierung der zutreffenden Architektur

Kommunikation	Architektur
Bestellung aufgeben; Bestellablehnung erhalten	A4 *Indirekte Kommunikation* A5 *beidseitige Vertrauensbeziehung*
Bestellung aufgeben; Bestellinformationen erhalten	*A4 Indirekte Kommunikation* A5 *beidseitige Vertrauensbeziehung*

2. Identifizierung der zugehörigen Anwendungsfälle

Kommunikation	Anwendungsfall
Bestellung aufgeben; Bestellablehnung erhalten	DS_U1 *Datenübermittlung*
Bestellung aufgeben; Bestellinformationen erhalten	DS_U1 *Datenübermittlung*

© TeleTrusT Deutschland e.V.

Anwendungsschritte

3. Auswahl der Entwurfsmusters

	(A4) mit (A5) Indirekte Kommunikation beidseitige Vertrauensbeziehung
(DS_U1) **Datenübermittlung**	→ **(P3)** Vertraulichkeit des Requests und der Response gewährleistet

4. Bestimmung des Schutzbedarfs

Kommunikation	Schutzziel	Schutzbedarf
Nr.1: Bestellung aufgeben	Vertraulichkeit	Hoch, da personenbezogene Daten übertragen werden

© TeleTrusT Deutschland e.V.

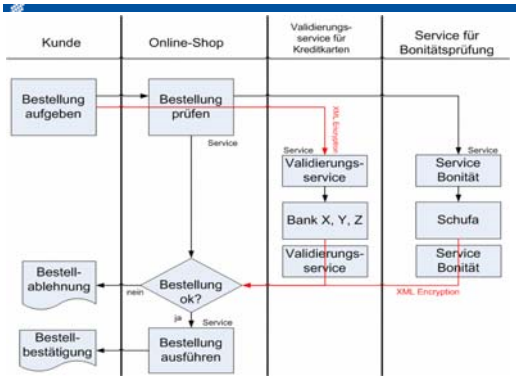
Anwendungsschritte

5. Auswahl der möglichen Technologien und Methoden

Schutzbedarf	Technologien und Methoden
normal	SSL/TLS XML Signature, XML Encryption
hoch	XML Signature, XML Encryption

6. Auswahl der umzusetzenden Technologien und Methoden auf der Grundlage von bereits existierender Infrastruktur

© TeleTrusT Deutschland e.V.



© TeleTrusT Deutschland e.V.

TeleTrusT-Studie "SOA Security"

**Dr. Bruno Quint, Michael Menzel,
Ivonne Thomas, Eva Saar, Dr. Thomas Störtkuhl**

© TeleTrusT Deutschland e.V.

Hasso Plattner Institut
IT Systems Engineering | Universität Potsdam

MODELLIERUNG UND UMSETZUNG VON SICHERHEITS-ANFORDERUNGEN IM SOA SECURITY LAB

DIPL. INF. MICHAEL MENZEL

Doktorand, Hasso-Plattner-Institut

Michael Menzel hat an der Universität Trier das Studium der Informatik absolviert. Er ist seit 2006 Doktorand im Forschungskolleg „Service-oriented Systems Engineering" am Hasso-Plattner-Institut und gehört zur Forschungsgruppe „Internet Technologien und Systeme" von Prof. Dr. Christoph Meinel. Seine Forschungsschwerpunkte liegen in den Bereichen Sicherheit in Service-orientierten Architekturen, Webservice Technologien und modellgetriebene Sicherheit. Seine Erfahrung in diesen Bereichen konnte er in verschiedene Projekte einbringen und hat unter anderem als Verfasser an dem SOA Security Kompendium 2.0 des Bundesamtes für Sicherheit in der Informationstechnik mitgewirkt.

ABSTRACT

Service-orientierte Architekturen ermöglichen eine dynamische Bereitstellung und Orchestrierung von Diensten, um eine schnelle Anpassung an Geschäftsanforderungen zu gewährleisten. Web Services bieten die technologische Grundlage zur Umsetzung dieses Paradigmas und unterstützen eine Vielzahl von verschiedenen Sicherheitsmechanismen und -ansätzen. Die Sicherheitsanforderungen eines Dienstes werden deklarativ in Sicherheitspolicies spezifiziert, ergänzen die Dienstbeschreibung und ermöglichen so Interoperabilität zur Laufzeit. Allerdings weisen Policysprachen für SOA eine hohe Komplexität auf, sie sind schwierig und fehleranfällig in der Kodifizierung.

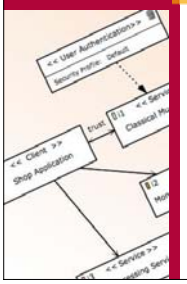
Um eine einfache Generierung von Sicherheitsanforderungen möglich zu machen, verfolgen wir einen modell-getriebenen Ansatz, basierend auf der Modellierung von Sicherheitsanforderungen in Architekturmodellen. Diese Anforderungen werden dann über ein domänenunabhängiges Modell in Sicherheitspolicies transformiert. Die Transformation der Anforderungen auf komplexe Policies kann allerdings nur erfolgen, wenn Expertenwissen darüber vorhanden ist, welche Sicherheitsprotokolle, Mechansimen und Optionen Verwendung finden sollen. Daher werden formalisierte Entwurfsmuster zur Transformation herangezogen, die dieses Wissen repräsentieren.

Hasso Plattner Institut
IT Systems Engineering | Universität Potsdam

Dieser Vortrag führt unsere Modellierungssprache SecureSOA ein, die eine Annotation von Sicherheitsanforderungen in Systemarchitekturen sowie die entwurfsmustergestützte Transformations auf Sicherheitspolicies ermöglicht. Die Umsetzung dieses Konzeptes wird anhand des SOA Security LABs demonstriert, das auf dem IEEE Service Cup den 1. Platz erzielt hat.

HPI Hasso Plattner Institut

IT Systems Engineering | Universität Potsdam



Modellierung und Umsetzung von Sicherheitsanforderungen im SOA Security Lab

Dipl. Inf. Michael Menzel

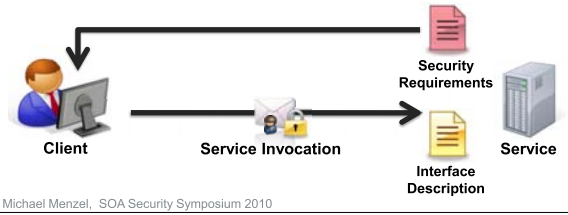
Research School
Hasso-Plattner-Institute
University of Potsdam, Germany

Security in SOA

HPI Hasso Plattner Institut

Services in SOA are self-descriptive

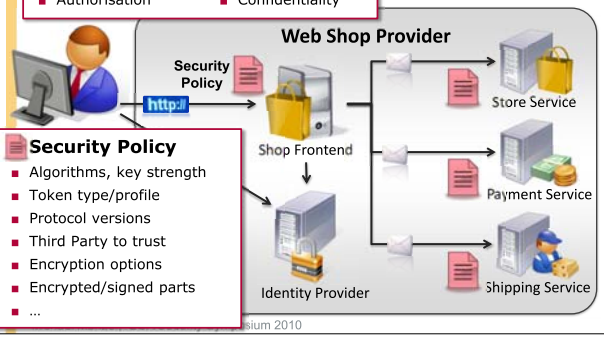
What about Security?



Security in SOA – Security Policies

HPI Hasso Plattner Institut

Security requirements
- Authentication
- Integrity
- Authorisation
- Confidentiality



Security Policy
- Algorithms, key strength
- Token type/profile
- Protocol versions
- Third Party to trust
- Encryption options
- Encrypted/signed parts
- ...

Security in SOA – Security Policies

HPI Hasso Plattner Institut

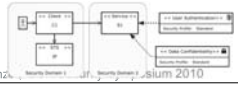
How to generate security policies for SOA?

security configurations depend on the use case and the desired security level.

- Policy Editor / Profiles

Our Recommendation:

- Model-driven Transformation



Security Requirements

↓

Visual Representation in System Models

↓

Security Policy

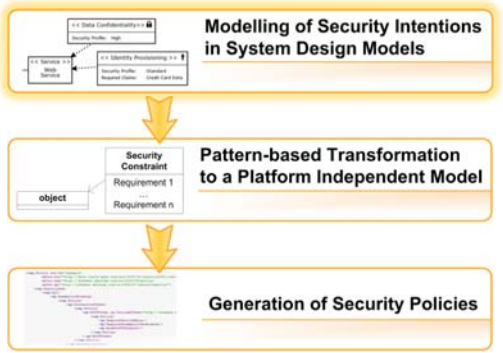
Agenda

HPI Hasso Plattner Institut

- Model-Driven Security in SOA
- The SOA Security LAB
- Conclusion

Model-driven Policy Generation

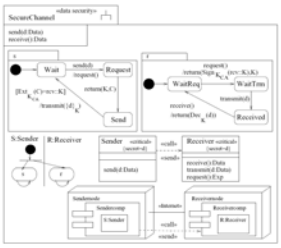
HPI Hasso Plattner Institut



Modelling Security – Related Work

UMLsec – Secure System Development with UML

- enables a formal verification of security requirements



➔ Does not provide a simple, high-level notion for security intensions

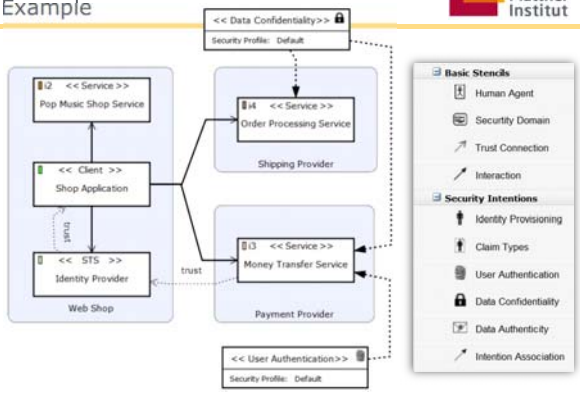
Modelling Security in SOA

SecureSOA

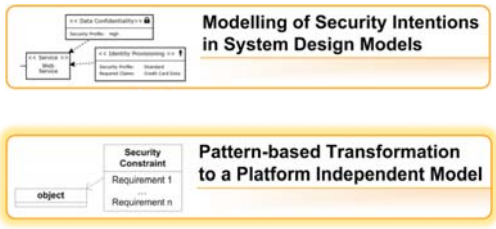
- Modelling language to state security intentions for Service-oriented Systems.
- Integration in any system design modelling language

Abstract Syntax	Concrete Syntax	Formal Semantics
Specifies the language elements.	Specifies the graphical notion.	1) Specifies the meaning. 2) Enables a formal verification.

Example



Security in SOA – Security Policies



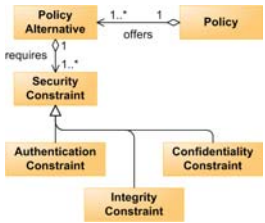
Policy Generation - SOA Security Meta Model

SOA Security Meta Model – Security Policy

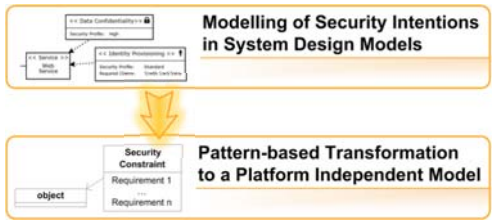
- Express sets of requirements as alternatives

Security Constraints

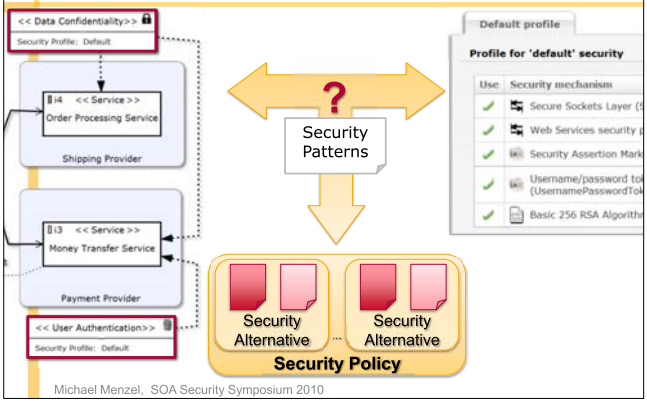
- State security requirements
- Constraints are defined for
  - Authentication
  - Confidentiality
  - Integrity



Security in SOA – Security Policies



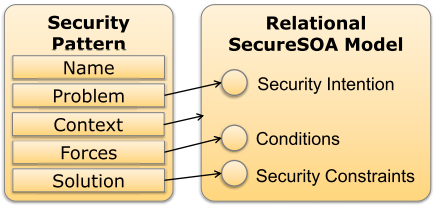
Policy Generation - Transforming Security Intentions



Policy Generation - Transforming Security Intentions

Using Security Patterns

- Security pattern are informal!
- → formal specification of security configuration pattern

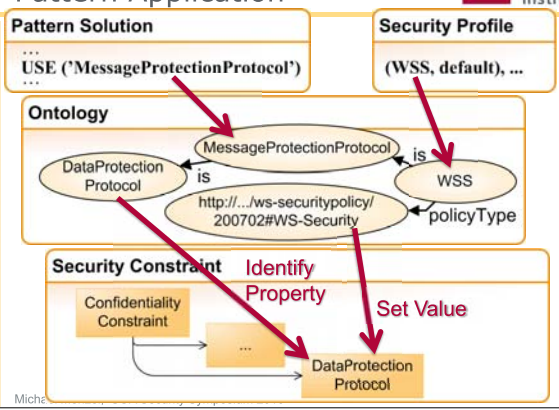


Policy Generation - Transforming Security Intentions

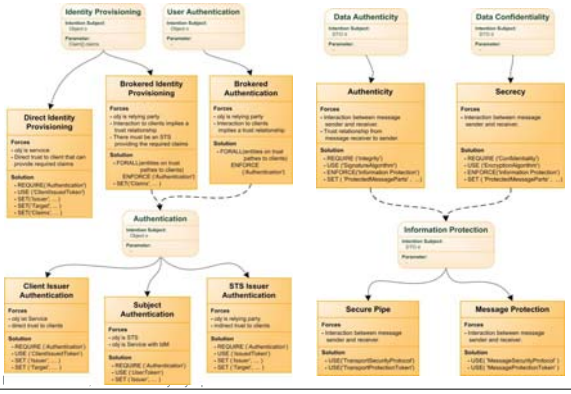
Security Pattern Example

Name:	Subject Authentication
Problem:	Authentication
Forces:	
1	ASSERT (Trust(intention.subject, Client))
2	ASSERT (
3	(STS CONTAINS intention.subject) OR
4	(Service CONTAINS intention.subject AND
5	NOT(TrustPath(intention.subject,Client) CONTAINS STS)))
Solution:	
1	REQUIRE ('*Authentication*')
2	USE ('*UserToken*')
3	SET ('*Issuer*', Clients.where({Trust(intention.subject, it)}))

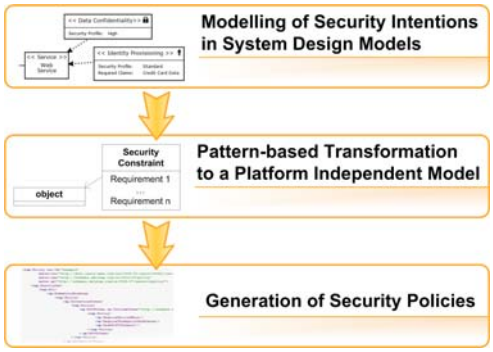
Policy Generation - Pattern Application



Policy Generation - A Pattern-System for SOA Security



Model-driven Policy Generation



Agenda

- Model-Driven Security in SOA
- The SOA Security LAB
- Conclusion

The SOA Security LAB

Building composed applications based on Web Services

- Required Service Configurations
  - Interface Definition (WSDL)
  - XML Schemata
  - Security Policies
  - Key Stores with certificates
  - Trust Stores with certificates
  - Security Callback Handlers
  - Access to Security Services

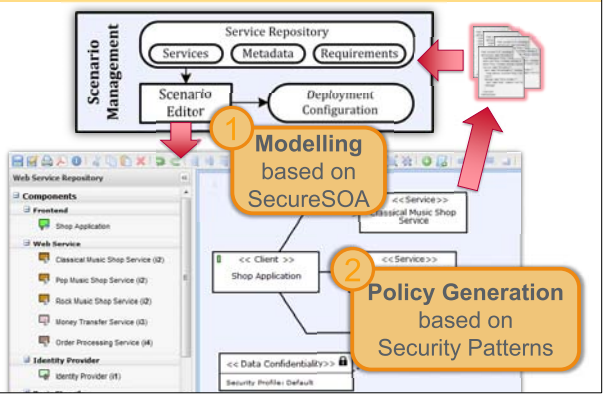
reusable

self-descriptive

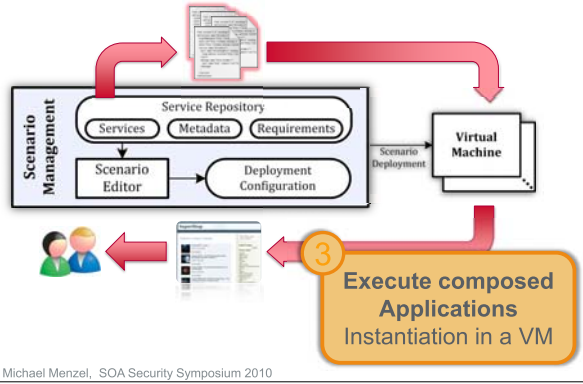
composable

➡ **Our Solution: A virtualized test environment for service security**

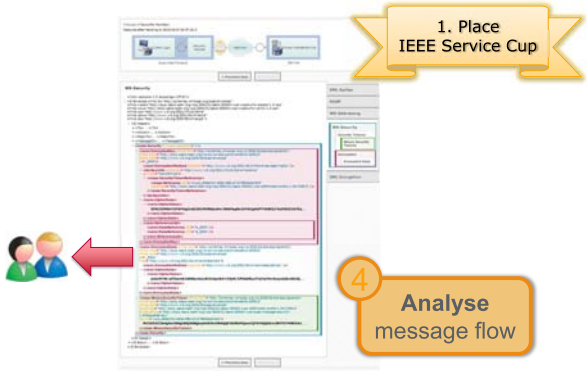
The SOA Security LAB



The SOA Security LAB



The SOA Security LAB

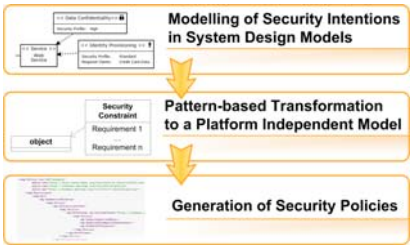


Agenda

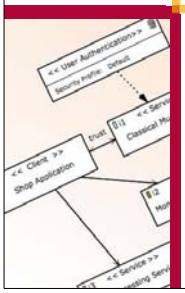
- Model-Driven Security in SOA
- The SOA Security LAB
- Conclusion

Conclusion

Model-driven Security in SOA



➔ **The SOA Security LAB:**
A model-driven Platform to test service security



Modellierung und Umsetzung von Sicherheitsanforderungen im SOA Security Lab

Dipl. Inf. Michael Menzel

Research School
Hasso-Plattner-Institute
University of Potsdam, Germany

FACETS OF SECURE IDENTIFICATION

PROF. DR. VOLKER ROTH

Lehrstuhl Secure Identity, Institut für Informatik, Freie Universität Berlin

Prof. Dr.-Ing. Volker Roth is Bundesdruckerei GmbH Endowed Professor for Secure Identity in the Mathematics and Computer Science department of Freie Universität Berlin, Germany. His work focuses on innovative applications of secure identity technology, systems security, and the usability and safety of information security technology. Before, he worked for a Fuji Xerox research laboratory in the Silicon Valley, as the Chief Technology Officer of a company in the midwest of the USA, and as a researcher and deputy department head at a Fraunhofer Institute.

ABSTRACT

Gestiftet von der Bundesdruckerei GmbH fing im April 2009 die Arbeitsgruppe Sichere Identität der Freien Universität Berlin mit ihrer Arbeit an. In diesem Vortrag stellen wir diese Arbeitsgruppe vor, und auch die Themen, mit denen sich die Gruppe bisher befasst hat und noch befassen moechte. Ein Aspekt der bisherigen Arbeiten, der besonders beleuchtet werden soll, ist die Untersuchung von Konzepten fuer sichere Identitäten in neuartigen und innovativen Anwendungsbereichen. Hierzu stellen wir Arbeiten zu sogenanntem Identitätskapital vor, zur sicheren Autorisierung von Smartcard-Operationen ohne zertifizierte Terminals, und zu Methoden, wie Interaktionen auf Multi-Touch Tischen sicher einzelnen Nutzern zugeordnet werden können.

MANAGING RELIABLE DIGITAL IDENTITIES

IVONNE THOMAS, MSC.
Doktorandin, Hasso-Plattner-Institut

Ivonne Thomas, MSc has been working in the area of identity and trust management for five years with a particular focus on web services technologies. During these years, she has been working with people at SAP Research in Brisbane, Australia as well as in the Security and Trust Group of SAP Research in Sophia Antipolis, France.

Since 2007, she is working full-time on her PhD as a member of the Hasso-Plattner Institute Research School on "Service-oriented Systems Engineering". As part of her research, she is working on models and technologies towards a trustworthy and reliable management of digital identities in decentralized environments as SOA and the Internet.

Ivonne Thomas is also one of the faces behind the new SOA Security Kompendium published by the Bundesamt für IT Sicherheit (BSI), author of several articles in magazines as for example in "kes- Die Zeitschrift für Informationssicherheit" and a frequent speaker at events as e.g. Cebit 2009: "SOA Security and the World of Digital Identities" or the European Identity Conference 2010.

ABSTRACT

Looking at the current online world, performing transactions as online banking, online shopping or communicating in social networks has become an inherent part of life. Hereby, personal, identity-related data plays a major role, since for many activities a service provider requires details about the identity of a user.

However, does a service provider always require our true identity? Often a service provider just needs to recognize a user on repeated visits in order to offer personalized services. Only if critical transactions are involved as for example in online banking transactions a service provider has to be sure that a user's identity matches with the real-life identity.

In her talk, Ivonne Thomas presents the HPI Identity Provider, which distin-

guishes between verified digital identities and user-created identities (anonymous identities). The identity provider is based on the Identity Metasystem and the notion of claims and has been extended to include trust-related identity meta information. In her talk, she shows how service providers can use this information to derive access control decisions according to the level of trust they require for a certain transaction.

Hasso Plattner Institut
IT Systems Engineering | Universität Potsdam

Managing Reliable Digital Identities in SOA and the Web

Ivonne Thomas

HPI Research School
Chair "Internet Technologies and Systems"
of Prof. Dr. Christoph Meinel

October 2010

Motivation

The law states that southkorean web sites with at least 100,000 daily visitors must force users to register with verifiable real names.

Real Name Policy Act, South Korea, 2009

- Very controversial!, BUT:
  - we find different requirements for the reliability of identity attributes in the online world
  - users have verified identities besides anonymous identities
  - user need to decide which identity to use in correspondence with the provider

Identity Assurance Frameworks

- need to trust on information from a foreign party is inherent to open identity management systems!
- basic principle: **cluster trust requirements** into levels of trust
- A level of trust (level of assurance (LoA))
  - reflects the **degree of confidence** that a relying party can assign to the assertions made by another identity provider with respect to a users identity information
- Several initiatives have formed and proposed approaches

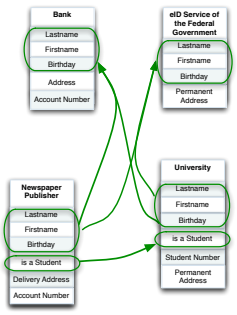
Identity Assurance Frameworks Examples

- UK Office of the e-Envoy
  - "Registration and Authentication – E-Government Strategy Frame-work Policy and Guideline"
- US e-Authentication Initiative
  - "E- Authentication Guidance for Federal Agencies" (OMB M-04-04)
- NIST
  - "Electronic Authentication Guideline"(NIST 800- 63)
- InCommon federation
  - Identity Assurance Assessment Framework
  - Bronce and Silver Profile

Assurance Frameworks Limitations

- Identity is mostly considered as a whole
  - no distinction between different qualities of trust
- no changes of a trust level over time
  - identity attributes are gathered during the registration and often fix
- hard to reflect the uniqueness of identity providers with regard to their ability to assert certain identity attributes

Everybody is Identity Provider Everybody is Relying Party



- Every Participant on the Internet
  - needs identity information
  - has identity information, he could share
- Aim:
  - Decentralized storage of identity information to
    - reduce redundancy
    - ease maintenance

AGENDA

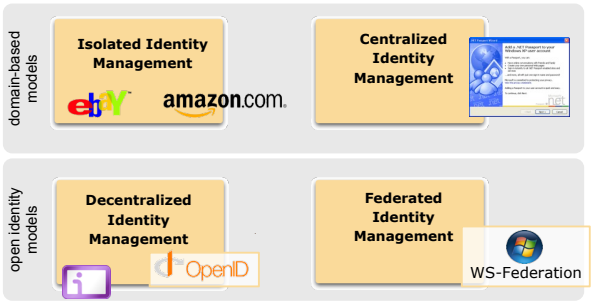
7

- Motivation & Introduction
- Related Work: Assurance Frameworks
  - Limitations
- The need for Levels of Assurance for Attributes
  - Background: Open Identity Management Models
  - A Layered Trust Model
  - Identity Trust Ontology
- An Identity Provider to manage Reliable Digital Identities
  - The HPI Identity Provider
  - Demo
- Conclusion

Identity Management in SOA

8

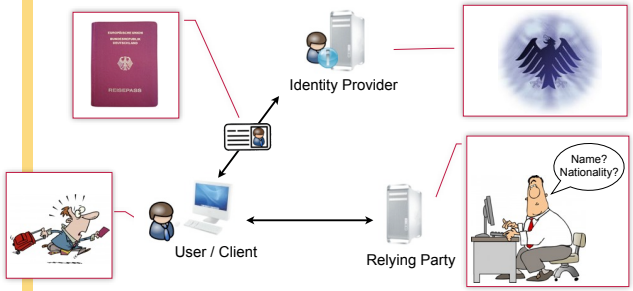
Various approaches exist to manage users in SOA:



Open Identity Management Models

9

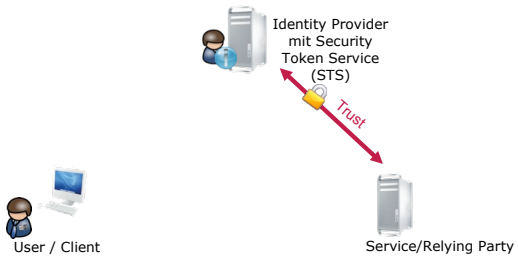
- Three different roles:



How does it work?

10

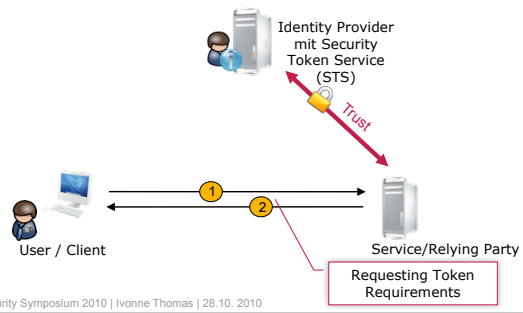
- Identity information is described by claims
- Information Card enable a user to manage and select his digital identities



How does it work?

10

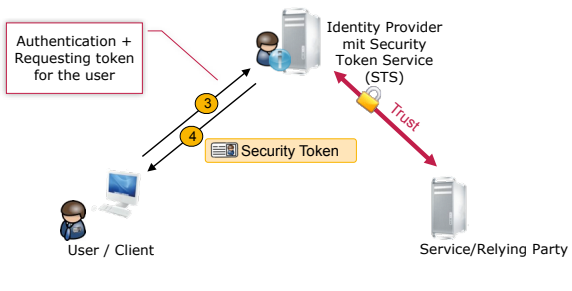
- Identity information is described by claims
- Information Card enable a user to manage and select his digital identities



How does it work?

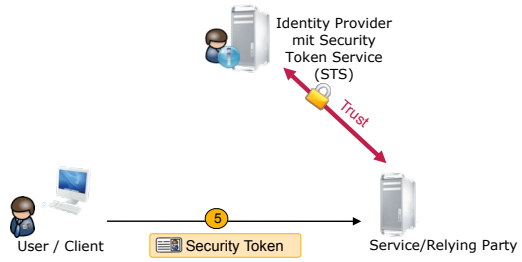
10

- Identity information is described by claims
- Information Card enable a user to manage and select his digital identities



How does it work?

- Identity information is described by claims
- Information Card enable a user to manage and select his digital identities



What about trust?

- Open Identity Management Models allow
  - to state the attributes a relying party requires on a per-claim basis

Online Store
Lastname
Firstname
Birthday
is a Student
Delivery Address
Customer ID
Account Number

- Trust
  - is usually defined in a general manner
    - between organizations
    - complex contracts balance the risk between independent organizations

Two-Layer Trust Model

Trust is required on two levels

- between the service provider and the identity provider
  - general requirement to trust the **issuer** of an assertion
  - **= Organizational Trust**
- for a request: between the service provider and the requester
  - for a concrete request to trust the **subject** of an assertion
  - **= Identity Trust**

Identity Assurance Meta Information - Motivating Example

Bank	highly trusted
Lastname	verified by In-Person Proofing
Firstname	verified by In-Person Proofing
Birthday	verified by In-Person Proofing
Address	verified by independent bank channel
Account Number	verified: issuer-controlled

eID Service of the Federal Government	highly trusted
Lastname	verified from ePa
Firstname	verified from ePa
Birthday	verified from ePa
Permanent Address	verified from ePa

underlying contract

well-known authority

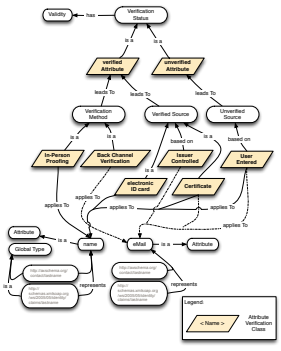
same federation

Newspaper Publisher	Requirements
Lastname	verified
Firstname	verified
Birthday	verified
is a Student	verified: issuer-controlled
Delivery Address	any
Account Number	verified: issuer-controlled

University	trusted
Lastname	unverified: user entered
Firstname	unverified: user entered
Birthday	unverified: user entered
is a Student	verified: issuer-controlled
Student Number	verified: issuer-controlled
Permanent Address	unverified: user entered

Identity Trust Ontology and Verification Classes

- Verification Classes can be
  - hierarchical
  - easily extended
  - apply to certain attribute types
- Examples
  - verified & unverified
  - In-Person Proofing
  - Independent Back Channel
  - Issuer-Controlled
  - Proof by electronic ID card
  - Proof by certificate
  - User-Entered



The model behind

- Facts, e.g.:
  - *attribute*(isStudent),
  - *identityprovider*(university), ..
  - *idPTrustLevel*(trusted), idPTrustLevel(highly_trusted)
  - *isHigherThan*(trusted, highlytrusted)
  - *attributeVerificationClass*(issuer-controlled)
  - *corresponds*(proof_by_certificate,verified)
  - *assertion*(university, isStudent, issuer_controlled)
  - *hasTrustLevel*(university,trusted)
  - *federatedIdP*(university)
- and rules:
  - *isTrusted*(I):=*federatedIdP*(I) ∨ *trustedIdP*(I) ∨ *hasTrustLevel*(I,TL).
  - *assertingIP*(I,A,V):= *corresponds*(X,V),*assertion*(I,A,X).
  - ...

The model behind

15

- Find matching verification context classes for a requested attribute
  - All attributes of type x that have been verified
- Find matching Identity Provider
  - The Relying Party requires an attribute age from the user who proved his age by registering in person at the IP
  - The Relying Party requires a verified credit card number from a federated Identity Provider
- Facts, e.g.:
  - *attribute(isStudent),*
  - *identityprovider(university), ..*
  - *idPTrustLevel(trusted), idPTrust*
  - *isHigherThan(trusted, highlytrus*
  - *attributeVerificationClass(issuer*
  - *corresponds(proof_by_certificat*
  - *assertion(university, isStudent, i*
  - *hasTrustLevel(university,trusted*
  - *federatedIdP(university)*
- and rules:
  - *isTrusted(I):=federatedIdP(I) ∨ tr*
  - *assertingIP(I,A,V):= correspond*
  - ...

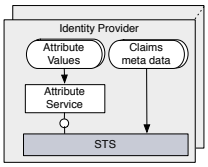
AGENDA

16

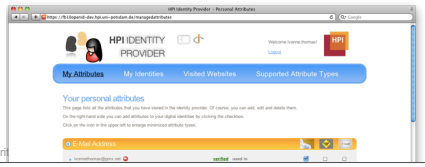
- Motivation & Introduction
- Related Work: Assurance Frameworks
  - Limitations
- The need for Levels of Assurance for Attributes
  - Background: Open Identity Management Models
  - A Layered Trust Model
  - Identity Trust Ontology
- An Identity Provider to manage Reliable Digital Identities
  - The HPI Identity Provider
  - Demo
- Conclusion

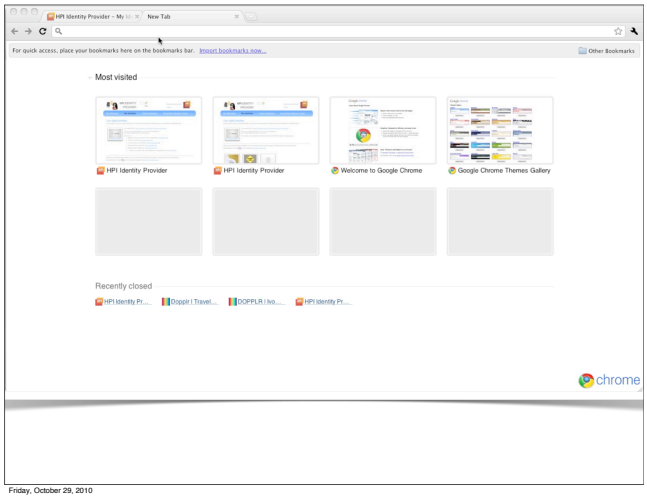
The HPI Identity Provider

17



- Identity Provider
  - Add, Edit, Remove Attributes
  - Manage various identities
  - Request identity information and receive security tokens
  - different protocols are possible:WS-Trust, OpenID
  - Verify certain attributes





Thank you.

19

Contact:

Ivonne Thomas
Research School on "Service-Oriented Systems Engineering"
Hasso-Plattner-Institute, University of Potsdam

Website: http://kolleg.hpi.uni-potsdam.de/index.php?id=3721

KEYNOTE: SOA SECURITY IN DEN ZEITEN DES CLOUD COMPUTING

JAN PETERS

Jan Peters, Dipl.-Informatiker, Security Architect
Global Business Services, IBM Deutschland GmbH

Jan Peters, Studium der Informatik an der Technischen Universität Darmstadt, anschließend wissenschaftlicher Mitarbeiter und Projektleiter in der Abteilung Sicherheitstechnologie des Fraunhofer-Instituts für Graphische Datenverarbeitung IGD, seit 2008 Security Architect & Consultant bei Global Business Services der IBM Deutschland GmbH. Er berät Kunden in den Themenbereichen IT-Sicherheit und Datenschutz, insbesondere im Bezug auf Service-orientierte Architekturen, erstellt Sicherheitskonzepte und ist in IT-Projekten für die Konzeption von IT-Sicherheitslösungen verantwortlich. Fachliche Schwerpunkte sind SOA- und Webservice-Sicherheit, Identity & Access Managment, Angewandte Kryptographie und PKI, sowie Infrastruktur- und Middleware-Design. Technische Spezialisierung ist die Integration von IBM WebSphere DataPower SOA Appliances in Service-orientierte Architekturen.

ABSTRACT

Die folgenden Themen sind Inhalt der Keynote:

- Web Services und XML-Sicherheit: Aktuelle Probleme
- SOA Security Appliances und das IBM SOA Reference Model
- Cloud Computing und Cloud Security
- IBM's Cloud Computing Strategie

IBM Deutschland GmbH

SOA Security in den Zeiten des Cloud Computing

Jan Peters (Security Architect)

2. SOA Security Symposium
Potsdam, 29. Oktober 2010

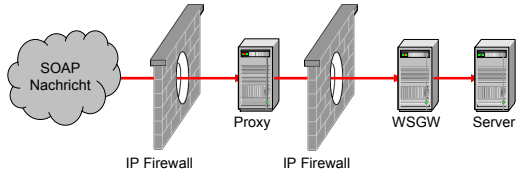
© 2010 IBM Corporation

Agenda

1. SOA Security
   - Web Services und XML-Sicherheit
   - SOA Security Appliances
   - IBM SOA Reference Model
2. Cloud Computing
   - Definition
   - Cloud Security
   - IBM Strategie
3. Zusammenfassung / Referenzen

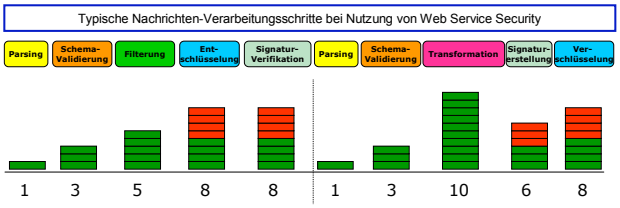
Problematik bei der Einführung von Web Services

1. Durch die Einführung von Web Services ohne weiter gehende Sicherheitsmechanismen werden Backend-Anwendungen einer neuen Klasse von Angriffen ausgesetzt.



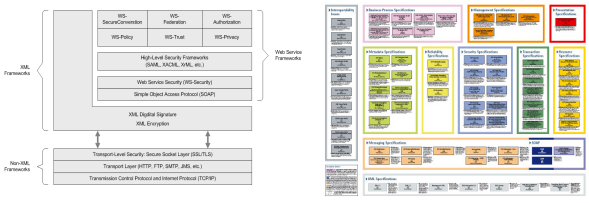
Problematik bei der Einführung von Web Services

2. Die Verwendung von Web Services Security ist aufwendig und benötigt typischer Weise deutlich mehr Hardware- und Software-Ressourcen bei den verarbeitenden Systemen.



Problematik bei der Einführung von Web Services

3. Die Vielfalt der existierenden Web Services Standards erfordert ein fundiertes Verständnis der Thematik und die entsprechende Unterstützung bei den beteiligten Komponenten.



[Quelle: innoQ; http://www.innoq.com/soa/ws-standards/poster/]

XML-spezifischen Gefahren und Attacken

- Single-Message X-DoS
  - XML Entity Expansion und Recursion Attacks
  - XML Document Size Attacks
  - XML Document Width Attacks
  - XML Document Depth Attacks
  - XML Wellformedness-based Parser Attacks
  - Jumbo Payloads
  - Recursive Elements
  - MegaTags – Jumbo Tag Names
  - Coercive Parsing
  - Public Key DoS
  - Schema Poisoning
- Multiple-Message X-DoS
  - XML Flood
  - Resource Hijack
- Unauthorized Access Attacks
  - Dictionary Attack
  - Falsified Message
  - Replay Attack
- Data Integrity/Confidentiality Attacks
  - Message Tampering
  - Data Tampering
  - Message Snooping
  - XPath/XSLT Injection
  - SQL injection
  - WSDL Enumeration
  - Routing Detour
  - Malicious Morphing
  - Signature Wrapping Attack
- System Compromise Attacks
  - Malicious Include / XML External Entity (XXE) Attack
  - Memory Space Breach
  - XML Encapsulation
  - XML Virus (X-Virus)

1. Beispiel – Single-Message X-DoS Attack

- Coercive parsing/recursive element example – Billion Laughs

```
<?xml version="1.0"?>
  <!DOCTYPE billion [
  <!ELEMENT billion (#PCDATA)>
  <!ENTITY laugh0 "ha">
  <!ENTITY laugh1 "&laugh0;&laugh0;">
  <!ENTITY laugh2 "&laugh1;&laugh1;">
  ...
  <!ENTITY laugh127 "&laugh126;&laugh126;">
  ]> <billion>&laugh127;</billion>
```

- A completely valid, well-formed XML document
- When submitted to parser, quickly exhausts memory/CPU

 © 2010 IBM Corporation

2. Beispiel – Single-Message X-DoS Attack

- SOAP Array Attack example

```
<soapenv:Envelope xmlns:soapenv="..." xmlns: soapenc:"...">
  <soapenv:Body>
    <ns1:FunctionWithArrayInput xmlns:ns1="...">
      <DataSet xsi:type="soapenc:Array„
       soapenc:arrayType="xsd:string[1000000]">
        <item xsi:type="xsd:string">Data1</item>
        <item xsi:type="xsd:string">Data2</item>
        <item xsi:type="xsd:string">Data3</item>
      </DataSet>
    </ns1:FunctionWithArrayInput>
  </soapenv:Body>
</soapenv:Envelope>
```

- A parser might reserve memory for 1000000 string elements

 © 2010 IBM Corporation

Gartner: Web Services Security Best Practices

Provide System Security
- Inspect ALL traffic
- Transform all messages
- Mask internal resources
- Implement XML filtering
- Secure logging
- Protect against XML DoS
- Require good authentication mechanisms

Ask for Compatibility
- SSL MA, SAML, x.509.
- WS-Security
- WS-* extensions

Provide Message Security
- Sign all messages
- Validate messages (Inbound+Outbound)
- Time-stamp all messages

Build Centralized Infrastr.
- SSL is key
- Use management/security platforms
- Manage your identities
- You may need PKI

sonstiges
- Build Expertise/Design From Strength
- Educate Business Leaders
- Trust (Really) Your Partners
- Use OTS Web Services with Caution
- Monitor and Control

Gartner

> "Therefore, enterprises should investigate tools such as security gateways, SSL concentrators and accelerators, and wire-speed SOAP/XML inspection hardware."

[Quelle: John Pescatore, Gartner]

 © 2010 IBM Corporation

Wo sollte XML Web Services Security umgesetzt werden

Erste Sicherungsebene: *XML Security Gateway*
- Performance – deutlicher Geschwindigkeitsgewinn gegenüber Softwaresystemen
- Skalierbarkeit – Minimierung der notwendigen Systemanzahl trotz Ausbaufähigkeit
- Handhabbarkeit – Einfache Konfiguration durch weniger Enforcement Points
- Einfachheit – Keine Notwendigkeit, Anwendungen anzupassen
- Sicherheit – Verschiebung der Sicherheit von der Anwendung auf das Gateway
- Verfügbarkeit – Schutz vor üblichen und XML-spezifischen Angriffen
- Interoperabilität – Mediation zwischen verschiedenen Transportstandards
- Monitoring-fähig – Einfache (Audit-)Protokollierung auf dem Enforcement Point

Zweite Sicherungsebene: Web Services Application
- Handhabbarkeit – Integration mit Container-basierter Sicherheit (e.g, .NET, J2EE)
- Sicherheit – Einbettung fachspezifischer Sicherheitsmechanismen in der Anwendung

 © 2010 IBM Corporation

SOA (Security) Appliances definiert – aus Sicht von IBM

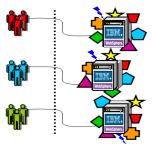
SOA Appliances sind
- gehärtete Sicherheitskomponenten – durch Penetrationstests validiert
- zielgerichtet entwickelte, eingebettete Systeme – optimiert für die SOA-Verarbeitung
- hoch konfigurierbar – vereinfachte Abbildung von SOA-Architekturmuster
- in der Lage, verschiedenste Datenformate zu verarbeiten – sowohl XML als auch andere
- standardbasiert – Integrationsfähigkeit in bestehende Infrastrukturen

SOA Appliances sind nicht
- ein universell nutzbarer Server mit vorinstallierter Software
- ein System mit installiertem Standard-Betriebssystem
- herkömmliche Netzwerkkomponenten (unterhalb Netzwerkebene 7)
- Java-basiert

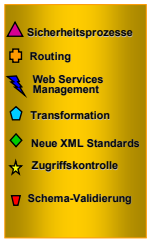
 © 2010 IBM Corporation

Zentralisierung und Vereinfachung von Schlüsselfunktionen

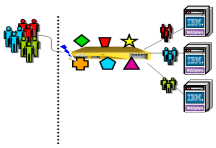
Ohne SOA Appliances



Aktualisierung einzelner Applikationsserver



Mit SOA Appliances



Bereitstellung zentraler Funktionen in einem Gerät

 © 2010 IBM Corporation

Eine spezialisierte Lösung: IBM WebSphere DataPower SOA Appliances

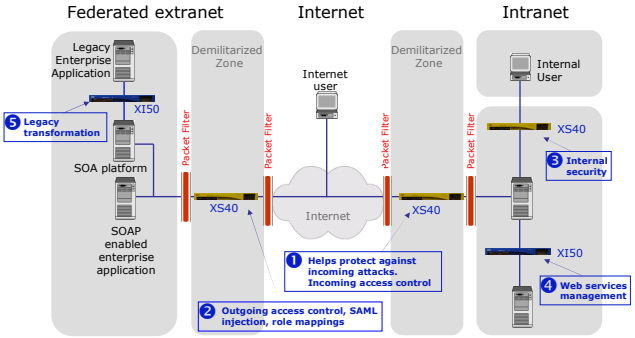
- Spezialisiert für die Integration, Absicherung und Beschleunigung von SOA
- Vielfältige Funktionen in einem einzelnen Gerät
- Tiefe Integration in IBM Software und Software anderer Anbieter
- Hohe Sicherheitszertifizierungen verlangen zuverlässige Hardware
- Hohe Performance durch Hardwarebeschleunigung
- Einfache Inbetriebnahme, benutzerfreundliches Systemmanagement

Mehrwert für Kunden durch hohe SOA-Performance und Sicherheit

- **Vereinfachung** von SOA durch spezialisierte Geräte
- **Beschleunigung** durch hohen XML-Durchsatz
- **Absicherung** von SOA/XML-Implementierung

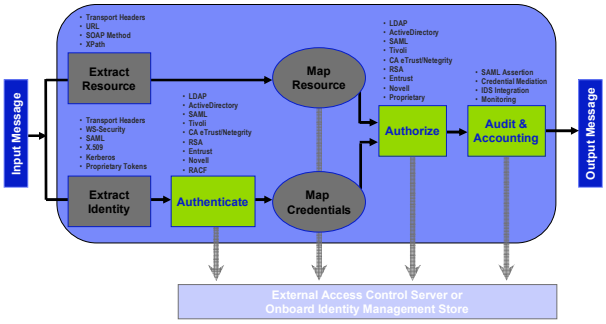
© 2010 IBM Corporation

Einsatzszenarios



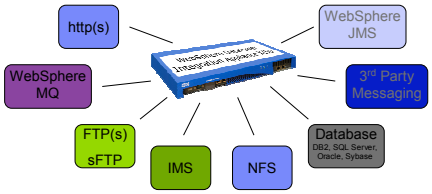
© 2010 IBM Corporation

Access Control Integration Framework (AAA)



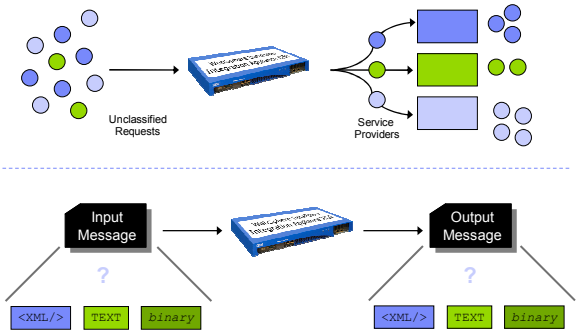
© 2010 IBM Corporation

Protokoll-Mediation



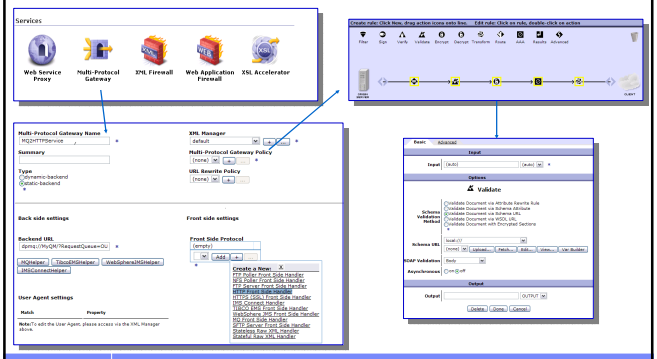
© 2010 IBM Corporation

Inhaltsbasiertes Routing / Nachrichten-Transformation



© 2010 IBM Corporation

Integrierte ESB-Funktionalität durch Konfiguration



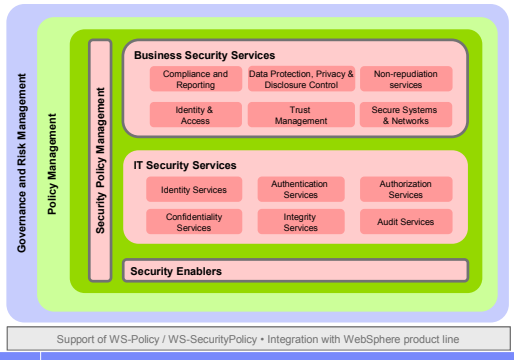
© 2010 IBM Corporation

Unterstützte Standards

- Network
  - SNMP (v1/v2c, v3), VRRP, NTP, NFS
  - Syslog, Syslog-NG
- Transport
  - HTTP/HTTPS, FTP/SFTP
  - ODBC (DB2, MS SQL, Oracle, Sybase)
  - MQ, JMS, IMS
  - JSON, REST
- Authentication/Authorization
  - LDAP, RBM, RADIUS, NSS/RACF, Kerberos
- XML
  - XML, XPATH, XSLT, XML Binary
  - SOAP (v1.1/v1.2), UDDI, WSDL
  - WSRR, WSDM
- WS-I
  - Basic Profile v1.1, Basic Security Profile v1.0
  - Attachments Profile v1.0, SwA Profile v1.0/v1.1
- Anti Virus
  - ICAP
- WS-Security
  - XML Digital Signature
  - XML Encryption
  - SAML (v1.0, v1.1, v2.0)
  - WS-Security
  - WS-SecureConversation
  - WS-Policy
  - WS-SecurityPolicy
  - WS-Trust
  - XACML
- WS-*
  - WS-ReliableMessaging
  - WS-Adressing
  - WS-Routing
- Cryptography
  - XKMS
  - RSA, 3DES, DES, AES, SHA
  - X.509, PKCS, CRL, OCSP
- Further Industry Standards (binary formats)
  - Electronic Data Interchange (EDI)
  - COBOL Copybook
  - ISO 8583 (Banking)
  - Unstructured Text

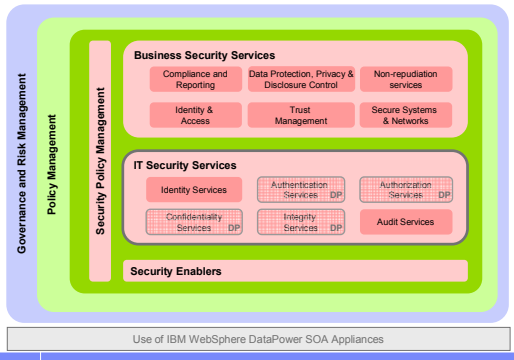
 © 2010 IBM Corporation

Positionierung im IBM SOA Security Referenzmodell



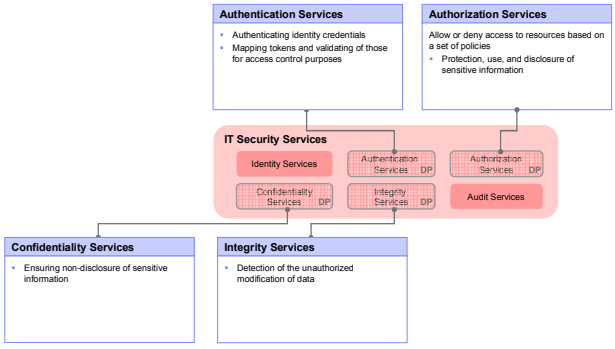
 © 2010 IBM Corporation

Positionierung im IBM SOA Security Referenzmodell



 © 2010 IBM Corporation

Positionierung im IBM SOA Security Referenzmodell



 © 2010 IBM Corporation

Agenda

1. SOA Security
   - Web Services und XML-Sicherheit
   - SOA Security Appliances
   - IBM SOA Reference Model
2. Cloud Computing
   - Definition
   - Cloud Security
   - IBM Strategie
3. Zusammenfassung / Referenzen

 © 2010 IBM Corporation

Cloud: eine Definition

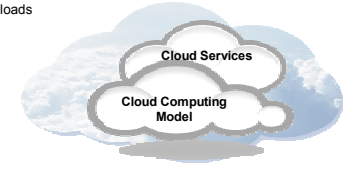
IBM: "Cloud is a new consumption and delivery model inspired by consumer Internet services."

Enabler-Technologien für Clouds

- **Pooling und Virtualisierung** von Ressourcen
- **Automatisierung** von Service Management
- **Standardisierung** von Workloads

Clouds als Enabler für:

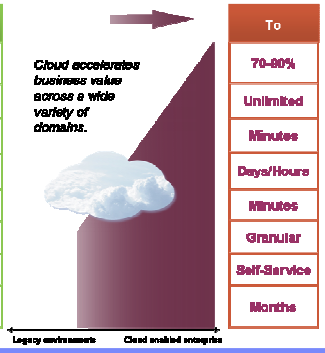
- Self-service
- Sourcing-Optionen
- Flexible Bezahlmodelle
- Skalierbarkeit



 © 2010 IBM Corporation

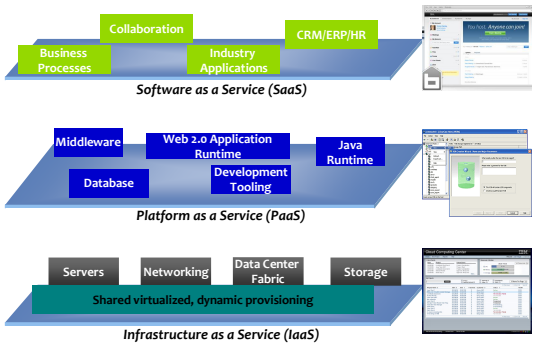
Domänenspezifische Vorteile von Cloud Computing

Capability	From	To
Server/Storage Utilization	10-20%	70-90%
Self service	None	Unlimited
Test Provisioning	Weeks	Minutes
Change Management	Months	Days/Hours
Release Management	Weeks	Minutes
Metering/Billing	Fixed cost model	Granular
Standardization	Complex	Self-Service
Payback period for new services	Years	Months



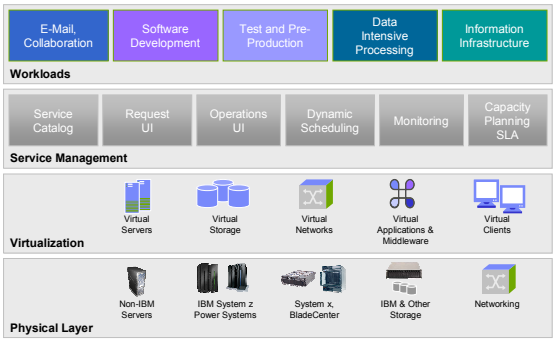
© 2010 IBM Corporation

"IT-as-a-Service"-Ebenen



© 2010 IBM Corporation

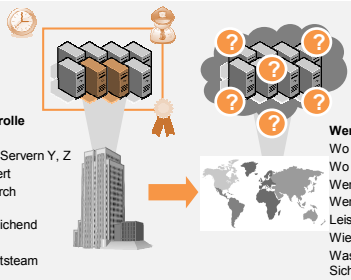
Workload-Analyse



© 2010 IBM Corporation

Gründe für teilweise neue Sicherheitsrisiken und -anforderungen

Rechenzentrum von heute | **Public Clouds von morgen**



Wir haben die Kontrolle
Befindet sich bei X
Gespeichert auf den Servern Y, Z
Backups implementiert
Zugriffssteuerung durch Administratoren
Betriebszeit ist ausreichend
Prüfer sind zufrieden
Motiviertes Sicherheitsteam

Wer hat die Kontrolle?
Wo ist der Standort?
Wo erfolgt die Speicherung?
Wer übernimmt die Backups?
Wer hat Zugriff?
Leistungsfähigkeit?
Wie prüfen die Prüfer?
Was leistet unser Sicherheitsteam?

© 2010 IBM Corporation

Sicherheit ist kritischstes Problem bei der Einführung von Cloud Lösungen

80 %
der Unternehmen betrachten das Thema Sicherheit als primäres Hemmnis für die Einführung von Cloud Lösungen.

48 %
der Unternehmen machen sich Gedanken über die Zuverlässigkeit von Clouds.

33 %
der Befragten machen sich Sorgen, dass sich Clouds negativ auf die Einhaltung von gesetzlichen Vorschriften auswirken könnten.

„Wie können wir sicher sein, dass keine Datenlecks existieren und die Anbieter über die Technologie und die Governance verfügen, um zu verhindern, dass ihre Mitarbeiter Daten stehlen?"

„Sicherheit ist unsere größte Sorge. Über andere Dinge wie Zuverlässigkeit, Verfügbarkeit usw. mache ich mir keine großen Gedanken."

„Ich ziehe interne Clouds IaaS vor. Wenn der Service intern gehalten wird, fühle ich mich mit der gebotenen Sicherheit wesentlich wohler."

[Quelle: Driving Profitable Growth Through Cloud Computing, IBM Studie]

© 2010 IBM Corporation

Individuelle Kundenprobleme beim Thema Sicherheit

Schutz des geistigen Eigentums und der Daten	30 %
Durchsetzung gesetzlicher/vertraglicher Verpflichtungen	21 %
Unberechtigte Nutzung von Daten	15 %
Vertraulichkeit der Daten	12 %
Verfügbarkeit der Daten	9 %
Integrität der Daten	8 %
Test und Auditierbarkeit der Providerumgebung	6 %
Andere	3 %

[Quelle: Deloitte Enterprise@Risk: Privacy and Data Protection Survey]

© 2010 IBM Corporation

Typische Kundenanforderungen zum Thema Sicherheit

Governance, Risk Management, Compliance
- Prüfung durch Dritte (SAS 70(2), ISO27001, PCI)
- Kundenzugriff auf mandantenspezifische Protokoll- und Prüfinformationen / -daten
- Effektives Incident Reporting für Mandanten
- Transparenz beim Change, Incident, Image Management usw.
- Flexible Service-Level-Agreements
- Support für Forensik
- Support für E-Discovery

Anwendungen und Prozesse
- Anwendungssicherheit für Clouds wird formuliert als Image-Sicherheit
- Compliance mit sicheren, bewährten Entwicklungsverfahren

Physischer Zugriff
- Überwachung und Steuerung des physischen Zugriffs

Personen und Identitäten
- Überwachung privilegierter Benutzer inkl. Protokollierung, physische Überwachung und Hintergrundprüfung
- Föderierte Identitäts-/Onboarding-prozesse: Koordination von Authentifizierungen mit Unternehmenssystemen oder Systemen anderer Anbieter
- Standardbasiertes SSO

Daten und Informationen
- Datentrennung
- Kundenseitige Kontrolle der Daten bzgl. den geografischen Standorten
- Behörden: Cloudweite Datenklassifizierung

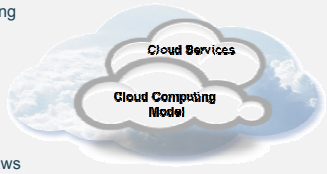
Netzwerk, Server, Endpunkte
- Isolierung zwischen Benutzerdomänen
- Vertrauenswürdige virtuelle Domänen: nichtlinienbasierte Sicherheitszonen
- Integrierte Erkennung und Vorbeugung
- Vulnerability Management
- Schutz von Maschinen-Images gegen Beschädigung und Missbrauch
- Behörden: Trennung auf MILS-Basis

[Quelle: Befragung von IT-Benutzern und verschiedenen Analystenberichte]

 © 2010 IBM Corporation

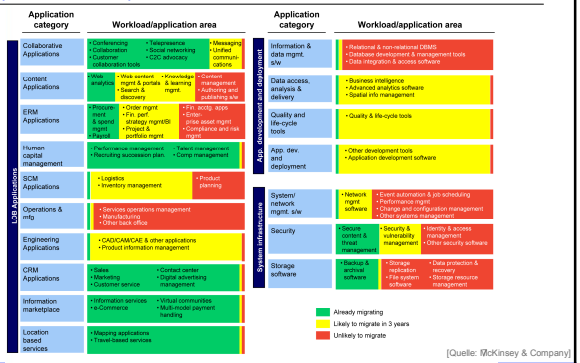
Anforderungen – Cloud Computing & Security

- Data Protection
- Access & Identity Management
- Application Provisioning & Deprovisioning
- Application & Environment Testing
- Service Level Agreement
- Vulnerability Management
- Business Resiliency
- Audit & Governance
- Cross-Border Protection
- Intellectual Property & Export Laws
- Accounting Information



 © 2010 IBM Corporation

Enterprise SaaS Adoption – Stand heute



[Quelle: McKinsey & Company]

 © 2010 IBM Corporation

IBM bietet ein breites Spektrum an Deploymentoptionen

Die wichtigsten privaten Workloads
- Data-Mining, Text-Mining oder andere Analysen
- Sicherheit
- Data-Warehouses oder Datamarts
- Business-Continuity und Disaster-Recovery
- Testumgebungsinfrastruktur
- Langfristige Datenarchivierung/-erhaltung
- Transaktionsdatenbanken
- Branchenspezifische Anwendungen
- ERP-Anwendungen

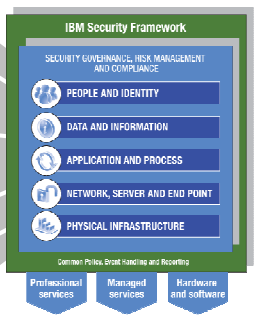
Die wichtigsten öffentlichen Workloads
- Audio/Video/Web-Conferencing
- Service-Help-Desk
- Infrastruktur für Schulungen und Demos
- WAN-Kapazität, VOIP-Infrastruktur
- Desktop
- Testumgebungsinfrastruktur
- Speicher
- Netzwerkkapazität im Rechenzentrum
- Server

Rechen-zentrum im Unternehmen	Rechen-zentrum im Unternehmen	Unternehmen	Unternehmen	Benutzer
Private Cloud	Managed Private Cloud	Gehostete Private Cloud	A B Shared Cloud Services	A B Öffentliche Cloud Services
Im Unternehmen betrieben	Von IBM betrieben	Im IBM Rechenzentrum von IBM betrieben	Im IBM Rechenzentrum von IBM betrieben	Im IBM Rechenzentrum von IBM betrieben

 © 2010 IBM Corporation

Gartners Einschätzung der Sicherheitsrisiken beim Cloud Computing
… lässt sich direkt auf den IBM Security Framework abbilden.

- Privilegierter Benutzerzugriff
- Datentrennung
- Datenwiederherstellung
- Investigativer Support
- Einhaltung gesetzlicher Bestimmungen
- Datenstandort
- Disaster Recovery

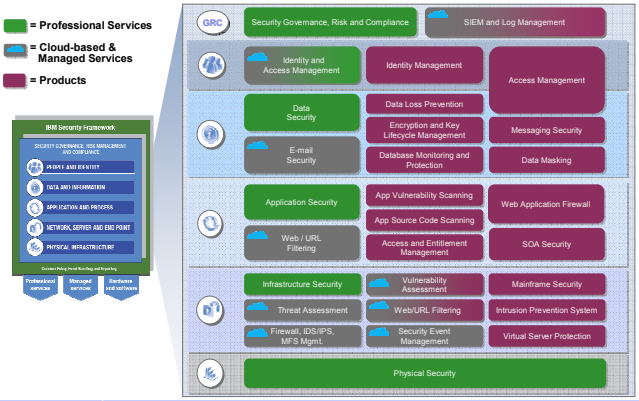


[Quelle: Assessing the Security Risks of Cloud Computing, Juni 2008]

 © 2010 IBM Corporation

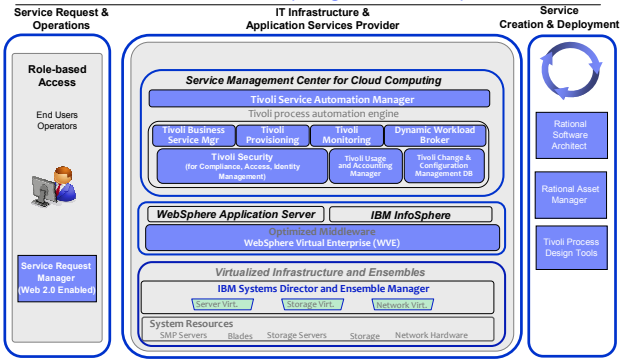
Wie lösen wir die Herausforderungen und gewinnen Mehrwerte?

= Professional Services
= Cloud-based & Managed Services
= Products



 © 2010 IBM Corporation

Architectural Model for Cloud Computing – IBM Produktpalette



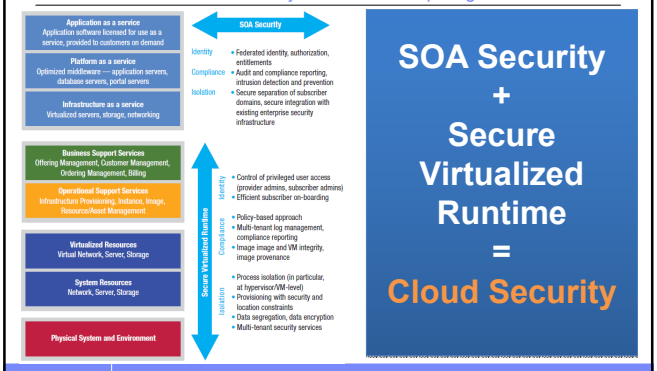
IBM Cloud Services Portfolio

	Analytics	Collaboration	Development and test	Desktop and devices	Infrastructure compute	Infrastructure storage	Business services
Smart business on the IBM cloud Standardized services on the IBM cloud		IBM Lotus Live IBM Lotus® iNotes®	Smart Business Development and Test on the IBM Cloud (beta)	IBM Smart Business Desktop Cloud Smart Business End User Support	IBM Computing on Demand	IBM Information Protection Services	BPM BlueWorks (design tools) Smart business expense reporting on the IBM cloud
IBM Smart Business Services Private *cloud services, behind your firewall*, built and/or managed by IBM	IBM Smart Analytics Cloud		IBM Smart Business Test Cloud	IBM Smart Business Desktop Cloud		IBM Smart Business Storage Cloud	
IBM Smart Business Systems Preintegrated, workload-optimized systems	IBM Smart Analytics System		IBM CloudBurst™ family			IBM Information Archive	Smart Business for Small or Midsize Business (backed by the IBM Cloud)

Agenda

1. SOA Security
   - Web Services und XML-Sicherheit
   - SOA Security Appliances
   - IBM SOA Reference Model
2. Cloud Computing
   - Definition
   - Cloud Security
   - IBM Strategie
3. Zusammenfassung / Referenzen

IBM Point of View: SOA Security and Cloud Computing



IBM RedBooks – Enterprise & SOA Security

- Enterprise Security Architecture Using IBM Tivoli Security Solutions, IBM RedBook 2007
  - http://www.redbooks.ibm.com/abstracts/sg246014.html
- Federated Identity and Trust Management, IBM RedPaper 2008
  - http://www.redbooks.ibm.com/abstracts/redp3678.html
- Case Study: SOA Security and Management Scenario, IBM RedPaper, 2008
  - http://www.redbooks.ibm.com/abstracts/redp4378.html
- IBM Tivoli Security Solutions for Microsoft Software Environments, IBM RedPaper 2008
  - http://www.redbooks.ibm.com/abstracts/redp4430.html
- Understanding SOA Security – Design and Implementation, IBM RedBook, 2008
  - http://www.redbooks.ibm.com/abstracts/sg247310.html
- IBM Tivoli Security Policy Manager, IBM RedPaper, 2009
  - http://www.redbooks.ibm.com/abstracts/redp4483.html
- Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security, RedPaper, 2009
  - http://www.redbooks.ibm.com/abstracts/redp4528.html
- IBM WebSphere DataPower SOA Appliances Series, IBM RedBooks, 2007-2009
  - http://www.redbooks.ibm.com/cgi-bin/searchsite.cgi?query=datapower+and+soa+and+appliances

IBM RedBooks – Cloud Computing & Cloud Security

- Cloud Computing: Save Time, Money, and Resources with a Private Test Cloud, IBM RedGuide, 2009
  - http://www.redbooks.ibm.com/abstracts/redp4553.html
- Cloud Security Guidance – IBM Recommendations for the Implementation of Cloud Security, RedPaper, 2009
  - http://www.redbooks.ibm.com/abstracts/redp4613.html
- WebSphere Cloudburst Appliance and PowerVM, RedBook, 2010
  - http://www.redbooks.ibm.com/abstracts/sg247806.html
- IBM Smart Analytics Cloud, RedBook, 2010
  - http://www.redbooks.ibm.com/abstracts/sg247873.html

Weitere Referenzen

- Guide to Secure Web Service, Special Publication 800-95, NIST, 2007
  - http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf
- WS Security – Scenarios, Patterns, and Implementation Guidance for WSE 3.0, Microsoft, 2005
  - http://msdn.microsoft.com/en-us/library/aa480545.aspx
- Dynamic Infrastructure – Delivering Superior Business and IT Services with Agility and Speed, IBM/Gartner, 2009
  - http://mediaproducts.gartner.com/gc/webletter/ibm_stg/issue3/index.html
- IBM Cloud Computing – Websites
  - http://www.ibm.com/ibm/cloud/
  - http://www.ibm.com/de/cloud/
- IBM WebSphere DataPower SOA Appliances – Website
  - http://www.ibm.com/software/integration/datapower/

© 2010 IBM Corporation

Ihr Ansprechpartner bei IBM

Jan Peters

Global Business Services
Security Architect

Telefon: +49-160-90493839
Mailadresse: jan.peters@de.ibm.com

© 2010 IBM Corporation

SSO MIT SOA: NEUE HERAUSFORDERUNGEN AN DIE EINMALANMELDUNG IM UNTERNEHMEN

MARTIN RAEPPLE

Technology Strategist, SAP AG

Martin Raepple gehört zum Technology Strategy Team im Office of the CTO bei der SAP AG. Hier liegt sein Schwerpunkt auf den Themen Sicherheit und Identitätsmanagement, wo er seit 2005 die Vertretung in Arbeitsgruppen internationaler Standardisierungsgremien wie OASIS und WS-I wahrnimmt. Dort arbeitet er aktiv an der Gestaltung neuer Technologiestandards. Als Schnittstelle zwischen den Gremien und der Entwicklung bei SAP lässt er die Anforderungen der SAP in die Gremiumsarbeit einfließen und bringt die neuesten Erkenntnisse in die Weiterentwicklung der Technologieplattform SAP NetWeaver ein. Darüber hinaus stimmt er sich eng mit Partnern der SAP bei der Planung und Umsetzung von Interoperabilitätsszenarien zwischen SAP NetWeaver und anderen Plattformen ab. Martin Raepple ist Autor mehrerer Fachbücher und regelmäßiger Referent auf internationalen Fachkongressen.

ABSTRACT

Single Sign-On entpuppt sich als Dauerbrenner in der Informationssicherheit, der von flüchtigen Hype-Themen wie Webservices, SOA oder Cloud Computing beflügelt wird. Das veränderte Umfeld stellt die Einmalanmeldung im Unternehmen jedoch vor neue Herausforderungen. Hierbei spielen Standards eine zentrale Rolle, um in heterogenen Systemlandschaften und über Unternehmensgrenzen hinweg Anwendungen und Services mit möglichst geringem Aufwand in bestehende SSO-Infrastrukturen zu integrieren. Der Vortrag gibt einen Überblick zu aktuellen Lösungsansätzen für typische Szenarien und zeigt auf, welche Herausforderungen in Bezug auf die Interoperabilität und Integration neuer Service-Technologien noch bestehen.

Single Sign-on in SOA
New Challenges for the Enterprise

HPI SOA Security Symposium 2010

Martin Raepple, Technology Strategy, SAP AG
29. Oktober 2010

THE BEST-RUN BUSINESSES RUN SAP™

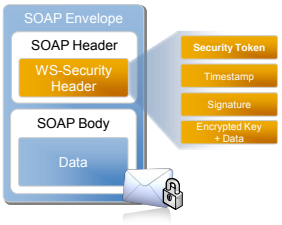
Agenda

1. Interoperability of SSO Tokens in WS-*
2. Single Sign-on for RESTful Services
3. Conclusion

© 2010 SAP AG. All rights reserved. / Page 2

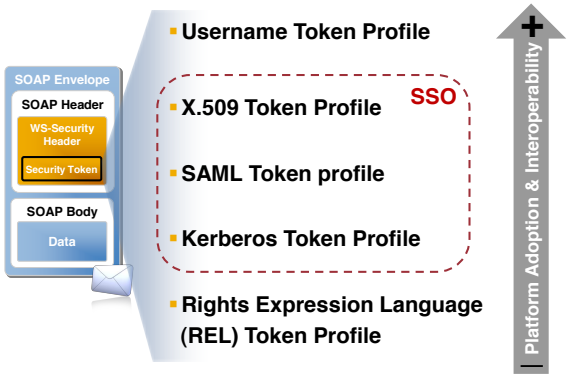
SOA Security with WS-Security

- The OASIS WS-Security Standard extends a SOAP message by one or more **WS-Security Headers** (wsse:Security) which contains security information for each recipient.
- This new SOAP Header contains all relevant security metadata to secure a SOAP message, such as
  - **Security Tokens** to carry security information (e.g. user authentication data, X.509 certificates)
  - A **Timestamp** to protect against Replay Attacks
  - **Signatures** to protect against message tampering
  - **Encrypted Keys** and **Data** to protect confidential information



© 2010 SAP AG. All rights reserved. / Page 3

WS-Security Token Formats for SSO



© 2010 SAP AG. All rights reserved. / Page 4

WS-I Basic Security Profile (BSP) 1.0 / 1.1 Interoperability Test Coverage

BSP 1.0

- **WS-Security 1.0**
- Authentication via **Username Token Profile 1.0**
- Authentication via **X.509 Certificate Token Profile 1.0**

BSP 1.1

- **WS-Security 1.1**
- Authentication via **X.509 Certificate Token Profile 1.1**
- **Thumbprint** Reference (Scenario 2)

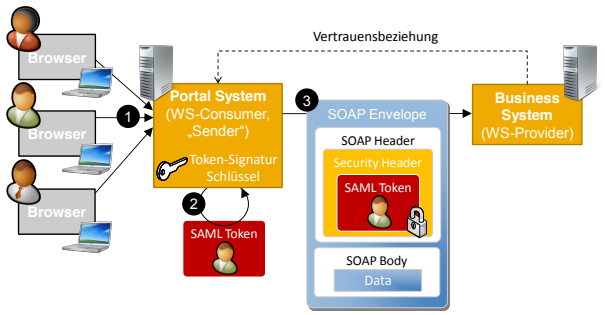
© 2010 SAP AG. All rights reserved. / Page 5

Comparing SSO Tokens for WS-*

	SAML	X.509	Kerberos
Interoperability	Based on widely adopted SAML industry standard Different support for SAML subject confirmation methods in WS-* runtimes	Based on mature X.509 standard Supported by almost all WS-* runtimes	Not supported on all WS-* runtimes
Identity Federation Capabilities	Name Mapping/ Persistent/Transient (aka Attribute/Claim-based)	None	None
Recommended Scenarios	Intranet and Internet / B2B	Intranet, SSO to non-SAML systems	Intranet

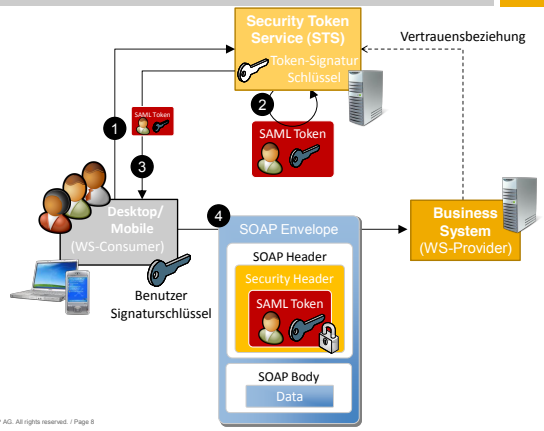
© 2010 SAP AG. All rights reserved. / Page 6

SAML Sender Vouches Confirmation Method



© 2010 SAP AG. All rights reserved. / Page 7

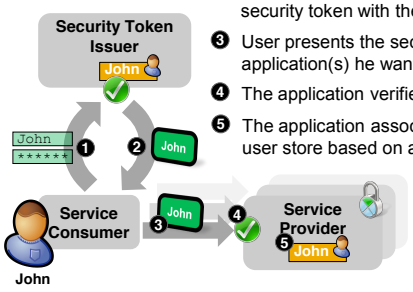
SAML Holder-of-Key Confirmation Method



© 2010 SAP AG. All rights reserved. / Page 8

Brokered Authentication – A core security pattern for Single Sign-on

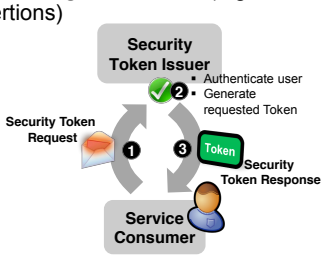
1. User proves his identity to a central Security Token Issuer by presenting his credentials.
2. The issuer verifies the correctness and trustworthiness of the credentials and issues a security token with the identity information.
3. User presents the security token to the application(s) he wants to Single Sign-on.
4. The application verifies the security token.
5. The application associates an identity from its user store based on a unique value in the token.



© 2010 SAP AG. All rights reserved. / Page 9

Role of an STS in SOA

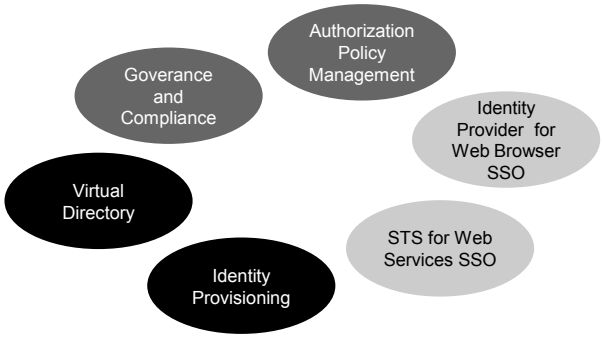
- The Security Token Service (STS) is a distinguished SOAP-based **Web service** that **issues**, **exchanges** and **validates** security tokens following the **WS-Trust**[1] standard
- The STS has broad applicability in that it can be used to issue **security tokens** in a **wide range of formats** (e.g. X.509 certificates, SAML assertions)
- Basic operations of an STS:
  - **Issue** a new token
  - **Renew** a token
  - **Validate** a token
  - **Cancel** a token



[1] http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.html

© 2010 SAP AG. All rights reserved. / Page 10

Evolution of IDM & Access Management Solutions



© 2010 SAP AG. All rights reserved. / Page 11

Supported Issued Token Types in common STS solutions

	Active Directory Federation Services 2.0	OpenSSO 8.0	Ping Federate	SAP NetWeaver IDM 7.20
Authentication Mechanisms	UNT, Kerberos, X.509, IWA, SAML 1.1/2.0	UNT, Kerberos, X.509, SAML 1.1/2.0	UNT, Kerberos, X.509, CA SiteMinder, Oracle Access Manager, OpenToken	UNT, X.509, SAP Logon Ticket, SPNEGO, SAML 1.1/2.0
Issued Tokens	SAML 1.1/2.0	SAML 1.1/2.0	SAML 1.1/2.0	SAML 1.1/2.0 X.509

© 2010 SAP AG. All rights reserved. / Page 12

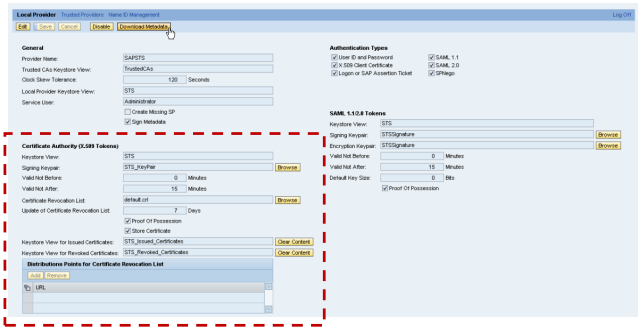
X.509 and SAML Support for SAP Application Server ABAP as Web Services Provider

Token Type	AS ABAP JAVA 6.40	AS ABAP 7.00 7.10	AS ABAP 7.01 7.11	AS ABAP 7.02 7.30	AS JAVA 7.10	AS JAVA 7.20 w. SAP STS
X.509*	X	X	X	X	X	X
SAML 1.1 (SV)	-	X	X	X	X	X
SAML 1.1 STS (HoK)	-	-	X	X	-	-
SAML 2.0 STS (HoK)	-	-	-	X	-	X

* SSL X.509 Client Certificates or X.509 WS-Security Token Profile as message authentication

© 2010 SAP AG. All rights reserved. / Page 13

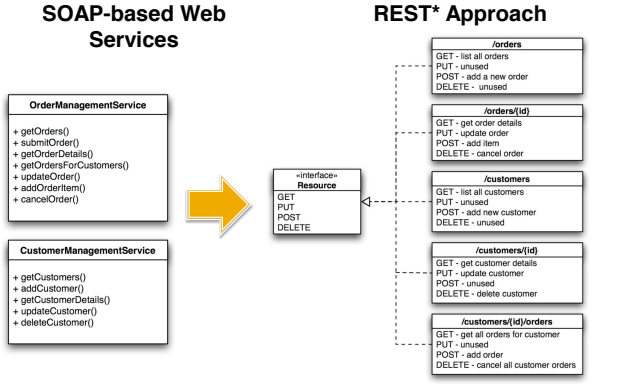
SAP NetWeaver IDM STS Configuration UI* for short-lived X.509 Token Issuing



* 7.20 Beta Release

© 2010 SAP AG. All rights reserved. / Page 14

SOA with REST



* Representational State Transfer

© 2010 SAP AG. All rights reserved. / Page 15

RESTful Web (Service) Frameworks

Java
- Project Jersey
- Restlet Framework
- JBoss RESTEasy
- Apache Wink
- RESTx
- Spring MVC 3.0
- Apache CXF

.NET
- WCF Data Services
- Open RASTA

Ruby
- Ruby on Rails

Python
- Django

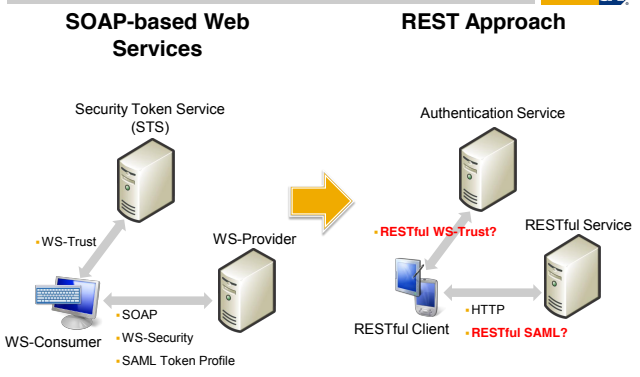
© 2010 SAP AG. All rights reserved. / Page 16

SSO for REST – Standardized options for passive Clients / Web Browser

- SSL/TLS Client Certificates
- OpenID
- SAML Protocol

© 2010 SAP AG. All rights reserved. / Page 17

Brokered Authentication with SOAP- and REST-based Services



© 2010 SAP AG. All rights reserved. / Page 18

RESTful WS-Trust

- RESTful STS
  - HTTP Binding of WS-Trust? → Mapping of WS-Trust actions to HTTP methods*

WS-Trust Actions	HTTP Method
Issue	POST
Renew	PUT
Cancel	DELETE

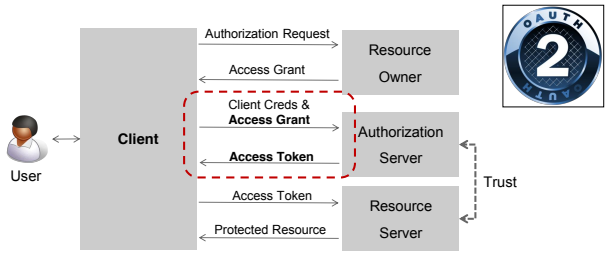
- OAuth 2.0**
  - Section 4: Obtaining an Access Token

* http://weblogs.asp.net/cibrax/archive/2009/03/06/brokered-authentication-for-rest-active-clients-with-saml.aspx

** http://tools.ietf.org/html/draft-ietf-oauth-v2-10

© 2010 SAP AG. All rights reserved.

Brokered Authentication in OAuth 2.0 (1/2)

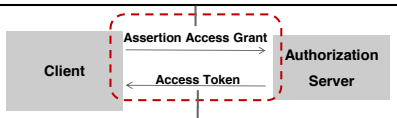


- Client: Web servers / user-agents / **native applications** / autonomous clients.
- Access Grant: Authorization code / **Assertion** / Resource owner password credentials

© 2010 SAP AG. All rights reserved.

Brokered Authentication in OAuth 2.0 (2/2)

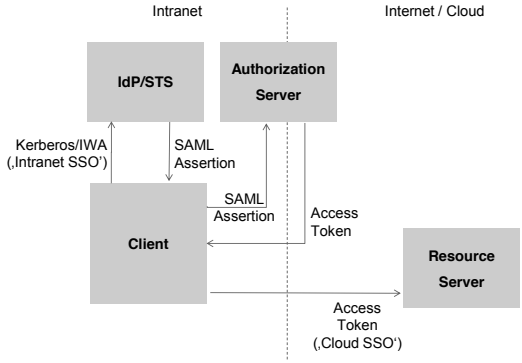
```
POST /token HTTP/1.1
Host: server.example.com
Content-Type: application/x-www-form-urlencoded
grant_type=assertion&
assertion_type=urn%3Aoasis%3Anames%3Atc%3ASAML%3A2.0%3Aassertion&
assertion=PHNhbWxwOl...ZT4%3D
```




```
HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-store
{
"access_token":"SlAV32hkKG",
"expires_in":3600,
"refresh_token":"8xLOxBtZp8"
}
```

© 2010 SAP AG. All rights reserved.

Brokered Authentication in OAuth 2.0 Cloud SSO Use Case



© 2010 SAP AG. All rights reserved.

Options for RESTful SAML

- Standard Auth Header with Basic Auth Scheme:

```
GET /private/index.html HTTP/1.0
Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
```

→ Define a custom HTTP Auth Scheme for SAML (e.g. SAML:2.0:Assertion)

→ Option 1: Pass the SAML Assertion base64-encoded in the **Authorization Header**

```
GET /private/index.html HTTP/1.0
Authorization: SAML:2.0:Assertion <base64-encoded saml assertion>
```

→ Option 2: Pass the SAML Assertion base64-encoded **in the body** of a HTTP POST

```
POST /private/index.html HTTP/1.0
Authorization: SAML:2.0:Assertion
...
SAMLAssertion=<url-encoded and base64-encoded saml assertion>
```

© 2010 SAP AG. All rights reserved.

Conclusion

- As of today, X.509 is the most interoperable SSO token format for WS-* runtimes
- Identity Management and Access Solutions have been extended by Security Token Service (STS) capabilites based on the OASIS WS-Trust protocol
- SAML is the most common token format across STS solutions today. Using the STS as a lightweight CA to issue short-lived X.509 certificates helps to integrate non-SAML WS-Providers
- Standards for brokered authentication and token formats for SSO to REST-based Web Service Providers are still evolving

© 2010 SAP AG. All rights reserved.

Hasso Plattner Institut
IT Systems Engineering | Universität Potsdam

IT SECURITY GOVERNANCE & MESSBARKEIT

DR. THOMAS STÖRTKUHL
Mitglied der Geschäftsleitung, Secaron AG

ABSTRACT

Zur Erfüllung der Anforderungen benötigt ein CISO (Chief Information Security Officer) ein Instrumentarium, um für das ISMS (Information Security Management System) von den Geschäftszielen ableitbare Ziele und Kennzahlen definieren und das ISMS steuern und kontrollieren zu können. Überdies muss dargestellt werden, ob Compliance Anforderungen erfüllt werden. Dabei muss der CISO alle Interessengruppen wie Kunden, Mitarbeiter und Lieferanten etc. berücksichtigen.
Ein solches Instrumentarium stellt ein Kennzahlensystem auf der Ebene des CISO dar. Der Vortrag schlägt ein Verfahren vor, mit dem ein Kennzahlensystem aus dem COBIT Standard nach Geschäftszielen abgeleitet und gemäß einer Balanced Scorecard geordnet werden kann.

SOA Security Symposium 2010
Hasso Plattner Institut

IT Security Governance & Messbarkeit

Dr. Thomas Störtkuhl, Secaron AG

28./29. Oktober 2010

Agenda

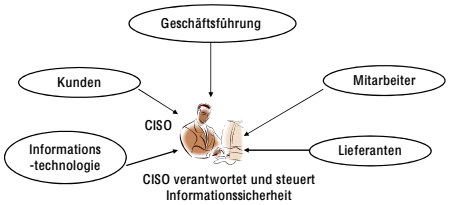
- Ausgangssituation: Aufgabenstellung des CISO, risikoorientiertes ISMS
- Vorschlag: Entwicklung eines Kennzahlensystem zur IT Security Governance nach COBIT
- IT Security Governance
- Zusammenfassung

das richtige Maß?

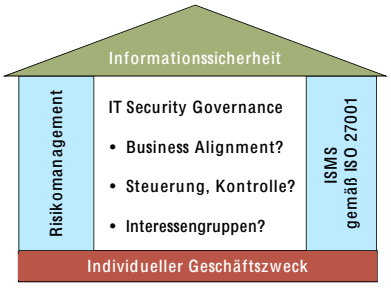
Wir hatten noch nie einen Sicherheitsvorfall – wir sind sicher!

Ausgangssituation: Aufgabenstellung des CISO

Interessengruppen, Themenfelder



Ausgangssituation: risikoorientiertes ISMS



Voraussetzung für IT Security Governance

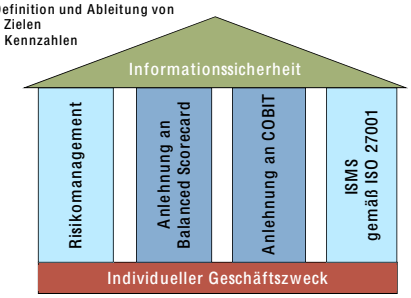
Nur das, was man messen kann, kann man steuern!

Beobachtung von Messwerten geeigneter Kennzahlen

Korrekturmaßnahmen bei Abweichungen vom SOLL-Wert

Vorschlag zur IT Security Governance

Definition und Ableitung von
- Zielen
- Kennzahlen



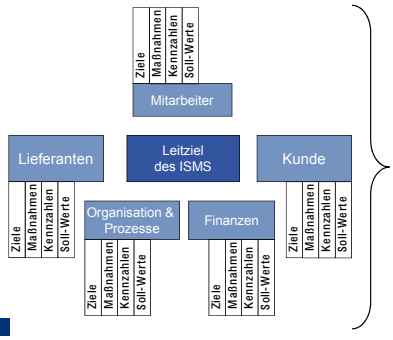
Vorschlag: Definition/Ableitung der Ziele und Kennzahlen

Anlehnung an COBIT

Hilfskonstrukt zur Ermittlung möglicher Kennzahlen

- Strukturierung nach Perspektiven (Interessengruppen)
- Ableitung von IT-Zielen aus den Geschäftszielen (Business Alignment)
- Jedem IT-Ziel werden über COBIT Prozesse bestimmte Kennzahlen zugeordnet

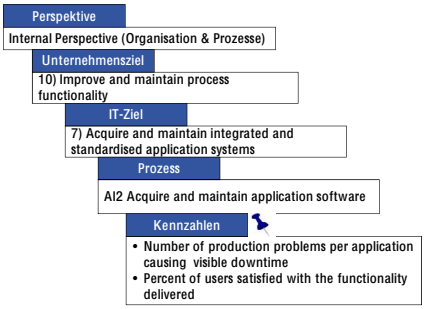
Vorschlag: Methodik der Balanced Scorecard



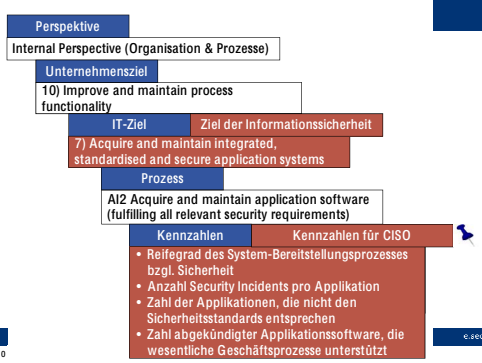
Ableitung aus
- Geschäftszielen

Anforderung bzgl.
- IT Security Governance

Vorschlag: Ableitung von Kennzahlen aus COBIT



Vorschlag: Ableitung von Kennzahlen aus CobiT

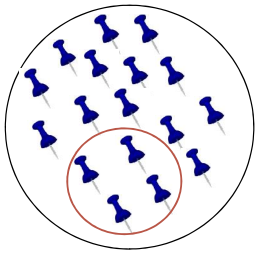


Reifegrad des System-Bereitstellungsprozesses

QM-Records / Projekte	Security Require-ments	Risiko-analyse	Security Testing	Code Review	Penetration Test /Audit
Applikation	yes	yes	yes	no	yes
SOA Projekt	no	no	no	yes	no
ESB	yes	no	yes	--	no
.....					
Mittelwert	66%	33%	66%	50%	33%

Reifegrad:
50%

Auswahl von 10 bis 15 Kennzahlen für CISO



Kriterien:

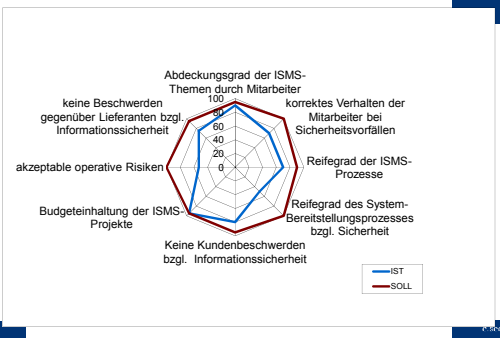
Quantifizierbar (SOLL-Wert)

Kostengünstig erhebbar

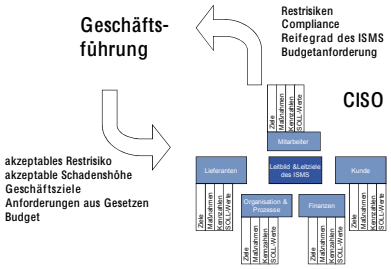
Unabhängigkeit von der IT-Infrastruktur

Ansprechpartner benennbar

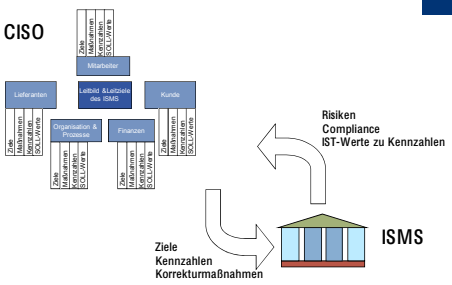
Beispiel für ein Kennzahlensystem



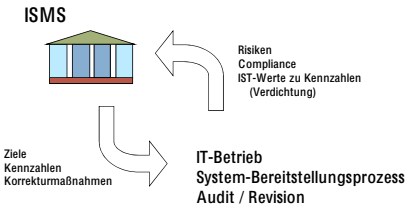
IT Security Governance: Geschäftsführung



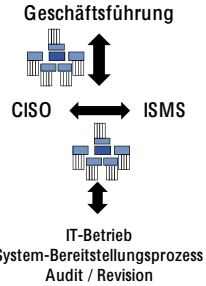
IT Security Governance: CISO



IT Security Governance: ISMS



IT Security Governance



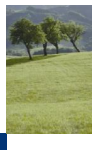
Zusammenfassung

Vorteile des Ansatzes:

- Business Alignment: Ableitung klarer Ziele für die Informationssicherheit aus Geschäftszielen
- IT Security Governance: über ein von den Zielen abgeleitetes Kennzahlensystem
- Vollständigkeit: Berücksichtigung aller involvierten Interessengruppen
- Vollständigkeit: umfasst alle Aspekte der Informationssicherheit

Kontakt

Secaron AG
Ludwigstr. 45
D-85399 Hallbergmoos
Tel. +49 811- 9594 - 0
Fax +49 811- 9594 - 220
www.secaron.de
Ansprechpartner:
Dr. Thomas Störtkuhl
E-Mail: stoertkuhl@secaron.de
twitter: http://twitter.com/secaron



Vielen Dank für
Ihre Aufmerksamkeit!

SECRT - DAS OPENSOURCE SECURITY FRAMEWORK DES BSI

DR. BRUNO QUINT
Geschäftsführer (Managing Director)

Dr. Bruno Quint is one of the founders and Managing Director of CORISECIO GmbH. CORISECIO is a leading provider of security solutions for SOA products. Bruno Quint has been working in the IT industry for more than twenty years. From Software Development up to Executive Board positions he held a variety of management functions in well-known European enterprises. CORISECIO is a leading manufacturer of security products for SOA infrastructures. The open-source platform secRT, an Eclipse Runtime Project, is the basis for a variety of security solutions.

ABSTRACT

Eine SOA (Service Oriented Architecture) Infrastruktur zeichnet sich meist dadurch aus, dass eine Vielzahl von Diensten zu komplexen Geschäftsprozessen verbunden wird. Eine Grundanforderung für den produktiven Einsatz solcher Systeme ist eine verlässliche Absicherung der beteiligten Services.

Mit der secRT (securityRunTime) wird eine gemeinsam mit dem BSI entwickelte SOA Security Lösung unter freier Lizenz zur Verfügung gestellt. Die Open Source Lösung erlaubt die automatisierbare Absicherung von Web Services mit den geforderten Sicherheitsrichtlinien. Die secRT stellt eine Vielzahl von Security Services zur Verfügung und liefert gleichzeitig die benötigte Infrastruktur mit. Beispielsweise ist eine vollständige PKI (Public Key Infrastructure) implementiert und gleichzeitig die Durchführung des Rollout der Zertifikate.

Parallel zur Modellierung von Geschäftsprozessen ergibt sich auch die Möglichkeit, eine zusätzliche sicherheitsspezifische Modellierungsebene für eine SOA einzufügen. Die Sicherheitsmechanismen sind dabei vollständig von der Business Logic entkoppelt. Die secRT selbst ist durchgängig nach SOA-Prinzipien aufgebaut, basiert auf offenen Standards wie Java, XML und Web Services und ist damit in alle Systemumgebungen integrierbar. Durch die Veröffentlichung als Open Source Software wird Transparenz geboten und die Anpassung an die eigenen Bedürfnisse ermöglicht.

OPEN SOURCE IDENTITY- UND ACCESS MANAGEMENT

MICHAEL KLEINHENZ
Leitender Architekt, tarent GmbH

Michael Kleinhenz arbeitet als leitender Architekt bei der tarent GmbH. Der Diplom-Technoinformatiker ist verantwortlich für Technologiestrategie und Partner-management beim Bonner Software-Mittelständler und beschäftigt sich mit SOA-Infrastrukturen, deren Sicherheitsaspekten und der Umsetzung komplexer Fachanwendungen insbesondere im Bereich Public Sector.

ABSTRACT

Für jede größere Organisation ist ein funktionierendes Identity- und Access-Management essentiell für die Effizienz der Mitarbeiterverwaltung. Moderne Systemlandschaften zeichnen sich durch eine große Heterogenität aus, die in Bezug auf Identitätsdaten aufgelöst werden muss, um beispielsweise konsequentes Single-Sign-On zu ermöglichen. Der Vortrag zeigt die unterschiedlichen Konzepte und Technologien hinter dem Begriff "Identity-Management" auf. Terminologien wie "Identity Federation" und "Provisioning" werden anhand von praktischen Beispielen aus einem großen Behördenprojekt erklärt. Demonstriert wird auch eine Beispiellösung, die vollständig auf Open-Source-Komponenten aufbaut und sicheres, skalierbares und flexibles Identity-Management bietet und gleichzeitig offen gegenüber Erweiterungen und Anpassungen ist.

↪ tarent

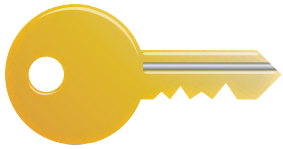
↪ tarent

Dipl.-Technoinform.
Michael Kleinhenz
Lead Architect, tarent GmbH

↪ tarent

↪ tarent

Identity & Access Management

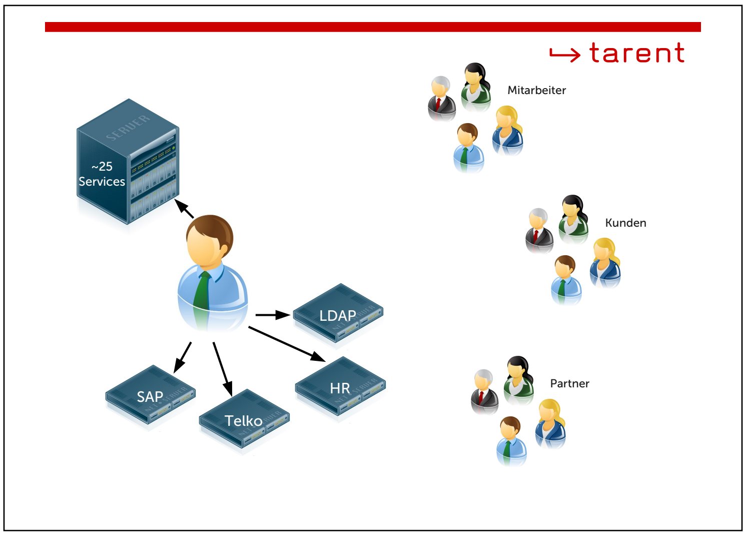


↪ tarent

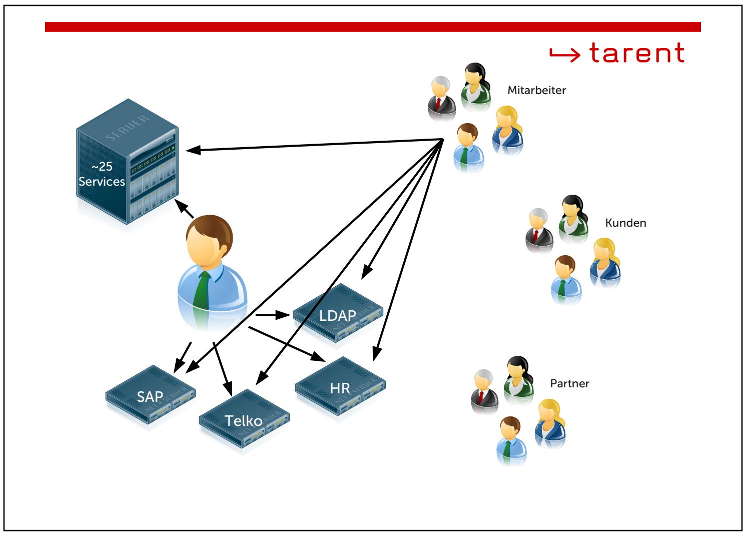
Kauf & Glück Versandhandel AG

100 000 Kunden
80 Angestellte
30 Partner

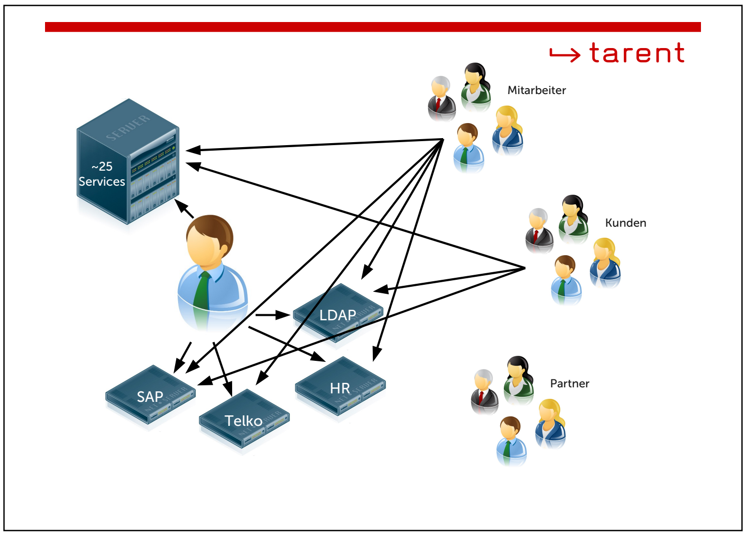
↪ tarent



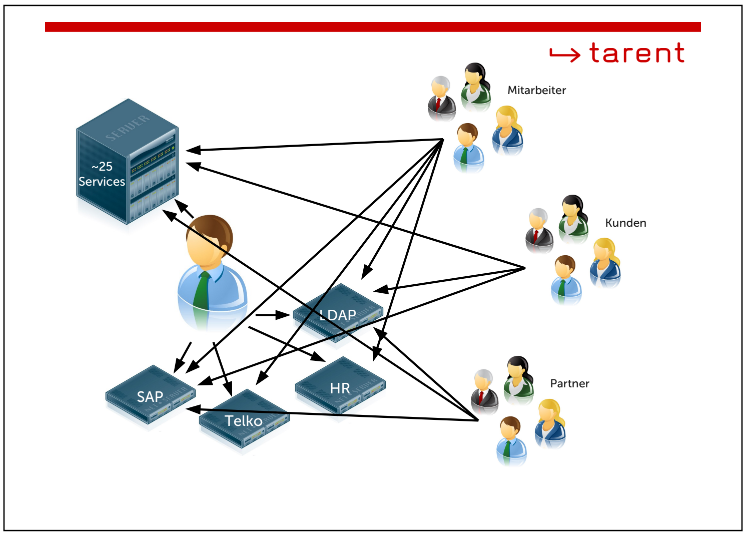
tarent
Mitarbeiter
~25 Services
Kunden
LDAP
SAP
Telko
HR
Partner



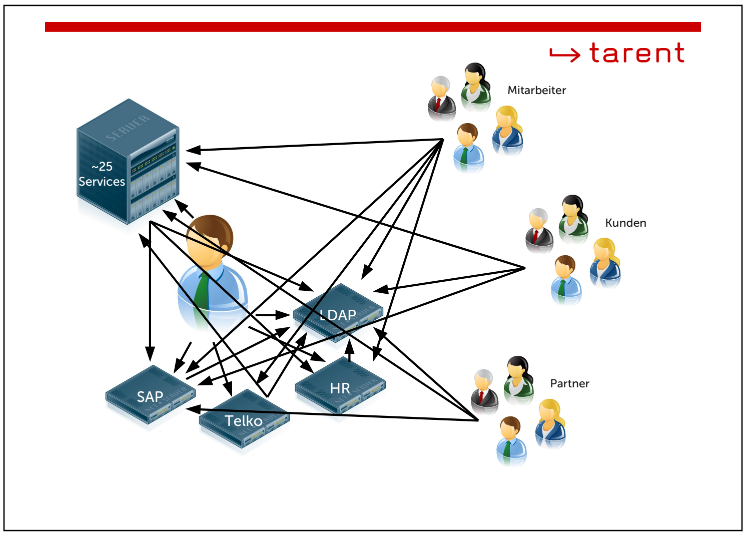
tarent
Mitarbeiter
~25 Services
Kunden
LDAP
SAP
Telko
HR
Partner



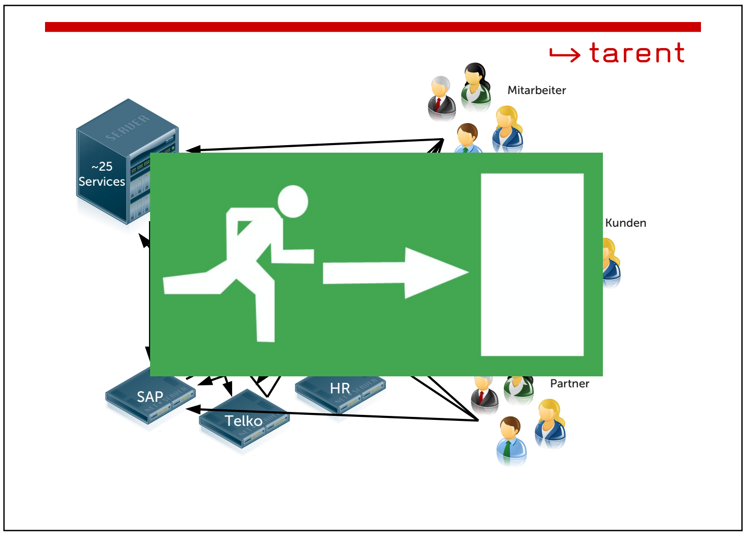
tarent
Mitarbeiter
~25 Services
Kunden
LDAP
SAP
Telko
HR
Partner



tarent
Mitarbeiter
~25 Services
Kunden
LDAP
SAP
Telko
HR
Partner



tarent
Mitarbeiter
~25 Services
Kunden
LDAP
SAP
Telko
HR
Partner



tarent
Mitarbeiter
~25 Services
Kunden
SAP
HR
Telko
Partner

↪ tarent

Administrative Kosten
Durchschnittliche Verwaltungskosten
pro Benutzer und Jahr: 350 US$

Helpdesk und Support
Durchschnittliche Kosten pro
Passwort Reset Call: 40 US$

Dauer: ~13 Minuten, 55% der gesamten Kosten!

Durchschnittliche Helpdesk-Kosten
Pro Benutzer und Jahr: 85 US$

Mitarbeiterverwaltung
Durchschnittliche IT-Verwaltungskosten
...eines neuen Mitarbeiters pro Jahr: 1 300 US$
...eines bestehenden Mitarbeiters: 450 US$

Sicherheit
30-60% der bestehenden Accounts sind nicht aktuell.

Quelle: Gartner / META Group

↪ tarent

Top 10 Probleme

1. Rollen nicht klar verteilt.
2. Zugangskontrollen zu Applikationen sind unsicher.
3. Zugangskontrollen zu Datenbanken sind unsicher.
4. Entwickler haben Zugriff auf Produktionsumgebung.
5. Zuviele Administratoren.
6. Ausgeschiedene Mitarbeiter haben Zugriff.
7. Berichtswesen nicht klar definiert.
8. Changemanagement unzureichend.
9. Dokumentation manueller Prozesse unzureichend.
10. Dokumentation und reale Prozesse divergieren.

Quelle: Ken Vander Wal, ISACA Sarbanes Conference 2004

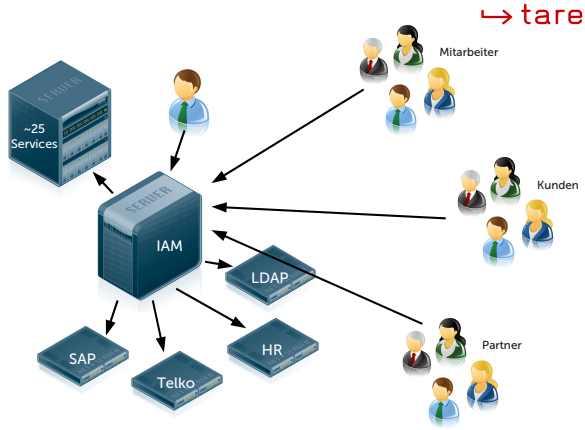
↪ tarent

Top 10 Probleme

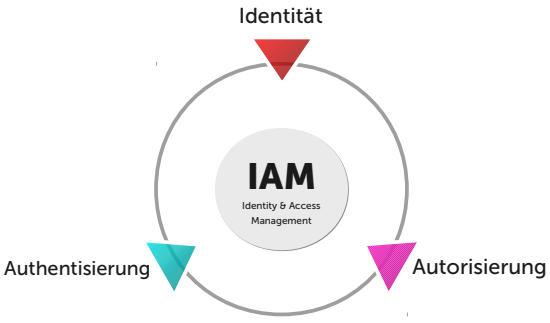
1. Rollen nicht klar verteilt.
2. Zugangskontrollen zu Applikationen sind unsicher.
3. Zugangskontrollen zu Datenbanken sind unsicher.
4. Entwickler haben Zugriff auf Produktionsumgebung.
5. Zuviele Administratoren.
6. Ausgeschiedene Mitarbeiter haben Zugriff.
7. Berichtswesen nicht klar definiert.
8. Changemanagement unzureichend.
9. Dokumentation manueller Prozesse unzureichend.
10. Dokumentation und reale Prozesse divergieren.

Quelle: Ken Vander Wal, ISACA Sarbanes Conference 2004

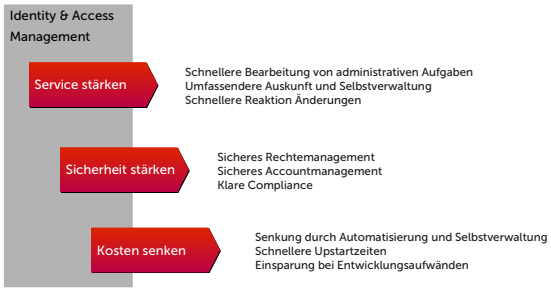
↪ tarent



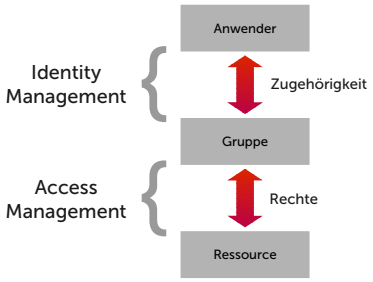
↪ tarent



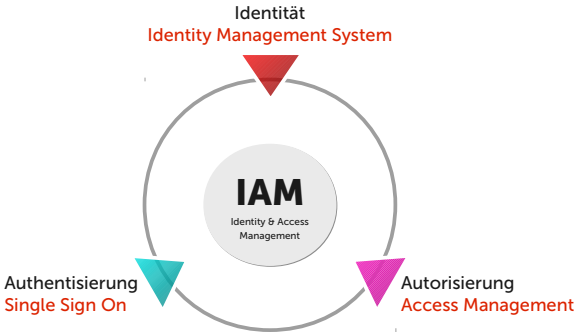
↪ tarent

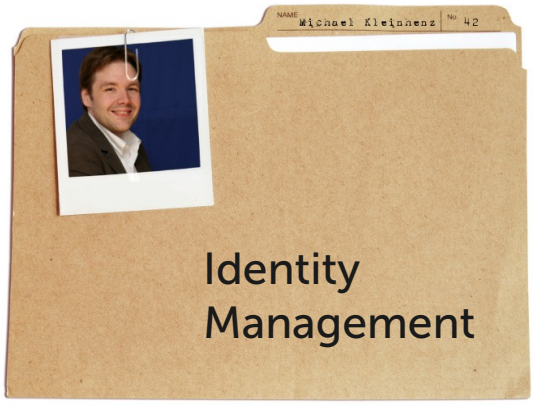


↪ tarent

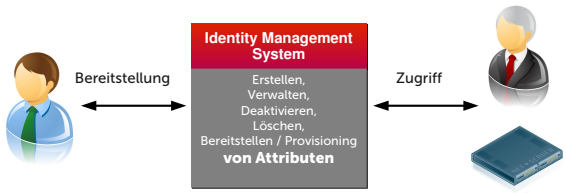


↪ tarent

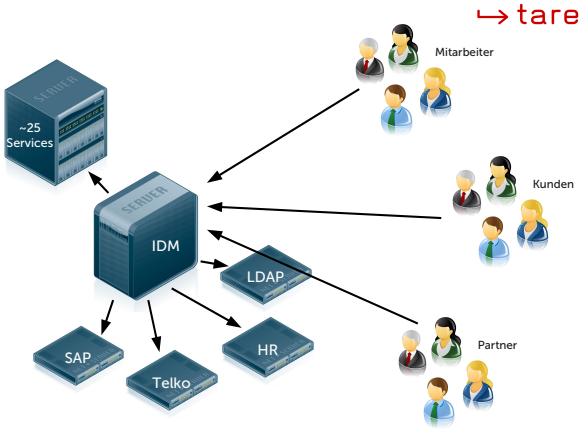




↪ tarent



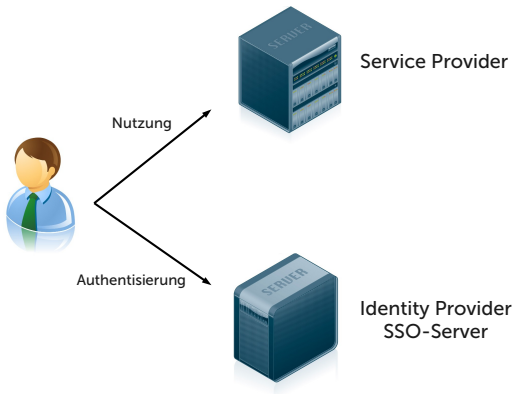
↪ tarent



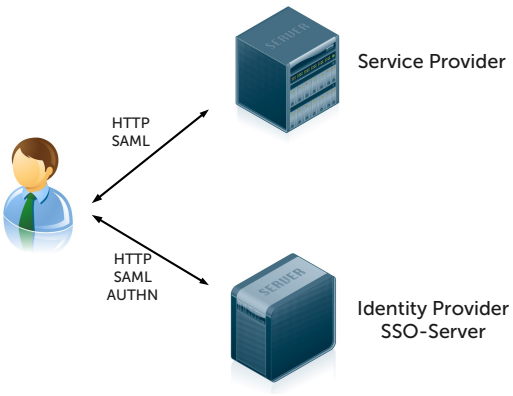
↪ tarent

Authentisierung
& Access Management

↪ tarent



↪ tarent

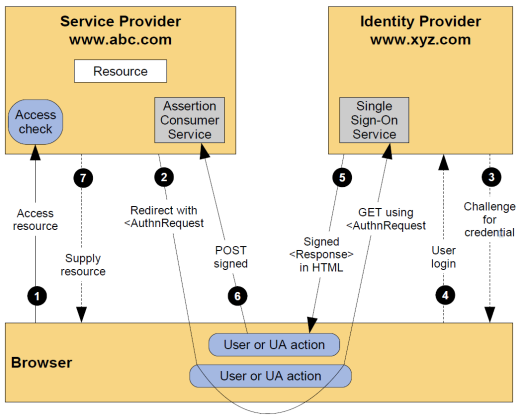


↪ tarent

SAML

The Security Assertion Markup Language

↪ tarent

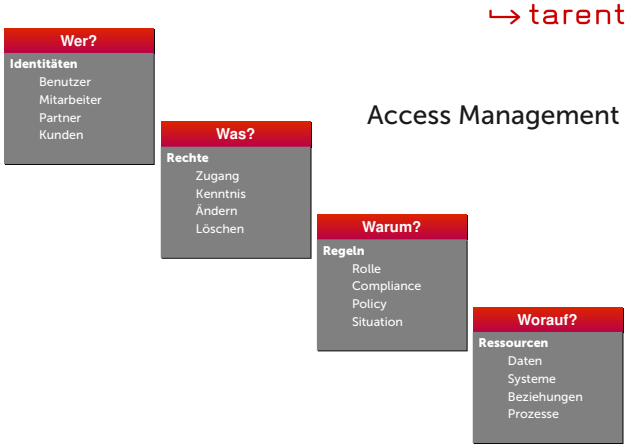


↪ tarent

Autorisierung

& Access Management

↪ tarent



Access Management

Methodiken

↪ tarent

- **RBAC** – Role based Access Control
- **ACLs** – Access Control Lists
- **Policies** – Rule based Access Control

Autorisierung

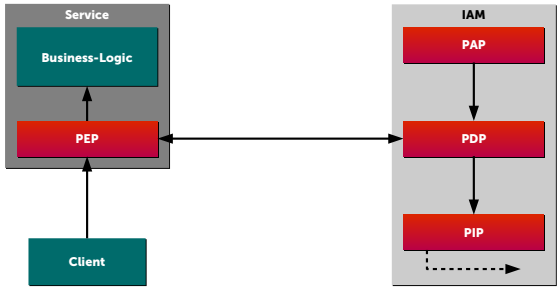
XACML

eXtensible Access Control Markup Language

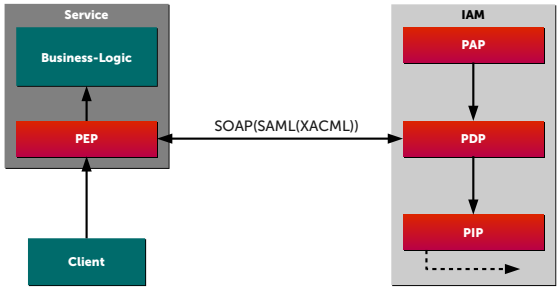
↪ tarent

- **Policies & Rules** – Regeln und Algorithmen für die Autorisierungsentscheidung
- **Contexts** – Request & Responses für die Policy-Queries
- **Architecture** – Modell für die Anwendung, Best-Practice

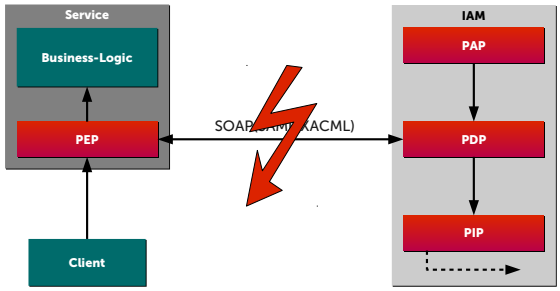
↪ tarent



↪ tarent



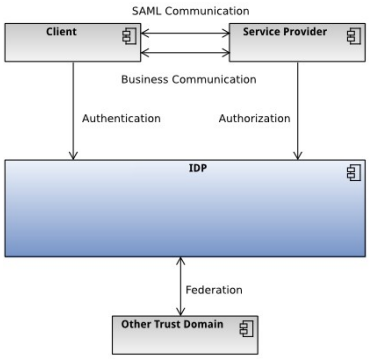
↪ tarent



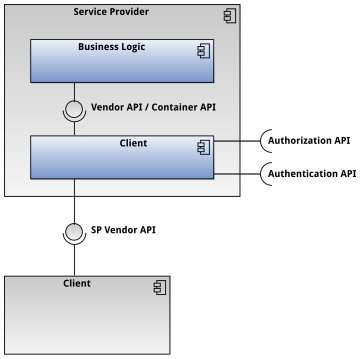
↪ tarent

OSIAM

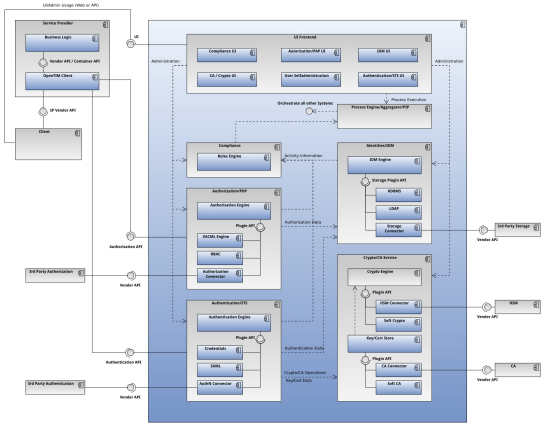
↪ tarent



↪ tarent



↪ tarent



↪ tarent

- Basiert auf OpenAM und Sun XACML
- Integriert eine vollständige IDM-Lösung
- Java Enterprise
- GNU General Public License / CDDL

https://evolvis.org/projects/osiam/

EINBRUCHSERKENNUNG IN SOA

DANIEL WAGNER

Business Unit Manager, SHE Informationstechnologie AG

Daniel Wagner, Diplom-Informatiker, leitet den Geschäftsbereich Softwareentwicklung bei der SHE Informationstechnologie AG in Ludwigshafen/Rhein (www.she.net).

Nach seinem Informatik-Studium an der Universität des Saarlandes arbeitete Herr Wagner zunächst mehrere Jahre als Softwarearchitekt und Consultant, bevor er 2005 die Leitung des Geschäftsbereiches Software Engineering der SHE AG übernahm. In dieser Funktion verantwortet und betreut er heute die Umsetzung von Projekten im Bereich Web-Portale und SOAs für Kunden mit meist sehr hohen Anforderungen an die IT-Sicherheit. Nebenberuflich hält er als Gastdozent Vorlesungen zu den Themen Verteilte Systeme und E-Business.

ABSTRACT

Service-orientierte Architekturen bilden in Unternehmen und Organisationen in zunehmendem Maße geschäftskritische Prozesse ab. Mit steigender Vernetzung sowohl innerhalb als auch zwischen Unternehmen sowie durch die mit SOA-Technologien verbundene höhere Komplexität der betriebenen IT-Landschaft steigt das Risiko der Anfälligkeit der Systeme gegenüber Angriffen von innen wie von außen.

Das im Rahmen eines für das BSI (Bundesamt für Sicherheit in der Informationstechnik) durchgeführten Projektes entwickelte SOA-IDS stellt eine Möglichkeit dar, bestimmte Angriffe gegen SOA-basierte IT-Systeme zu erkennen. Dazu arbeitet das SOA-IDS mit dezentralen Sensoren, die an kritischen Punkten in der SOA eingebracht werden und Ereignisse an einen zentralen Korrelationsmechanismus senden, womit das System in der Lage ist, sowohl lokale Auffälligkeiten zu erkennen (z.B. Angriffe gegen XML-Parser, WebService-Manipulationen etc.) aber auch komplexere verteilte Angriffsmuster, basierend auf STATL-Graphen aufzudecken.

Der Vortrag skizziert die Architektur des SOA-IDS, beschreibt aktuelle Angriffsvektoren gegen SOA und zeigt, wie das System diese erkennen kann.

Einbruchserkennung in SOA

Dipl.-Inform. Daniel Wagner

SHE AG

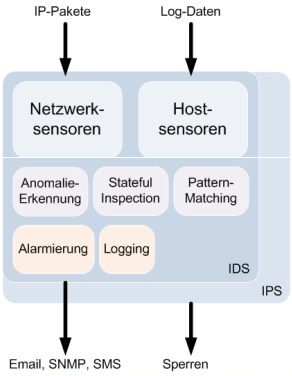
© SHE Informationstechnologie AG, 2010 www.she.net

Inhalt

- Einbruchserkennung / IDS
- Angriffsvektoren gegen Web-Services
- SOA-IDS-Projekt:
  - Infrastrukturen
  - Sensor-Authentifizierung
  - Ereignis-Korrelation
  - Sicherheit

- Daniel Wagner
  - seit 1995 tätig als Softwareentwickler und Projektleiter
  - seit 2002 Beschäftigung mit dem Thema Application Security
  - seit 2005 Leiter des Geschäftsbereichs SW-Entwicklung der SHE
- SHE IT AG: Dienstleister für Software / Infrastruktur / Security
  - Insgesamt > 100 Mitarbeiter an den Standorten Ludwigshafen, Bonn und Frankfurt
  - Software-Bereich: Spezialisiert auf die Themen High-End-Portale, Web/Cloud Services, Application Security
- Projekte mit dem BSI im Umfeld Java/Security:
  - Java IDS
  - Secure Java Code Filter
  - SOA-IDS

IDS / IPS



Herausforderungen bei IDS / IPS

- Angreifbarkeit des IDS vermeiden (z.B. Denial of Service)
- False negative – Rate in den Griff bekommen
- False positive – Rate in den Griff bekommen
- „Security“ trifft auf „Business“…

  → Nutzbarkeit der Anwendungen gewährleisten

  → IT-Sicherheit gewährleisten

SOAP-Request

```
POST /Service/Stockquotes HTTP/1.0
Content-Type: text/xml
SOAPAction: "urn:getQuote"

<env:Envelope
   xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
   <env:Body>
        <ns:getQuote xmlns:ns="urn:example-quotes">
                <ns:symbol>NYSE:IBM</ns:symbol>
        </ns:getQuote>
   </env:Body>
</env:Envelope>
```

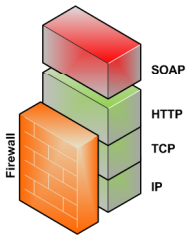
SOAP-Response

```
HTTP/1.0 200 OK
Content-Type: text/xml

<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
    <env:Body>
        <ns:getQuoteResponse xmlns:ns="urn:example-quotes">
            <ns:result>91.35</ns:result>
        </ns:getQuoteResponse>
    </env:Body>
</env:Envelope>
```

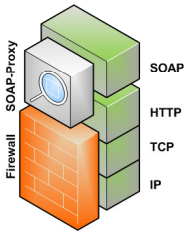
SOAP-Web-Services sind gefährdet

- Wird SOAP-Traffic in der Firewall erlaubt können Angriffe auf Anwendungsebene / gegen XML-Parser durchgeführt werden.
- SSL-Transportverschlüsselung bis zum Applikations-Server verschärft das Problem häufig → Angreifer wird unsichtbar durch die Firewall getunnelt.
- REST-basierte Web-Services etwas unkritischer durch URL-Whitelisting in Firewall (aber aufwändig).

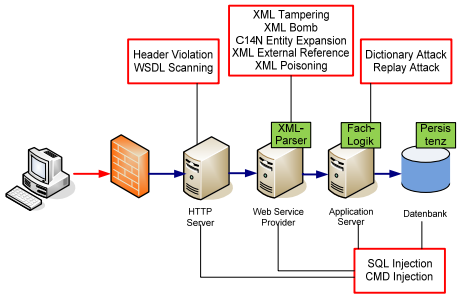


SOAP-Web-Services sind gefährdet

- Schutz der HTTP/SOAP-Ebene notwendig!



Angriffspunkte



Angriffsmuster gegen SOA / Web-Services

- Denial of Service (DoS)
- Wörterbuch-Angriffe gegen Anmelde-Funktionen
- Replay-Angriffe (statisch und dynamisch)
- Injection-Angriffe (z.B. SQL-Injection)
- Angriffe gegen den XML-Parser
  - XML-Bomben / Entity Expansion
  - XML External Reference Attacks
  - XML / Schema Poisoning
- WSDL Scanning
- Buffer Overflow
- …

WSDL

```
<definitions name="StockQuotes">
    <service name="StockQuoteService">
      <port name="StockQuotePort" binding="tns:StockQuoteSoapBinding">
        <soap:address location="http://192.168.134.17/stockquote"/>
      </port>
    </service>

    <message name="getQuote">
        <part name="symbol" type="string"></part>
    </message>

    <message name="getQuoteResponse">
        <part name="return" type="float"></part>
    </message>
</definitions>
```

Bsp.: Entity Expansion

```
<!DOCTYPE foo [
<!ENTITY a "1234567890" >
<!ENTITY b "&a;&a;&a;&a;&a;&a;&a;&a;&a;" >
<!ENTITY c "&b;&b;&b;&b;&b;&b;&b;&b;&b;" >
<!ENTITY d "&c;&c;&c;&c;&c;&c;&c;&c;&c;" >
<!ENTITY e "&d;&d;&d;&d;&d;&d;&d;&d;&d;" >
<!ENTITY f "&e;&e;&e;&e;&e;&e;&e;&e;&e;" >
<!ENTITY g "&f;&f;&f;&f;&f;&f;&f;&f;&f;" >
<!ENTITY h "&g;&g;&g;&g;&g;&g;&g;&g;&g;" >
<!ENTITY i "&h;&h;&h;&h;&h;&h;&h;&h;&h;" >
<!ENTITY j "&i;&i;&i;&i;&i;&i;&i;&i;&i;" >
<!ENTITY k "&j;&j;&j;&j;&j;&j;&j;&j;&j;" >
<!ENTITY l "&k;&k;&k;&k;&k;&k;&k;&k;&k;" >
<!ENTITY m "&l;&l;&l;&l;&l;&l;&l;&l;&l;" > ]>
<foo>&m;</foo>
```

Buffer Overflow

```
POST /Service/Stockquotes HTTP/1.0
Content-Type: text/xml
SOAPAction: "urn:getQuote"

<env:Envelope
   xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
   <env:Body>
        <ns:getQuote xmlns:ns="urn:example-quotes">
        <ns:symbol>XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</ns:
   symbol>
        </ns:getQuote>
   </env:Body>
</env:Envelope>
```

SQL Injection

```
POST /Service/Stockquotes HTTP/1.0
Content-Type: text/xml
SOAPAction: "urn:getQuote"

<env:Envelope
   xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
   <env:Body>
        <ns:getQuote xmlns:ns="urn:example-quotes">
        <ns:symbol>';-- DROP ALL TABLES</ns:symbol>
        </ns:getQuote>
   </env:Body>
</env:Envelope>
```

Gegenmaßnahmen

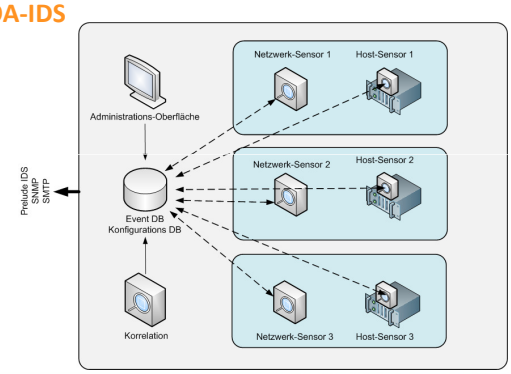
- Eingabevalidierung:
  - Länge, Anzahl der Header etc. überprüfen.
  - Muster-Validierung mit konfigurierbaren regulären Ausdrücken.
- XML prüfen (Wohlgeformtheit, DOM-Größe, …)
  - aber: viele Tests erfordern Parsen des XML-Dokuments.
  - Gefahr dass der SOAP-Proxy selbst zum Opfer des Angriffs wird.
    → XML-DOM-Tests durch separate VMs.
- Replay-Attacken
  - Mitführen einer Historie der letzten n Anfragen.
  - Erkennung wiederholter ähnlicher Anfragen pro Zeiteinheit.
- Komplexe Angriffsmuster (verteilte Angriffe, WSDL-Scanning, etc.)
  - Frei definierbare STATL-Szenarien.

Projekt SOA-IDS

Bundesamt für Sicherheit in der Informationstechnik

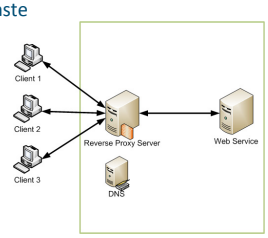
- Projekt wurde 2009 vom BSI ausgeschrieben.
- Realisierung zwischen 07/2009 und 04/2010 durch SHE.
- Vorgaben / Ziele:
  - Entwicklung eines Systems zur Einbruchserkennung in SOA-basierten Systemen.
  - Überwachung der SOAP-Kommunikation mittels dezentraler Sensoren auf Netzwerk- und Hostebene.
  - Übermittlung erkannter Ereignisse („Events“) an zentralen Dienst.
  - Korrelation von Sensormeldungen und adäquate Reaktion auf erkannte Angriffsversuche.
  - Administration über Web-basierte Oberfläche.
  - Einsatz von Java-Technologien und Public License Bibliotheken.

SOA-IDS

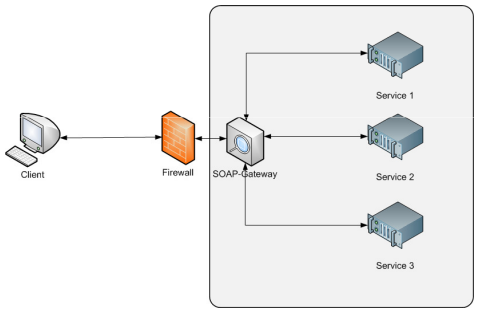


Entwurfsentscheidung: Reverse Proxy

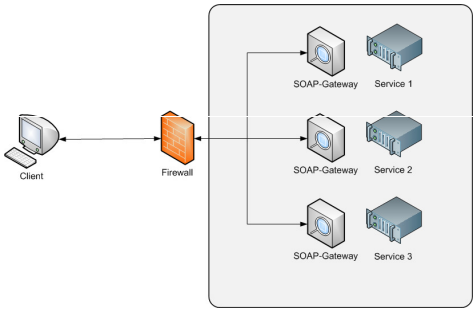
- Keine Änderung der Client-Umgebung notwendig
- Terminierung und Neuaufbau von http-Verbindungen → hohe Sicherheit für nachgelagerte Dienste
- WSDL-Rewriting wird notwendig
- Ggfs. SSL-Terminierung



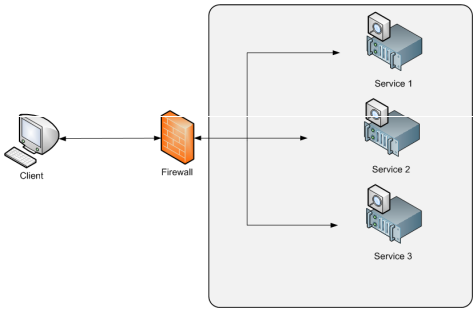
Option 1: Zentrales SOAP-Gateway



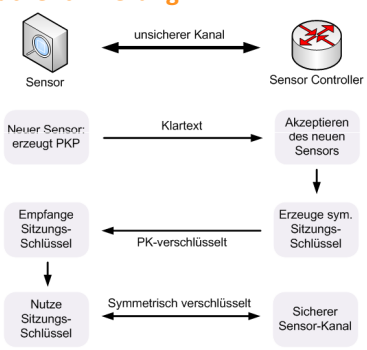
Option 2: Dezentrale Netzwerk-Sensoren



Option 3: Sensorintegration in Service-Provider



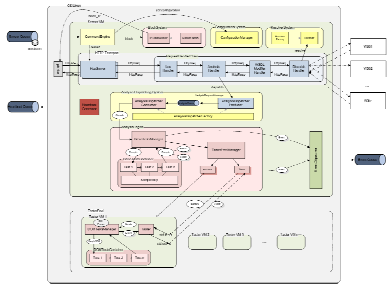
Sensor-Authentifizierung



Aufgaben des Netzwerksensors

- Nimmt Verbindungen auf Transportebene entgegen.
- Verarbeitet HTTP-Anfragen/Antworten, erkennt SOAP-Nutzlast.
- Agiert als HTTP/SOAP-Client gegenüber Zielsystem.
- Erkennt WSDL-Anfragen und führt WSDL-Rewriting durch.
- Überprüft HTTP/SOAP-Request (asynchron) mehrstufig:
  - Basis-Tests: Prüfung von Längen, Größen und Mustern (reguläre Ausdrücke).
  - Verwaltung einer Request-Historie für Replay-Tests.
  - DOM-Tests: Expansion des XML-Dokuments für Tests.
- Verwaltung eines Pools von Java-VMs für die Tests.
- Kommunikation mit zentralen Diensten über JMS-Nachrichten.
- Robustheit: vollständige Rekonfiguration zur Laufzeit möglich.

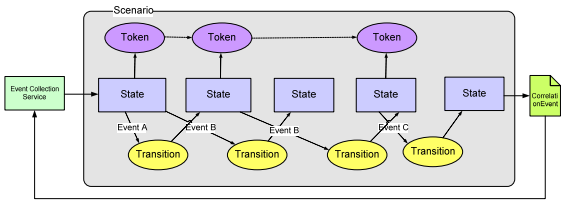
Architektur Netzwerksensor



STATL - Szenarien

- STATL: Erweiterbare Angriffsbeschreibungssprache, basierend auf Zuständen / Transitionen.
- Verwaltung mehrerer STATL-Szenarien durch die Correlation Engine möglich.
- Erweiterbarkeit durch Java-Code-Sequenzen innerhalb der Zustände/Transitionen.
- Generierung von Java-Klassen für Szenarien, Zustände und Transitionen zur Laufzeit → Kompilierung und Instanziierung dieser Klassen durch Java-Compiler bzw. ClassLoader.
- Weiterleitung von Sensor-Ereignissen an die Szenario-Objekte → Erzeugung von Tokens innerhalb der CorrelationEngine.

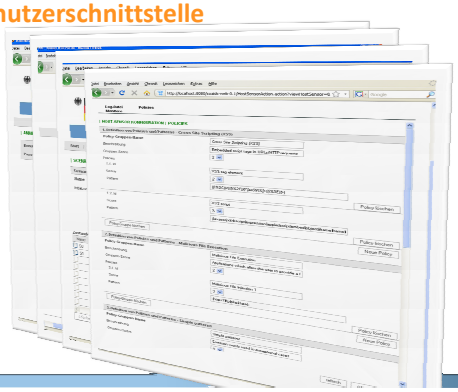
Korrelation mit Szenarien



Angreifbarkeit des SOA-IDS?

- Ausgelagerte DOM-Tests.
- Sorgfältige Authentifizierung von Sensoren.
- Vermeidung des WebService-Paradigmas in der SOA-IDS-Implementierung.
- (Optionale) Verschlüsselung aller System-internen Nachrichten.

Benutzerschnittstelle



Fragen?

Kontakt:
Daniel Wagner
SHE Informationstechnologie AG
Donnersbergweg 3
67059 Ludwigshafen
Tel: 0621-5200204
Email: daniel.wagner@she.net