University of Cambridge

Master's Thesis

User Authentication for Pico

Author:
Cristian M. Toader

Supervisor:
Doctor Frank Stajano

A thesis submitted in fulfilment of the requirements for the degree of 'Master of Philosophy'

in the

Computer Security Group
Computing Department

April 2014

Abstract

The abstract needs to be written at the end.

Acknowledgements

The acknowledgements and the people to thank go here, don't forget to include your project advisor…

Contents

List of Figures

List of Tables

Abbreviations

LAH	**L**ist **A**bbreviations **H**ere

Symbols

a	distance	m
P	power	W (Js^{-1})
ω	angular frequency	rads^{-1}

Chapter 1

Introduction

Chapter 2

Literature Review

2.1 Pico: no more passwords!

In the paper “Pico: no more passwords!” [?], Frank Stajano describes an alternative design to passwords. It is based on a hardware token called “Pico”, which replaces all instances where passwords could be used. The reason for designing this alternative authentication mechanism is that passwords are not as usable and secure as they used to be.

Computation power has increased significantly since passwords became popular. This makes passwords easier to break using either brute-force or dictionary attacks. As a result, restrictions were imposed to make passwords stronger, such as requiring at least an upper case letter or a numeric character. Furthermore, in order to reduce the threat of dictionary attacks, authentications systems recommend, if not enforce, passwords to be harder to guess, meaning they should not contain dictionary words. Furthermore, after imposing all these restrictions, it is also recommended to change them regularly. This rule is sometimes enforced in the case of larger companies.

The changes previously described are reasonable from a security point of view, but completely lack user focus. With an increasing number accounts requiring authentication, whether web based or local, passwords become increasingly difficult to remember. Reusing them is not recommended, as compromising one account would lead to multi-account exposure. This leads to having users remember a large number of unique passwords, which is not realistic in practice. Therefore security compromises are made by the user such as writing passwords down, or reusing them, therefore breaking the theoretical security of the password.

The token based alternative designed by Frank Stajano improves the security offered by passwords. It transforms something you know in something you have. This makes the authentication memory effortless. Unlike other hardware tokens, Pico is theft resistant thanks to small devices called Picosiblings. The Pico uses wireless communication with the Picosiblings and becomes unlocked only in their presence. It is also responsible for generating authentication credentials therefore ensuring that they are not weak or reused.

The Pico device uses for authentication purposes two buttons and a camera. The buttons are used for pairing and creating a new account. The authentication process is multi channel. It relies on a visual code created by the app in order to transmit its public key and unique id. The rest of the authentication process is performed over radio communication via nonce challenges to prove that the other participant has the private key corresponding to the public. The authentication protocol is described in detail in paper [**?**].

Authentication between the Pico device and its owner is performed using small devices called Picosiblings. These are meant to be embedded in everyday items that the owner carries around, such as earrings, rings, keys, chains, etc. Communication with the Picosiblings uses short range radio. The initialisation protocol for Picosiblings is called the resurecting ducklings [**?**]. Further enquiries are performed using picosibling pings once every predefined time interval. This tests whether the picosiblings are within the range of the Pico.

The communication between Pico and its Picosiblings is meant to reconstruct the Pico master key. Each Picosibling has a k-out-of-n secret used by the Pico device to reconstruct its master key. Pico tracks each Picosibling based on a timer. If the timer expires and the Picosibling is unable to generate a response, the secret is deleted.

There are two special shares with a longer time out period: a biometric authentication mechanism, and a remote server communication. These are used for special cases such as having your Picosiblings and Pico both stolen. The biometric authentication would only allow the new user to have limited access time, while the remote server communication can be used to lock Pico remotely.

2.2 Framework for evaluating web authentication schemes

In the paper "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes" [] the authors develop a framework for evaluating web based authentication mechanisms. The purpose of the framework is to identify authentication schemes which outperform passwords. The framework is intended to provide a benchmark for future web authentication proposals.

The framework focuses of three classes of properties which are abbreviated as UDS: usability, deployability, and security. Each class contains a set of properties, totalling a number of 25 benefits. A mechanism may either offer, quasi-offer, or not offer a property. Properties which are not applicable to a mechanism are marked as "offered" to simplify the framework.

Using the framework to evaluate 35 password replacement schemes shows that no scheme is dominant over passwords. According to the evaluation, passwords score perfectly in deployability. They score reasonably in terms of usability, excelling in properties such as: nothing-to-carry, efficient-to-use, and easy-recovery-from-loss. In terms of security however, passwords don't perform as well, only receiving points in resilience-to-theft (not applicable), no-trusted-third-party, requiring-explicit-consent, and unlinkable. The full list of properties and their description can be found within the paper itself.

Biometric mechanisms receive mixed scores on usability. None of them have the infrequent-errors property which is a precision problem related to false negatives. More importantly if the biometric data is exposed by malware for instance, the authentication mechanism may not be used by the user any more. They score poorly in deployability due to the additional hardware required. In terms of security they perform worse than passwords. Replay attacks can be used by an attacker using a recording of some sort in order to trick the sensor. They are not resilient to theft, since they require an additional device. The fact that they uniquely link the owner to the recording means that the owner may be linked back to the data, therefore not granting the "unlinkable" property.

The paper notes that the memory-effortless property versus nothing-to-carry is only achieved by biometric schemes. None of the mechanisms manage to fully achieve memory-effortless and be resilient-to-theft. This is due to the fact that most mechanisms replace something you know with something you have.

The authors do not produce aggregate scores or rankings. This is due to the fact that not all properties are equal in importance, but different properties would have different weights depending on the scheme's application domain.

Combining schemes is mentioned as a two factor arrangement. This would result in a mechanism which in terms of usability and deployability would only have the properties which are granted by both schemes. In security however it would have the properties of both mechanisms. As shown in the paper, according to [**?**] the presence of a two factor authentication would lead the user to creating weaker passwords.

Chapter 3

Main work todo

3.1 Main Section 1

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam ultricies lacinia euismod. Nam tempus risus in dolor rhoncus in interdum enim tincidunt. Donec vel nunc neque. In condimentum ullamcorper quam non consequat. Fusce sagittis tempor feugiat. Fusce magna erat, molestie eu convallis ut, tempus sed arcu. Quisque molestie, ante a tincidunt ullamcorper, sapien enim dignissim lacus, in semper nibh erat lobortis purus. Integer dapibus ligula ac risus convallis pellentesque.

3.1.1 Subsection 1

Nunc posuere quam at lectus tristique eu ultrices augue venenatis. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Aliquam erat volutpat. Vivamus sodales tortor eget quam adipiscing in vulputate ante ullamcorper. Sed eros ante, lacinia et sollicitudin et, aliquam sit amet augue. In hac habitasse platea dictumst.

3.1.2 Subsection 2

Morbi rutrum odio eget arcu adipiscing sodales. Aenean et purus a est pulvinar pellentesque. Cras in elit neque, quis varius elit. Phasellus fringilla, nibh eu tempus venenatis, dolor elit posuere quam, quis adipiscing urna leo nec orci. Sed nec nulla auctor odio aliquet consequat. Ut nec nulla in ante ullamcorper aliquam at sed dolor. Phasellus fermentum magna in augue gravida cursus. Cras sed pretium lorem. Pellentesque eget ornare odio. Proin accumsan, massa viverra cursus pharetra, ipsum nisi lobortis velit, a malesuada dolor lorem eu neque.

3.2 Main Section 2

Sed ullamcorper quam eu nisl interdum at interdum enim egestas. Aliquam placerat justo sed lectus lobortis ut porta nisl porttitor. Vestibulum mi dolor, lacinia molestie gravida at, tempus vitae ligula. Donec eget quam sapien, in viverra eros. Donec pellentesque justo a massa fringilla non vestibulum metus vestibulum. Vestibulum in orci quis felis tempor lacinia. Vivamus ornare ultrices facilisis. Ut hendrerit volutpat vulputate. Morbi condimentum venenatis augue, id porta ipsum vulputate in. Curabitur luctus tempus justo. Vestibulum risus lectus, adipiscing nec condimentum quis, condimentum nec nisl. Aliquam dictum sagittis velit sed iaculis. Morbi tristique augue sit amet nulla pulvinar id facilisis ligula mollis. Nam elit libero, tincidunt ut aliquam at, molestie in quam. Aenean rhoncus vehicula hendrerit.

Chapter 4

Conclusion

4.1 Main Section 1

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam ultricies lacinia euismod. Nam tempus risus in dolor rhoncus in interdum enim tincidunt. Donec vel nunc neque. In condimentum ullamcorper quam non consequat. Fusce sagittis tempor feugiat. Fusce magna erat, molestie eu convallis ut, tempus sed arcu. Quisque molestie, ante a tincidunt ullamcorper, sapien enim dignissim lacus, in semper nibh erat lobortis purus. Integer dapibus ligula ac risus convallis pellentesque.

4.1.1 Subsection 1

Nunc posuere quam at lectus tristique eu ultrices augue venenatis. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Aliquam erat volutpat. Vivamus sodales tortor eget quam adipiscing in vulputate ante ullamcorper. Sed eros ante, lacinia et sollicitudin et, aliquam sit amet augue. In hac habitasse platea dictumst.

4.1.2 Subsection 2

Morbi rutrum odio eget arcu adipiscing sodales. Aenean et purus a est pulvinar pellentesque. Cras in elit neque, quis varius elit. Phasellus fringilla, nibh eu tempus venenatis, dolor elit posuere quam, quis adipiscing urna leo nec orci. Sed nec nulla auctor odio aliquet consequat. Ut nec nulla in ante ullamcorper aliquam at sed dolor. Phasellus fermentum magna in augue gravida cursus. Cras sed pretium lorem. Pellentesque eget ornare odio. Proin accumsan, massa viverra cursus pharetra, ipsum nisi lobortis velit, a malesuada dolor lorem eu neque.

4.2 Main Section 2

Sed ullamcorper quam eu nisl interdum at interdum enim egestas. Aliquam placerat justo sed lectus lobortis ut porta nisl porttitor. Vestibulum mi dolor, lacinia molestie gravida at, tempus vitae ligula. Donec eget quam sapien, in viverra eros. Donec pellentesque justo a massa fringilla non vestibulum metus vestibulum. Vestibulum in orci quis felis tempor lacinia. Vivamus ornare ultrices facilisis. Ut hendrerit volutpat vulputate. Morbi condimentum venenatis augue, id porta ipsum vulputate in. Curabitur luctus tempus justo. Vestibulum risus lectus, adipiscing nec condimentum quis, condimentum nec nisl. Aliquam dictum sagittis velit sed iaculis. Morbi tristique augue sit amet nulla pulvinar id facilisis ligula mollis. Nam elit libero, tincidunt ut aliquam at, molestie in quam. Aenean rhoncus vehicula hendrerit.

Appendix A

Appendix Title Here

Write your Appendix content here.