IoTSec - Security in IoT for Smart Grids

AFSecurity Seminar, Secure October - Security R&D @ UiO and Partners

Habtamu Abie, Norwegian Computing Center - NR

IFI/Oslo

09/10/2015
IoTSec - Challenges

► Physical access security
► Communication network security
► Big data security
► Value added IoT services security
  ▪ addressing both business and end-user needs

► IoT from three related viewpoints
  ▪ the *things* that are connected
  ▪ the *environments* in which they are situated, and
  ▪ the *interactions* that occur between things, their environments, and their human users
IoTSec - vision

► Develop
  ▪ secure IoT-enabled smart power grid infrastructure

► Achieve
  ▪ reliable and efficient power distribution network
  ▪ distributed, connected smart and value-added services

► Become
  ▪ start-up of a research cluster in security for IoT, industrially
    applied by members of the NCE Smart Energy Markets
IoTSec - Objectives

► Extend the IoTSec project to a research cluster to include
  ▪ 14 Professors/Senior Researchers
  ▪ 15 PhDs/PostDocs
  ▪ 30 Master students
  ▪ international visibility with 5 projects and memberships in 5 networks/clusters

► Tailor the research towards an operational Smart Grid Security Centre at the NCE Smart
  ▪ supported by at least 15 companies
  ▪ identified as an International Centre of Excellence
IoTSec – research and approach

Research focuses
- Semantic provability
- Adaptive security
- Privacy negotiations
- Measurable security and privacy
- Risk analysis for IoT ecosystem

Application areas
- Smart Grid
- Smart Home
- Health

Smart Grid Security Centre
Semantic description and provability

► Objectives
  ▪ create the semantic descriptions for the infrastructure components and the attack surface
  ▪ establish the semantic model for the IoT system
  ▪ establish formal technologies for semantic provability

► Expected results
  ▪ completion of a PhD
  ▪ nontrivial case studies
  ▪ tool for semantic provability
  ▪ minimum of 6 papers, including two journal papers
Adaptive security

► Objectives: 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
Adaptive security …

► Expected results
  ▪ functional architecture of adaptive security models
  ▪ working prototype of adaptive security models
  ▪ working prototype of adaptive user interface
  ▪ optimized adaptive security models
  ▪ 8 conference papers and 5 journal papers
Privacy-aware models and measures

► Objectives
  ▪ establish privacy-aware models and related privacy measures
  ▪ introduce privacy design patterns for industrial devices and programs
  ▪ harmonize security models for business interactions between stakeholders

► Expected results
  ▪ construction of privacy by Design patterns and the deployment of user-centric privacy technology
  ▪ cooperation and competition framework among different players in the smart grid
  ▪ processes integrating technology, business model, security model and privacy requirements
Measurable security and privacy

► Objectives
- establish the multi-metrics model for the Smart Grid
- adapt to the real world infrastructure
- analyze the most relevant sub-systems
- apply specific goals for security, privacy and dependability

► Expected results
- system analysis for main subsystems on current infrastructure
- identification of 3-5 use cases
- feedback from industry on applicability of system analysis
- extension of the Smart Grid system to include at least 2 new functionalities
- identification of challenges for industrial applicability
Security usability in IoT ecosystem

► Objectives
- analyze conflicting incentives for IoT, based on the IoTSec ecosystem
- establish a platform for multi-shareholder risk analysis
- create impact assessment for stakeholder in the IoTSec ecosystem

► Expected results
- functional description of risk platform for IoT multi-operators
- a platform for cost effective risk analysis platform based on CIRA/PETweb II results
- risk analysis of the system to be used by the infrastructure operators in their decision making
- completion of a PhD
Smart Grid Security Centre

► Objectives
  ▪ establish the industrial requirements, analyze the IoTSec ecosystem and ensure industrial applicability
  ▪ perform the detailed assessment of modules applicable for the Centre and the pre-industrial pilots
  ▪ perform the gap analysis of security methods for critical infrastructures

► Expected results
  ▪ clearly defined scope of the project in terms of stakeholders, their interests, technological components and their functionality and interconnection
  ▪ clarification of what is considered to be outside of the research and industrial applicability
Smart Grid Security Centre …

► Expected results …

▪ industrial network enhanced by at least 4 members
▪ industrial workshops and defined industrial shareholders
▪ Smart Grid Security Center with visualization platform
▪ models or modules into the visualization platform
▪ operational Smart Grid Security Centre
▪ analysis of IoT ecosystems similar to Smart Grids,
▪ contacts for applicability in IoT-based critical infrastructures
▪ roadmap of the operational applicability of IoTSec results
IoTSec - Facts

► 25 MNOK budget – RCN-IKTPLUSS
► 1 Oct 2015 – 30 Sep 2020
► 10 founding partners
► 18 partners (Aug 2015)
► Project owner UiO/IFI/UNIK
► Project manager Prof Josef Noll
► Semantic web site: http://iotsec.no/
► Seeking for partnership, collaboration, and liaison
Partners

- Founding partners
  - University of Oslo (UiO) through the Institute for Informatics (Ifi) and the University Graduate Centre (UNIK),
  - Norwegian Computing Centre (NR)
  - Simula Research Laboratory (SRL)
  - Gjøvik University College
  - NCE Smart Energy Markets (NCE Smart)
  - eSmart Systems (eSmart)
  - Frederikstad Energi (FEN)
  - EB Nett (EB)
  - Movation (MOV)

- Associated Academic Members
  - Mondragon Unibersitatea, Spain
  - University of Victoria, Canada
  - Universidad Carlos III de Madrid, Spain
  - University of Roma La Sapienza, Italy

- Associated Industrial Members
  - Mondragon Unibersitatea, Spain
  - Fredrikstad kommune
  - EyeSaaS
  - Nimbeo

- H2020 and ECSEL projects
- COINS Academic Research School