Hochschule Wismar
University of Applied Sciences
Technology, Business and Design
Faculty of Engineering, Area E&I

Master-Thesis

Security Evaluation of Multi-Factor Authentication in Comparison with the Web Authentication API

Submitted by: July 7, 2019

from: Tim Brust
born 03/31/1995
in Hamburg, Germany

Tutor: Prof. Dr.-Ing. habil. Andreas Ahrens
Second tutor: Prof. Dr. rer. nat. Nils Gruschka

Contents

1 Introduction

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special contents, but the length of words should match the language.

2 Two-factor

Wording: Two-Factor Auth vs Two-Factor Verification

2.1 OTP

2.1.1 HMAC

Variants

1. TOTP
2. HOTP

pros

1. Collisions in MD5 or SHA1 are no problem, already stated/analyzed in the RFC

cons

1. synchronization
2. invalidation
3. nobody knows how the algorithm is implemented (RFC = no standard)
4. Differences (e.g. Steam - only 5 digits, limited Alphabet)

2.2 Transportation

2.2.1 introduction

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special contents, but the length of words should match the language.

2.2.2 SMS

pros

1. Every mobile is capable of receiving SMS (from old Nokia’s ranging to new iPhone Xs)
2. No apps required, works everywhere (worldwide)
3. easy to use

cons

1. Relies on the SS7 security, which is broken
2. SMS eveasdropping is very easy
3. Forward phishing attacks are possible, too
4. Mobile phone trojans can intercept all incoming SMS
5. costs millions for bigger companies (each SMS is charged)
6. Roaming costs
7. Delivery time
8. Routing mainly unknown

9. Third party companies send the SMS - countries very it's cheap (Africa, ...) are used - how are those data protection laws

2.2.3 App

pros

1. Works offline
2. cheaper

cons

1. Secret can be phished while setup (either on phone or computer)
2. Trusted apps? OSS?
3. Vulnerabilities –> e.g. Authy

2.2.4 E-Mail

pros

cons

3 WebAuth

3.0.1 Questions - To resarch

1. How does the Authenticator talk to the browser
2. How does the Authenticator store the keys

3.0.2 Problems

- Identify theft if not as 2FA and key is lost (e.g. Yubikey without fingerprint sensor)

List of Figures

Listings

List of Tables

Declaration of Academic Integrity

Hereby, I declare that I have composed the presented paper independently on my own and without any other resources than the ones indicated. All thoughts taken directly or indirectly from external sources are properly denoted as such.

Hamburg, July 7, 2019

Tim Brust