Formal Security Analysis

OAuth and OpenID Connect

Daniel Fett, yes.com
Guido Schmitz, Royal Holloway University of London

Security Analysis of Web Protocols

Web protocols = Protocols running on top of the web infrastructure

Challenges:

- Web infrastructure is complex (Browsers, Javascript, Network, TLS, DNS, …)
- Accurate and comprehensive modeling of web protocols is hard
- No comprehensive and tool-supported models available

→ pen-and-paper model/proofs (sorry, Jonathan)

Detailed Dolev-Yao style model: “Web Infrastructure Model” (WIM).

Formal Analysis of OAuth

“A Comprehensive Formal Security Analysis of OAuth 2.0” (2016)
Analysis of RFC6749 and related specs based on WIM.

- Helped to uncover new & unexpected problems (e.g., mix-up attack)
- Creation of “OAuth Security Best Current Practices” and RFC9207

Challenges:

- No attacker model
- No clearly defined security goals
- OAuth is not one protocol, but many

OIDF: Formal Analysis for High-Security OAuth Profiles

FAPI: High-security profile of OAuth & OpenID Connect

- FAPI 1: New attacks found via formal analysis using WIM
- FAPI 2: Formal analysis as explicit goal:
  - Lessons learned from FAPI 1:
    - Clearly defined and described attacker model
    - Explicit security goals
    - Reducing optionality is important
  - External funding for researchers
  - Close collaboration with analysis team @ University of Stuttgart
  - Results:
    - Proof of security (within bounds of the model) finished before final publication
    - Well-documented expectations on security of FAPI 2

Ongoing work: DY*

Formal protocol analysis framework built on top of F* verification ecosystem

- Enables Dolev-Yao-style trace-based analysis in F*
- protocols are modelled as F* algorithms / programs
- analysis can also reason on unbounded loops, recursive and detailed data structures, modular composition of sub protocols, state management, ...

Case studies: Signal, ISO-KEM, ACME, (OAuth Device Flow - in progress)

Executable code can be extracted from model (e.g., interoperable ACME client)

Links

Web Infrastructure Model: https://www.sec.uni-stuttgart.de/research/wim/

DY*: https://reprosec.org/

OAuth formal analysis: https://arxiv.org/abs/1601.01229

FAPI 1 formal analysis: https://arxiv.org/abs/1901.11520