

CALL FOR PAPERS

Submission deadline:
June 29, 2018

MobiSec 2018: The 3rd International Symposium on Mobile Internet Security

Cebu, Philippines, August 29 – September 1, 2018

Organized By

KIISC Research Group on 5G Security
Department of Computer Engineering, University of San Carlos

General Co-Chairs

Fang-Yie Leu (ThungHai University, Taiwan)
Isun You (Soonchunhyang University, S. Korea)

Program Co-Chairs

Hsing-Chung Chen (Asia University, Taiwan)
Tianhan Gao (Northeastern University, China)

Local Arrangement Chairs

C. M. Gohetia
(University of San Carlos, Philippines)

L. E. Saavedra
(University of San Carlos, Philippines)

International Advisory Committee

Karl Andersson
(Luleå Univ. of Technology, Sweden)

Kyung-Hyune Rhee
(Pukyong National Univ., South Korea)

Antonio Skarmeta
(Universidad de Murcia, Spain)

Huachun Zhou
(Beijing Jiaotong University, China)

Publicity Chair

Nan Guo (Northeastern University, China)

Publication Chairs

Yuh-Shyan Chen
(National Taipei University, Taiwan)

Igor Kotenko
(SPIIRAS and ITMO University, Russia)

Zheng Yan
(Xidian Univ., China and Aalto Univ., Finland)

Web Chair

Vishal Sharma
(Soonchunhyang University, South Korea)

Program Committee

Ramon Alcarria

Hiroaki Anada

Benjamin Aziz

Joonsang Baek

Andrey Chechulin

Seong-je Cho

Luigi Coppolino

Salvatore D'Antonio

Jianfeng Guan

Hsu-Chun Hsiao

Antonio J. Jara

Shinsaku Kiyomoto

Igor Kotenko

Kyung Ho Lee

Yong-Hwan Lee

Alessio Merlo

Evgenia Novikova

Vladimir A. Oleshchuk

Roland Rieke, Igor Saenko,

Sang Uk Shin

Kunwar Singh, Fei Song

Chul Sur, Chunhua Su

Xin Su, Kunlin Tsai

Isaac Woungang

Toshihiro Yamauchi

Neil Yen, Jeong Hyun Yi

Baokang Zhao

During the past two decades, mobile internet technologies have been dramatically growing while leading to a paradigm shift in our life. Despite their revolution, mobile internet technologies open doors to various security threats, which should be addressed to keep mobile Internet environments to be secure and trust. Even worse, the latest technologies (e.g. distributed mobility management, mobile internet of things, 5G networks, and so forth) continuously have introduced new security challenges. Therefore, it is of paramount importance to study mobile internet security. The purpose of MobiSec 2018 is to bring together the academic and industry working on different aspects, exchange ideas, and explore new research directions for addressing the challenges in mobility internet security. MobiSec 2018 also aims to publish high quality papers, which are closely related to various theories and practical applications in mobility management to highlight the state-of-art research. In spite of focusing on security aspects, this symposium welcomes papers which are related to mobile internet technologies. We expect that MobiSec 2018 will be a trigger for further research and technology improvements related to this important subject.

Topics (not limited to):

- Vulnerabilities and threats in mobile internet and networks
- Security issues and protocols for mobile internet and networks
- Privacy and trust for mobile internet and networks
- Security for cross-layer handover
- Security for vertical handover in heterogeneous networks
- New advances in the AAA infrastructure and EAP
- Security for 4G and 5G networks
- Security for mobile WIMAX and WIBRO, and WIFI
- Security for IoT and wearable devices
- Security for mobile internet services and applications
- Advances in mobile internets and networks
- Others and emerging new topics

PAPER SUBMISSION GUIDELINES:

Authors are invited to submit original papers: they must not substantially duplicate work that any of the authors have published elsewhere or have submitted in parallel to any other conferences that have proceedings. An accepted paper must be registered before the registration deadline and presented at the workshop. Failure to register before the deadline will result in automatic withdrawal of the paper from the workshop proceedings and the program.

The submission of contributions to MobiSec 2018 must occur through the workshop submission system: <https://easychair.org/conferences/?conf=mobisec2018>

- The submission file is in PDF or PS file format produced via the EasyChair Latex Class file (US letter size) [Available at <http://jowua.yolasite.com/resources/easychair.zip>]
- Each paper should be at least 5 pages long based on the EasyChair style.
- Submission of a paper implies that should the paper be accepted, at least one of the authors will register and present the paper at the workshop)

PROCEEDINGS & POST PUBLICATIONS

Proceedings of MobiSec 2018 will be available to the attendees.

All accepted papers will be published in *Research Briefs on Information & Communication Technology Evolution (ReBICTE)* and *Journal of Internet Services and Information Security (JISIS)*.

All the accepted papers will be invited to be extended and submitted to the followings:

- International Journal of Ad Hoc and Ubiquitous Computing and IEEE Access special issues
- Special Issue on Secure Computation on 4G/5G Enabled Internet-of-Things Wireless Communications and Mobile Computing (SCIE-1.899) <http://www.hindawi.com/journals/WCMC/si/513209/cfp/>
- Special Issue on Internet of Things for Smart Homes Sensors (SCIE-2.677) http://www.mdpi.com/journal/sensors/special_issues/IoT_smart_home.

Contact: For further information, please contact the cyber chair via cyberchair.mobisec@gmail.com.

Submission link: <https://easychair.org/conferences/?conf=mobisec2018>

Conference website: <http://isyou.info/conf/mobisec18/>