Formal analysis of Julia Key Agreement protocol

Navya Sivaraman[1][0000-0003-0123-1970], Simin Nadjm-Tehrani[1][0000-0002-1485-0802], and Thomas Johansson[2][0000-0003-1798-570X]
[1] Linköping University, Sweden
{navya.sivaraman,simin.nadjm-tehrani}@liu.se
[2] Lund University, Sweden
thomas.johansson@eit.lth.se

Abstract

The evolution of the fifth-generation network (5G) increases the demand and use of Internet of Things (IoT) devices extensively. The increased number of IoT devices increases the possibility of new attack surfaces, and thus even resource-constrained IoT devices need secure communication. In this work, we consider the Julia Key Agreement (JKA) protocol, which has been proposed as a secure and efficient protocol for communication among resource-constrained IoT devices. We formally model two variants of the JKA protocol and verify the intended security requirements, such as mutual authentication, forward secrecy, backward secrecy, and resilience to key impersonation attacks, using the Tamarin prover. Our formal analysis shows that the JKA protocol is susceptible to replay attacks under the Dolev Yao threat model. We also expand the threat model by including several strong threat assumptions to discover interesting attack vectors.

Keywords: Key Agreement protocol, IoT security, Formal verification, Tamarin