Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 7079037, 4 pages
https://doi.org/10.1155/2018/7079037

Editorial

Rethinking Authentication on Smart Mobile Devices

Ding Wang[1], **Jian Shen**[2], **Joseph K. Liu**[3] and **Kim-Kwang Raymond Choo**[4]

[1]*School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China*
[2]*School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing, China*
[3]*Faculty of Information Technology, Monash University, Melbourne, Australia*
[4]*Department of Information Systems and Cyber Security, The University of Texas at San Antonio, San Antonio, TX 78249, USA*

Correspondence should be addressed to Ding Wang; wangdingg@pku.edu.cn

Received 14 November 2018; Accepted 14 November 2018; Published 18 December 2018

1. Introduction

Rapid advances in wireless technologies (e.g., LTE, LTE-A, WiMAX, 3G, Bluetooth, ZigBee, Z-Wave, and LoRaWAN) have partly contributed to the proliferation of smart mobile devices (e.g., sensors), unmanned vehicles, wearable and embedded devices, and so on. The amount and nature of communications and transactions on such devices and the underpinning systems require a secure and effective authentication mechanism to prevent unauthorized access from illegitimate entities (including both devices and users).

Authentication has been widely deployed to prevent unauthorized access and, in many cases, is also the primary line of defense. A large number of authentication mechanisms and schemes exist for conventional systems, but they may not be suitable for the smart mobile computing paradigm. Firstly, smart mobile devices generally have limited computation and storage and energy capabilities (in comparison to servers, personal computers and laptops), and thus deploying authentication schemes that employ expensive cryptographic primitives will not be viable. Secondly, smart mobile devices are typically small devices with a small screen, keyboard, and so forth, and thus existing authentication schemes may not be sufficiently user-friendly. Thirdly, smart mobile devices often deal with sensitive applications, activities, and data (e.g., location, preferences, and physical condition), and thus privacy demands are much more stringent than traditional authentication schemes. Consequently, it is necessary to perform a critical rethink the way we perform authentication for smart mobile devices and promote new methods that are both robust and easy to use, in order to minimize impact on the user's primary task.

This special issue aims to provide a forum for researchers to publish and exchange their recent research ideas and results about authentication on smart mobile devices. The following 20 papers were selected for inclusion in this special issue after several rounds of reviews by experts in the respective domains. The topics covered in the accepted papers range from attacks against fingerprint sensor hardware, biometric template protection, privacy-preserving message authentication, new lightweight cryptographic primitives (e.g., random number generation and oblivious transfer from lattice-based cryptography) for authentication, to various authentication schemes (one-factor, two-factor, and three-factor) designed for varied specific environments (such as Cloud, RFID, Vehicular, and Wireless Sensor Networks).

2. In This Special Issue

The paper entitled "Attack Potential Evaluation in Desktop and Smartphone Fingerprint Sensors: Can They Be Attacked by Anyone?" by I. Goicoechea-Telleria et al. explains how one can hack into a fingerprint sensor using fake fingers made of Play-Doh and other easy-to-obtain materials. The authors also perform three evaluations in order to demonstrate the attacks on desktop fingerprint sensors and smartphones with embedded sensors, using 15 simulated attackers with no prior background in biometrics. The authors also analyze the attack potential of each of the presented case, based on ISO/IEC 30107-3.

The paper entitled "Biometrics Based Privacy-Preserving Authentication and Mobile Template Protection" by W. Yang et al. presents a new cancelable fingerprint template, which not only mitigates the negative effect of nonlinear distortion by combining multiple feature sets, but also defeats ARM attacks through a proposed feature decorrelation algorithm. Experimental results on public databases and security analysis show the validity of the proposed cancelable template.

The paper entitled "Muscle Activity-Driven Green-Oriented Random Number Generation Mechanism to Secure WBSN Wearable Device Communications" by Y. Cao et al. presents a muscle activity-driven green-oriented random number generation mechanism for wireless body sensor network (WBSN). Specifically, the mechanism uses the human muscle-activity as the green energy resource to generate random numbers (RNs). In comparison to other methods, their scheme could generate random numbers with comparable performance but at a higher speed (128 bits per second).

The paper entitled "Oblivious Transfer via Lossy Encryption from Lattice-Based Cryptography" by Z. Li et al. presents an efficient authentication protocol by improving the performance of the UC-secure OT protocol. The authors first design a multibit lossy encryption under the decisional learning with errors (LWE) assumption and then develop a new variant of UC-secure OT protocol for authenticated protocol via lossy encryption scheme. Additionally, the proposed OT protocol is shown to be secure against semihonest (static) adversaries in the common reference string (CRS) model within the UC framework.

The paper entitled "Efficient Message Authentication Scheme with Conditional Privacy-Preserving and Signature Aggregation for Vehicular Cloud Network" by Y. Xie et al. gives an efficient message authentication in a Vehicular cloud network (VCN) setting. The scheme is shown to be secure and achieves conditional privacy-preserving. Compared with other similar conditional privacy-preserving authentication schemes, the proposed scheme has better performance for both computation and communication. Simulation analysis further demonstrates that the new scheme has reduced verification loss rate and message delay.

The paper entitled "Secure Certificateless Authentication and Road Message Dissemination Protocol in VANETs" by H. Tan et al. presents a certificateless authentication and road message dissemination protocol for a VANET environment. In their scheme, the certificateless signature and the relevance feedback mechanism are adapted for authentication and group key distribution. Subsequently, a message evaluating and ranking strategy is introduced. The security analysis shows that the proposed protocol achieves the desirable security properties.

The paper entitled "An Anonymous Authentication Protocol Based on Cloud for Telemedical Systems" by W. Li et al. introduces an anonymous authentication protocol for cloud-based telemedical systems. Compared with similar related works, the proposed scheme allows patients to remotely access medical services with privacy and achieves better efficiency. A formal security proof is also presented and the performance evaluation suggests better efficiency.

The paper entitled "A Provably Secure Anonymous Authenticated Key Exchange Protocol Based on ECC for Wireless Sensor Networks" by K. Zhang et al. presents an anonymous authenticated key exchange protocol, based on Elliptic Curves Cryptography (ECC). This protocol provides strong user anonymity, such that even the gateway node and the sensor nodes do not know the real identity of the user. The security of the proposed protocol is proven in a well-defined security model under the CDH assumption. Compared with other related protocols, their protocol is efficient in terms of communication and enjoys stronger security.

The paper entitled "An Enhanced User Authentication Protocol Based on Elliptic Curve Cryptosystem in Cloud Computing Environment" by C. Wang et al. revealed security weaknesses in Amin et al's protocol. Then, the authors design a secure authentication protocol and use BAN logic and heuristic analysis method to prove the security of the proposed protocol.

In the paper "Cryptanalysis and Security Enhancement of Three Authentication Schemes in Wireless Sensor Networks", W. Li et al. cryptanalyze and enhance three password-based user authentication schemes designed for WSNs (i.e., several security vulnerabilities loopholes are in the first protocol, the second protocol is not able to achieve the claimed security goal of forward secrecy and is vulnerable to user anonymity violation and offline password guessing attacks, and the third anonymous scheme does not provide forward secrecy and user-friendliness). In addition, by adopting the "perfect forward secrecy (PFS)" principle proposed by Ding Wang et al. (IJCS, 2014), the authors provide several effective countermeasures to mitigate the identified weaknesses. To test the necessity and effectiveness of their countermeasures, the authors conduct a comparison of 10 representative schemes in terms of the underlying cryptographic primitives used for realizing forward secrecy.

The paper entitled "Trusted Authority Assisted Three-Factor Authentication and Key Agreement Protocol for the Implantable Medical System" by D. Mao et al. proposed an improved AKA scheme which achieves strong security features including user anonymity and known key security. It is provably secure under the Real-Or-Random model. Moreover, a comprehensive heuristic security analysis shows that their scheme can resist various attacks and satisfy the desired requirements. Finally, the performance analysis shows that the superiority of their protocol is suitable for the implantable medical system.

The paper entitled "A Secure Three-Factor Multiserver Authentication Protocol against the Honest-But-Curious Servers" by H. Gao et al. took Chengqi Wang et al.'s protocol (PLoS ONE, 2016) as an example, to exhibit how an honest-but-curious server can attack their protocol. To remedy this weakness, a novel three-factor multiserver authentication protocol is presented. By introducing the registration centre into the authentication process, the new protocol can resist the passive attack from the honest-but-curious servers. Security analysis is given to demonstrate the correctness and validity of the new protocol. Compared with related protocols, the proposed protocol possesses more security features

and practical functionalities than others at a relatively low computation cost and communication cost.

The paper entitled "Efficient Multifactor Two-Server Authenticated Scheme under Mobile Cloud Computing" by Z. Han et al. proposed a Kerberos-like authentication method using two servers (adding another authentication server in addition to the Web server) and considering multiple factors to avoid the leakage of users' private data stored on the server side. The proposed scheme aims at the security issue of fingerprint information in the mobile payment environment. The main idea of the proposed solution is to separate certain security-related functions from a Web server to an independent server.

The paper entitled "The Research of Mobile Location Privacy Protection Access Control Method Based on Game Theory" by L. Zheng et al. develops a mobile location privacy access control method based on game theory aiming at the leakage of private information in the mobile location of the Internet of Things users. It controls access behaviour of the privacy information according to the specified location access policy from the perspective of the service provider. The access control can guarantee the server to make a dynamic response to illegal access behaviour to the private information and at the same time, according to tolerance setting, avoid the indirect leakage of mobile location and privacy information caused by the superposition of information.

The paper "A Data Leakage Prevention Method Based on the Reduction of Confidential and Context Terms for Smart Mobile Devices" by X. Yu et al. suggests a model of Data Leakage Protection Based on Context (or CBDLP), a data leakage prevention model based on confidential terms and their context terms, which can detect the rephrased confidential contents effectively. In CBDLP, a graph structure with confidential terms and their context involved is adopted to represent documents of the same class, and then the confidentiality score of the document to be detected is calculated to justify whether confidential contents is involved or not. Based on the attribute reduction method from rough set theory, the authors further present a pruning method. According to the importance of the confidential terms and their context, the graph structure of each cluster is updated after pruning.

The paper "LIP-PA: A Logistics Information Privacy Protection Scheme with Position and Attribute-Based Access Control on Mobile Devices" by Q. Gao et al. constructs a logistics information privacy protection scheme with position and attribute-based access control on mobile devices. First, in order to realize fine-grained access control of encrypted logistics information, the authors adopt ciphertext-policy attribute-based encryption (CP-ABE) scheme, which encrypts segmented logistics information in different access policies. Different couriers can only decrypt different segments of the express order in accordance with their respective attributes. Second, the authors apply position-based key exchange, which uses the courier's physical position information as the credential, to realize position-based access control on couriers. Third, the authors utilize public key encryption to achieve the confidentiality of personal information. Meanwhile, the authors use the digital signature to ensure the verifiability of the parcel and the undeniability of customers.

The paper "Multidevice Authentication with Strong Privacy Protection" by J. Hajny focuses on the card-based physical access control systems and proposed a novel cryptographic scheme based on efficient zero-knowledge proofs and Boneh-Boyen signatures. The proposed scheme is provably secure and provides the full set of privacy-enhancing features that is the anonymity, untraceability, and unlinkability of users. Furthermore, the proposed scheme supports distributed multidevice authentication with multiple RFID (Radio-Frequency IDentification) user devices. This feature is particularly important in applications for controlling access to dangerous sites where the presence of protective equipment is checked during each access control session.

The paper "Identity-Based Fast Authentication Scheme for Smart Mobile Devices in Body Area Networks" by C. Wang et al. proposes an identity-based fast authentication scheme for smart mobile devices in wireless body area networks (WBANs). The scheme can shorten the time of device authentication in an emergency to achieve fast authentication. The analysis of the scheme shows the security and efficiency of the proposed scheme.

The paper "An SDN-Based Connectivity Control System for Wi-Fi Devices" by T. Nguyen-Duc and T. Kim introduces a remote connectivity control system for Wi-Fi devices based on software-defined networking (SDN) in a wireless environment. The main contributions of the proposed system are twofold: (i) it enables network owner/administrator to manage as well as approve connection request from Wi-Fi devices through remote services, which is essential for easy connection management across diverse IoT devices; it also allows fine-grained access control at the device level through remote control. They describe the architecture of SDN-based remote connectivity control of Wi-Fi devices.

The paper "Lightweight Cryptographic Techniques for Automotive Cybersecurity" by A. K. Jadoon et al. presents a survey about developments in vehicular networks from the perspective of lightweight cryptographic protocols and privacy preserving algorithms. Meanwhile, the authors increase awareness about the possible threats to the future automotive industry and give an interesting overview of lightweight cryptographic solutions to these threats. In all, the paper deals with a very interesting and up to date subject: Cryptographic Techniques for Automotive Cyber Security.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

In closing, the guest editors would like to thank all authors who have submitted their papers to this special issue. We would also like to appreciate all the precious time and efforts that the reviewers devoted to the review process of these submissions. The launch of this special issue was in

part supported by the National Key Research and Development Plan under Grants Nos. 2016YFB0800600, and by the National Nature Science Foundation of China under Grant No. 61802006, No. U1836115, and No. 61672295. It is our hope that this special issue will advance the understanding and research of User Authentication on Smart Mobile Devices. We hope you enjoy the papers.

Ding Wang
Jian Shen
Joseph K. Liu
Kim-Kwang Raymond Choo