Seminar: Password-composition policies

Designing a secure and usable password policy

Daniel Bosk Lennart Franked

13th March 2019

Abstract

The part of security that perhaps most affect the users is user authentication. The predominant mechanism to achieve this is passwords. Thus, design decisions in this are are important for both the usability and the security of the system.

During this seminar you will train your ability to comprehend and apply research results in the area of security and usable security. You will combine results from different areas to analyse different aspects and to evaluate the security and usability of different designs.

We need Chap. 2 'Usability and Psychology' of [And08]. Further, we need a basic understanding of information theory [Sha48], for this you are recommended to read 'Chapter 6: Shannon entropy' [Uel]. Finally, we will discuss the results of 'Of passwords and people: Measuring the effect of password-composition policies' [Kom+11], 'Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms' [Kel+12] and 'Can long passwords be secure and usable?' [Sha+14].

1 Introduction

User authentication is present in most systems. There is one security mechanism which can be found almost everywhere, which is intended to solve this problem: passwords. From a usability perspective, passwords generally perform very poorly. This will, of course, also yield security implications.

Usually, in systems using passwords, the password selection of the users are governed by some password-composition policy to help (or force) the users to select strong passwords. Thus, how these policies are designed has great impact on the resulting passwords the users choose. This impact is not always what is expected, in fact, sometimes a password policy can result in weaker passwords.

There is no indication that passwords will be replaced any time soon, so if we must use passwords, we would better use them well. This is the goal of this assignment.

1.1 Aim

The aim of this seminar is to evaluate password-composition policies. We want to find out how different policies affect users' password choices and how we can

use this knowledge for designing better policies. During this seminar you should show that you are able to:

- *comprehend and apply* research results in the area of security and usable security.
- *combine* results from different areas to analyse different aspects.
- *evaluate* the security and usability of different designs.

1.2 Outline

The next section covers what you must read before you understand this assignment and how to do the work. Section 3 covers the work to be done, i.e. how you should learn this. Section 4 covers how it will be examined, i.e. how you show that you have fulfilled the intended learning outcomes given above.

2 Theory

First you must read Chap. 2 'Usability and Psychology' in [And08]. Further, you need a basic understanding of information theory [Sha48] for this assignment, for this you are recommended to read 'Chapter 6: Shannon entropy' [Uel].

Then, to participate in this seminar you must have read the papers 'Of passwords and people: Measuring the effect of password-composition policies' [Kom+11], 'Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms' [Kel+12] and 'Can long passwords be secure and usable?' [Sha+14]. In these papers the authors have studied how different password-composition policies affects users' choice of passwords.

3 Assignment

You should read the material. While reading, write down your thoughts. Let these questions guide your reading:

- What are the main results of the research paper?
- How did they conclude them? I.e., what is the research method?

After reading and reflection, think about the following questions:

- How do these results compare to your experience of what is used in practice?
- What is your strategy for remembering passwords?
- How do you react to different password policies?
- What would be a good password-composition policy? Why would that be good?
- How much information do you think a password policy reveals about the passwords? Is there any way we can estimate that?

- Is it fine to write down passwords or not?
- In the situation where you have forgotten you password, what kind of password recovery schemes have you encountered?
- What is your reaction towards the different password recovery schemes?
- How should password recovery be dealt with in a secure way?
- What problems do you perceive with authentication of users in general?
- In which situations are passwords suitable and in which are they not?

Finally, look at the University's password-composition policy, what are the strengths and weaknesses of this policy?

During the seminar we will first discuss the papers and your reflections from reading them. After that we will work in groups of 3–4 students. We will first discuss how we can estimate how much a password policy reveals about the passwords, i.e. how the password policy can make guessing easier. Then every group will design a password-composition policy, drawing from both the papers and the discussions. Finally, every group will present their policy and analysis, then we will evaluate it together.

4 Examination

To pass this assignment you need to come prepared and actively participate in the seminar.

Acknowledgements

References

[And08] Ross J. Anderson. *Security Engineering. A guide to building dependable distributed systems*. 2nd ed. Indianapolis, IN: Wiley, 2008. ISBN: 978-0-470-06852-6 (hbk.) URL: `http://www.cl.cam.ac.uk/~rja14/book.html`.

[Kel+12] Patrick Gage Kelley, Saranga Komanduri, Michelle L Mazurek, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor and Julio Lopez. 'Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms'. In: *Security and Privacy (SP), 2012 IEEE Symposium on*. IEEE. 2012, pp. 523–537. URL: `http://ieeexplore.ieee.org/abstract/document/6234434/`.

[Kom+11] Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L. Mazurek, Lujo Bauer, Christin Nicolas, Lorrie Faith Cranor and Serge Egelman. 'Of passwords and people: Measuring the effect of password-composition policies'. In: *CHI*. 2011. URL: http://cups.cs.cmu.edu/rshay/pubs/passwords_and_people2011.pdf.

[Sha+14] Richard Shay, Saranga Komanduri, Adam L Durity, Phillip Seyoung Huh, Michelle L Mazurek, Sean M Segreti, Blase Ur, Lujo Bauer, Nicolas Christin and Lorrie Faith Cranor. 'Can long passwords be secure and usable?' In: *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*. ACM. 2014, pp. 2927–2936. URL: http://lorrie.cranor.org/pubs/longpass-chi2014.pdf.

[Sha48] C. E. Shannon. 'A Mathematical Theory of Communication'. In: *The Bell System Technical Journal* 27 (July 1948), pp. 379–423, 623–656.

[Uel] Daniel Ueltschi. 'Chapter 6: Shannon entropy'. URL: http://www.ueltschi.org/teaching/chapShannon.pdf.