Secure UML

Security Engineering-Seminar SS2009

Dennis Schulz

University Duisburg-Essen, Faculty of Engineering,
Department of Computational and Cognitive Sciences,
Working Group Software Engineering, Prof. Dr. M. Heisel

3. August 2009

Einfuehrung I

Motivation

- Rechteverwaltung in der Planungsphase.
- Uebersichtliche Darstellung der Zugriffsrechte

Einfuehrung II

Motivation

- Automatische Transformierung zu Quelltext
- Weniger Fehler hierbei
- Verschiedene Plattformen.

SecureUML I
Warum UML

- Uebersichtliche Darstellung der Architektur
- Standardisiert
- Praezise

SecureUML I
Role-Bases Access Control

- Bewaehrtes Konzept der Zugriffssteuerung

SecureUML II
Role-Bases Access Control

- Benutzer
- Rollen
- Berechtigungen

SecureUML III
Role-Bases Access Control

Eine Berechtigung besteht dabei aus

- beliebig vielen Operationen auf
- einer Ressource

SecureUML I
Metamodell

- Erweiterung des UML2-Modells
- User,Role,Permission aus RBAC uebernommen

SecureUML II
Metamodell

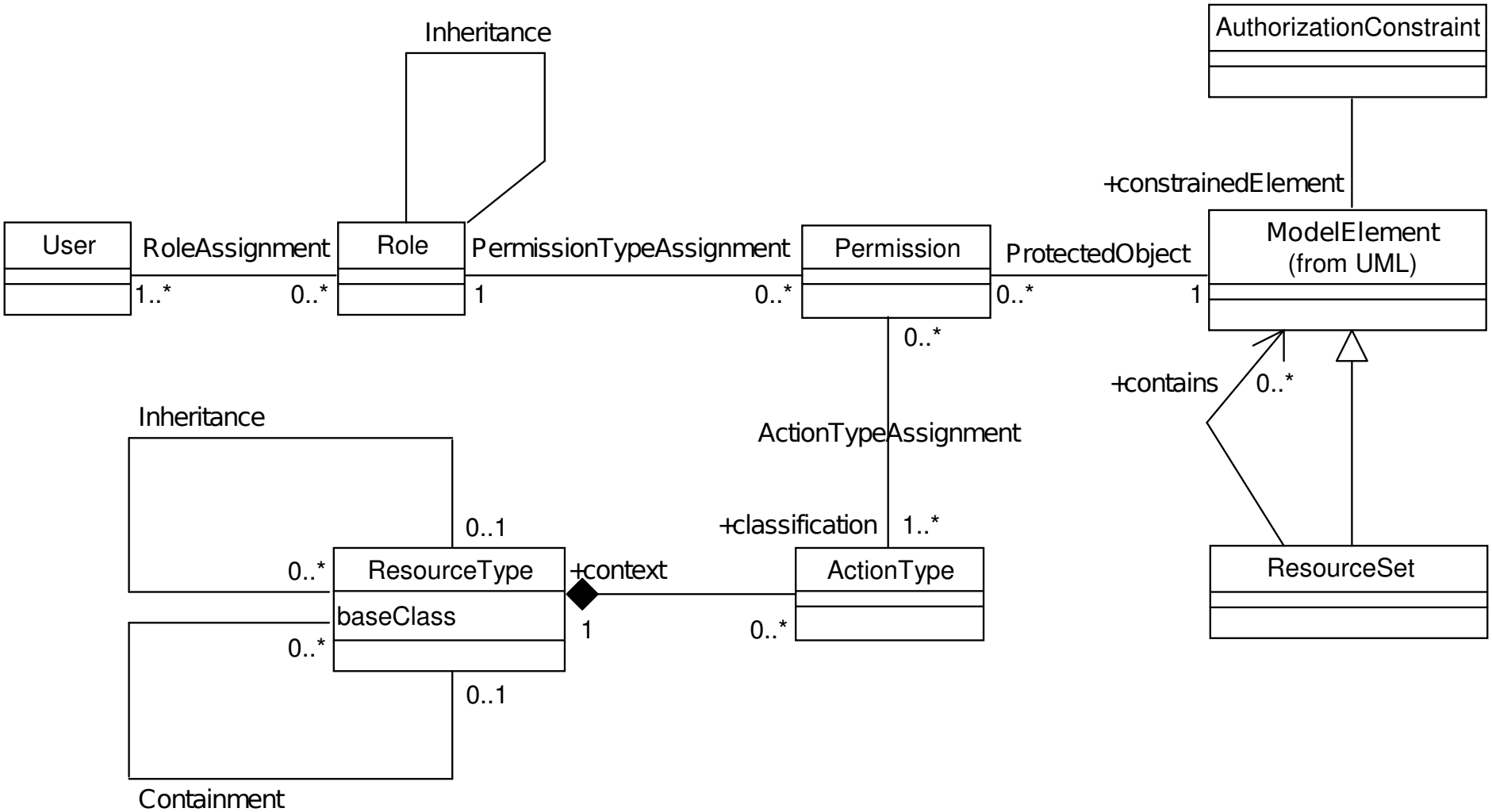


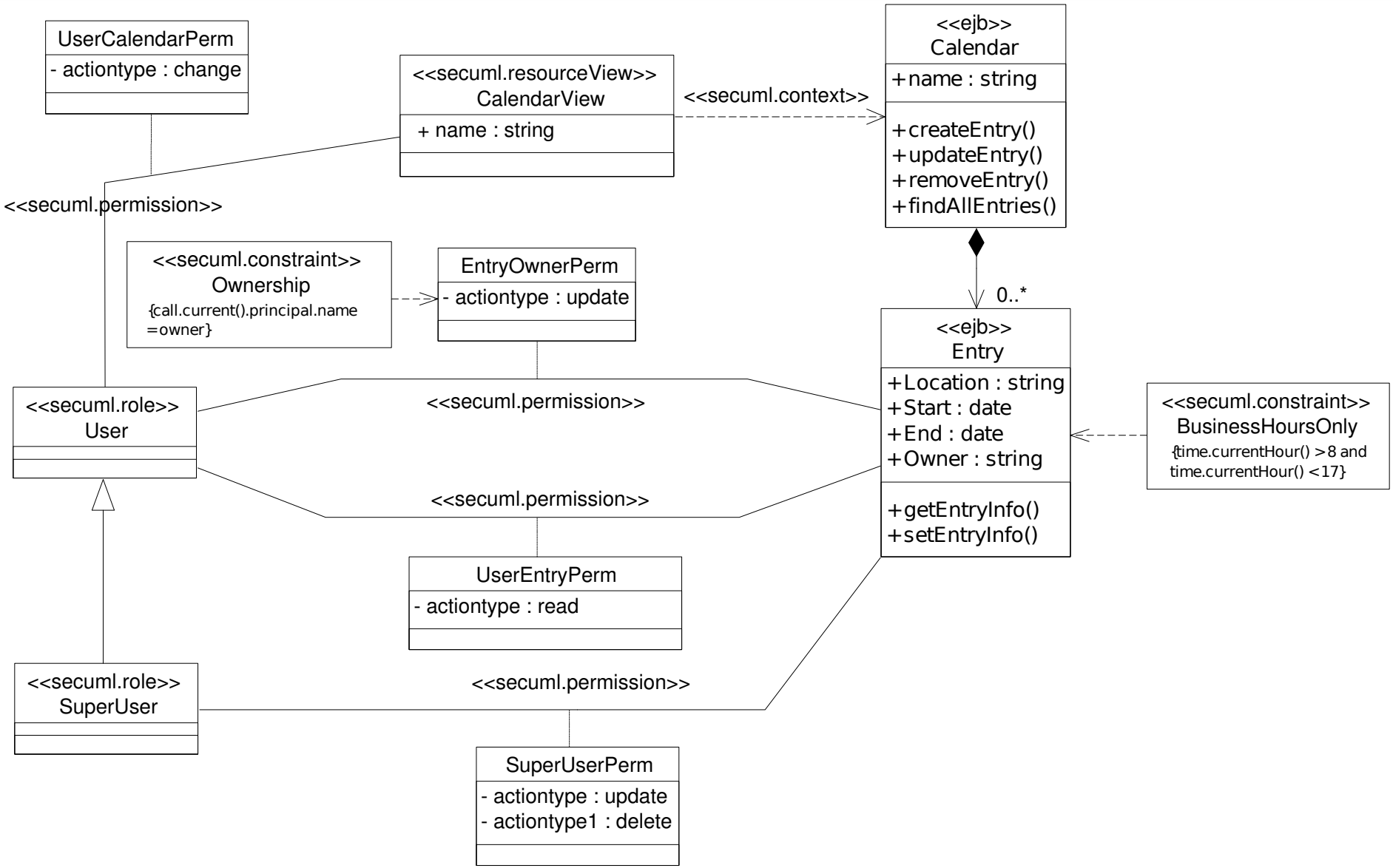
Abbildung: SecureUML Metamodell

SecureUML I
Kalender-UML

Kalenderapplikation auf EJB, dargestellt mit UML 2.0 und SecureUML

SecureUML II

Kalender-UML



SecureUML und Enterprise JavaBeans I

EJB

- Standardisierte Softwarekomponenten
- Laufen innerhalb einer JavaEE-Servers (JBoss, IBM WebSphere, BEA WebLogic)
- Vereinfachen entwicklung verteilter mehrschicht Anwendungen

SecureUML und Enterprise JavaBeans I

Rollen

Eine Rolle kann in EJB folgendermassen im Deployment-Descriptor definiert werden:

```
<security-role>
    <role-name>User</role-name>
</security-role>
```

SecureUML und Enterprise JavaBeans I

Berechtigungen

- Permission „UserEntryPerm“
- fuer Rolle „User“
- mit ActionType „read“
- EJB kennt keine vererbung von Rollen

SecureUML und Enterprise JavaBeans II

Berechtigungen

```
<method-permission>
  <role-name>User</role-name>
  <method>
    <ejb-name>Entry</ejb-name>
    <method-name>findByPrimaryKey</method-name>
  </method>
  <method>
    <ejb-name>Entry</ejb-name>
    <method-name>getEntryInfo</method-name>
  </method>
```

SecureUML und Enterprise JavaBeans III

Berechtigungen

```
<method>
  <ejb-name>Calendar</ejb-name>
  <method-name>findByPrimaryKey</method-name>
 </method>
 <method>
  <ejb-name>Calendar</ejb-name>
  <method-name>createEntry</method-name>
 </method>
 ...
 </method-permission>
```

SecureUML und Enterprise JavaBeans IV

Berechtigungen

- „findByPrimaryKey“ ist eine Standardmethode, die nicht im Diagramm zu sehen ist.
- Problem: Zugriff auf Eigenschaften nicht direkt beschraenkbar
- Loesung: Private Attribute und oeffentliche Get- und Set-Methoden

SecureUML und Enterprise JavaBeans V

Berechtigungen

```
public class CalendarView {
private String name;

public getName();
public setName(String name);
}
```

SecureUML und Enterprise JavaBeans VI

Berechtigungen

```
<method-permission>
  <role-name>User</role-name>
  <method>
    <ejb-name>CalendarView</ejb-name>
    <method-name>setName</method-name>
  </method>
</method-permission>
```

SecureUML und Enterprise JavaBeans I

Authorization Constraints

- securml.constraint
- Object Constrain Language

SecureUML und Enterprise JavaBeans II

Authorization Constraints

```
time.currentHour() > 8
and time.currentHour() < 17

context Entry::getEntryInfo():EntryInfo
pre: time.currentHour() > 8
and time.currentHour() < 17

context Entry::setEntryInfo():EntryInfo
pre: time.currentHour() > 8
and time.currentHour() < 17
```

SecureUML und Enterprise JavaBeans I

Benutzerrollenzuweisung

Darstellung der Benutzer-Rollen-Relation fuer BEA WebLogic im Deployment-Descriptor

```
<security-role-assingment>
<role-name>User</role-name>
<principal-name>Smith</principal-name>
</security-role-assignment>
```

Fazit I

- SecureUML baut auf RBAC und UML2 auf
- Modellgetriebene Softwareentwicklung mit SecureUML kann Sicherheitsprobleme vorbeugen
- Generatoren erzeugen Quelltext und Konfigurationen fue verschiedene Plattformen.
- Generator: ArcStyler von Interactive Objects
- Sicherheitsrelevanter-Code automatisiert erzeugt. Weniger Fehler.
- Wartbarkeit erhoeht
- Verwendbar auch fuer die .NET-Plattform

SecureUML I

Stefan Queins Chris Rupp, Juergen Hahn.
UML 2 glasklar, Praxiswissen fuer die UML-Modellierung und -Zertifizierung.
HANSER, 2005.

Object Management Group.
Object constraint language 2.0: Specification, 2006.
http://www.omg.org/docs/formal/06-05-01.pdf.

Richard Kuhn Rvai Sandhu, David Farraiolo.
The nist model for role-based access control: Towards a unified standard, 2000.

SecureUML II


J. Doser T. Lodderstedt, D. A. Basin.
Secureuml: A uml-based modeling language for model-driven security.
In Proceedings of the 5th International Conference on The Unified Modeling Language (UML'02), pages 426–441, London, UK, 2002. Springer-Verlag.