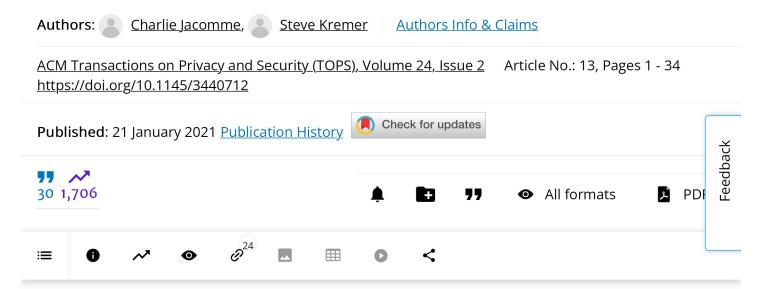
#### ACM Transactions on Privacy and Security 🗸

# An Extensive Formal Analysis of Multi-factor Authentication Protocols



## **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

1 of 5 28/05/2025, 11:57 am

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

ACM Transactions on Privacy and Security 

✓

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 | S 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. | S Google Scholar
- [3] Alessandro Armando, Roberto Carbone, and Luca Zanetti. 2013. Formal modeling and automatic

Show all references



#### 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. Feedback

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

Show More Cited By

#### Index Terms

An Extensive Formal Analysis of Multi-factor Authentication Protocols

Security and privacy

Formal methods and theory of security

Security services

Formal security models

Authentication

Multi-factor authentication

3 of 5 28/05/2025, 11:57 am smart card, and highertric 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 Mo

**Comments** 



4 of 5 28/05/2025, 11:57 am

#### VICTO ISSUE S TUDIC OF CONTENTS

## ACM Transactions on Privacy and Security 🗸

Categories	About		
Journals	About ACM Digital Library		
Magazines	ACM Digital Library Board		
Books	Subscription Information		
Proceedings	Author Guidelines		
SIGs	Using ACM Digital Library		
Conferences	All Holdings within the ACM Digital Li	brary	
Collections	ACM Computing Classification System	ACM Computing Classification System ΄ ☆	
People	Accessibility Statement	Feedback	
Join	Connect		
Join ACM			
Join SIGs	<b>f</b> ACM on Facebook		
Subscribe to Publications	X ACM DL on X		
Institutions and Libraries	in ACM on Linkedin		
	Send Feedback		
	Submit a Bug Report		

The ACM Digital Library is published by the Association for Computing Machinery. Copyright © 2025 ACM, Inc.

Terms of Usage | Privacy Policy | Code of Ethics







5 of 5 28/05/2025, 11:57 am