

Master thesis : FIDOLOGY : A Measurement Study of FIDO2 Adoption Across the Web

Auteur : Krumm, Macha

Promoteur(s) : Donnet, Benoît

Faculté : Faculté des Sciences appliquées

Diplôme : Master : ingénieur civil en informatique, à finalité spécialisée en "computer systems security"

Année académique : 2025-2026

URI/URL : https://gitlab.uliege.be/Macha.Krumm/tfe_krumm; <http://hdl.handle.net/2268.2/26194>

Avertissement à l'attention des usagers :

Tous les documents placés en accès ouvert sur le site le site MatheO sont protégés par le droit d'auteur. Conformément aux principes énoncés par la "Budapest Open Access Initiative"(BOAI, 2002), l'utilisateur du site peut lire, télécharger, copier, transmettre, imprimer, chercher ou faire un lien vers le texte intégral de ces documents, les disséquer pour les indexer, s'en servir de données pour un logiciel, ou s'en servir à toute autre fin légale (ou prévue par la réglementation relative au droit d'auteur). Toute utilisation du document à des fins commerciales est strictement interdite.

Par ailleurs, l'utilisateur s'engage à respecter les droits moraux de l'auteur, principalement le droit à l'intégrité de l'oeuvre et le droit de paternité et ce dans toute utilisation que l'utilisateur entreprend. Ainsi, à titre d'exemple, lorsqu'il reproduira un document par extrait ou dans son intégralité, l'utilisateur citera de manière complète les sources telles que mentionnées ci-dessus. Toute utilisation non explicitement autorisée ci-avant (telle que par exemple, la modification du document ou son résumé) nécessite l'autorisation préalable et expresse des auteurs ou de leurs ayants droit.

University of Liège - Faculty of Applied Sciences
MASTER OF SCIENCE IN COMPUTER SCIENCE AND ENGINEERING

FIDOLOGY:
A Measurement Study of FIDO2 Adoption
Across the Web

Macha Krumm

Supervisor: Benoit Donnet

Academic year: 2025–2026

While passwords are outdated and need to be replaced, a new successor is emerging: FIDO2. Developed by the FIDO Alliance and the W3C, this standard enables passwordless user authentication using security tokens and combines the Web Authentication specification (WebAuthn) with the new Client-to-Authenticator Protocol (CTAP2) protocol. Since its launch in 2018, websites have gradually begun to adopt it, but to date, the real state of adoption of FIDO2 in the wild is not known.

This work aims to fill this gap by creating FIDOLOGY, a tool that categorizes the authentication mechanisms implemented by websites into five categories: **None/Error**, **Password-Based**, **Password-Extended**, **Fido2-Native** and **Unknown**, by implementing, in a non-intrusive and deterministic way, an automated pipeline using headless browser and multi-layered signals inference. First applied to a manually crafted groundtruth, FIDOLOGY revealed to be capable of correctly categorizing the authentication methods in more than half of the cases, particularly for the **Password-Based** and **Fido2-Native** categories. Evaluated then against a much larger dataset, this tool has shown that classical password-based mechanisms continue to dominate the world of authentication, whilst FIDO2 clues are detected on a small but non-negligible proportion of websites, resulting in a minority of fully enabled passwordless authentication processes.

In addition to this state of FIDO2 deployment, authentication flows are captured to analyse cryptographic challenges and other metrics, with the aim to evaluate the security level of websites previously identified as belonging to the **Fido2-Native** category. While most of them meet, and in some cases even exceed, the expected FIDO requirements, critical issues like challenge reuse across sessions are discovered, revealing weaknesses in the implementations and leaving websites vulnerable to replay attacks.

Keywords: FIDOLOGY, FIDO2, password, authentication, signals, classification, challenge