

Bachelor Thesis

Preventing Supply Chain Insecurity by Authentication on Layer 2

Stephan Neuhaus

2017-06-15

1 Introduction

The SSH protocol [RFC253, RFC6668, RFC8268, RFC8308, RFC8332] is now over twelve years old in its current form. One of the problems with SSH is its complexity, both in the initial phase when key material is exchanged, but also later, for example because the server must always decide whether to return a character that has been sent to it or not (echo).

The goal of this work is a radically simplified protocol, which in its functions is similar to SSH. (N.B. the similarity concerns the functions, not necessarily the protocol details). You develop the protocol, as well as a client and a server. You demonstrate that your software can replace SSH by showing that it can handle several common use cases, among them:

- Interactive session
- Rsync with the SSH replacement as transport protocol

2 Task

To this end, this thesis will

- design and implement a client-server protocol that can manage interactive sessions
- design and implement a privilege-separation architecture on the server side that allows safe dropping of privileges once a client establishes a connection

For a passing grade (4.0), the work must contain at least the following:

- in the thesis, an introduction to the problem and why the envisaged solution will solve it;
- in the thesis, a survey of related work in the area;
- in the thesis, a detailed design of the solution;
- in the thesis, an evaluation of the performance of the implemented solution; and

- in the software, a privilege-separation architecture.

These requirements do not contain anything related to security. This is not an accident.

Incorporating the following components will improve the grade. The more components are included, the better the grade will be.

- In the related work section of the thesis, a comparison of all the related work with the envisaged solution, outlining why the envisaged solution is better;
- in the thesis, a detailed analysis of the security of the solution, including possible attacks and defenses;
- use of TLS as the transport layer;
- the software in a public repository, ideally on Github;
- a proof-of-concept client that can handle interactive sessions;
- a proof-of-concept client that works as a transport for rsync;

ZHAW's School of Engineering no longer provides formal language lessons for its students as part of the curriculum. I am therefore giving notice that submitting a thesis with large amounts of orthographical or grammatical errors lead to a lower grade.

The thesis can be submitted in German or English. English is preferred, but submitting in German will not lead to a lower grade.