CALL FOR PAPERS

==========

Workshop on Security Tools and Techniques for Internet of Things (SeTTIT)
http://settit.bodynets.org/2013/show/home
Co-located with the BODYNETS 2013 conference
http://bodynets.org/2013/show/home
Boston, Massachusetts, United States, September 30–October 2, 2013

==========

Workshop Objectives

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 eHealth 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 eHealth 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 of 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 eHealth
- Identification and description of new attack scenarios that are specific to IoT architectures
- Context-awareness for IoT security in eHealth
- Soft trust management in IoT
- Risk-based adaptive security for IoT
- Analytics and predictive models for adaptive security in IoT
- Adaptive security decision-making models for IoT
- Evaluation and validation models for adaptive security in IoT
- Lightweight cryptographic protocols for IoT

- 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 eHealth applications
- Implementing practical testbeds that allow the analysis of the security performance of BANs
- Monitoring the security level of the eHealth applications relying on IoT
- Analyzing the results of experiments conducted using real patient data and studying the security performance of the associated architectures

Paper Submission

Authors should submit original papers in English, carefully checked for correct grammar and spelling, using the on-line submission procedure. The proceedings will be published by ACM. The submission must have between 4 to 6 pages using the ACM format.
For author instructions follow this link: http://settit.bodynets.org/2013/show/home

Keynote Speeches

Two keynote speeches will be given by reputed experts in security in IoTs and Sensor networks.

Best Paper Award

The program committee will designate one paper accepted to the workshop as ICST Best Paper Award and will be given to the best paper's author during the conference dinner.

Special Issue

Selected papers will be considered for publication in a special issue of Wiley's Security and Communication Networks Journal.

Important Dates

Paper submission deadline:	May 6, 2013
Acceptance notification:	June 3, 2013
Camera ready submission:	July 2, 2013

Technical Sponsors

IEEE EMB, ACM SIGCHI, CREAT-NET

Organizing Committees

Workshop Co-Chairs

Habtamu Abie, Norwegian Computing Center, Norway
Mohamed Hamdi, School of Communication Engineering, Tunisia

Technical Program Committee

Jemal Abawajy, Deakin University, Australia
Manel Abdelkader, Tunis Business School, Tunisia
Evesti Antti, VTT Technical Research Centre of Finland, Finland
Ilangko Balasingham, Oslo University Hospital, Norway
Jim Clarke, Waterford Institute of Technology - TSSG, Ireland
Ilesh Dattani, Q-Sphere Ltd, UK
Soufiene Djahel, University College Dublin, Ireland
Dieter Gollmann, Hamburg University of Technology, Germany
Tai-Hoon Kim, School of Computing & Information Science, University of Tasmania, Australia
Wolfgang Leister, Norwegian Computing Center, Norway
Shiguo Lian, France Telecom R&D, China
Javier Lopez, University of Malaga, Spain
Antonio Mana, University of Malaga, Spain
Amel Meddeb-Makhlouf, ISECS, Tunisia
Mohamed Mejri, University of Laval, Canada
Edmundo Monteiro, University of Coimbra, Portugal
Mohammad Mozumdar, California State University, Long Beach, USA
Peter Mueller, IBM Zurich Research Laboratory, Switzerland
Piers O'Hanlon, University of Oxford, Oxford Internet Institute, UK
Eiji Okamoto, University of Tsukuba, Japan
Ebenezer Paintsil, Norwegian Computing Center, Norway
Stefan Poslad, Queen Mary University of London, UK
Rodrigo Roman, Institute for Infocomm Research, Singapore
Domenico Rotondi, TXT e-solutions, Italy
Hossein Sarrafzadeh, Unitech, New-Zealand
Reijo Savola, VTT Technical Research Centre of Finland, Finland
Pekka Savolainen, VTT Technical Research Centre of Finland, Finland
Einar Snekkenes, Gjøvik University College, Norway
Srinivas Srivathsanagopalan, CTS/VISA, USA
Denis Trcek, University of Ljubljana, Slovenia
Jari Veijalainen, University of Jyväskylä, Finland