h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
fbi
FACULTY OF COMPUTER SCIENCE

ATHENE
National Research Center
for Applied Cybersecurity

Master Thesis or R&D study
Formal Verification of Protocols
Analysis of the symbolic approach techniques

acsd applied cyber security darmstadt

Motivation

Cryptographic protocols are ubiquitous, they are used to secure information exchange among users and service providers. They are present in a variety of applications: internet navigation browser requests, banking card payment, e-mail exchange, aircraft and ground control communication; and so on. Thus, it is not only necessary to design protocols taking into account security goals with desired performance, but to formally proof these security properties hold against adversaries that want to corrupt them. There are two approaches when proving cryptographic security of protocols each one with advantages and drawbacks. The classical one is considering protocols as exchange of bit string messages and cryptographic primitives as probabilistic. The goal here is to prove that the attacker can gain some information from the protocol only with a negligible probability. The advantage is that this approach provides strong security guarantees, nevertheless the proofs are manual, using pen-and-pencil, or mechanized but with some limitations. The second approach considers protocol messages as composable terms and cryptographic primitives as secure black-box entities; both linked by relational equations. The protocols are built using some set of rules which are also at the disposition of the attacker. The goal is to prove the security properties hold when the attacker exploit these rules and the protocol logic. The drawback is that in most of the cases we can only proof Syntactic security, nevertheless that allows to find protocol vulnerabilities and frequently automation tools are at hand.

Goal

Study the different mechanisms and techniques that are used by the symbolic approach for proving protocols. The work will be conceptual and no implementation is required.

Tasks (selection from the following)

- Overview, applicability, constraints of one or more these models:
  - Dolev-Yao and the applied pi-calculus models
  - Multiset Rewriting (MSR) model
  - Satisfiability Module Theroies (SMT) applied to formal verification of cryptographic protocols
  - Banna And Comon (BNC) model

Prerequisites

- Interest and basic knowledge in cryptography
- Some background in formal proofs or language theory will be helpful
- Thesis language will be in English.

The **Applied Cyber Security Darmstadt** (ACSD) Research Group is specialized in the protection of IT systems and applications in the fields of automotive, railway, computer networks, embedded systems, IoT and cloud. Our application-oriented and user-friendly solutions are based on the use, adaption, or development of cryptographic technologies.

Contact
M. Sc. Miguel Robles
miguel.robles@h-da.de

Prof. Dr. Alexander Wiesmaier
alexander.wiesmaier@h-da.de

Websites
https://acsd.h-da.de

Office
Schöfferstr. 10
64287 Darmstadt

Start

Right away or by arrangement

Further use

The project artifacts may be build on existing material and/or may be used in further projects and shall be subject to the MIT license (`https://opensource.org/licenses/MIT`).