1. Privacy-Preserving Contact Tracing Protocol for Mobile Devices: A Zero-Knowledge Proof Approach

Liu, Joseph K. (1); Au, Man Ho (2); Yuen, Tsz Hon (2); Zuo, Cong (4); Wang, Jiawei (1); Sakzad, Amin (1); Luo, Xiapu (3); Li, Li (1); Choo, Kim-Kwang Raymond (5)

Source: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, v 13107 LNCS, p 327-344, 2021, *Information Security Practice and Experience - 16th International Conference, ISPEC 2021, Proceedings*; **ISSN:** 03029743, **E-ISSN:** 16113349; **ISBN-13:** 9783030932053; **DOI:** 10.1007/978-3-030-93206-0_20; **Conference:** 16th International Conference on Information Security Practice and Experience, ISPEC 2021, December 17, 2021 - December 19, 2021; **Publisher:** Springer Science and Business Media Deutschland GmbH

Author affiliation: (1) Department of Software Systems and Cybersecurity, Faculty of Information Technology, Monash University, Melbourne, Australia (2) The University of Hong Kong, Pok Fu Lam, Hong Kong (3) The Hong Kong Polytechnic University, Hung Hom, Hong Kong (4) Nanyang Technological University, Singapore, Singapore (5) The University of Texas at San Antonio, San Antonio, United States

Abstract: In this paper, we propose a privacy-preserving contact tracing protocol for smart phones, and more specifically Android and iOS phones. The protocol allows users to be notified, if they have been a close contact of a confirmed patient. The protocol is designed to strike a balance between privacy, security, and scalability. Specifically, the app allows all users to hide their past location(s) and contact history from the Government, without affecting their ability to determine whether they have close contact with a confirmed patient whose identity will not be revealed. A zero-knowledge protocol is used to achieve such a user privacy functionality. In terms of security, no user can send fake messages to the system to launch a false positive attack. We present a security model and formally prove the security of the protocol. To demonstrate scalability, we evaluate an Android and an iOS implementation of our protocol. A comparative summary shows that our protocol is the most comprehensive and balanced privacy-preserving contact tracing solution to-date. © 2021, Springer Nature Switzerland AG. (25 refs)

Main heading: Scalability
Controlled terms: Android (operating system) - Data privacy - Mobile security - Smartphones
Uncontrolled terms: Contact tracing - False positive - Privacy preserving - Security modeling - Smart phones - User privacy - Zero-knowledge proofs - Zero-knowledge protocols
Classification Code: 718.1 Telephone Systems and Equipment - 723 Computer Software, Data Handling and Applications - 723.2 Data Processing and Image Processing - 961 Systems Science
Database: Compendex
Data Provider: Engineering Village