

# Problem Description

## Human Computable Passwords - design and analysis.

Managing passwords is a significant problem for most people in the modern world. This project will be based around the paper "Human Computable Passwords" by Blocki et al. [1], proposing a method for humans to be able to re-compute passwords from public and reliable storage. Passwords are calculated using a memorized mapping from objects, typically letters or pictures, to digits; the characters of the passwords are then calculated in the users head, using a human computable function.

The main objectives of the project can be summarized as the following:

- Understand and compare the "Human Computable Passwords" scheme with other related password management schemes.
- Design and implement a password management scheme applying the ideas of the scheme.
- Analyze if the construction could be utilized to provide secure password management in practical situations.
- Validate if the scheme is feasible to use, comparing the user efforts required to the security rewards.

[1] J. Blocki, M. Blum, and A. Datta, "Human Computable Passwords," CoRR, vol. abs/1404.0, 2014.

**Assignment given:** 12 January, 2015

**Student:** Anders Kofoed

**Professor:** Colin Boyd, ITEM



## Abstract



## Preface



# Contents

<b>List of Figures</b>	<b>ix</b>
<b>List of Tables</b>	<b>xi</b>
<b>List of Algorithms</b>	<b>xiii</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Motivation . . . . .	1
1.2 Related Work . . . . .	1
1.3 Scope and Objectives . . . . .	1
1.4 Method . . . . .	1
1.4.1 Development . . . . .	1
1.4.2 Experiments . . . . .	1
1.5 Outline . . . . .	1
<b>2 Background</b>	<b>3</b>
2.1 Passwords . . . . .	3
2.1.1 Password strength . . . . .	4
2.1.2 Attacks . . . . .	5
2.1.3 Password Storage . . . . .	5
2.1.4 Alternative authentication methods . . . . .	5
2.2 Human Behavior . . . . .	5
2.3 Password Management . . . . .	5
2.4 Usability and Security Challenges . . . . .	5
2.5 Mnemonic Techniques . . . . .	5
2.6 Browser Extensions . . . . .	5
2.7 Usability Model . . . . .	5
2.8 Security Model . . . . .	5
<b>References</b>	<b>7</b>





# List of Figures



# List of Tables



# List of Algorithms













# Chapter 1

## Introduction

### 1.1 Motivation

[2]

### 1.2 Related Work

### 1.3 Scope and Objectives

### 1.4 Method

#### 1.4.1 Development

#### 1.4.2 Experiments

### 1.5 Outline



# Chapter 2

## Background

### 2.1 Passwords

Passwords are the common way of authenticating users upon access to sites on the Internet, the idea is that only the user and the target service knows the password, and the user have to provide the correct password before access are granted. Passwords are a much discussed theme and claiming that passwords are usually not used in the correct manner is not an overreaction. The main problem seems to be the fact that good passwords and the human memory does not go well together. For passwords to be sufficient as authentication each user has to be forced into using long complex password, or even use one generated for them, with the problem being that it is easily forgotten. Further more, if a user was able to memorize *one* "good" password, he will probably use this for all of his accounts, so that if one of the services is compromised and user information leaked, all his accounts may be compromised. With all of this in mind it is easy to say that everybody should use complex, unique passwords for each account, but in practice this is not feasible. Florêncio and Herley [3] conducted a large scale study of passwords habits in 2007, revealing that a user on average has 25 different accounts protected by passwords. On average these sites are protected by about 7 distinct password, where 5 of them are rapidly re-used.

Password authentication requires the authenticating server to store something related to the password, if this is stolen the password will in most cases be compromised as well, even if the server did not store the clear text password, attackers will, in most cases, be able to retrieve the password eventually. After obtaining the username and password for one service the attacker would try this user data on other services and compromise these as well.

If a user was to have different passwords for each site, these might still easily be compromised. Ives et al. [4] discuss this "domino effect", where intrusion to one domain can compromise several others, if users have re-used passwords. A normal user will typically try to log in by trial-and-error [5], if the first password does not

work, the user will try with another of his passwords. This way many passwords might be lost through phishing attacks where a user is tricked into trying to log in to a fake site. It is thus clear that some kind of system is needed to allow a human user to manage strong passwords. The best case would be if each user, for each of his 25 accounts had a unique password of satisfying strength, this is of course not possible.

### 2.1.1 Password strength

How to measure the strength of passwords is a well known and discussed problem, but the general idea is that password strength is related to how strong a password is against brute force attacks. Length and complexity is the most thought of parameters to measure such strength. A perfect password would thus be one as long as allowed by the system consisting of random characters from all possible characters, this one would also be changed frequently. All these characteristics despite how the human brain works. Yan et al. [6] investigate the trade off between security of passwords versus memorability allowing humans to remember them. An important point regarding this trade-off is that most sites applying advice and policies on how to create strong passwords, does not take into account if the advice passwords are hard or easy to remember. The point being that there is no point in having a strong password if the user is going to forget it. They suggest that passwords should appear random but be constructed using a mnemonic structure such as passphrases. The idea here is to generate a random looking password by memorizing a familiar sentence and using the first letters of each word as the password. Florêncio et al. [7] investigate another matter; do strong passwords accomplish anything? The point being that no matter how long and complex password users choose they are still subject to the most dangerous and common threats (phishing, keylogging or access attacks), as discussed in the previous section. The reason for enforcing strong passwords seems to be to protect against bulk guessing attacks, against other attacks, typically offline attacks, shorter passwords is usually sufficient.

**Password strength meters** are a common way used by many sites on the Internet to aid their users when selecting passwords

The conclusion on what "good" passwords are, is clearly not an easy question to answer, but the one thing agreed upon seems to be that re-use of passwords are the biggest threat. It is a fact that the human brain is not capable of remembering different passwords for each account on the Internet, thus the need for an aiding application such as the one discussed in this project.

Miller [8] showed that the human brain cannot store more than  $7 \pm 2$  chunks of information in immediate memory.

### **2.1.2 Attacks**

### **2.1.3 Password Storage**

active and passive attacks

### **2.1.4 Alternative authentication methods**

## **2.2 Human Behavior**

"Good passwords" as discussed in 2.1.1 does not go well with the human memory. The first limitation which will be an important property later are the limitation to how much data we can store in immediate memory, this limit was showed to be 7 chunks of data at once [8]. This data can not be from a random selection which is what a good password requires.

## **2.3 Password Management**

## **2.4 Usability and Security Challenges**

## **2.5 Mnemonic Techniques**

## **2.6 Browser Extensions**

## **2.7 Usability Model**

## **2.8 Security Model**





# References

- [1] J. Blocki, M. Blum, and A. Datta, “Human Computable Passwords,” *CoRR*, vol. abs/1404.0, 2014.
- [2] J. Blocki, *Usable Human Authentication: A Quantitative Treatment*. PhD thesis, School of Computer Science, Carnegie Mellon University, 2014.
- [3] D. A. F. Florêncio and C. Herley, “A large-scale study of web password habits,” in *Proceedings of the 16th International Conference on World Wide Web, {WWW} 2007, Banff, Alberta, Canada, May 8-12, 2007* (C. L. Williamson, M. E. Zurko, P. F. Patel-Schneider, and P. J. Shenoy, eds.), pp. 657–666, ACM, 2007.
- [4] B. Ives, K. R. Walsh, and H. Schneider, “The domino effect of password reuse,” *Commun. {ACM}*, vol. 47, no. 4, pp. 75–78, 2004.
- [5] T. Acar, M. Belenkiy, and A. Küpçü, “Single password authentication,” *Computer Networks*, vol. 57, no. 13, pp. 2597–2614, 2013.
- [6] J. Yan, A. Blackwell, R. Anderson, and A. Grant, “The memorability and security of passwords: some empirical results,” *Technical Report-University Of Cambridge Computer Laboratory*, p. 1, 2000.
- [7] D. Florêncio, C. Herley, and B. Coskun, “Do Strong Web Passwords Accomplish Anything?,” in *2nd {USENIX} Workshop on Hot Topics in Security, HotSec’07, Boston, MA, USA, August 7, 2007*, {USENIX} Association, 2007.
- [8] G. A. Miller, “The magical number seven, plus or minus two: some limits on our capacity for processing information.,” *Psychological review*, vol. 63, no. 2, p. 81, 1956.