A Security Analysis of MinSky

Aleksander Våge
Alek@vage.com

30. April 2018

Contents

1 Introduction

This is a security analysis of Telenor's service; MinSky. This analysis is done in co-operation with Telenor as my project for the course INF219: Project in Informatics, under the supervision of Marc Bezem (UiB) and Raymond Strandheim (Atea). This would not be possible without the help from Mark from Telenor's customer service, who helped me gain a deeper understanding of the system that runs MinSky.

1.1 Problem

Software-as-a-Service (SaaS) is a form of cloud computing in which the customer runs software on a remote server of the service provider instead of on the computer of the customer. The advantages of this licensing and deliviery model (which seem to facour mostly the probider) are:

The provider keeps full control of the software and how it is used;
The customer only needs only a thin client to use the service.
There are obvious security problems (mostly for the customer), including;
In- and output data of the customer reside on the provider's computer;
The customer has no guarantee that the software has not been modified;
The customer could compromize the vendor's server via the input data.

File sharing services like Dropbox, as well as version control systems like Git and subversion offer a simple way to implement SaaS, at least for batch processing. Customer and provider would share a common directory structure which is syncornized on their respective computers. The probider's computer is running a script which looks for new input. If new input is found, it is processed by the provider's software on his computer and the result is puched to shared directory. After synchronization (which may be automatic, like in Dropbox), the customer finds the output on his comuter.

The aim of the project is to implement the above model SaaS in the form of MinSky, and to evaluate it on important aspects like performance, stability and security.