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

GUC's contribution

GUC as an academic institution offers BSc, MSc and PhD programmes in the topic area covered by the project. GUC is contributing to developing new research results that can be published through reputed and approved channels and integrated into courses and teaching programmes. GUC is supervising one PhD student and administrating the two PhD candidates' participation in the PhD program.

OUH's contribution

OUH performs more than 50 per cent of the total medical research in Norwegian medical centres and is contributing research in verifying the trust and security for emerging IoT in the case study patient monitoring in particular and many eHealth applications in general. OUH manages the case study (patient monitoring) by providing test-bed, co-supervises a PhD student, and contributes to the specification, analysis and evaluation of the adaptive security mechanisms developed within the project.

QMUL's contribution

QMUL is one of London and the UK's leading research-focused higher education institutions, delivers world class degree programmes and research across a wide range of subjects, and has a strong track record in the IoT. QMUL is contributing to the technical research aspects of the project, in particular in the elaboration of the interplay between adaptive security and data transmission using information of the link quality, data transmission rate, and processing

Period

January 2012 – June 2015

Web site

http://asset.nr.no/

Funding

The Research Council of Norway

The Research Council of Norway
Grant agreement no: 213131/O70

Norwegian partners

Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

Norwegian Computing Center (NR) (Coordinator)
NR Contact: Dr. Habtamu Abie
E-mail: habtamu.abie@nr.no

Gjøvik University College (GUC)
GUC Contact: Prof. Einar Arthur Snekkenes
E-mail: einar.snekkenes@hig.no

Oslo universitetssykehu

Oslo University Hospital (OUH)
OUH Contact: Prof. Ilangko Balasingham
E-mail: ilangko.balasingham@medisin.uio.n

International partners

Queen Mary University of London

Queen Mary University of London
QMUL Contact: Prof Stefan Poslad
E-mail: stefan@eecs.qmul.ac.uk

VTT

VTT Technical Research Centre of Finland
VTT Contact: Reijo Savola
E-mail: Reijo.Savola@@vtt.fi

capabilities of sensor nodes and smart phones. QMUL is lecturing about the project at QMUL in the courses on network security and IoT, Security, safety, trust and privacy for open distributed services, and will publish in reputed international security and privacy journals.

VTT's contribution

VTT's research in information security is based on strong experience from various topics of information security, both in research and R&D projects. The focus areas are security metrics, security assurance, including security testing, monitoring and analysis, risk and vulnerability analysis. VTT is contributing research in the technical research aspects of the project, in particular elaborating the design of a metrics development methodology for risk-driven adaptive security.

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)

- Training two PhD fellows.
- Training three master's students
- Organized International Workshop on *Security Tools and Techniques for Internet of Things in eHealth*.
- Specified and published risk-based adaptive security framework for IoT in eHealth
- Specified and published metrics-driven adaptive security management in eHealth IoT applications

PhD Fellows

Kashif Habib Sheikh
Waqas Aman