The 7ᵗʰ International Symposium on
Security and Privacy in Next-Generation Networks (SPNGN 2016)

In association with

13th International Conference on
Information Technology : New Generations

ITNG 2016

April 11-13, 2016, Las Vegas, Nevada, USA
www.itng.info

King Saud University

Center of Excellence in Information Assurance

ORGANIZING COMMITTEE

Kashif Saleem, Center of Excellence in Information Assurance (CoEIA), King Saud University, KSA.

Abdelouahid Derhab, CoEIA, King Saud University, KSA.

Haider Abbas, CoEIA, King Saud University, KSA.

Basit Shahzad, King Saud University, KSA.

TECHNICAL PROGRAM COMMITTEE

Abdulrahman Mirza, King Saud University, KSA

Adel Ali Ahmed, King Abdulaziz University, KSA

Al-Sakib Khan Pathan, Islamic University in Madinah, KSA

Alois Paulin, Technische Universität München-KRI, Germany

Amjad Gawanmeh, Khalifa University, UAE

Armin Schneider, Klinikum r. d. Isar der Technischen Universität München, Germany

Christoph Thuemmler, Edinburgh Napier University, UK

Fernando Koch, Samsung Research Institute Brazil

Jalal Al-Muhtadi, CoEIA, King Saud University, KSA

Joel Rodrigues, Instituto de Telecomunicações, University of Beira Interior, Portugal

Kalloniatis Christos, University of the Aegean, Greece

Mehmet Orgun, Macquarie University, Australia

Mohamed H. Eldefrawy, CoEIA, King Saud University, KSA

Mohd Adib Sarijari, University Technology Malaysia, Johor, Malaysia

Mohssen Mohammed Zain Elaabdeen, Al-Imam Muhammad Ibn Saud Islamic University, KSA

Mubashir Rehmani, COMSATS Institute of Information Technology , Pakistan

Muhammad Imran, King Saud University, KSA

Muhammad Khurram Khan, CoEIA, King Saud University, KSA

Yacine Challal, SURES Research Team, Ecole nationale Supérieure d'Informatique, Algiers

Yaqoub S. Baguda, King Abdulaziz University, KSA

Scope:
Next Generation Network (NGN) nowadays plays an important role in the sector of telecommunication and has huge importance for future research. NGN communication is making the world's life easier by giving round the clock connectivity with high data transfer. The NGN communication includes number of promising architectures as Internet of things, Personal wireless networks: body area wireless sensor network, wireless sensor and actuator network, Wireless Mesh networks, Next generation Internet, Cloud computing, LTE advanced, Machine-to-Machine network. The NGN communication must be secure and preserve the privacy of its users and requires innovative methods to address the continuous and emerging security threats.

This track is a forum for researchers, academics, and industries to debate the different issues related to security and privacy in next-Generation Networks, discuss relevant theoretical and practical solutions, and explore areas related to the theory, applications, development, experiences, and evaluation studies.

Topics:
Topics of the track consist of all aspects related to security and privacy issues for Next generation. They include but are not limited to:

- Vulnerability assessment
- Mobile Identity management
- Authentication, security access policies
- Privacy-respecting Authentication
- Privacy issues in the Internet of Things
- Privacy issues in wireless networks
- Security Management of Machine-to-Machine network

- Forensics analysis
- Remote and wireless-based Biometrics system
- Mobile malware
- Mobile botnets
- Security and privacy issues in Smartphones
- Intrusion and fraud detection
- Socio-economic issues

Paper Submission
Papers should be original and contain contributions of theoretical or experimental nature, or be unique experience reports. Interested authors should submit a 6-page summary of their original and unpublished work including 5 keywords. Electronic submission in the PDF, PS or MS Word format is strongly encouraged. For instructions on electronic submissions, Click here.

Evaluation Process
Papers will be evaluated for originality, significance, clarity, and soundness. Per ITNG policy, except for invited papers, all papers will be reviewed by at least two independent reviewers. Accepted papers will be published in the conference proceedings with an ISBN.

Consideration for Journals
Best papers will be selected and considered for publication in the following Special issues, after further extension and normal peer reviewed process according to Journal policy

- Special issue of **ANNALS OF TELECOMMUNICATIONS** on
  "Security and Privacy Issues in Cloud Computing" (CONFIRMED)
- Special issue of **Mobile Information Systems** on
  "Fundamental Issues in Mobile Healthcare Information Systems" (CONFIRMED)

Important Dates
Paper Submission: November 27th, 2015 (Extended)
Acceptance Notification: December 18th, 2015
Advance Registration: January 15th, 2016
Camera Ready Submission: February 19th, 2016