SecureSOA

Bernhard Groll

Fakultät für Informatik
Technische Universität Dortmund

9. Juli 2012

Übersicht

Motivation

- IT-Systeme sind allgegenwärtig
- Vernetzung nimmt zu, oft serviceorientiert
- Mögliche Folgen fehlender Datensicherheit:
  - Finanzielle Verluste
  - Verlust informationeller Selbstbestimmung
  - Gefährdung von Menschenleben
- Frühzeitige Berücksichtigung von Sicherheit im Systementwurf
- Bedarf an Modellierungstools

Übersicht

Begriffsbestimmung[1]

- Authentizität (authenticity):
  Echtheit einer vorgegebenen Identität
- Datenintegrität (data integrity):
  Ausschluss oder Erkennung unautorisierter Datenmanipulation
- Vertraulichkeit (confidentiality):
  Ausschluss unautorisierten Informationsgewinns
- Verbindlichkeit (non-repudiation):
  Nichtabstreitbarkeit ausgeführter Handlungen

[1] nach Eckert [11]

Angriffsmöglichkeiten

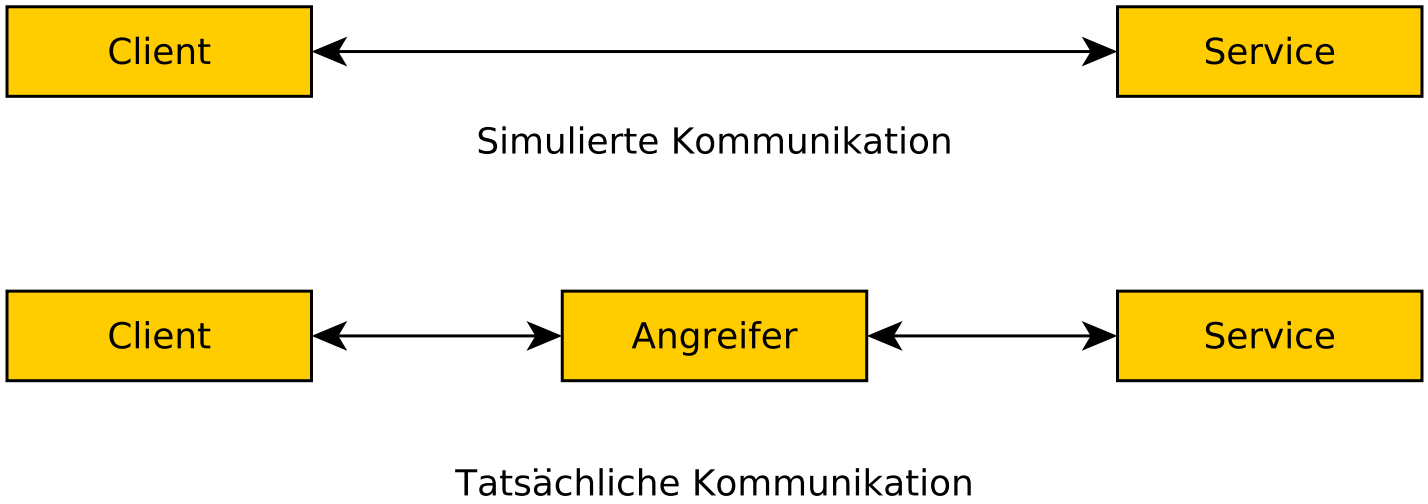


Abbildung: *Man in the middle*-Angriff

Übersicht

Service Oriented Architecture (SOA)[2]

- Designmuster für verteilte IT-Systeme
- Autoren: Schulte, Natis (1996) [31, 30]
- Kapselung von Funktionen in wiederverwendbare Dienste (Services)
- Abstrakte Interfaces, verborgene Implementierung
- Orchestrierung: Verknüpfung verschiedener Dienste zu einer Anwendung
- Besonders geeignet zur Abbildung von Geschäftsprozessen

[2] vgl. OASIS Referenzmodell [19]

Services finden und nutzen

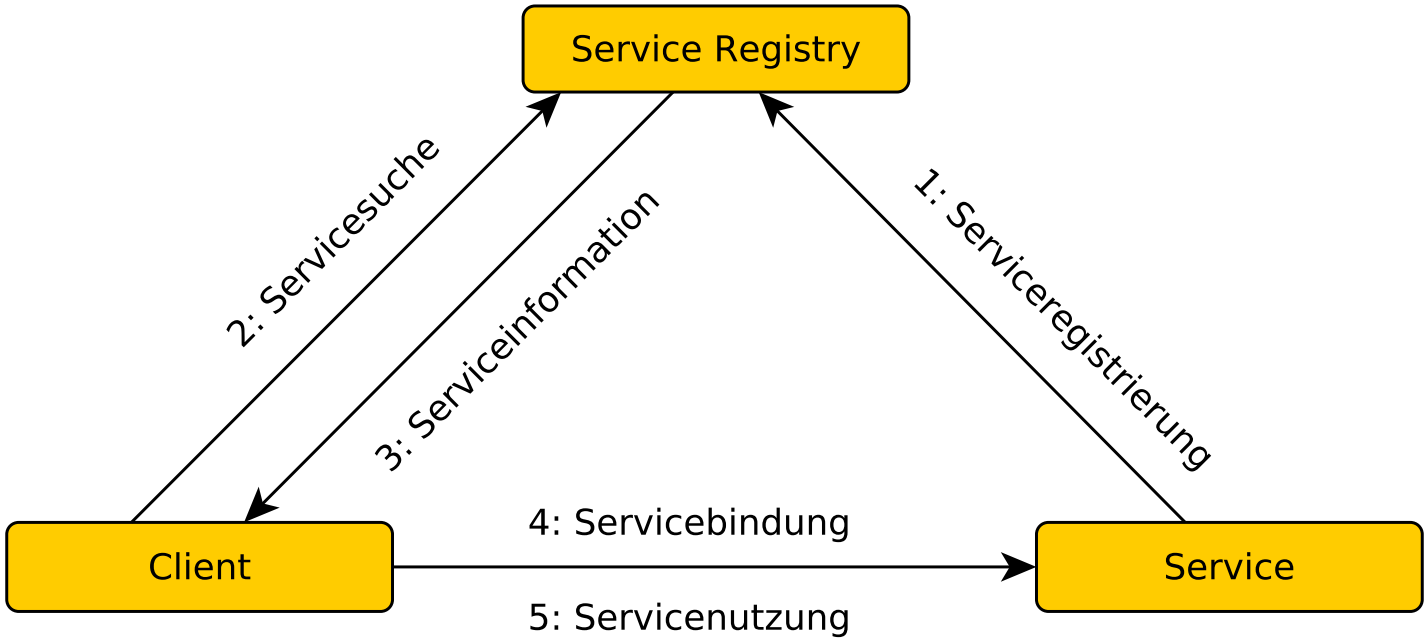


Abbildung: Nutzung einer Service-Registry

Web-Services

- Eine Umsetzung von SOA
- HTTP [12] als Kommunikationsprotokoll
- XML-basierte [5] Web-Service-Protokolle:
  - SOAP [13]: Nachrichtenformat
  - WSDL [6, 7]: Interface-Beschreibung
  - UDDI [8]: Verzeichnisdienst

Sicherheit in Web-Services

- WS-Policy [32]: WSDL-Erweiterung, beschreibt technische und nicht-technische Anforderungen an die Interaktion mit dem Dienst
- WS-Security-Policy [24]: Spezialisierung von WS-Policy für Sicherheitsanforderungen
- WS-Security [22]: Erweiterung des SOAP-Nachrichtenformates für den Einsatz von Sicherheitsfeatures
- WS-SecureConversation [23]: Erweiterung von WS-Security zur effizienteren Sicherung längerer Nachrichtenaustausche
- WS-Trust [25]: definiert Security-Token-Services (Identity-Provider), Einsatz unter Verwendung von WS-Security

Übersicht

SecureSOA

- Autoren: Michael Menzel, Christoph Meinel (Univ. Potsdam)
- 2010 IEEE International Conference on Services Computing [21]
- Frühere Ansätze anderer Autoren:
  - UMLSec [16]
  - SecureUML [4]
  - Verschienede Erweiterungen von BPMN [29, 34]
  - ...

Merkmale von SecureSOA

- Designt speziell für serviceorientierte Systeme
- Beliebige Entwurfssprachen Grundlagen für Dialekte
- Gemeinsames Meta-Modell zur einheitlichen Weiterverarbeitung
- Hohes Abstraktionsniveau geeignet für frühes Grobdesign
- Einfache Handhabung erfordert keine Fachkenntnisse

Übersicht

SOA-Basis-Modell

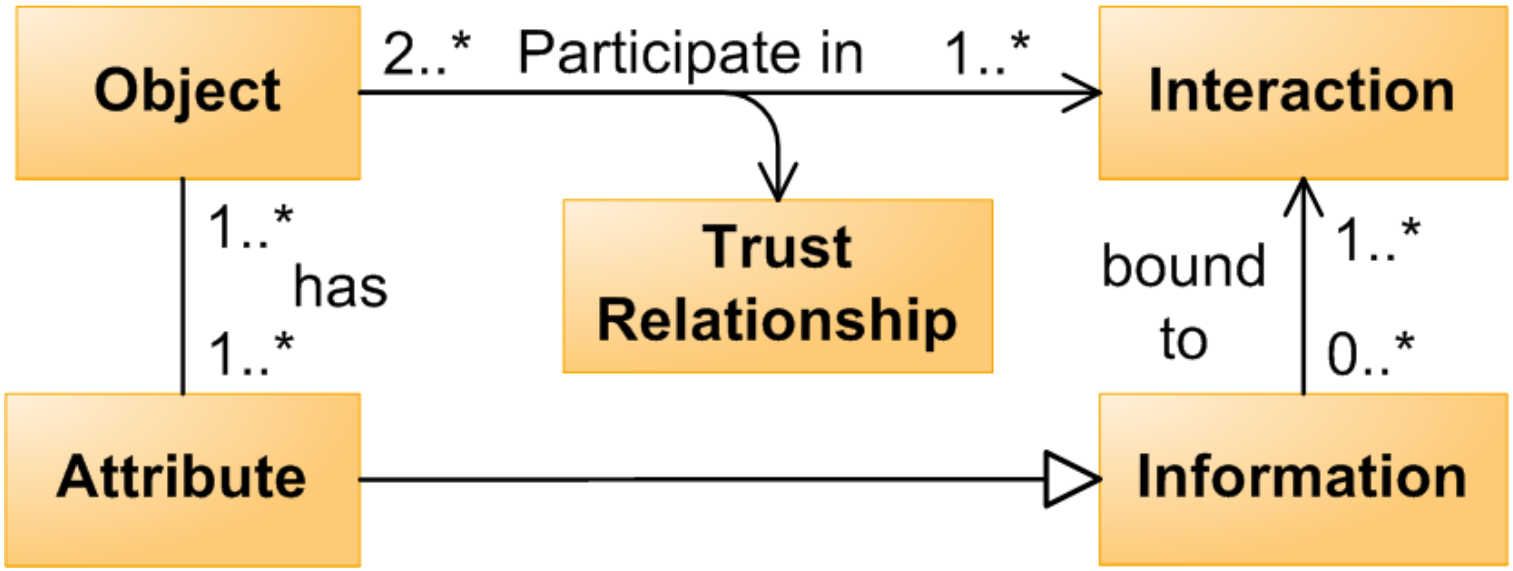


Abbildung: SOA-Basis-Modell [21, Abb. 2]

Erweiterung des Modells um Rollen

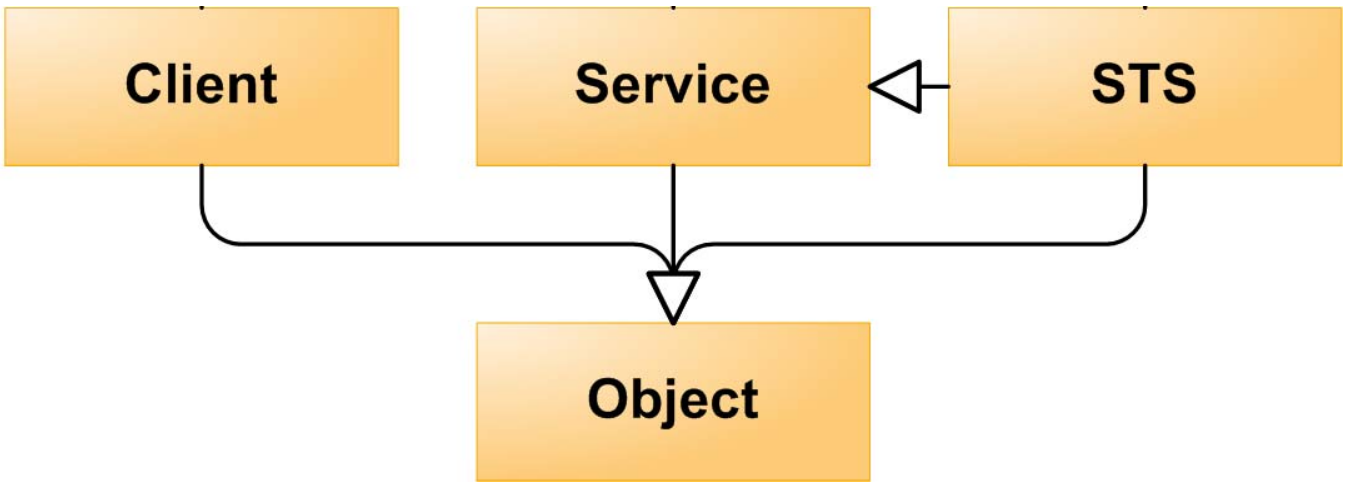


Abbildung: SOA-Rollen [20, Abb. 6]

Erweiterung des Modells um Data-Transfer-Objekte

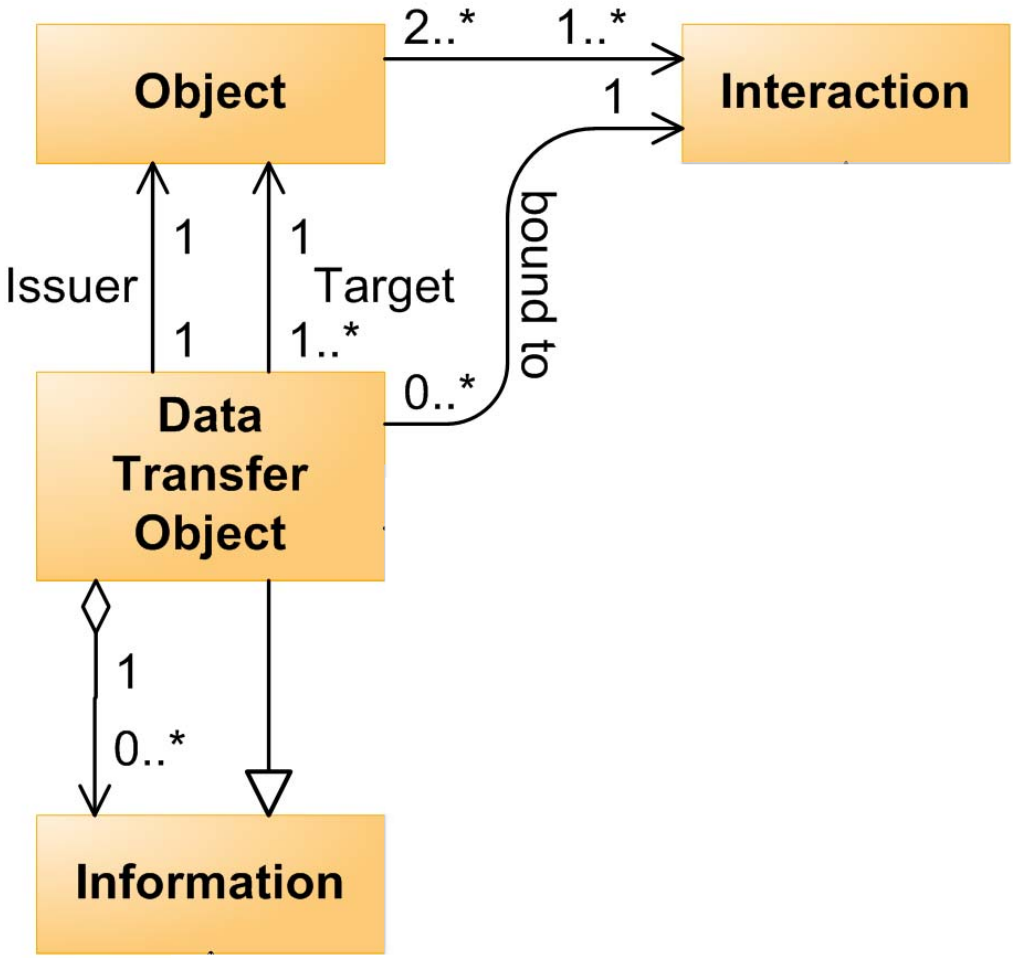


Abbildung: Data-Transfer-Objects [20, Abb. 3]

Security-Intentions

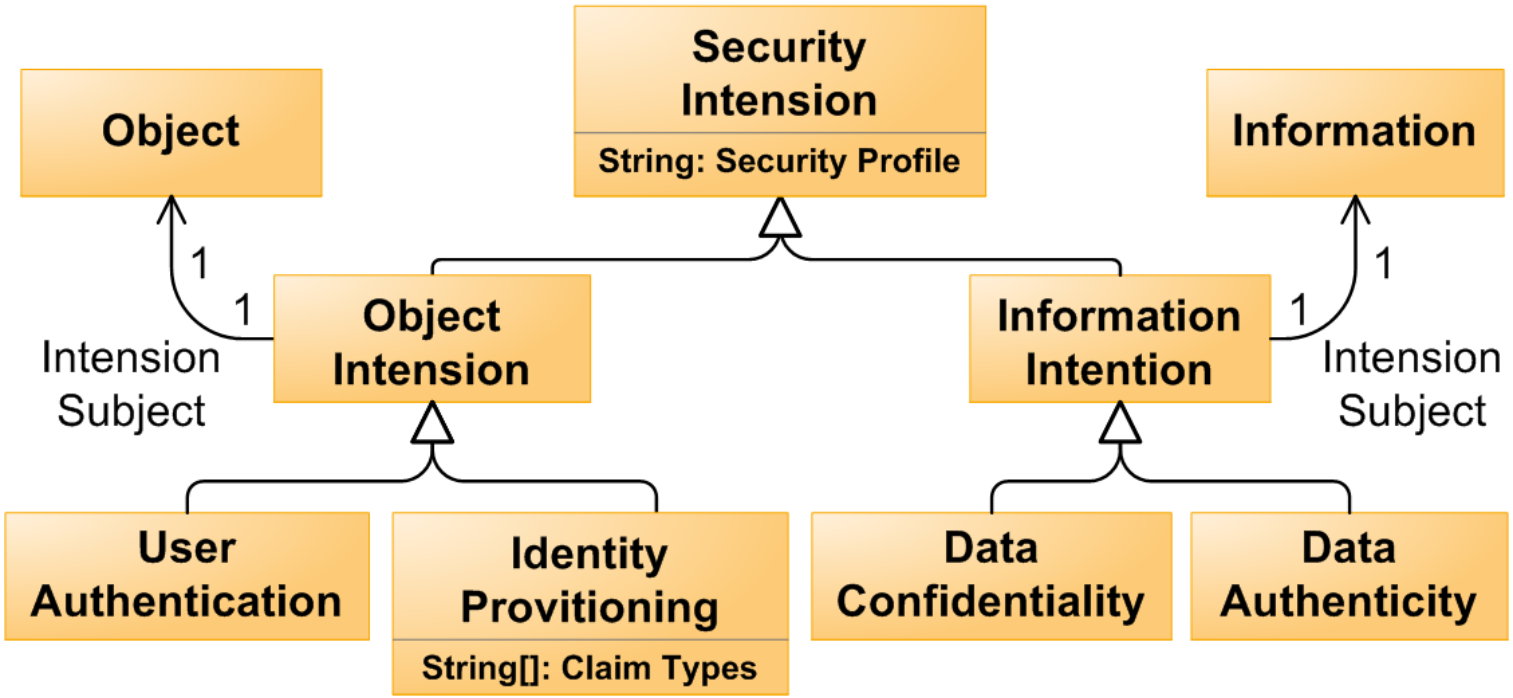


Abbildung: Modell für Sicherheitsziele [21, Abb. 3]

Übersicht

Konstruktion eines neuen Dialektes

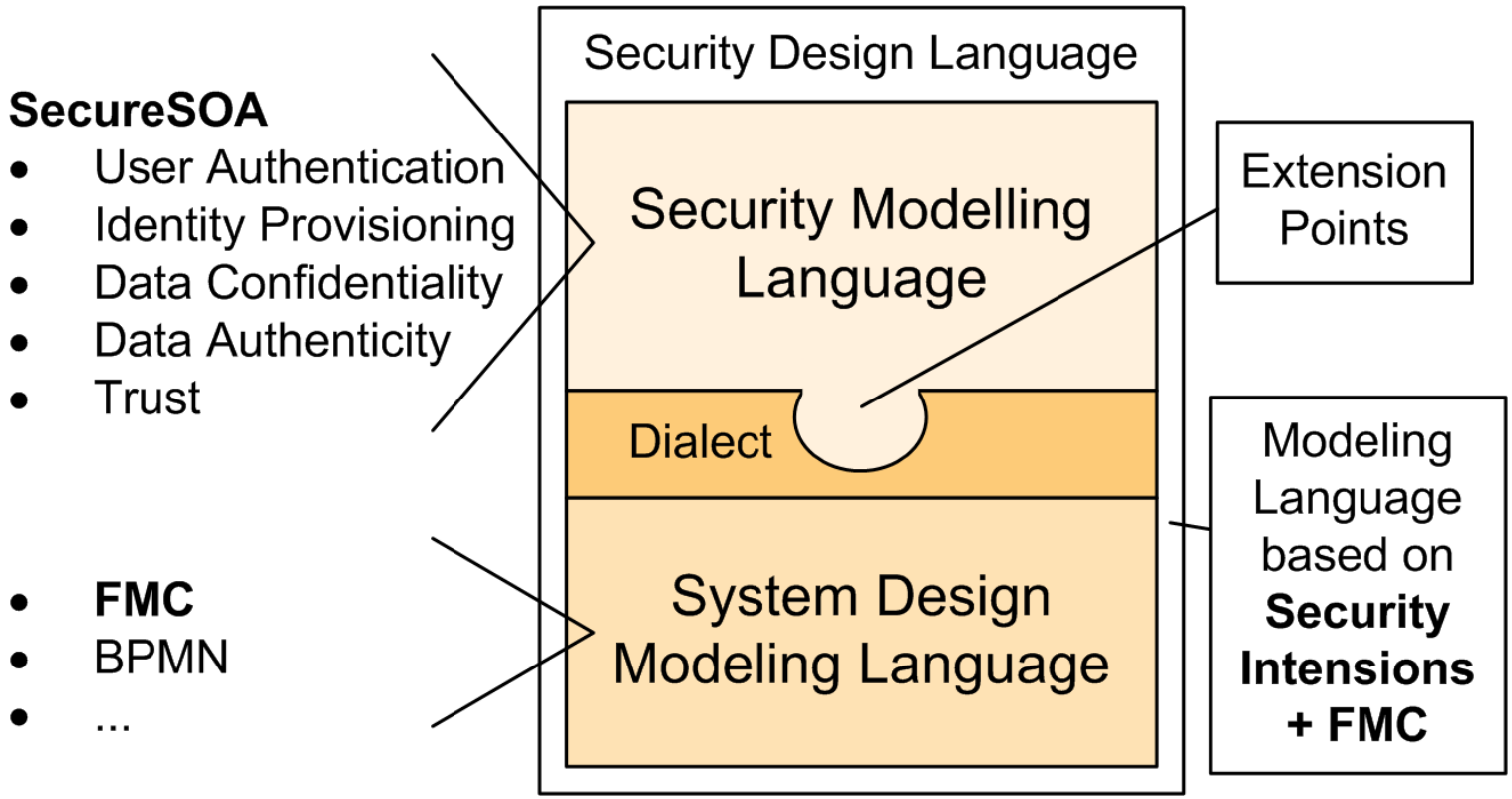


Abbildung: Konstruktion von SecureSOA-Dialekten [21, Abb. 1]

Extension-Points

Erweiterung des Modells der Zielsprache durch Verbindung mit den Klassen des SecureSOA-Basismodells:

- Direkte Abbildung
- Einführung neuer Klassen
- Assoziationen

Erweiterung durch direkte Abbildung

Die Klasse s_i in SecureSOA ist eine Abstraktion der vorhandenen Klasse m_j.

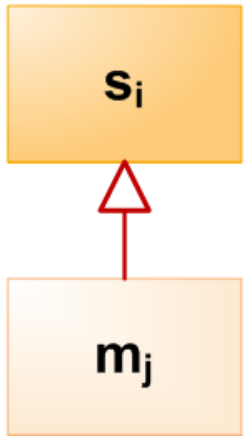


Abbildung: Integration durch einfache Vererbung [21, Tab. 1]

Erweiterung durch neue Klassen

Die Klasse s_i in SecureSOA ist eine Abstraktion der vorhandenen Klasse m_j, s_i wird jedoch durch $s_{i'}$ weiter spezifiziert, wofür es keine direkte Entsprechung gibt.

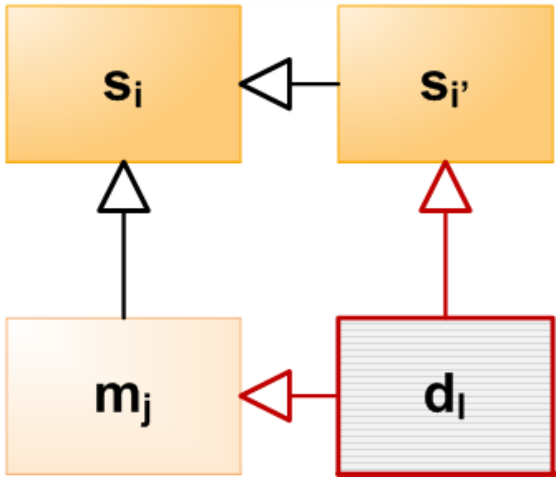


Abbildung: Integration durch Mehrfachvererbung [21, Tab. 1]

Erweiterung durch Assoziation

Die Klasse s_i entspricht mehreren vorhandenen Klassen m_j, m_k. OCL (Object Constraint Language [28]) kann zur näheren Bestimmung genutzt werden.

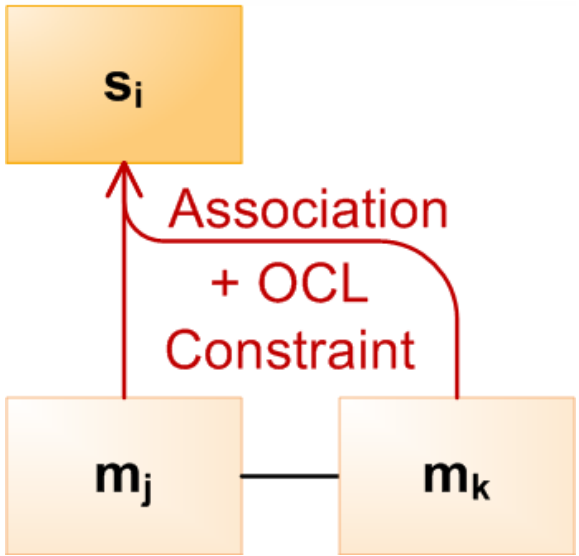


Abbildung: Integration durch Assoziationen [21, Tab. 1]

Syntax der SecureSOA-Komponenten

- Elemente des Basismodells: Syntax der Zielsprache
- Security-Intentions: UML-Klassen mit Stereotypen, Assoziationen

UML-Stereotyp	Symbol
«User Authentication»	
«Non-Repudiation»	
«Identity Provisioning»	
«Data Authenticity»	
«Data Confidentiality»	
«Trust»	

Tabelle: Syntax für Security-Intentions [21, Tab. 2]

Übersicht

Fundamental Modeling Concepts (FMC)[3]

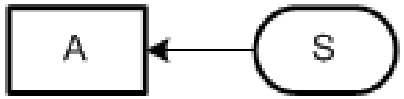
- Framework zur graphischen Modellierung dynamischer Softwaresysteme
- Hohes Abstraktionsniveau
- Hier: Compositional Structure Diagrams (Block Diagrams)

[3] nach FMC Quick Introduction [17]

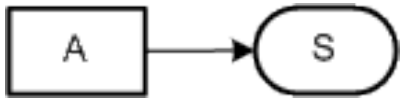
Syntax für FMC-Blockdiagramme

Agent, aktive Systemkomponente
(rechts: menschlicher Agent)

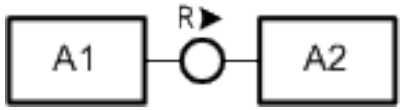
Location, passive Systemkomponente
(links: Storage, rechts: Channel)



Lesezugriff



Schreibzugriff



Request-Response-Kommunikation

Tabelle: Syntax für FMC-Blockdiagramme [3]

Metamodell für FMC

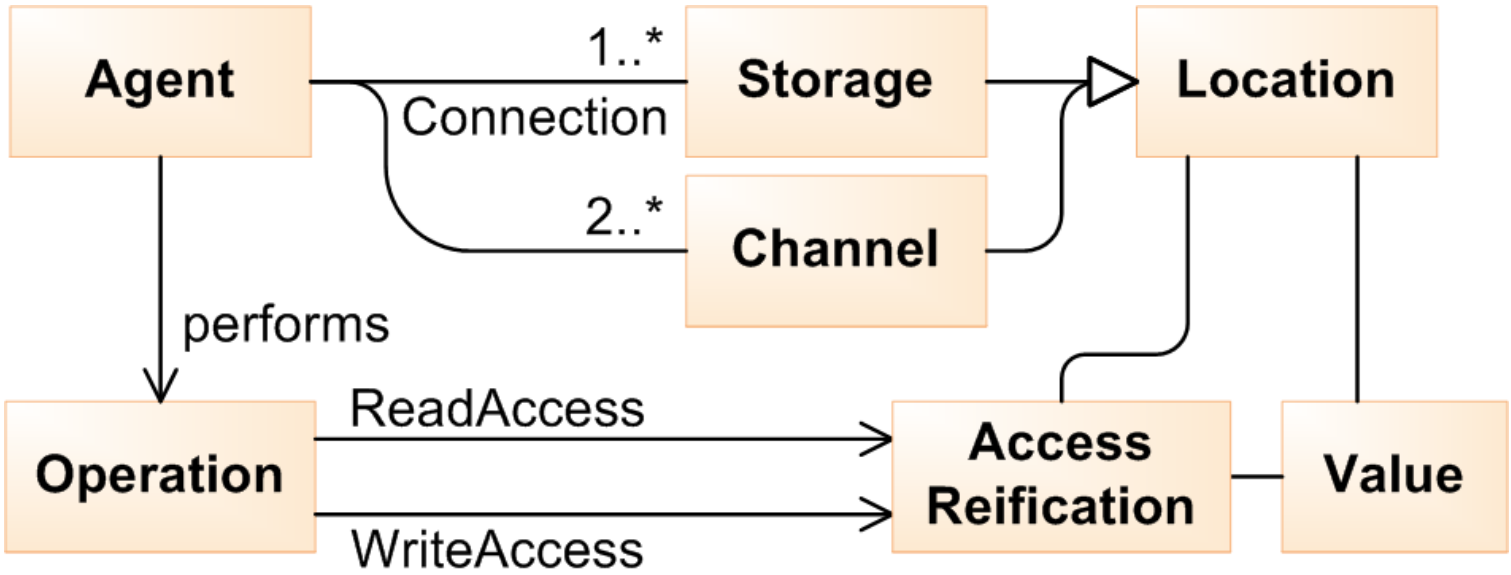


Abbildung: Meta-Modell für FMC [21, Abb. 4]

Kombiniertes Dialekt-Modell

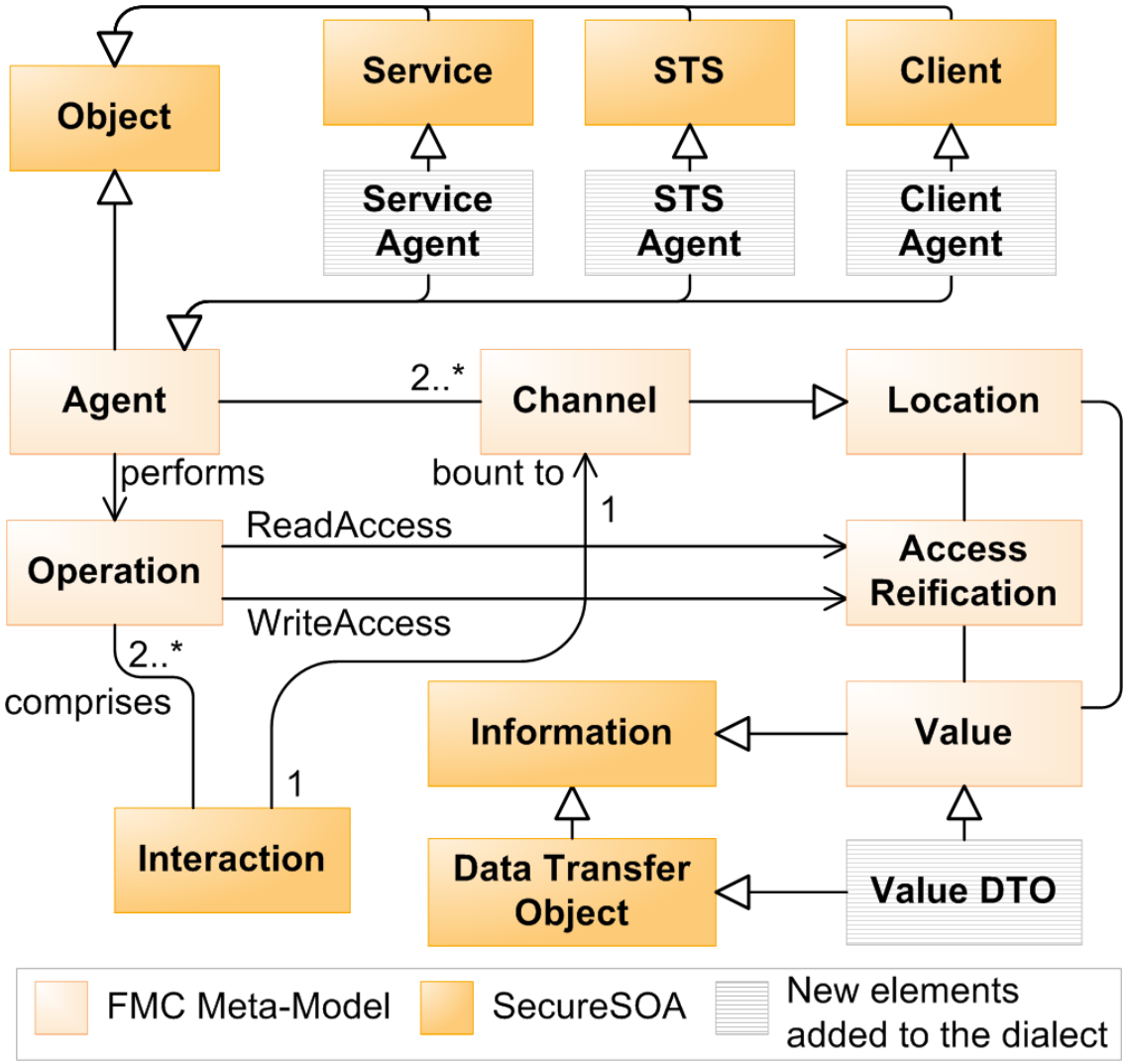


Abbildung: FMC-Dialekt basierend auf SecureSOA [21, Abb. 5, korrigiert]

Anwendungsbeispiel

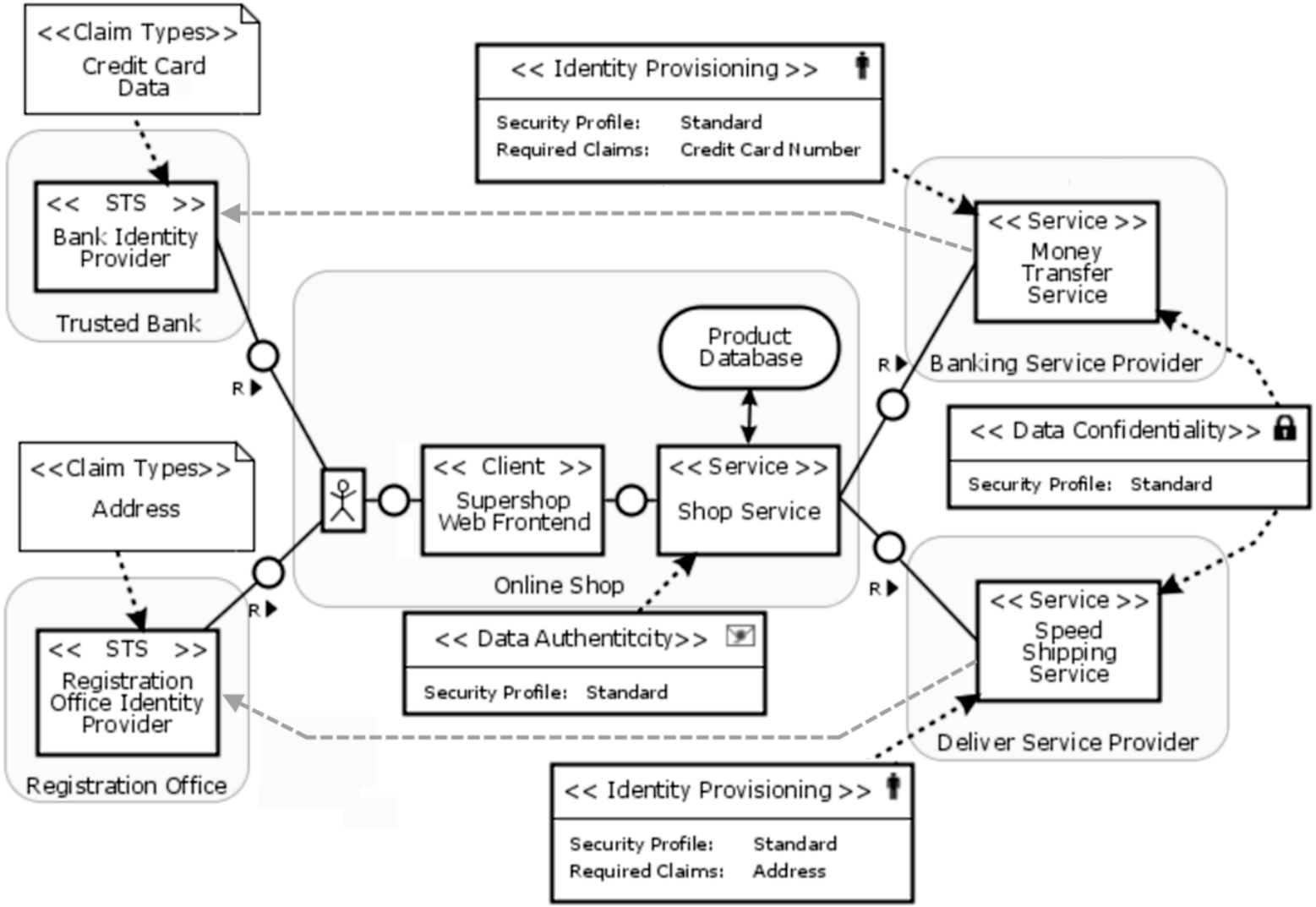


Abbildung: Modellierungsbeispiel [21, Abb. 6]

Übersicht

Zusammenfassung

- Motivation
- Grundlagen
  - Sicherheitsbegriffe
  - Service-Oriented Architecture
  - Web-Services
- SecureSOA
  - Sprachdesign
  - Meta-Modell
  - Erweiterung anderer Sprachen
  - Beispiel: FMC

Fazit

- Leicht zu verwenden, flexibel erweiterbar
- Informationen weiterverwendbar (Policy-Generierung [20])
- Fehlender Test in der Praxis
- Auch als Designstudie interessant

Weiterführendes Material

[1] *ACM Transactions on Software Engineering and Methodology*. Bd. 15. 1. Association for Computing Machinery. 2006.

[2] Gustavo Alonso, Peter Dadam und Michael Rosemann, Hrsg. *BPM '07: Proceedings of the 5th international conference on Business process management*. Bd. 4714. 2007.

[3] Rémy Apfelbacher und Anne Rozinat. *FMC Compositional Structures*. Reference Sheet. 2005.

[4] David Basin, Jürgen Doser und Torsten Lodderstedt. "Model driven security: From UML models to access control infrastructure". In: *ACM Transactions on Software Engineering and Methodology*. Bd. 15. 1. Association for Computing Machinery. 2006.

[5] *Extensible Markup Language (XML) 1.0 (Fifth Edition)*. Standard. World Wide Web Consortium, 26. Nov. 2008. URL: http://www.w3.org/TR/2008/REC-xml-20081126/.

Weiterführendes Material (Forts.)

[6] *Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language*. Standard. World Wide Web Consortium, 26. Juni 2007. URL: http://www.w3.org/TR/wsdl20/.

[7] *Web Services Description Language (WSDL) Version 2.0 Part 2: Adjuncts*. Standard. World Wide Web Consortium, 26. Juni 2007. URL: http://www.w3.org/TR/wsdl20-adjuncts/.

[8] *UDDI Version 3.0.2*. Standard. OASIS, 19. Okt. 2004. URL: http://uddi.org/pubs/uddi_v3.htm.

[9] *Documents Associated With Business Process Model And Notation (BPMN) Version 2.0*. Standard. Object Management Group, Jan. 2011. URL: http://www.omg.org/spec/BPMN/2.0/.

[10] *Documents Associated With Unified Modeling Language (UML), V2.4.1*. Standard. Object Management Group, Aug. 2011. URL: http://www.omg.org/spec/UML/2.4.1/.

Weiterführendes Material (Forts.)

[11] Claudia Eckert. *IT-Sicherheit. Konzepte – Verfahren – Protokolle*. 7. Aufl. München: Oldenbourg Wissenschaftsverlag GmbH, 2012. ISBN: 978-3-486-70687-1.

[12] *Hypertext Transfer Protocol – HTTP/1.1*. Standard. The Internet Society, Juni 1999. URL: http://www.ietf.org/rfc/rfc2616.txt.

[13] *SOAP Version 1.2 Part 1: Messaging Framework (Second Edition)*. Standard. World Wide Web Consortium, 27. Apr. 2007. URL: http://www.w3.org/TR/soap12-part1/.

[14] *IEICE Transactions on Information and Systems*. Bd. E90-D. 4. The Institute of Electronics, Information und Communication Engineers. 2007.

Weiterführendes Material (Forts.)

[15] Jean-Marc Jézéquel, Heinrich Hußmann und Stephen Cook, Hrsg. *UML '02: Proceedings of the 5th International Conference on The Unified Modeling Language*. 2002.

[16] Jan Jürjens. "UMLsec: Extending UML for Secure Systems Development". In: *UML '02: Proceedings of the 5th International Conference on The Unified Modeling Language*. Hrsg. von Jean-Marc Jézéquel, Heinrich Hußmann und Stephen Cook. 2002.

[17] Andreas Knöpfel. *FMC Quick Introduction*. 2007.

[18] Thomas Kühne, Wolfgang Reisig und Friedrich Steimann, Hrsg. *Modellierung 2008*. Gesellschaft für Informatik e. V. 2008.

[19] *Reference Model for Service Oriented Architecture 1.0*. Standard. OASIS, 12. Okt. 2006. URL: http://docs.oasis-open.org/soa-rm/v1.0/.

Weiterführendes Material (Forts.)

[20] Michael Menzel und Christoph Meinel. "A Security Meta-Model for Service-oriented Architectures". In: *2009 IEEE International Conference on Services Computing*. Hrsg. von Lisa O'Conner. IEEE Computer Society Technical Committee on Services Computing. 2009.

[21] Michael Menzel und Christoph Meinel. "SecureSOA – Modelling Security Requirements for Service-oriented Architectures". In: *2010 IEEE International Conference on Services Computing*. Hrsg. von Lisa O'Conner. IEEE Computer Society Technical Committee on Services Computing. 2010.

[22] *Web Services Security: SOAP Message Security 1.0 (WS-Security 2004)*. Standard. OASIS, März 2004. URL: http://www.oasis-open.org/standards#wssv1.0.

Weiterführendes Material (Forts.)

[23] *WS-SecureConversation 1.4*. Standard. OASIS, 2. Feb. 2009. URL: http://docs.oasis-open.org/ws-sx/ws-secureconversation/v1.4/ws-secureconversation.html.

[24] *WS-SecurityPolicy 1.3*. Standard. OASIS, 2. Feb. 2009. URL: http://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.3/os/ws-securitypolicy-1.3-spec-os.html.

[25] *WS-Trust 1.4*. Standard. OASIS, 2. Feb. 2009. URL: http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/ws-trust.html.

[26] Lisa O'Conner, Hrsg. *2009 IEEE International Conference on Services Computing*. IEEE Computer Society Technical Committee on Services Computing. 2009.

Weiterführendes Material (Forts.)

[27] Lisa O'Conner, Hrsg. *2010 IEEE International Conference on Services Computing*. IEEE Computer Society Technical Committee on Services Computing. 2010.

[28] *OMG Object Constraint Language (OCL). Version 2.3.1 without change bars*. Standard. Object Management Group, 1. Jan. 2012.

[29] Alfonso Rodríguez, Eduardo Fernández-Medina und Mario Piattini. "A BPMN extension for the modeling of security requirements in business processes". In: *IEICE Transactions on Information and Systems*. Bd. E90-D. 4. The Institute of Electronics, Information und Communication Engineers. 2007.

[30] W. Roy Schulte. *"Service Oriented" Architectures, Part 2*. Research Note. Gartner Inc., 12. Apr. 1996.

[31] W. Roy Schulte und Yefim V. Natis. *"Service Oriented" Architectures, Part 1*. Research Note. Gartner Inc., 12. Apr. 1996.

Weiterführendes Material (Forts.)

[32] *Web Services Policy 1.5 – Framework*. Standard. World Wide Web Consortium, 4. Juli 2007. URL: http://www.w3.org/TR/ws-policy/.

[33] Christian Wolter, Michael Menzel und Christoph Meinel. "Modelling security goals in business processes". In: *Modellierung 2008*. Hrsg. von Thomas Kühne, Wolfgang Reisig und Friedrich Steimann. Gesellschaft für Informatik e. V. 2008.

[34] Christian Wolter und Andreas Schaad. "Modeling of task-based authorization constraints in BPMN". In: *BPM '07: Proceedings of the 5th international conference on Business process management*. Hrsg. von Gustavo Alonso, Peter Dadam und Michael Rosemann. Bd. 4714. 2007.