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 goal of the project is to determine if the scheme is usable and if it could be used to greater effect in real scenarios. The project will include an implementation of the password management scheme, testing the usability of it and assessing the validity through experiments. 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

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 Authentication

2.1.1 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.

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.

Miller [3] showed that the human brain cannot store more than 7 ± 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

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] 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.