IEEE Communications Magazine
Feature Topic “5G Security: Can 5G Be Verifiably Secure?” Call for Papers

5G heralds the advent of the true convergence of IT and Wireless and Wireline networks. In the midst of this transition, security and the operationalization of the technology are critical areas. Traditional security has seen a focus on network access and communication channel protection, but the new system will challenge the emerging standards and requires something beyond channel- and component-level analysis. Network slicing, e-SIM, MEC along with SDN/NFV and massive IoT pose new challenges that are not addressed with the legacy understanding of network security. This feature topic aims at putting together various paradigms and techniques needed to address 5G security in a holistic manner.

How to assess the fundamental security of deployed 5G networks? Implementation security seems to be crucial. The dependence on source code requires a focus on software assessment methods, and yet these are closely guarded as a manufacturer's intellectual property. Can secure and trustworthy software and hardware platforms, such as operating systems, hypervisors and CPUs, significantly protect against source code vulnerabilities? Can their (lifecycle) security be practically verified, possibly by formal methods?

Is component-level analysis, as seen in engineering requirements, sufficient? Or, will the 5G system need to be deployed as an integrated and functional system alongside its underlying platforms to be truly assessed for the ultimate security outcome? How much benefit can threat and trust modelling along with new deployment architectures make to the security of 5G?

There are a lot of areas for exploration but the focus here is on delivering a secure 5G system to the market and ensuring an overall secure outcome for mobility consumers, regardless of the underlying complexity. This focus may, arguably, be beyond what has been practiced to date, but is important to explore in this feature. Analysis of the current security framework trends and proposals from organisations such as GSMA, 3GPP and NGMN is also relevant.

Potential topics include, but are not limited to:

- comparative analysis of existing security certification programs towards a provably secure 5G technology and implementation
- methods and techniques for verifying supply chain integrity of 5G products.
- techniques towards independent and trustworthy security evaluation and assertion of 5G product integrity
- formal method analysis and design of 5G protocol security
- threat modelling techniques for the evaluation of 5G end-to-end systems and for 5G full stack, hardware and software included

- expected adversarial methods for proposed future 5G architectures
- security testing for end-to-end network slices
- impact of hardware side-channel security attacks on 5G deployments
- secure architectures towards 'zero-trust' 5G deployments
- security orchestration across all components of a fully deployed 5G system
- fundamentals for establishing a 5G security reference model and data set, enabling repeatable results, research and analysis

Submission Guidelines

Manuscripts should conform to the standard format as indicated in the Information for Authors section of the Manuscript Submission Guidelines. Please, check these guidelines carefully since they have been updated recently.

All manuscripts to be considered for publication must be submitted by the deadline through Manuscript Central. Select the "March 2020/5G Security" topic from the drop-down menu of Topic/Series titles. Please observe the dates specified here below noting that there will be no extension of submission deadline.

Important Dates

Submissions Due: 15 September 2019
Decision Notification: 15 December 2019
Final Manuscript Due: 15 January 2019
Publication Date: March 2020

Guest Editors

Marc Kneppers (Lead Guest Editor)
Chief Security Architect, TELUS Fellow
TELUS Communications, Canada

Imad Elhajj
Professor, Department of Electrical and Computer Engineering
American University of Beirut, Lebanon

Jovan Golic
Prof. Dr., Senior Technical Leader
Telecom Italia