NR Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

Project factsheet

ASSET — Adaptive Security for Smart Internet of Things in eHealth

Project description

The ASSET project develops risk-based adaptive security methods and mechanisms for Internet of Things (IoT) in eHealth, using game theory and context-awareness techniques that increase security to an appropriate level. Emerging IoT technologies provide many benefits to the improvement of eHealth. IoTs are, however, vulnerable to attacks since they are unattended, communicate wireless, and constrained by energy and computation capabilities necessary for the implementation of complex security-supporting schemes. Most security models and mechanisms for the IoT's problems are hard to change, reuse, and analyze. This results in inflexible infrastructures, lost investments, damages resulting from mechanisms not matching the threats, etc. The ASSET project builds risk-based adaptive security methods and mechanisms that will adapt to the dynamic changing conditions of IoTs.

ASSET's case study will lead to the design of adaptive strategies for the dynamic interplay between security and data transmission in a mobile patient monitoring system. This will use information of link quality, data transmission rate, and processing capabilities of sensor nodes and smart phones. The security adaptation will take into account the various quality of service (QoS) metrics. This will allow us to verify the necessary security and trust for the emerging IoTs in many e-Health applications in general and in the case study patient monitoring in particular. This will constitute a key innovator for future e-Health solutions in the Norwegian hospitals and health services.

NR's contribution

NR's research in ICT has a basis in security, privacy and interactive, network-based technology. NR is contributing research capabilities in adaptive security, privacy, risk assessment, modeling and simulation. NR

Period

January 2012 – June 2015

Web site

http://asset.nr.no/

NR contact

Habtamu Abie

Funding

Research Council of Norway (Grant agreement no: 213131/O70)

Norwegian partners

- Norwegian Computing Center (Norsk Regnesentral)
- Gjøvik University College (Coordinator)
- Oslo University Hospital

International partners

- Queen Mary University of London (UK)
- VTT Technical Research Center of Finland (FI)

is supervising one PhD student and managing the coordination of the project.

Benefit for participants

- Models for estimating and predicting risks and benefits using game theory and context awareness
- Methodology for security measurement and metrics for the effectiveness of the adaptation based on best practice
- Prototyping IoT adaptive methods for authentication and access control in a simulated eHealth patient monitoring in Oslo University Hospital
- Light-weight abilities for smart things that will allow them to detect, respond, and adapt to security and privacy threats.

Benefit for society

Through development of adaptive and context-aware security for the next generation of IoTs, the ASSET project will enable health organizations both in public and private sector to design and implement context aware security and privacy protection and thus adaptive to patients’ needs. This will improve end user’s confidence in service providers. The project builds risk-based adaptive security models that dynamically detect in real-time unknown security and privacy threats, respond to them, and adapt to the environment and changing degree of security and privacy breaches. This will allow health organizations to securely and adaptively track objects and people (staff and patients), identify and authenticate people, patient mobility, and automatic sensing and collection of real time patient health data which will reduce the delay for treatment of critical patients thereby enhancing traditional medical services.

Project results (preliminary)

- Organizing International Workshop on *Security Tools and Techniques for Internet of Things in eHealth*.
- Two PhD positions have been filled.
- Enrolling 1–3 Master’s students: Master Thesis in in Adaptive Internet of Things (IoT) in eHealth