Java und Information Flow

von Andreas Schober

Inhaltsverzeichnis

Einleitung

- Zeitdruck während der Entwicklung
- Vernachlässigung von sicherheitstechnischen Aspekten
- Gefahr bei Informationsflüssen beim Mobile Banking

Informationsflüsse 1 / 3: Einführung

- ein kleines Beispiel:

```
1 int x = 0;
2 int y = x;
```

- x stellt die Information 0 zur Verfügung
- die Information wird von x zu y übermittelt

Informationsflüsse 2 / 3: Angreifer

- passiver Angreifer:
  - beobachtet ein System

- aktiver Angreifer:
  - beobachtet ein System
  - kann das Systemverhalten und Daten verändern

Informationsflüsse 3 / 3
implizite Flüsse

- geringer Bekanntheitsgrad
- werden daher selten behoben

```
1  int l;
2  boolean h = true;
3  if ( h == true ) then {
4     l := 3
5  }
6  else {
7     l := 42
8  }
```

JIF 1 / 8:
Einführung

- sicherheitstypische Java – Erweiterung
- Verbesserung der Integrität von Daten
- Absichern von Informationsflüssen
- Anwendung während der Kompilierung / Laufzeit
- Einbindung in bereits vorhandene Java - Klassen

- Beispiel ohne JIF:

```
1 int x;
2 int y;
3 x = y;
4 y = x;
```

- Beispiel mit JIF:

```
1 int {Alice->Bob} x;
2 int {Alice->Bob, Chuck} y;
3 x = y; // OK: policy on x is stronger
4 y = x; // BAD: policy on y is not as strong as x
```

JIF 4 / 8:
Principals

- Vergleichbar mit Entitäten und Rollen
- können für einander arbeiten:

  $q \geq p \Leftrightarrow$ „q handelt für p“
- reflexiv und transitiv
- Abbildung einer Rollenhierarchie mit Principals
- Top- und Bottom-Principals

JIF 5 / 8: Vertraulichkeitsrichtlinien

- Regeln für den Lese-Zugriff auf Informationen
- o → r ⇔ Principal o erlaubt principal r das Lesen
- Einbeziehung der Transitivität

$$readers(p,\ o \rightarrow r) \equiv \{q \mid if\ o \geq p\ then\ (q \geq o\ or\ q \geq r)\}$$

$$readers(p,\ c \sqcup d) \equiv readers(p,\ c) \cap readers(p,\ d)$$

$$readers(p,\ c \sqcap d) \equiv readers(p,\ c) \cup readers(p,\ d)$$

JIF 6 / 8: Vertraulichkeitsrichtlinien

- Konjunktion $c \sqcup d$:

  c und d müssen das Lesen gestatten

- Disjunktion $c \sqcap d$:

  c oder d müssen das Lesen gestatten

JIF 7 / 8:
Integritätsrichtlinien

- Regeln für den Schreib-Zugriff auf Informationen
- o ← r ⇔ Principal o erlaubt principal r das Verändern
- Einbeziehung der Transitivität

$$writers(p,\ o \leftarrow w) \equiv \{q \mid \mathit{if}\ o \geq p\ \mathit{then}\ (q \geq o\ \mathit{or}\ q \geq w)\}$$
$$writers(p,\ c \sqcap d) \equiv writers(p,\ c) \cap writers(p,\ d)$$
$$writers(p,\ c \sqcup d) \equiv writers(p,\ c) \cup writers(p,\ d)$$

- Konjunktion und Disjunktion analog

JIF 8 / 8:
Methoden und Klassen

```
1  int {Alice->Bob} x;
2  public class Vector[label L] extends
3  AbstractList[L] { private int{L} length;
4      private Object{L}[]{L} elements;
5
6      public Vector() ...
7      public Object elementAt(int i):{L; i}
8                          throws IndexOutOfBoundsException {
9          ...
10         return elements[i];
11     }
12     public void setElementAt{L}(Object{L} o, int{L} i) ...
13     public int{L} size() { return length; }
14     public void clear{L}() ...
15     ...
16 }
```

Anwendungsbeispiel 1 / 2: Jifclipse

- Erweiterung für die Entwicklungsumgebung Eclipse
- Aufgaben:
  - Unterstützung bei der Bestimmung der Principals
  - Sinnvolle Darstellung von Labels und Richtlinien
  - Hilfe bei der Fehlerbehebung

Anwendungsbeispiel 2 / 2: JPMail

- Ziel: vertraulicher Empfang und Versand von EMails
- Versuch eine Anwendung komplett mit JIF zu entwickeln
- Markieren der Daten mit Sicherheitsleveln
- Vielfache Anwendung von Labels
- Nachrichtentransfer ist mit Richtlinien abgesichert

Zusammenfassung

- Informationsflüsse sind oft nicht als Gefahr anerkannt
- Einschränkung von Vertraulichkeiten mittels Labels in JIF
- Rollenhierarchie durch Principals und Richtlinien
- verbesserte Kontrolle über den Zugriff auf Daten

Fazit

- Informationsflüsse sind sicherheitstechnisch oft verkannt
- komplexe Programmcodes mit JIF wirken anfangs überladen
- Realitätsnahe Programmierung mittels Principals
- gute Entwicklungsunterstützung dank Eclipse - Plugin

Vielen Dank für Ihre Aufmerksamkeit!

Haben Sie noch Fragen?

Quellen

http://www.cs.cornell.edu/jif/

(zuletzt gesehen am 02.07.2012, 17:55)