ACM Transactions on Privacy and Security

An Extensive Formal Analysis of Multi-factor Authentication Protocols

Authors: Charlie Jacomme, Steve Kremer | Authors Info & Claims

ACM Transactions on Privacy and Security (TOPS), Volume 24, Issue 2 Article No.: 13, Pages 1 - 34
https://doi.org/10.1145/3440712

Published: 21 January 2021 Publication History Check for updates

Abstract

Passwords are still the most widespread means for authenticating users, even though they have been shown to create huge security problems. This motivated the use of additional authentication mechanisms in so-called multi-factor authentication protocols. In this article, we define a detailed threat model for this kind of protocol: While in classical protocol analysis attackers control the communication network, we take into account that many communications are performed over TLS channels, that computers may be infected by different kinds of malware, that attackers could perform phishing, and that humans may omit some actions. We formalize this model in the applied pi calculus and perform an extensive analysis and comparison of several widely used protocols—variants of *Google 2-step* and *FIDO's U2F* (Yubico's

we demonstrate their feasibility in practice, even though our experiments are run in

different protocols. It allows us to suggest several small modifications of the existing protocols that are easy to implement, as well as an extension of *Google 2-step* that improves security in several threat scenarios.

References

[1] Martín Abadi, Bruno Blanchet, and Cédric Fournet. 2017. The applied Pi calculus: Mobile values, new names, and secure communication. J. ACM 65, 1, Article 1 (Oct. 2017), 41 pages.

Digital Library | Google Scholar

[2] Martín Abadi and Cédric Fournet. 2001. Mobile values, new names, and secure communication. In Proceedings of the 28th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL'01). ACM, New York, NY, 104--115.

Digital Library | Google Scholar

[3] Alessandro Armando, Roberto Carbone, and Luca Zanetti. 2013. Formal modeling and automatic

Online publication date: Aug-2025.

ACM Transactions on Privacy and Security

Chawla D, Jain K, Mehra P, Das A and Bera B. (2025). Quantum cryptography as a solution for secure Wireless Sensor Networks: Roadmap, challenges and solutions. Internet of Things. 10.1016/j.iot.2025.101610. **32**. (101610). Online publication date: Jul-2025.

https://doi.org/10.1016/j.iot.2025.101610

and Aravind Raghu . (2025). Enhancing Financial Transaction Security Using OAuth2, MFA, and Azure AD Authentication: A Java-Based Integrated Approach. International Journal of Computational and Experimental Science and Engineering. 10.22399/ijcesen.2068. **11**:2. Online publication date: 13-May-2025.

https://doi.org/10.22399/ijcesen.2068

Show More Cited By

Feedback

Index Terms

An Extensive Formal Analysis of Multi-factor Authentication Protocols

Security and privacy

Formal methods and theory of security

Formal security models

Security services

Authentication

Multi-factor authentication

smart card, and biometric in wireless communication is an important and significant issue that researchers have bee

ACM Transactions on Privacy and Security

AISC '10: Proceedings of the Eighth Australasian Conference on Information Security - Volume 105

We consider a new form of authenticated key exchange which we call *multi-factor password-authenticated key exchange*, where session establishment depends on successful authentication of multiple short secrets that are...

Read More

Unveiling the Covert Vulnerabilities in Multi-Factor Authentication Protocols: A Systematic Review and Security Analysis

Nowadays, cyberattacks are growing at an alarming rate, causing widespread havoc to the digital community. In particular, authentication attacks have become a dominant attack vector, allowing intruders to impersonate legitimat.

Read Mor

Feedback

Comments

View Issue's Table of Contents

ACM Transactions on Privacy and Security