Emerging Attacks and Solutions for Secure Hardware in the Internet of Things

GUEST EDITORS
Chip-Hong Chang, Nanyang Technological University, Singapore, echchang@ntu.edu.sg
Marten van Dijk, University of Connecticut, USA, marten.van_dijk@uconn.edu
Ulrich Rührmair, Ruhr-University Bochum, Germany, ruehrmair@ilo.de
Mark M. Tehranipoor, University of Florida, USA, tehranipoor@ece.ufl.edu

SCOPE
This special issue is concerned with the specific threat landscape and new, innovative security solutions for the upcoming Internet of Things (IoT) era. As predicted by Gartner in 2015, there will be around 21 billion devices connected in the IoT by 2020, creating a spending of about 3,000 billion dollars per year. This makes the IoT clearly one of the most massive and impactful endeavours of our time. Security failures of its endpoints will not just be tolerable nuisances, but will personally affect billions of users, causing immediate risks to privacy, savings, well-being, or even their lives.

At the same time, the development of appropriate security strategies seems to lag behind the rapid, actual spread of the IoT. The security community has clearly recognized that many of the established, classical recipes do not transfer easily (or not at all) to an IoT-setting. But in many cases, no fully convincing substitute strategies have been developed yet. This is partly due to the special threat landscape in the IoT: It connects billions of low-cost devices, which often have no suitable means for tamper-protection or strong computational resources on board; in the worst case, some of them may not even carry classical ICs. Establishing security under such circumstances is more than demanding, leading to a host of vital problems and open questions. Some of the most pressing include:

- How can we get individual cryptographic keys into billions of hardware devices?
- How can we securely identify low-cost, low-resource hardware systems remotely over digital channels? Can we even identify systems that do not carry digital signal processor or memory on board, or merely passive devices powered by scavenged energy?
- How can we realize tamper-protection in small, mobile and lightweight devices? How can we guarantee and remotely verify the functionality and integrity of connected devices?
- How can we establish long-term security and confidentiality with computationally constrained hardware?
- How can we protect and safeguard physical data storage in typical IoT-settings?
- How can we preserve the privacy of users in pervasive IoT-scenarios?

It seems generally agreed that new strategies must be developed to fully address these issues. The purpose of this special issue is to foster and bring to prominence such promising novel approaches. Suitable topics include, but are explicitly not limited to:

- Physical unclonable functions (and new/emerging variants thereof)
- Device fingerprinting and hardware forensics
- Use of emerging computing technologies in security (incl. quantum computing)
- New materials in hardware security
- Nanophysics and nanotechnology for secure hardware (incl. quantum mechanical devices)
- Security of sensors and sensor networks
- New techniques for tamper sensing and tamper protection
- Physical attacks in IoT-settings (fault injection, side-channels, etc.), including new attack vectors
- Biometric approaches for IoT-security
- Lightweight security solutions, primitives and protocols
- Security of reconfigurable and adaptive hardware platforms
- Protocols and application scenarios for emerging security primitives
- Trust and trusted hardware in the IoT
- Formal mathematical treatments, standardization, or categorization of the area (incl. surveys and solicitation of knowledge papers)
**SUBMISSION GUIDELINES**

Submissions must possess an inherent and genuine connection to IoT-security. Submission without such connection will be kindly redirected to authors for consideration of regular submission. Authors are invited to submit original research contributions by following the detailed instructions given in the “Information for Authors” under [https://www.computer.org/web/tdsc/author](https://www.computer.org/web/tdsc/author). Manuscripts should be submitted via Scholar One (Manuscript Central) at [https://mc.manuscriptcentral.com/tdsc-cs](https://mc.manuscriptcentral.com/tdsc-cs). Questions about the special issue should be directed to the Guest Editors.

**IMPORTANT DATES**

<table>
<thead>
<tr>
<th>Event</th>
<th>Date</th>
<th>Event</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper submission deadline (ext.)</td>
<td><strong>July 31, 2017</strong></td>
<td>Final manuscript due</td>
<td>February 15, 2018</td>
</tr>
<tr>
<td>First round of reviews</td>
<td>October 15, 2017</td>
<td>Publication</td>
<td>IEEE Explore as soon as authors approve galley proofs</td>
</tr>
<tr>
<td>Revised paper submission</td>
<td>November 31, 2017</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Final notification</td>
<td>December 15, 2017</td>
<td>Expected inclusion in issue</td>
<td>June 2018</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event</th>
<th>Date</th>
<th>Event</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revised paper submission</td>
<td></td>
<td>Expected inclusion in issue</td>
<td>June 2018</td>
</tr>
</tbody>
</table>