# CALL FOR PAPERS

## *IEEE Transactions on Computers*

### Special Section on: Secure Computer Architectures

Nowadays, computer architectures are profoundly affected by a new security landscape, caused by the dramatic evolution of information technology over the past decade. First, secure computer architectures have to support a wide range of security applications that extend well beyond the desktop environment, and that also include handheld, mobile and embedded architectures, as well as high-end computing servers. Second, secure computer architectures have to support new applications of information security and privacy, as well as new information security standards. Third, secure computer architectures have to be protected and be tamper-resistant at multiple abstraction levels, covering network, software, and hardware. This Special Section from Transactions on Computers aims to capture this evolving landscape of secure computing architectures, to build a vision of opportunities and unresolved challenges. It is expected that contributed submissions will place emphasis on secure computing in general and on engineering and architecture design aspects of security in particular.

IEEE Transactions on Computers seeks original manuscripts for a Special Section on Secure Computer Architectures tentatively scheduled to appear in the July 2017 issue. The topics of interest for this special section include:

**Cryptographic Engineering:**

- Cryptographic Primitives
- Homomorphic Computing and Multiparty Computing
- Scalability Issues of Server-level Secure Computing
- High Performance/Low Power Cryptography
- Oblivious RAM

**Secure Architectures:**

- Computing Architectures for Isolation
- Smartphone Security
- Embedded Systems Security
- Secure Processors and Systems
- Hardware Security
- Secure Virtualization and Memory Safety

**Application-specific Architecture Optimizations:**

- Instruction-Sets for Security and Cryptography
- Dedicated and Protected Storage
- Secure Computer Interfaces

**Implementation Attacks:**

- Side-Channel Analysis
- Side-channel attacks and defenses
- Hardware Trojans and Backdoors
- Hardware Vulnerabilities - Counters, Caches, Shared Memory

**Design Tools for Secure Computing Architectures:**

- Security Simulation, Testing, Validation and Verification
- Metrics for Tamper Resistance
- Security Metrics
- Standards in Secure Computing

The submitted papers must describe original research which is not published nor currently under review by other journals or conferences. Extended conference papers should contain at least 50% substantially-new technical material and will pass through the normal review process. Authors are invited to submit manuscripts to *Transactions on Computers (TC)* at https://mc.manuscriptcentral.com/tc-cs. Please address all correspondence regarding this Special Section to the Guest Editors (email: tc2017secarch@gmail.com). To increase the impact and visibility of their work, interested authors of accepted papers will be invited to prepare a brief video of their manuscript to be published as supplemental material on the TC website.

**IMPORTANT DATES:**

- Submission deadline: **June 20, 2016 (extended)**.
- First decision to authors: August 31, 2016.
- Revision due: September 30, 2016.
- Acceptance notification: December 15, 2016.
- Publication material due: January 15, 2017.
- Special Section publication: July 2017.

**GUEST EDITORS:**

- Ruby Lee, Princeton University
- Patrick Schaumont, Virginia Tech
- Ron Perez, Cryptography Research Inc
- Guido Bertoni, ST Microelectronics