

Formal verification of the YubiKey and YubiHSM APIs in Maude-NPA

Antonio González-Burgueño

University of Oslo
Oslo, Norway
antonigo@ifi.uio.no

Catherine Meadows

Naval Research Laboratory
Washington, USA
meadows@itd.nrl.navy.mil

Damián Aparicio* Santiago Escobar *

DSIC-ELP
Universitat Politècnica de València
Valencia, Spain
{daapsnc, sescobar}@dsic.upv.es

José Meseguer

University of Illinois at Urbana-Champaign
Urbana IL, USA
meadows@itd.nrl.navy.mil

We perform an automated analysis of two devices developed by Yubico: *YubiKey*, designed to authenticate a user to network-based services, and *YubiHSM*, Yubico's hardware security module. Both are analyzed using the Maude-NPA cryptographic protocol analyzer. Although previous work has been done applying formal tools to these devices, there has not been any completely automated analysis. This is not surprising, because both YubiKey and YubiHSM, which make use of cryptographic APIs, involve a number of complex features: (i) discrete time in the form of *Lamport clocks*, (ii) a mutable memory for storing previously seen keys or nonces, (iii) event-based properties that require an analysis of sequences of actions, and (iv) reasoning modulo exclusive-or. Maude-NPA has provided support for exclusive-or for years but has not provided support for the other three features, which we show can also be supported by using constraints on natural numbers, protocol composition and reasoning modulo associativity. In this work, we have been able to automatically prove security properties of YubiKey and find the known attacks on the YubiHSM, in both cases beyond the capabilities of previous work using the Tamarin Prover due to the need of auxiliary user-defined lemmas and limited support for exclusive-or. Tamarin has recently been endowed with exclusive-or and we have rewritten the original specification of YubiHSM in Tamarin to use exclusive-or, confirming that both attacks on YubiHSM can be carried out by this recent version of Tamarin.

References

- [1] Antonio González-Burgueño, Damián Aparicio-Sánchez, Santiago Escobar, Catherine Meadows & José Meseguer (2018): *Formal verification of the YubiKey and YubiHSM APIs in Maude-NPA*. In: *LPAR-22. 22nd International Conference on Logic for Programming, Artificial Intelligence and Reasoning, EPiC Series in Computing 57*, EasyChair, pp. 400–417.

*Partially supported by the EU (FEDER) and the Spanish MCIU under grant RTI2018-094403-B-C32, by the Spanish Generalitat Valenciana under grant PROMETEO/2019/098, and by the US Air Force Office of Scientific Research under award number FA9550-17-1-0286.