WP2

Security Models and Modules

by Habtamu Abie

WP 2 Team Y1

NR (Habtamu Abie, Åsmund Skomedal, Ivar Rummelhoff, Sigurd Eskeland)

UiO/IFI (Olaf Owe, Christian Johansen)

UNIK (Josef Noll, Christian Johansen)

Simula (Ming-Chang Lee, Yan Zhang)

WP2 Activities

T2.1 Development of privacy-aware models and measures

- Establish privacy-aware models and related measures of privacy.
- Introduce privacy design patterns for industrial devices and programs.
- Address security models for business interactions between shareholders.

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

- Adapt security through predication and advanced behavioural analysis of big-real-data
- Address real-time security monitoring of the smart grid operations
- Achieve prevention, detection and recovery from the failures of security and privacy protections

T2.3 Formal technologies for semantic provability

- Establish formal technologies for semantic provability

Major Achievements and Ongoing Work

T2.1 Development of privacy-aware models and measures

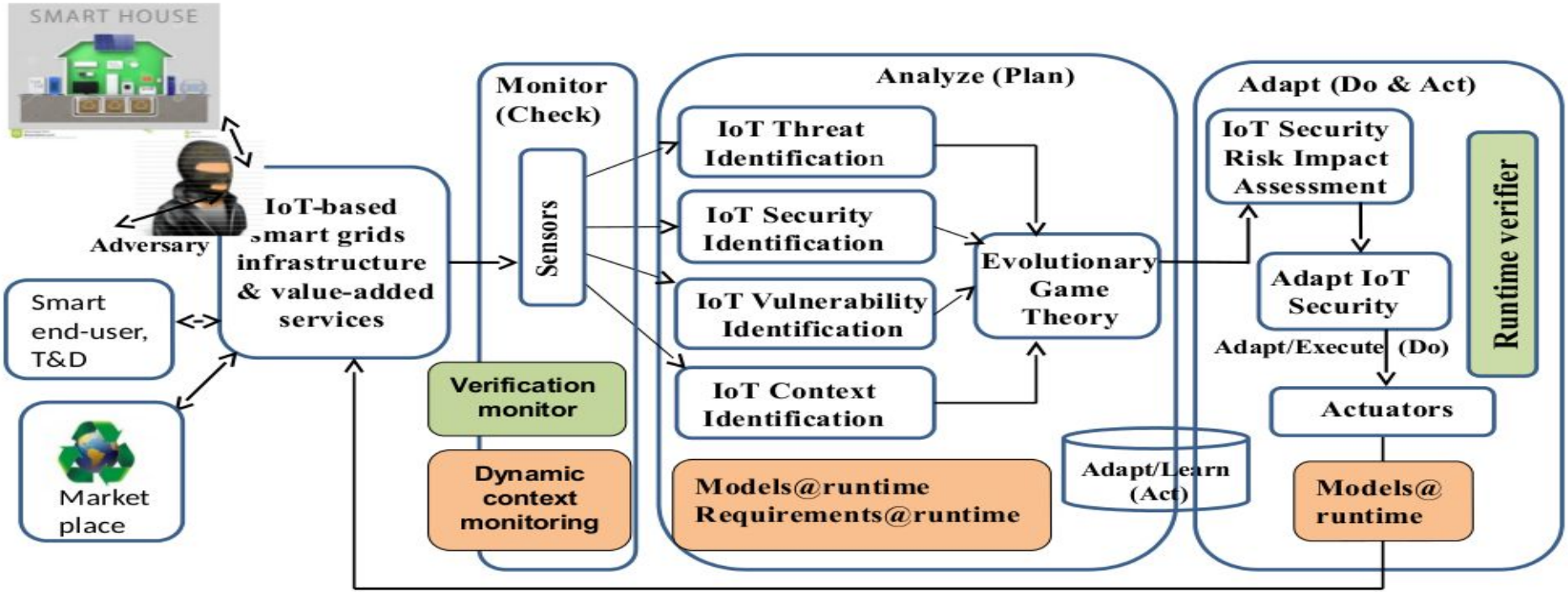
- Major Achievements
  - We have developed an intelligent eavesdropping scheme for smart environments, such as smart homes or smart offices.
  - The goals:
    - to expose the layout of a smart environment
    - to expose the users' privacies (e.g., activity behaviors and daily routines)
- Ongoing Work
  - Four case studies regarding to different smart homes have been finished.
  - The experimental results show that the layout of these smart homes can be inferred by our scheme and the users' privacies will be compromised.
  - Now we are authoring the corresponding paper and would like to submit it to *IEEE Intelligent Systems*.

Challenges and Future Work

T2.1 Development of privacy-aware models and measures

- Challenges
  - To propose an ideal privacy-prevention model that
    - Be able to invalidate any attackers' eavesdropping tools,
    - Allow the remote monitor center to distinguish data traffics that is faked for confusing attackers and data traffics that is sent from real sensors, and
    - Result in low bandwidth consumption, energy consumption, and/or hardware cost.
- Future Work
  - To propose a privacy-prevention framework for smart environments.
  - The goal is to prevent users' privacies form exposing.

Anticipatory adaptive security + semantic provability



Later this will be integrated with machine learning for Integrated analysis and decision making, and optimized adaptation

Major Achievements

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

- Security Metrics as measures for enhancing security in mobile devices [1]
  - Adaptive security for flexibility, securing applications in smart house, ehealth
- Compromise-protection of smart meters in the smart grid using co-dependent authentication [2],
  - Cryptographic based compromise protection of smart meters
- Security Metrics for Informed Decision Making [3],
  - techniques to understand and scale the needs in both measurement and analytics
  - basis for security situational awareness in the modern complex software infrastructure.
  - support security adaptation and architecture-based evolution.
- Scalable secure broadcasting in the smart grid [4]

Major Achievements - T2.2...

- H. Abie, "IoTSec - Security in IoT for Smart Grids", AF Security Seminar, Oct 2015, Oslo
- **Co-organizer, co-sponsor and co-chair**: MeSSa 2016 (Monitoring and Measurability of Software and Network Security) workshop to be held in Copenhagen, November 28 to December 2, 2016
- **Guest editors**: Special issue on "Advances in Security and Privacy for Mobile Users in Intelligent Environments" of Mobile Information Systems - An Open Access Journal with impact factor 1.5
- **Co-chairing**: Ubiquitous Computing, Services and Applications (UCSA) symposium of WiMob 2016 (The 12th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications)
- IEEE Norway IoT Security SIG

Major Achievements

T2.3 Formal technologies for semantic provability [List of publications 2]

- Formal technologies for semantic provability and verification
- for distributed and object-oriented systems
-
- Results related to a distributed concurrency model and late binding
- Modular and scalable methods

Ongoing work

- Recruit master student(s) for simulation of evolutionary game theory
- Submit journal article in February 2017
  - on evolutionary game theory for IoT-Based Smart grid security
  - Scalable secure broadcasting in the smart grid to Int. Journal of Security and Communication Networks
  - on broadcast and threshold encryption
- Continue with the formulation and simulation of the evolutionary games
  - using MATLAB, and machine learning based benchmarking using Microsoft Cognitive Toolkit (aka CNTK) for 3 scenarios:
    - Smart House,
    - Smart grid distribution, and
    - interfaces between these two

Challenges

Research challenges:

- Improving the detection of unknown threats to IoT systems
  - formal run-time verification
  - formal methods for increasing the prediction precision
  - strong adaptivity
  - cognitive capabilities as human like
- Improved techniques for privacy-aware security monitoring, analysis

Suggestions

Adaptive Cyber-Physical System (CPS) Security to tackle dynamicity, ambiguity, uncertainty, and multiplicity

- The integration of computer networks with the physical environment - Internet of Things (IoT) - raises a whole new class of concerns with regard to security, forensics, safety and privacy.
- The dynamic nature of the threats to IoT requires the ability to anticipate, detect, respond, and predict attacks, and effectively recover from attacks.
- CPS and their associated services, as humans, should therefore possess cognitive capabilities, of which situation awareness is one of the components of these capabilities, the ability to perceive the environment, comprehend the situation, project that comprehension into the near future, and determine the best action to execute.

List of Publications

[1] Journal: R. M. Savola, M. Kylänpää, H. Abie, Risk-driven Security Metrics for an Android Smartphone Application, submitted to International Journal of Information and Computer Security (IJICS), 06/08/2016

[2] Sigurd Eskeland, Compromise-protection of smart meters in the smart grid using co-dependent authentication, ECSA November 28 - December 02, 2016, Copenhagen, Denmark, ACM ISBN 978-1-4503-4781-5/16/11

[3] Reijo Savola, Habtamu Abie, and Antti Evesti, Security Metrics for Informed Decision Making, ECSA, November 28 - December 02, 2016, Copenhagen, Denmark, ACM

[4] Sigurd Eskeland, Scalable secure broadcasting in the smart grid, to be submitted to Int. Journal of Security and Communication Networks (hindawi)

List of Publications 2

- Journal: R. Bubel , F. Damiani, R. Haehnle, E.B. Johnsen, O. Owe, I. Schaefer, I.C. Yu: Proof Repositories for Compositional Verification of Evolving Software Systems: Managing Change When Proving Software Correct. In Proof Repositories for Software Verification In the Large, LNCS Transactions on Foundations for Mastering Change (FOMAC) (27 pages), 2016,
- Chapter in book: Olaf Owe: Verifiable Programming of Object-Oriented and Distributed Systems. In Luigia Petre and Emil Sekerinski (eds.) From Action System to Distributed Systems: The Refinement Approach CRC Press Taylor & Francis, pp. 61–80, 2016
- LNCS: Olaf Owe: Reasoning about Inheritance and Unrestricted Reuse in Object-Oriented Concurrent Systems, iFM'16 Iceland, in Lecture Notes in Computer Science 9681, Springer, pages 210-225, June 2016. (pluss presentation) 30% acceptance
- Pluss extended abstract and presentation at NWPT'15 (Owe&Lin&Yu), and at NWPT'16 (Din&Johnsen&Owe&Yu).
- Pluss presentation at SINTEF by Owe. Dec 2015.