==========

Call for Chapters on the Security of Ubiquitous Computing Systems (UCS)

==========

Calendar:

Abstract submission deadline: 15th January 2018

Acceptance notification: 4th February 2018

Deadline for full chapter submission: 30th April 2018

Deadline for revised version: 25th June 2018

Estimated Publication: November 2018

Title of the book: Security of Ubiquitous Computing Systems (Working Title)

Editors:

Prof. Gildas Avoine, INSA, IRISA, Institut Universitaire de France, Rennes, France

Prof. Julio Hernandez-Castro, School of Computing, University of Kent, UK

Submission and Review procedure

Authors are invited to submit to cryptacus.editors@irisa.fr on or before January 15th, 2018 a 1-2 page chapter proposal clearly explaining the objectives, contents, structure and format of their proposed chapter. Authors will be notified by 4th of February, 2018 about the outcome of their abstract proposals and chapter guidelines will be sent accordingly.

In the second stage the selected authors will be invited to submit a full version of the book chapter. All chapters will be crossed reviewed. Based on the outcome of the review, the authors may be requested to revise their book chapters. The authors will then be invited to submit a camera-ready version.

It is expected that the book will have around 15 chapters, with an average 15 pages each.

Publisher

The editors are currently in negotiation with various prestigious publishing houses and the decision on the publisher will be discussed during the Nijmegen Cryptacus meeting in November 2017.

The book will be open access, and the associated costs will be covered by the Cryptacus project.

Topics

Any topic relevant to the Cryptacus project will be considered, including those in the following non-exhaustive list:

- Surveys of existing research-oriented and engineering-oriented literature about security and privacy in ubiquitous computing systems.
- How to analyze the security of ubiquitous computing systems (academia vs real life).
- Privacy in UCS: regulations and tools to enforce privacy.
- A catalogue of lightweight cryptographic primitives.
- Security of communication protocols (LoRaWAN, GlobalPlateform, etc.)
- Distance bounding protocols, industrial applications and theoretical developments.
- Side channels attacks against low-cost systems.
- From hardware to software attacks.
- State of the art on existing attacks and broken systems.
- General or multi-purpose tools and methodologies to attack UCS.
- Physically Unclonable Functions (PUFs), their current state, deployed implementations, and future evolutions.
- Security Certification for Ubiquitous Computer Systems.
- Attacks and tools against authentication protocols.
- Lightweight Cryptography: New primitives and new attacks.
- Random number generation and testing in embedded devices.
- Car security: Past achievements and current challenges.
- Smarthome security: Attacking from lightbulbs to smartlocks, and their impact in the IoT ecosystem.
- Security and privacy models in ubiquitous computing systems.
- Tools and developments for/in reverse engineering existing proprietary protocols.
- IoT forensics: the challenge of performing forensics with minimalistic data, and/or by aggregating multiple micrologs from different devices.
- Future trends in UCS.