IoTSec - Security in IoT for Smart Grids

Development of security models and modules for IoT systems (WP2)

Habtamu Abie & Åsmund Skomedal
Norwegian Computing Center

Project Kick-off Meeting, Halden

05/09/2015

WP2- Development of security models and modules for IoT systems

- T2.1 - Development of privacy-aware models and measures
- T2.2 - Adopting and enhancing adaptive security for system of systems
- T2.3 - Formal technologies for semantic provability

WP2 - T2.1 - Development of privacy-aware models and measures

- Objectives
  - establish privacy-aware models and related measures of privacy
  - introduce privacy design patterns for industrial devices and programs
  - security models for business interactions between stakeholders
- Expected results
  - construction of privacy by Design patterns and the deployment of user-centric privacy technology (M12)
  - cooperation and competition framework among different players in the smart grid (M12)
  - processes integrating technology, business model, security model and privacy requirements (M24)

WP2 - T2.2 - Adopting and enhancing adaptive security for system of systems

- Objective: review, extend and establish *models* for
  - adaptive security through predication and advanced behavioral analysis of big-data
  - real-time security monitoring of the entire grid operations
  - prevention, detection and recovery from the failures of security and privacy protections
- Sub-objectives
  - develop and implement anticipatory adaptive security using evolutionary game theory and behavioral analysis
  - develop adaptive user interface with contextual intelligence
  - optimize adaptive security models using optimized machine learning

WP2 - T2.2 – Intro
What is adaptive security

- Security solution
  - learns, and adapts to changing environment dynamically
  - anticipates (unknown) threats
- Involves
  - collecting situational/contextual information both from within the system and from the environment
  - analyzing the collected information
  - measuring security level and metrics
  - responding to changes
  - learning from changing environment

WP2 - T2.2 – Intro
Adaptive security for IoT

- from three related viewpoints:
  - from the *things* that are connected
  - from the *environments* in which they are situated, and
  - from the *interactions* that occur between Things, their environments and their human users
- some types of modern IoT applications (smart grids)
  - require instant adaptation of their security mechanisms due to their exposure to increasing situational dynamics
- In this emerging environments/settings
  - a large-scale sources of potential data (a la big-data)

WP2 - T2.2 – Intro - Human-Computer Interaction – adaptive user interface

- Analyzing feedback types
  - human-computer interaction, collected information and how this is used in the adaptation
- Devising novel mechanisms
  - exposing the control loops to the users
  - keeping the users of self-adapting systems “in the loop” to ensure their trust
- Give the users the option
  - visual feedback of the adaptation
  - disable the self-adaptive features and the system should not contradict this (expert user)

NR

WP2 - T2.2 - Adopting and enhancing adaptive security for system of systems

- Expected results
  - Functional architecture of adaptive security models (M12)
  - Working prototype of adaptive security models (M24)
  - Working prototype of adaptive user interface (M30)
  - Optimized adaptive security models (M48)
  - 8 conference papers (M6-M48) and 5 journal papers (1 paper per year)

WP2 - T2.3 - Formal technologies for semantic provability

- Objective
  - establish formal technologies for semantic provability
- Expected results:
  - a non-trivial case study (M12)
  - a tool for semantic provability (M48)
  - a minimum of 3 papers, including one journal paper (M12-36)

WP2 – Inter-tasks research integration