Automatic Learning and Verification of Cryptographic Protocols: the Case of PKCS11

Anonymous Author(s)
Anonymous Institute(s)
Anonymous Email(s)

***Abstract*—**

I. Introduction

TODO: crypto protocols, automata learning

cryptographic protocols are hard to verify as adhering to their specs

we devise a framework based on hardware-software contracts for the verification of protocol specs and protocol implementations wrt their specs.

TODO: fit automata learning

TODO: proofs sul framework?

we instantiate the framework on the PKCS11 protocol, we verify its specs as insecure, we verify their patched specs as secure, we learn the behaviour of modern implementations of PKCS11 (list: securosys,

TODO: more

) and prove they are secure

II. Background

III. Related Work

IV. Conclusion