Wireless Communications and Mobile Computing

WILEY | Hindawi

Special Issue on

Resilient and Secure Mobile Systems and Networks

CALL FOR PAPERS

The improved level of sophistication and computing power of current mobile systems and networks allows the development of complex and always connected applications, like mobile ticketing and banking that are increasingly playing a key role in our everyday business and entertainment life. More importantly, several research proposals envision the use of mobile systems in critical scenarios, for example, unmanned smart mobility, large-scale mobile cloud computing systems, wireless control of robots and UAVs, ambient assisted living, mobile crowd-sensing, and inclusion of humans in the computation loop, remote surgery, and so forth. In these scenarios, a device freeze or a network failure, either accidental or malicious, could result in a major loss or hazard, such as an e-health application not being able to report a critical alert to the medical center on time.

However, the increased level of sophistication makes these systems more and more vulnerable to accidental failures and security attacks. A first example of mobile malware, named Cabir and affecting Symbian OS devices, emerged in 2004. Since then, there has been a proliferation of worms, trojans, and malware affecting mobile systems, such as HummingBad which has recently infected over 10 million Android devices.

A variety of research studies have been produced proposing methods, proof-of-concept prototypes, and disciplines to model, design, develop, verify, and maintain mobile systems and services. Despite these efforts, it is still unclear how the resiliency and security of mobile systems and networks are affected by the continuous increase in their complexity, and if current solutions are sufficient to increase resiliency and security levels. This is with respect to not just normal communications but also life-critical and business-critical activities where mobile systems are in increasing usage.

The goal of this special issue is to put on the foreground all the above issues, by providing a consistent source of timely information and research advances in the area of resilient and secure mobile systems and networks, by identifying open research issues, discussing the limitations and/or advantages of existing solutions, and/or proposing original and innovative solutions in this challenging arena.

Potential topics include but are not limited to the following:

- Design principles, models, and techniques for building resilient, secure mobile systems
- Formal and runtime verification of mobile cloud systems and services
- End-to-end approaches for the quality of experience (QoE) of mobile services
- Autonomous systems for resiliency and security
- Mobile middleware architectures and standards for heterogeneous, resilient ad-hoc, or infrastructure-based networks
- Architectures for resiliency and security monitoring in mobile systems
- Resiliency and security measurement studies of mobile systems and services
- Cellular networks and mobile phones resiliency and security issues
- Real-world applications and prototypes of resilient/or secure mobile systems
- Resilience of evolvable/adaptive mobile systems and services
- Model-driven engineering of resilient secure mobile systems
- Proposals for increasing security and resiliency of mobile systems, also considering usability and accessibility aspects
- Testing methodologies for assessing the resilience and security of mobile cloud services and applications
- Virtualization techniques for improving the resilience of mobile services
- Metrics analyzing the crowd in terms of security and behavioral profiles
- Metrics investigating how to measure the resiliency of mobile crowd sensing platforms

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

Lead Guest Editor
Marcello Cinque, Federico II University of Naples, Naples, Italy
macinque@unina.it

Guest Editors
Carlos R. Dominguez, University of Granada, Granada, Spain
carlosrodriguez@ugr.es

Luca Foschini, University of Bologna, Bologna, Italy
luca.foschini@unibo.it

Veena Mendiratta, Nokia Bell Labs, New Jersey, USA
veena.mendiratta@nokia.com

Manuscript Due
Friday, 11 August 2017

First Round of Reviews
Friday, 3 November 2017

Publication Date
Friday, 29 December 2017