Wireless Communications and Mobile Computing

WILEY | Hindawi

Special Issue on
Rethinking Authentication on Smart Mobile Devices 2020

CALL FOR PAPERS

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

Authentication, as a first line of defense, 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, and 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 personal computers and laptops), and thus authentication schemes that employ expensive cryptographic primitives will not be viable. Secondly, smart mobile devices are typically small devices with a small screen, keyboard, etc., and thus existing authentication schemes may not be sufficiently user-friendly. Thirdly, smart mobile devices often deal with very sensitive applications, activities, and data (e.g., location, preferences, and physical conditions), and thus privacy demands are much more stringent than traditional authentication schemes. Consequently, it is necessary to perform a critical rethinking on authentication for smart mobile devices, and promote new methods that are both robust, easy to use, and minimize the impact on users' primary tasks.

This Special Issue aspires to bring together contributions from researchers and practitioners working in the broad area of entity authentication. We seek high-quality articles presenting state-of-the-art authentication mechanisms, frameworks, protocols, algorithms, policies, user studies, as well as threat models for mobile computing environments.

Potential topics include but are not limited to the following:

- Mutual authentication on smart mobile devices
- Group authentication on smart mobile devices
- Anonymous authentication on smart mobile devices
- Implicit authentication on smart mobile devices
- Evaluation metrics for authentication schemes on smart mobile devices
- Foundational principles for authentication on smart mobile devices
- Impact of authentication on a mobile user's primary task
- Surveys and comparisons of known authentication techniques for smart mobile devices
- Existing authentication techniques applied in specific mobile applications
- New paradigms for authentication on smart mobile devices
- New lightweight cryptographic primitives for mobile authentication
- New device to device authentication techniques for mobile environments
- New user authentication techniques for mobile environments
- Authentication for mobile cloud computing
- Authentication for data aggregation on smart mobile devices
- Attacks and challenges on authentication for smart mobile devices
- Privacy enhancing technologies for authentication on smart mobile devices

Authors can submit their manuscripts through the Manuscript Tracking System at https://mts.hindawi.com/submit/journals/wcmc/rasmd20/.

Papers are published upon acceptance, regardless of the Special Issue publication date.

Lead Guest Editor
Ding Wang, Nankai University, Tianjin, China
wangding@nankai.edu.cn

Guest Editors
Kun Sun, George Mason University, Virginia, USA
ksun3@gmu.edu

Qi Jiang, Xidian University, Xian, China
jiangqixdu@xidian.edu.cn

Submission Deadline
Friday, 7 August 2020

Publication Date
December 2020