

Verifying the SSH Transport Layer Protocol in the Computational Domain

Alfredo Pironti, Riccardo Sisto

Politecnico di Torino

{alfredo.pironti,riccardo.sisto}@polito.it

SSH is a widely deployed protocol providing a secured communication between a client (usually ran by a remote user) and a server (the controlled system). The SSH protocol suite is composed of three protocols, the first of them is the Transport Layer Protocol (SSH-TLP). The SSH-TLP is responsible for establishing the client-server secured channel, by providing confidentiality and server authentication to the client, by means of public key cryptography. Thus, SSH-TLP plays a key-role on the overall security assurance offered by the whole protocol suite.

Consequently, there have been several research works that concentrated on the analysis of SSH-TLP. A considerable part of them focused on the formal verification of SSH-TLP in the Dolev-Yao model. Essentially, the Dolev-Yao model subsumes perfect cryptography. That is, cryptographic functions are algebraic operators that apply on data; for example, the encryption of M with key k is represented by the symbol $\{M\}_k$, and M can be retrieved only if k is available. The Dolev-Yao model is amenable to formal verification, because it allows to reason about security protocols in a symbolic way, abstracting away the computational hardness theories that stand at the basis of modern cryptography. Thanks to these abstractions, verification at the Dolev-Yao level is effective in efficiently discovering logical errors in protocols, that depend on erroneous usage of cryptographic primitives (rather than on computational properties of cryptography). Some tools, like ProVerif, even offer full automation in the verification of Dolev-Yao models, making adoption of these verification techniques more affordable.

However, it is often the case that protocols being secure at the Dolev-Yao level, are in fact flawed at the computational level, where the computational complexity of cryptography, and interactions between cryptographic operations and the bitstrings they operate on, is taken into account. Released recently, the CryptoVerif tool allows to perform fully automatic verification of computational models, as opposed to the classical computational proofs carried out by hand.

In this paper, we make some experiments in analyzing the SSH-TLP in the computational model, in order to verify whether the secrecy and server authentication properties that have been successfully proven in the Dolev-Yao model, also hold in the more refined computational domain. The CryptoVerif tool is used to verify the model. This computational model is then compared with similar models developed for the Dolev-Yao context, and verified with ProVerif. The computational analysis clearly highlights that, due to the SSH-TLP design, strong secrecy is impossible to achieve. We also investigate minor modifications to the protocol that would make strong secrecy possible, while maintaining server authentication.