Workshop on “Security Tools and Techniques for Internet of Things”

Co-located with the BodyNets conference

(Accepted papers will be published in the Journal of Biomedicine and Biotechnology, Impact Factor 1.25)

E-health systems have the objective to continuously monitor the state of patients in order to increase knowledge and understanding of their physical status. Being a system of systems, the Internet of Things (IoT) has to master the challenge of integrating heterogeneous systems across technology boundaries. Timely delivery of observation data is a key aspect to identifying potential diseases and anomalies. IoT systems are vulnerable to attacks since communication is mostly wireless and thus vulnerable to eavesdropping, things are usually unattended and thus vulnerable to physical attacks, and most IoT elements are short on both the energy and computing resources necessary for the implementation of complex security-supporting schemes. Among the plethora of applications that can benefit from the IoT, the workshop will have a particular focus on security aspects in e-Health and in the broad-sense of well-being. Security aspects in other application domains of the IoT are also of interest.

The workshop will address security issues that are particular to the context of using IoT for e-health including threat modeling, risk assessment, privacy, access control, and fault-tolerance. Theoretical, modeling, implementation, and experimentation issues will be discussed to build an accurate general view on the security of medical BANs. One the major challenges that will be underlined by the workshop participants is the combination of different security models needed for the sub-networks of the IoT (e.g., BAN,PAN, LAN, MANET) with consideration of the severe computational, storage, and energy limitations of the elementary smart nodes.

We encourage contributions describing innovative work addressing the use of information and communication technologies in medical applications. Topics of interest include, but are not limited to:

- ✓ Definition of accurate metrics to assess the threats and the risks associated to IoT for e-health
- ✓ Identification and description of new attack scenarios that are specific to IoT architectures
- ✓ Investigation of the security properties that should be fulfilled by the transmission of patient data across body area networks
- ✓ Designing secure heterogeneous BAN architectures for e-health applications
- ✓ Implementing practical testbeds that allow the analysis of the security performance of BANs
- ✓ Monitoring the security level of the e-health applications relying on IoT
- ✓ Analyzing the results of experiments conducted using real patient data and studying the security performance of the associated architectures

Authors should submit original papers in English, carefully checked for correct grammar and spelling, using the on-line submission procedure. The initial submission must have between 4 to 6 pages using the IEEE format. A "double-blind" paper evaluation method will be used. To facilitate that, the authors are kindly requested to produce and provide the paper, WITHOUT any reference to any of the authors. This means that is necessary to remove the authors personal details, the acknowledgements section and any reference that may disclose the authors identity.

WORKSHOP CO-CHAIRS

Mohamed Hamdi, *Sup’Com Tunisia*

Habtamu Abie, *NR, Norway*

PROGRAM COMMITTEE

Ilangko Balasingham, *Oslo University Hospital*

Stefan Poslad, *Queen Mary University of London*

Einar Snekkenes, *Gjøvik University College*

Reijo Savola, *VTT*

Denis Trcek, *University of Ljubljana*

Wolfgang Leister, *NR*

Tai-Hoon Kim, *GCKU*

Joel Rodrigues, *University of Beira Interior*

Manel Abdelkader-Hamdi, *Tunis Business School*

Amel Meddeb-Makhlouf, *ISECS*

Samia Jones, *Texas A&M University of Qatar*

Soufiene Djahel, *UCD*

Nabil Tabbane, *Sup’Com*

Ilesh Dattani, *Q-Sphere*

Pekka Savolainen, *VTT*

IMPORTANT DATES

Paper submission	June 30, 2012
Acceptance notification	July 31, 2012
Camera ready submission	August 15, 2012