Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Master Thesis

An Isolated, Secure and Air-Gapped Signing System

Supervisor:	Brian Trammell
Professor:	Adrian Perrig
Issue Date:	October 4, 2017
Submission Date:	April 4, 2018

1 Introduction & Motivation

For hundreds of years, people have been using signatures, typically to bind a person to a contract. Since the digital age, digital signatures have appeared which basically have the same ulterior motivates, i.e., *binding* two objects to each other. Typical examples are binding a name to a person or a name to an IP-address. Such signing mechanisms most likely use a public key infrastructure (PKI). The very crucial part in every system that uses PKI is to keep the private/signing-key secure. This not always an easy task to solve, as a system where the signing key is stored might be compromised or even stolen physically. The goal of this thesis is to figure out if it is possible to build a rather simple signing system that is located in a totally isolated and safe environment such that it can be used to sign assertions (e.g., the mapping of a name to an address) over an air-gapped *channel*. Based on the idea of [2], the air-gapped channel will consist of two monitors standing in front of each other and two cameras pointing to the opposite monitor. The reason why we want to use such a visual air-gap is that one can easily monitor and audit what happens on the screens, i.e., on the channel. Furthermore, the system should be of relatively low cost and yet effective, since this system will mainly be used to sign assertions from the RAINS protocol used in the new Internet architecture SCION [1], where a lot of requests have to be handled.

2 Assignment

The student's core task is to build a secure, air-gapped system for signing assertions. Furthermore, the thesis includes estimating the cost of the system, running a performance analysis and testing the system for security issues. The following breakdown into subtasks is suggested (a further refinement in the time schedule is possible):

1. Design of the system
2. Implementation of the system
3. Performance analysis
4. Cost estimation
5. Testing the system for security issues.

6. (Optional) Implementation of an auditor for auditing the signing process

7. Write-up

3 Deliverables

1. The final report must be written in English and typeset in LaTeX. It should include an introduction and motivation, an overview of the related work, and a detailed description of the obtained results. Three copies of the final report must be delivered to the supervisor.

2. At the end of the thesis, a presentation giving an overview as well as highlighting the most important details of the work must be given. (Duration and the location of the presentation is not yet defined).

3. All developed code must be available as source code that runs on a recent Google Chrome browser and on a Linux machine.

4. All source code developed during the thesis (including the LaTeX-code for the final report) must be checked into a version-controlled repository managed by the Network Security group. This code may be used by the Network Security group in any form for all purposes the group sees fit provided appropriate credit to the student is given.

References

[1] David Barrera, Laurent Chuat, Adrian Perrig, Raphael M. Reischuk, and Pawel Szalachowski. The scion internet architecture. *Commun. ACM*, 60(6):56–65, May 2017.

[2] Stephanos Matsumoto, Samuel Steffen, and Adrian Perrig. Castle: Ca signing in a touchless environment. In *Proceedings of the 32Nd Annual Conference on Computer Security Applications*, ACSAC '16, pages 546–557, New York, NY, USA, 2016. ACM.