How to Not Lose Your Keys

Approaches to Managing Multiple Identities and Devices for Single Users

Mark MacIntyre Wheatley
University of Waterloo
200 University Ave. W
Waterloo, ON N2L 3G1
ms3macin@uwaterloo.ca

ABSTRACT

In today's day and age, the average computer user finds at their disposal a plethora of computing devices of various sizes, form factors and computing power, targeted at different aspects of the user's lifestyle. Indeed, it is not uncommon to find the average user in possession of at least two devices, namely, a computer and a smartphone. Additionally, we find new devices being released everyday: smart accessories, smart appliances and the ilk. The average user expects all their applications to work seamlessly across their devices. A challenge in security arises when the user needs to manage their multiple interconnected devices and their multiple identities for their applications. The devices usually share the user's cryptographic private key. This key sharing can often be insecure and expose the user to grave security concerns of theft and malware. Devices such as phones and watches are frequently removed or replaced. Also, the loss of a single device can compromise the security of the user and their remaining devices.

This paper aims to provide an overview of recent developments in approaches to managing multiple devices and identites for single users. **Comment:** [list of names and some findings]

1 INTRODUCTION

Comment: Might consider moving some of the content from the abstract here instead

2 BACKGROUND INFORMATION

3 THE *PERSONAL* KEY INFRASTRUCTURE

3.1 PorKI

3.2 Personal PKI for Smart Devices

3.3 CONIKS

4 THRESHOLD CRYPTOGRAPHY

5 REFERENCES

6