FH | JOANNEUM
University of Applied Sciences

Best Practice Authentication and Authorization

in distributed Business Scenarios with OpenID Connect and OAuth 2.0

Master Thesis
submitted in conformity with the requirements for the degree of
Master of Science in Engineering (MSc)
Master's degree programme **IT & Mobile Security**

FH JOANNEUM (University of Applied Sciences), Kapfenberg

Supervisor: Elmar Krainz, FH JOANNEUM Kapfenberg

submitted by: Cornelia Rauch
personnel identifier: 1610419026

June 2016 <edit date!>

Assignment for the master thesis of
<your name>
Matr. no. 1400000000

Subject:
"<Title of Your Thesis>"

Abstract

Write your abstract here.

<place>, <date>

Academic adviser:
<firstname lastname>

<your name>

Formal declaration

I hereby declare that the present master's thesis was composed by myself and that the work contained herein is my own. I also confirm that I have only used the specified resources. All formulations and concepts taken verbatim or in substance from printed or unprinted material or from the Internet have been cited according to the rules of good scientific practice and indicated by footnotes or other exact references to the original source.

The present thesis has not been submitted to another university for the award of an academic degree in this form. This thesis has been submitted in printed and electronic form. I hereby confirm that the content of the digital version is the same as in the printed version.

I understand that the provision of incorrect information may have legal consequences.

Kapfenberg, 28.09.2018

Cornelia Rauch
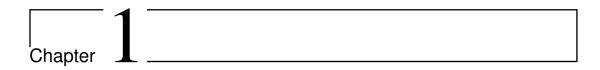
Acknowledgement

Thanks to . . .

Contents

List of Tables

List of Figures

Chapter 1

Introduction

This template shall provide some considerations and text examples for your Master's thesis.

Background. Describe the background, the prerequisites for your work ...

Objective. The aim of this master's thesis is ...

Terms and definitions. Technical terms ... abbreviations are summarised at the end (in "Acronyms"), e.g. application binary interface (ABI) or man-in-the-middle (MITM). If ABI is referenced again, only the acronym is printed (as hyperlink though).

Corre et al. (2017), *Why can't users choose their identity provider* (ibid.) Boyed (2012), Lynch (2011), Todorov (2007), Procházka, Kouřil, and Matyska (2010), Tomkins (2009), Corre et al. (2017), Neumann (2013), Foundation (2018), Tome et al. (2011), Grassi, Garcia, and L. (2017), Brooks et al. (2017), Dingle and Bary (2015), Xu (2015), Dasgupta, Arunava, and Abhijit (2017)

Harvard citation style is implemented in this template: Batina et al. (2012), Fernàndez-Mir et al. (2012), Li et al. (2008)

1.1   Some LATEX Basics

This section is a *really very short* summary of LATEX features. Do not forget to remove it after finishing your thesis.

Here you have an included graphic (figure 1.1).

Figure 1.1: Train engine in Kapfenberg

Code listings require the *listings* package which, in turn, requires some settings[1]; see command \lstset{} in preamble of this template. Additionally the package *courier* should be used because the defaults do not provide for proper syntax highlighting.

```
1 void main(int argc, char *argv[])
2 {
3   printf("Hello world!");
4 }
```

Listing 1.1: Main programme

In order to see what's possible – here are two fancy tables: 1.1 and 1.2.

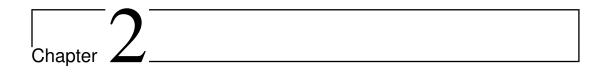| Version	Description	Author(s)	Date
1.0	Initial	Ohrt	July 15, 2014
1.1	Filled section "Open Issues"	Ohrt	July 16, 2014
1.2	Added section "Restrictions"	Ohrt	September 15, 2014

Table 1.1: Olive green heading

View also the preamble of this file for explanations.

---

[1]...because the defaults do not fit all purposes

Error	Solution
Java.lang.OutOfMemoryError: PermGen space *(32-/64-bit issue)*	-XX:MaxPermSize=1024M
Error occurred during initialization of VM *or* Could not reserve enough space for object heap	increase or remove -Xms value e.g. -Xms128m -Xmx512m (Eclipse default: -Xms40m -Xmx512m)

Table 1.2: A grey table

Here is a reference to listing 1.1.

Chapter 2

Authentication and Authorization

"Cloud-based services, the social Web, and rapidly expanding mobile platforms will depend on identity management to provide a seamless user experience." Corre et al. (2017).

Modern Devices are changing our every day life. They change the way how we access information, interact with each other and share content. With this change of user behavior also the way we think of authentication and authorization methods has to adjust. Users are find themselves struggling using multiple devices, accounts and services. The users burden of this site-by-site account management is putting security at risk. The goal of new authentication and authorization solutions is to help the user managing his accounts by providing single-sign-on, based on an exchange of identity-related assertion across security domains in a scalable way Corre et al. (ibid.).

2.1 Authentication

"Digital identity is the unique representation of a subject engaged in an online transaction. The process used to verify a subject's association with their real-world identity is called identity proofing" Grassi, Garcia, and L. (2017)

A digital identity as explained above is the result of what we call the authentication process. It is a way of identifying the user as whom he claims to be. A very typical authentication process is performed by asking the user for its username and password. If the user provides a correct user name and password, an application assumes the user is indeed the owner of the account he wants to log on Boyed (2012).

The evidence provided by the user in the authentication process is called credentials. Most of the time as mentioned above credentials are provided in the form of username and password. However credentials also may take other forms like PIN's, key cards, eye scanners and so on Todorov (2007).

Credentials, which prove the identity of an entity and are used as authenticators in authentication systems, are called factors. Grassi, Garcia, and L. (2017) categorize following types of factors:

- Something the user knows - Cognitive information the user has to remember. Examples include passwords, PIN, answers to secret questions.

- What the user has - something the user owns. Examples include a security token, driving license, one-time password (OTP). What the user is - biometric information of the user. Examples include fingerprint, voice, and face.

- What the user is - biometric information of the user. Examples include fingerprint, voice, and face.

Other types of information which are not considere athentication factors but can be used to enrich the authentication proceess according to Dasgupta, Arunava, and Abhijit (2017) are:

- Where the user is - the location was the user can be used as a fourth factor of authentication of a user. Examples include GPS, IP addresses.

- When the user logs on - Time can also be extracted as a separate factor. Verification of employee's identification in different office hours can prevent many kinds of grave data breaches. The time factor can easily prevent online banking fraud events to a great extent.

To secure a solution properly it should at least use two factors of the three listed above.To make use of more then one factor of a pool of potential credentials to verify the identity of a user is referred to as Multi-factor Authentication (MFA). The goal of multi-factor authentication is it to provide a layered defense and make it harder for unauthorized individuals to gain access. If one of the factors breaks, the service can still rely on the non-compromised authentication factors Dasgupta, Arunava, and Abhijit (ibid.).
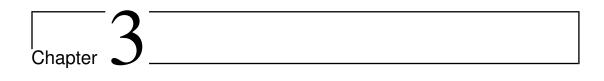
When designing an authentication process with using multiple factors the designers of the process should be very aware of the type of application and the information that has to be secured. For example a solution for an international bank should have different standards then an app for a making an grocery list. On the one hand, difficult and

complex authentication processes for trivial applications might scare away users. On the other hand simple methods for applications protecting sensitive data might drive users away as well Grassi, Garcia, and L. (2017) .

The factors are an important part of the authentication process which result should be an authenticated user. Todorov (2007) identifies three typical components that are part of the authentication:

- The Supplicant, which is the party that provides the evidence to prove the identity of a user or client. The result of the authentication process should be the authenticated user or client.

- The Authenticator, also called server, is responsible for ascertaining the user identity. Once the identity is proved, the authenticator can authorize or audit the user access to resources.

- Security authority database, which is storage or mechanism to check the user's credentials. The storage can be represented by as much as a flat file, a server on the network providing centralized user authentication or a distributed authentication server.

It is vital that all the components of a user authentication system can communicate independently of each other. Whether or not all communication channels are used depends on the authentication mechanism and the model of trust that it implements. For example, the Kerberos authentication protocol does not feature direct communication between the authenticator and security server Todorov, 2007.

2.2 Authorization

Conclusion and Outlook

Your text here . . .

Acronyms

ABI   application binary interface

ACL   access control list

GUI   graphical user interface

KISS   keep it small and simple

MITM   man-in-the-middle

OS   operating system

UART   universal asynchronous receiver/transmitter

UID   unique identifier

Bibliography

Batina, Lejla, Stefaan Seys, Dave Singelée, and Ingrid Verbauwhede (2012). "Hierarchical ECC-Based RFID Authentication Protocol". In: *Proceedings of the 7th International Conference on RFID Security and Privacy*. RFIDSec'11. Amherst, MA: Springer-Verlag, pp. 183–201. ISBN: 978-3-642-25285-3. DOI: 10.1007/978-3-642-25286-0_12. Available from: <http://dx.doi.org.acm.perm.fh-joanneum.at/10.1007/978-3-642-25286-0_12>.

Boyed, Ryan (2012). *Getting Started with OAuth 2.0 - Programming Clients for Secure Web API Authorization and Authentication*. O'Reilly Media.

Brooks, Sean, Michael Garcia, Naomi Lefkovitz, Suzanne Lightman, and Ellen Nadeau (Jan. 2017). *An Introduction to Privacy Engineering and Risk Management in Federal Systems*. NISTR 8062. NIST (National Institute of Standards and Technology).

Corre, Kevin, Oliver Barais, Gerson Sunyé, Frey Vincent, and Jean-Michel Crom (2017). *Why can't users choose their identity provider*. Available from: <https://petsymposium.org/2017/papers/issue3/paper18-2017-3-source.pdf> [May 2018].

Dasgupta, Dipankar, Roy Arunava, and Nag Abhijit (2017). *Advances in User Authentication*. Springer International Publishing AG. ISBN: 978-3-319-58808-7.

Dingle, P. and T. Bary (Sept. 2015). *OpenID AccountChooser Basic API Profile 1.0*. draft-accountchooser-basic-profile-07. Google Inc.

Fernàndez-Mir, Albert, Rolando Trujillo-Rasua, Jordi Castellà-Roca, and Josep Domingo-Ferrer (2012). "A Scalable RFID Authentication Protocol Supporting Ownership Transfer and Controlled Delegation". In: *Proceedings of the 7th International Conference on RFID Security and Privacy*. RFIDSec'11. Amherst, MA: Springer-Verlag, pp. 147–162. ISBN: 978-3-642-25285-3. DOI: 10.1007/978-3-642-25286-0_10. Available from: <http://dx.doi.org/10.1007/978-3-642-25286-0_10>.

Foundation, OpenID (2018). *Account Cooser - Developer's Guide*. Available from: <http://www.accountchooser.net/developers> [June 2018].

Grassi, Paul A., Michael E. Garcia, and Fenton James L. (July 2017). *Digital Identity Guidelines*. Special Publication 800-63-3. NIST (National Institute of Standards and Technology).

Li, Yingjiu, Robert H. Deng, Junzuo Lai, and Changshe Ma (Dec. 2008). "On Two RFID Privacy Notions and Their Relations". In: *ACM Trans. Inf. Syst. Secur.* 14.4, 30:1–30:23. ISSN: 1094-9224. DOI: 10.1145/2043628.2043631. Available from: <http://doi.acm.org.acm.perm.fh-joanneum.at/10.1145/2043628.2043631>.

Lynch, Lucy (Sept. 2011). "Inside the Identity Game". In: *IEEE Internet Computing* 15.5, pp. 78–82.

Neumann, Peter G. (2013). *Principled Assuredly Trustworthy Composable Architectures*. Available from: <http://www.csl.sri.com/users/neumann/chats4.pdf> [May 2018].

Procházka, Michal, Daniel Kouřil, and Luděk Matyska (May 2010). "User centric authentication for web applications". In: *Collaborative Technologies and Systems (CTS)*. Chicago, IL, USA: IEEE. ISBN: 978-1-4244-6622-1.

Todorov, Dobromir (2007). *Mechanics of User Identification and Authentication - Fundamentals of Identity Managment*. Auerbach Publications. ISBN: 978-1-4200-5219-0.

Tome, Basheer, John Bradley, Nat Sakimura, Long Kevin, Janrain P. Dingle, Axel Nennker, Andrew Csinger, Eric Sachs, Chuck Sievert, Wei Tu, Andrew Daheley, and Chris Messina (2011). *Account Chooser Working Group Chater proposal*. Available from: <http://ac.openid.net/wgproposal> [June 2018].

Tomkins, Benjamin (2009). "Dealing With Password Fatigue". In: *Forbes*.

Xu, Fangyuan (2015). *Security and Privacy Concern for Single Sign-on Protocols*. Tech. rep. Tufts University.