Lab: Evaluating and designing authentication

Daniel Bosk

5th November 2020

Abstract

Summary: ...
Intended learning outcomes: After this module you should be able

- to *evaluate* authentication methods from a usability, security and privacy perspective.
- to *design* authentication suitable for a particular use-case.

Reading: ...

1 Introduction

Authentication is a vital part of most services. The still most dominant authentication method is password based. Passwords have their place in security, but they are over-used. A person should need one or two passwords, not one or two *hundred* passwords. Password reuse is very bad for security, so there must be one strong, unique password for every service the user is interested in. However, the need to keep track of hundreds of strong, unique passwords has developed the need for password managers. Since no user remember any of these two hundred passwords, they could just as well be cryptographic keys, which would allow for more secure authentication methods.

When users must remember their credentials they tent to converge to using the same credentials for all services. As pointed out above, such password reuse is bad. But there is also a privacy issue. Such systems use identity-based authentication. Usually the email address is used as the identifier, and all of a user's actions can be attributed to this identity. One issue with this practice of authentication is that it in many cases violates the principle of data minimization[1]. For example, most services use identity-based authentication although it would do fine with another (less informative) attribute.

In this lab we are interested in exploring this topic from a security, privacy and usability perspective.

[1] Data minimization requires that one uses only the bare minimum data that is absolutely needed. This is one of the guiding principles of the EU General Data Protection Regulation (GDPR).

1.1 Organization

This lab is divided into two parts: evaluating authentication and designing authentication. Each part is then divided over several sessions. Work is done in groups. During the session the groups work on a problem, present and discuss the results so that every group can learn the from the others.

2 Assignment

Design evaluation criteria During the first session, design evaluation criteria in groups. Remember to capture all perspectives: security, privacy and usability. Present each group's criteria to the class.

Evaluate services For the second session, evaluate a few services (per group). Pick one good example and one bad example to present to the class. During the session, after the presentations, we will synthesize the results (lessons learned).

Designing authentication During the third (and last) session, we will design proper authentication for some services. Each group chooses a target service. Then the groups work on designing the required authentication. Finally, the results are presented for the whole class.

3 Examination

You must participate actively in the group work.