FAPI 2.0 Security Analysis Project

Version 1.0
Feb 28 2022

Methodology

For cryptographic protocols, only formal analysis and verification methods enable rigorous scrutiny including the possibility to prove security, at least within the bounds of the model used.

For protocols that are based upon web technologies, the tools and models used for cryptographic protocols cannot be applied. Where cryptographic protocols are often based on a direct network connection between participants and cryptographic primitives are used to secure the connection, web protocols depend on the web infrastructure and messages are often relayed on higher network layers via other participants in these protocols. Crucially, web browsers bring a complex, dynamic, and concurrent application model where web sites with very high security requirements are often executed alongside untrusted, potentially malicious web sites. To capture protocol flaws at this abstraction level, models do not need to focus on the details of cryptographic primitives, but instead accurately capture details of the security mechanisms and protections provided by web browsers, in scripting environments, DNS and other parts of the web infrastructure.

The Web Infrastructure Model (WIM) is, to date, the most comprehensive model for this task. It has been successfully used to analyze the BrowserID SSO protocol[1], OAuth[2], OpenID Connect[3], Financial-Grade API 1.0[4], and W3C Web Payment API[5]. The results of these WIM studies have been published at leading international security conferences such as IEEE Symposiums, ACM SIGSAC, and ESORICS. Just as the OpenID Foundation supports the use of the WIM approach on its FAPI 1.0 standard, it also sees the merit of this approach for the FAPI 2.0 family of standards. It's premature for other reputable entities like

---

[1] Daniel Fett, Ralf Küsters, and Guido Schmitz, Analyzing the BrowserID SSO System with Primary Identity Providers Using an Expressive Model of the Web. Computer Security - ESORICS 2015 - 20th European Symposium on Research in Computer Security, 2015. (Technical report.) *and* Daniel Fett, Ralf Küsters, and Guido Schmitz, An Expressive Model for the Web Infrastructure: Definition and Application to the BrowserID SSO System. 35th IEEE Symposium on Security and Privacy (S&P 2014). (Technical report.)

[2] Daniel Fett, Ralf Küsters, and Guido Schmitz, A Comprehensive Formal Security Analysis of OAuth 2.0. In Proceedings of the 23rd ACM SIGSAC Conference on Computer and Communications Security (CCS 2016). (Technical report.)

[3] Daniel Fett, Ralf Küsters, and Guido Schmitz, The Web SSO Standard OpenID Connect: In-Depth Formal Security Analysis and Security Guidelines. IEEE 30th Computer Security Foundations Symposium (CSF 2017). (Technical report.)

[4] Daniel Fett, Pedram Hosseyni, and Ralf Küsters, An Extensive Formal Security Analysis of the OpenID Financial-grade API. 2019 IEEE Symposium on Security and Privacy (S&P 2019). (Technical report.)

[5] Quoc Huy Do, Pedram Hosseyni, Ralf Küsters, Guido Schmitz, Nils Wenzler, and Tim Würtele, "A Formal Security Analysis of the W3C Web Payment APIs: Attacks and Verification," 43rd IEEE Symposium on Security and Privacy (S&P 2022), 2022.

the IEEE to formally endorse the WIM model, but the academic selection process for publication in a range of security conferences is testimony to the rigor of the approach and its importance to the security community.

Furthermore, from an OpenID Foundation perspective, FAPI 2.0 was designed with the lessons learned from the security analysis of FAPI 1.0 in mind, both with regards to the security mechanisms used as well as the overall design including a defined attacker model to facilitate an efficient and precise analysis using the WIM. The goal of this project is therefore to fund a WIM-based analysis of FAPI 2.0, and to ensure that this analysis is conducted in a timely manner before the final FAPI 2.0 standards are released and it is adopted widely in the marketplace. Although FAPI 2.0 standards were developed with WIM in mind, if other security analysis approaches emerge in future, the OpenID foundation and FAPI WG are open to exploring them.

Work Plan

The security analysis is to be conducted in two Work Packagess. Work Package 1 focuses on the FAPI 2.0 Baseline profile including the standards it is based upon. In Work Package2, the Advanced profile will be analyzed.

Work Package 1

Scope of analysis:

- **FAPI 2.0 Baseline Profile** when used with OAuth 2.0 and OpenID Connect Core 1.0, analysis to be conducted in this order, and to include at a minimum the following components[6]
    - Proof Key for Code Exchange by OAuth Public Clients (PKCE) [RFC7636]
    - OAuth 2.0 Pushed Authorization Requests (PAR) [RFC9126]
    - OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens (MTLS) [RFC8705]
    - OAuth 2.0 Demonstrating Proof-of-Possession at the Application Layer (DPoP) [I-D.ietf-oauth-dpop]
    - OAuth 2.0 Rich Authorization Requests (RAR) [I-D.ietf-oauth-rar]
    - OAuth 2.0 Authorization Server Metadata [RFC8414]
    - OAuth 2.0 Authorization Server Issuer Identifier in Authorization Response [I-D.ietf-oauth-iss-auth-resp]
    - OAuth 2.0 Dynamic Client Registration Protocol [RFC7591]
        - Note: Include comment on security risks (if any) on implementations that do not use RFC7591, and instead use a signed JWT as the main request body, instead of JSON, e.g. Australian DCR spec: (https://consumerdatastandardsaustralia.github.io/standards/#dcr-apis)

[6] The analysis results regarding the supporting standards listed here will be applicable in the context of FAPI 2.0 Baseline. When used in the context of other specifications, the level of security that can be achieved is likely to be different.

    - OAuth 2.0 Dynamic Client Management (RFC7592)
- The security model will be based upon **FAPI 2.0 Attacker Model**[7]

A version of FAPI 2.0 to serve as the basis for the analysis will be communicated.

Security properties:
- Authorization (using OAuth 2.0)
- Authentication (using OpenID Connect)
- Session Integrity

Focus questions:
- Is an ID Token in the front end a potential security problem? Does encryption of the ID Token provide any benefit? What security properties could be violated?
- Does the DPoP nonce add any value in the FAPI2 environment?

A. Initial Work

Time estimate: two months
- Definition of the formal model for the specifications in scope of Block 1, based on the WIM.
- Definition of the security properties to prove and the formal attacker model based on FAPI 2.0 Attacker Model.
- Where required, coordination with the FAPI working group, in particular regarding the scope of the analysis, security properties, focus areas and required level of detail.
- The FAPI Working Group will provide a review of the finished model.

B. Complete Work Package

Time estimate: two months
- Proof based on the previously defined formal model.
- In case flaws are identified in FAPI 2.0, coordination with the working group to develop and apply fixes and, when possible, include them into the formal model.
- Creation of a technical report describing the scope, model, and results.

Work Package 2

Scope of analysis:
- FAPI 2.0 Advanced Security Profile when used with OAuth 2.0 and OpenID Connect Core 1.0, including*
    - JARM
- FAPI CIBA

[7] The FAPI 2.0 Attacker Model document defines basic assumptions about attackers to delineate the kinds of attacks that FAPI 2.0 aims to defend against and those that are considered out of scope. For example, compromised servers within an ecosystem are considered in scope, whereas attacks on cryptographic primitives or compromised TLS keys are considered out of scope. The Attacker Model does not define individual attacks, like cross-site request forgery, to be in or out of scope, but defines broad attacker capabilities, like reading or modifying messages, compromising endpoints, etc.

    - May include comments on why this does not merit security analysis

A. Initial Work

Time estimate: two months or less?

- Definition of the formal model for the specifications in scope of Block 2, based on the WIM.
- Definition of the security properties to prove and the formal attacker model based on FAPI 2.0 Attacker Model.
- Where required, coordination with the FAPI working group, in particular regarding the scope of the analysis, security properties, focus areas and required level of detail.
- The FAPI Working Group will provide a review of the finished model.

B. Complete Work Package

Time estimate: two months or less?

- Proof based on the previously defined formal model.
- In case flaws are identified in FAPI 2.0 advanced, coordination with the working group to develop and apply fixes and, when possible, include them into the formal model.
- Creation of a technical report describing the scope, model, and results.

Notes:

- The OpenID Foundation intends to fully fund Block 1 Part A, the first two months of this analysis.
- University will be able to publish the results of this final analysis at conferences or in publications, at the end of Block 1 and Block 2 respectively. The OIDF requests courtesy of a pre-publication copy prior to release.
- The OpenID Foundation will be able to reference and/or re-publish the final analyses at the end of Block 1 and Block 2 respectively, given the importance of this work to the wider community.
- The following deliverables are out of scope, for Block 1 & 2 but are likely to be covered in a subsequent scope of work
    - FAPI Grant Management (OIDF standard, but formal security analysis may not be interesting)
    - Shared Signals & Events/ CAEP (OIDF standard)
    - OpenID Connect for Identity Assurance 1.0 (IDA, OIDF standard)