Universität Potsdam
- Informatik -
Lehrstuhl für Sotfwareengineering

Bachelor- / Masterarbeit

im Studiengang <Studiengang> - Schwerpunkt <Schwerpunktfach>

zur Erlangung des akademischen Grades
Bachelor / Master of Science

Title:	Service authorization in an orchestrated (micro) service architecture
Autor:	Name <name@mail.de> MatNr. 12345...
Version vom:	February 22, 2021
1. Supervisor:	Prof. Dr. Christian Hammer
2. Supervisor:	Dr. Ragnar Nevries

Zusammenfassung

Hier steht der Text, welcher den Inhalte der Arbeit zusammenfasst...

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Abstract

Here goes the English text which summarizes the content of the thesis...

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Contents

List of Figures

List of Tables

Listingverzeichnis

1 Introduction

Hier steht die Einleitung der Arbeit... Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

1.1 Motivation

1.2 Terminology

2 Related research

Text des ersten Abschnitts... Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

2.1 Workflowengine

Erstes Unterabschnitt

2.1.1 In general

- workflow engines in context of BPM and the context of application integration within business software architectures - history of the technology (from SOA to micro service)

2.1.2 In context with microservices

- use cases of workflowengines within micro service architectures - keyword: micro service Orchestration - Outlook Cloud technologies and Software as a Service.

2.2 Service authorization

Zweiter Unterabschnitt

2.2.1 Micro service security

- General new security challenges with micro service architectures. Responsibilities for security within the team (each team gets a security person, which could lead to different security implementations for each micro service), or a central security team, . . . take into account that micro services not just define a new architecture but also change the way of defined rolls for developer teams and address therefore organizational problems as well

2.2.2 Service authorization implementations

-Layers of authorization (SSO Server / Service itself) -Common patterns and technologies for authorization in micro service technologies - JWT, OAuth2, Database lock up

3 Service authorization for workflowengines

Overview of the current state of service authorization for services with workflowengines -(Netflix conductor, Uber candence and ING Backer, Camunda Plattform, Zeebe)

3.1 Analysis of security vulnerabilities

- Identify the vulnerabilities and name the attack vectors - Thread to confidentiality and integrity of process and process data

3.2 Critical use cases

- In which use cases can the identified vulnerability lead to a risk - Examples: - 1.scenario: distributed micro service architecture with critical business process, like credit application (one malicious services writes and reads data from another service) - 2. scenario: Software as a Service: Multiple customers use the same workflow engine in the cloud:tenant based: without authorization different clients could read and write to process variables of different customers

4 Design a secure service authorization with a workflow engine

- Present a design to implement authorization

4.1 Process properties to be protected

-discuss different elements of the process that can or should be protected based on the example Camunda. Platform: Process variables (read, update) Allowed calls Process definitions Rolls for service tasks

4.2 Define authorization

- Analyze concrete implementation rolls and layers for the identified resource above

4.2.1 Layers of authorization

- Define which of the identified resource above can be protected by authorization on a higher level (like for example a SSO server) - Define the resource that needs to have authorization defined within the workflow engine:

4.2.2 Life cycle and rolls for authorization

- Define where the authorization, that need to be defined in the workflowengine, can be set in the life cycle of a workflow: - Implementation phase: Groups of services with the same roll (e.g. a group where every service can access the subscription with a defined prefix, like payment-): Can be set in the process model, needs to be set before deployment - execution phase: UI were an administrator can set fain grained authorization, can be set and managed after deployment as wel

4.3 Implementation of design

5 Discussion

Text des Ausblicks - sofern dies in der Arbeit gewünscht ist... Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

5.1 Evaluate the performance of the proposed design

- Using the authorization is there any loss of performance. A load test can be preformed to measure the performance with and without implementation

5.2 Evaluate the mitigation of the identified security vulnerabilities

- Argue why certain identified attack vectors are mitigated by the implemented design - Identify what might be still weak points - Complexity of maintaining the authorization

6 Conclusion

- Summarize the findings from the discussion - Describes further possibilities for research and an outlook for implementation in the industry

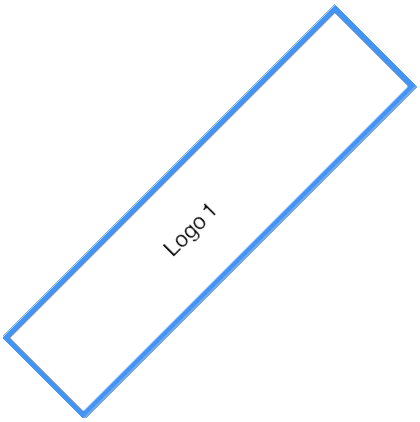

Figure 1: Beispiel einer Bildbeschreibung[1]

Figure 2: Beschreibung

Abbildung 2 [S.6]

Überschrift 1	Überschrift 2
Info 1	Info 2
Info 3	Info 4
Info in einer Zelle	

```
<dataConfig>
  <dataSource type="JdbcDataSource"
              driver="com.mysql.jdbc.Driver"
              url="jdbc:mysql://localhost/bms_db"
              user="root"
              password=""/>
  <document>
    <entity name="id"
        query="select id, htmlBody, sentDate, sentFrom, subject, textBody
        from mail">
    <field column="id" name="id"/>
    <field column="htmlBody" name="text"/>
    <field column="sentDate" name="sentDate"/>
    <field column="sentFrom" name="sentFrom"/>
```

[1]Bildquelle: Beispiel einer Bildquelle

```
15      <field column="subject"  name="subject"/>
16      <field column="textBody" name="text"/>
17      </entity>
18    </document>
19 </dataConfig>
```

Listing 1: Die Datei `data-config.xml` dient als Beispiel für XML Quellcode

```
1  /* generate TagCloud */
2  Cloud cloud = new Cloud();
3  cloud.setMaxWeight(_maxSizeOfText);
4  cloud.setMinWeight(_minSizeOfText);
5  cloud.setTagCase(Case.LOWER);
6
7  /* evaluate context and find additional stopwords */
8  String query = getContextQuery(_context);
9  List<String> contextStoplist = new ArrayList<String>();
10 contextStoplist = getStopwordsFromDB(query);
11
12 /* append context stoplist */
13 while(contextStoplist != null && !contextStoplist.isEmpty())
14   _stoplist.add(contextStoplist.remove(0));
15
16 /* add cloud filters */
17 if (_stoplist != null) {
18   DictionaryFilter df = new DictionaryFilter(_stoplist);
19   cloud.addInputFilter(df);
20 }
21 /* remove empty tags */
22 NonNullFilter<Tag> nnf = new NonNullFilter<Tag>();
23 cloud.addInputFilter(nnf);
24
25 /* set minimum tag length */
26 MinLengthFilter mlf = new MinLengthFilter(_minTagLength);
27 cloud.addInputFilter(mlf);
28
29 /* add taglist to tagcloud */
30 cloud.addText(_taglist);
31
32 /* set number of shown tags */
33 cloud.setMaxTagsToDisplay(_tagsToDisplay);
```

Listing 2: Das Listing zeigt Java Quellcode

Die Zuordnung aller möglichen Werte, welche eine Zufallsvariable annehmen kann nennt man *Verteilungsfunktion* von X.

Die Funktion F: $\mathbb{R} \rightarrow [0,1]$ mit $F(t) = P(X \leq t)$ heißt Verteilungsfunk-

tion von X.[2]

Für eine stetige Zufallsvariable $X : \Omega \to \mathbb{R}$ heißt eine integrierbare, nichtnegative reelle Funktion $w : \mathbb{R} \to \mathbb{R}$ mit $F(x) = P(X \leq x) = \int_{-\infty}^{x} w(t)dt$ die *Dichte* oder *Wahrscheinlichkeitsdichte* der Zufallsvariablen X.[3]

[2]Mustermann, vgl. [Mus09] [S.55]
[3]Mustermann, vgl. [Mus05] [S.56]

Literaturverzeichnis

[Mus05] Musterfrau, Maxi: *Ein weiteres Beispielbuch*. `http://www.example.com`. Version: 08 2005

[Mus09] Mustermann, Max: *Ein Beispielbuch*. `http://www.example.com`. Version: 11 2009

Anhang

Der Anhang bestehend aus Bildern und Texten...

Figure 3: Abbildung im Anhang

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Eidesstattliche Erklärung

Eidesstattliche Erklärung zur <-Arbeit>

Ich versichere, die von mir vorgelegte Arbeit selbstständig verfasst zu haben. Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten oder nicht veröffentlichten Arbeiten anderer entnommen sind, habe ich als entnommen kenntlich gemacht. Sämtliche Quellen und Hilfsmittel, die ich für die Arbeit benutzt habe, sind angegeben. Die Arbeit hat mit gleichem Inhalt bzw. in wesentlichen Teilen noch keiner anderen Prüfungsbehörde vorgelegen.

$Unterschrift$: $Ort, Datum$: