Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

Note

Anticipatory Adaptive Security for IoT-based Smart Grids Infrastructure and Value-added Services

Deliverable D2.2.2

Note no. DART/09/20

Authors **Habtamu Abie, Svetlana Boudko**

Date **21. sep. 2020**

Authors

Habtamu Abie, PhD, is currently a Chief Research Scientist at NR. He received his B.Sc., M.Sc. and Ph.D. from the University of Oslo, and has many years of experience in computing, both as practitioner and researcher. He has a solid and extensive background in the design and development of real-time systems, and the design, modelling and development of security for distributed computing systems. He is NR's principal investigator of the IoTSec project and WP leader.

Svetlana Boudko, PhD, is currently a Senior Research Scientist at NR. She received her M.Sc. from Moscow Aviation Institute and Ph.D. from the University of Oslo and has been engaged in various research and development projects. Her interests include modelling and analysis, distributed systems, game theory, multi-agent systems, and machine learning. In the IoTSec project, she modelled and analysed security attacks and defences in advanced metering infrastructures and developed adaptive data collection for real-time security analytics.

Norsk Regnesentral

Norsk Regnesentral (Norwegian Computing Center, NR) is a private, independent, non-profit foundation established in 1952. NR carries out contract research and development projects in information and communication technology and applied statistical-mathematical modelling. The clients include a broad range of industrial, commercial and public service organisations in the national as well as the international market. Our scientific and technical capabilities are further developed in co-operation with The Research Council of Norway and key customers. The results of our projects may take the form of reports, software, prototypes, and short courses. A proof of the confidence and appreciation our clients have in us is given by the fact that most of our new contracts are signed with previous customers.

<Name of collaborating institute>

<Info on collaborating institute can go here>

Norsk Regnesentral
Norwegian Computing Center
Postboks 114, Blindern
NO-0314 Oslo, Norway

Besøksadresse
office address
Gaustadalleen 23a
NO-0373 Oslo, Norway

Telefon · telephone
(+47) 22 85 25 00
Telefaks · telefax
(+47) 22 69 76 60

Bankkonto · bank account
8200.01.48888
Org.nr. · enterprise no.
NO 952125001 VAT

Internett · internet
www.nr.no
E-post · e-mail
nr@nr.no

Title	**Anticipatory Adaptive Security for IoT-based Smart Grids Infrastructure and Value-added Services**
Authors	**Habtamu Abie, Svetlana Boudko**
Quality assurance	Wolfgang leister
Date	21. sep. 2020
Year	2020
Publication number	DART/09/20

Abstract

The deliverable reports the research and development of adaptive security addressing the protection of "IoT-based smart grids" against evolutionary threats and attacks through the prediction and advanced behavioural analysis of big data from IoT Smart Grids by automating prevention, detection, and recovery from the failures of security and privacy protections at run-time and by re-configuring control parameters and security goals.

Keywords	Anticipatory security models, adaptive security, IoT-enabled Smart Grids, evolutionary game theory
Target group	Research Council of Norway and Partners
Availability	Public
Project number	320548 (248113/O70)

Research field	Anticipatory Adaptive Security for IoT-based Smart Grids
Number of pages	13

Grant Agreement Number: **248113/O70**

Project acronym: **IoTSec**

Project full title:

Security in IoT for Smart Grids

D 2.2.2

Anticipatory Adaptive Security for IoT-based Smart Grids Infrastructure and Value-added Services

Due delivery date: M24

Actual delivery date: M60

Organization name of lead participant for this deliverable:

Norwegian Computing Center

Dissemination level		
PU	Public	**X**
RE	Restricted to a group specified by the consortium	
CO	Confidential, only for members of the consortium	

Deliverable number:	D 2.2.2
Deliverable responsible:	Habtamu Abie
Work package:	WP2
Editor(s):	Habtamu Abie

Author(s)	
Name	**Organisation**
Habtamu Abie	Norwegian Computing Center
Svetlana Boudko	Norwegian Computing Center

Document Revision History			
Version	**Date**	**Modifications Introduced**	
		Modification Reason	**Modified by**
V01	12.04.2017	Initial input	Habtamu Abie
V02	17.09.2017	Risk-based Adaptive Authentication for Internet of Things in Smart Home eHealth	Habtamu Abie
V03	25.06.2018	Evolutionary Game for Integrity Attacks and Defences	Svetlana Boudko
V04	10.05.2019	Adaptive Cybersecurity Framework for Healthcare Internet of Things	Svetlana Boudko
V05	10.05.2019	Cognitive Cybersecurity for CPS-IoT Enabled Healthcare Ecosystems	Habtamu Abie
V1.0	21.09.2020	Final	Habtamu Abie

1 Anticipatory Adaptive Security for IoT-based Smart Grids Infrastructure and Value-added Services

The deliverable reports the research and development of adaptive security addressing the protection of "IoT-based smart grids" against evolutionary threats and attacks through the prediction and advanced behavioural analysis of big data from IoT Smart Grids by automating prevention, detection, and recovery from the failures of security and privacy protections at run-time and by re-configuring control parameters and security goals.

The development and implementation involved the implementation of the main models addressing the protection of IoT-based smart grids against evolutionary threats, unknown threats, using a combination of evolutionary game theory and advanced behavioural analysis of big data from IoT Smart Grids, and automating the activities of adaptation (monitoring, analysing, planning, and execution) at run-time by re-configuring of control parameters and security goals.

The following use cases described in [8] and depicted in Figure 1 are used to validate adaptive security models implementations:

- Smart home [1,9]
- DSO/AMI (Advanced Metering Infrastructure) [2, 5, 6]
- Value added services: IoT-enabled healthcare [3] and CPS/IoT-Enabled healthcare ecosystems [4]

As also depicted in Figure 1, the models addressed are IoT Security Identification (authentication [1,9], integrity [2] and confidentiality services [5,6]), IoT Threat Identification (DDoS, identity, integrity, confidentiality), IoT Context Identification and Semantic description [10], Evolutionary Game Theory [2,5,6], and IoT Security Risk Impact Assessment [7]. This report describes the main results published.

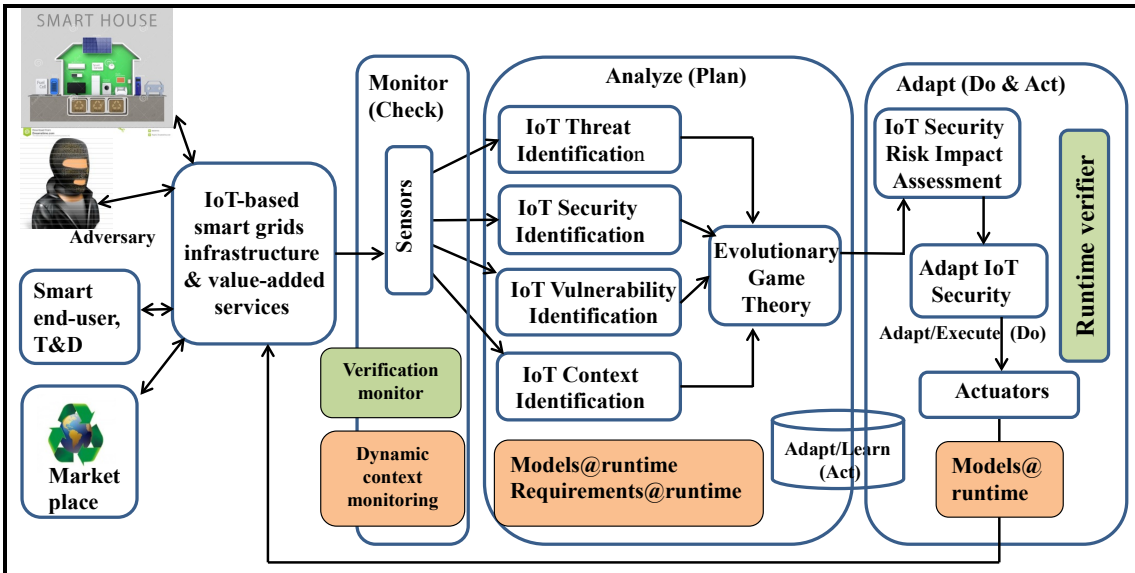

Figure 1 - Anticipatory adaptive security and semantic provability

The Monitor model plays an important role for real-time adaptive data collection for real-time security analytics. Figure 2 depicts our adaptive data collection framework which helps to detect security threats and prevent attacks by monitoring and collecting different categories of data for data analytics, improve collection efficiency by reducing the amount of collected data /collect relevant data that reflect the current state of the system using environmental sensors / other sources, and ensuring detection accuracy. The framework adapts the data collection routines to different contexts and situations. For instance, it can adapt to security threats (confidentiality, integrity, availability), network changes (content, bandwidth variations, protocols, topology changes), application (periodic data flows and from smart meters to higher level collectors), storage capacity, and environmental changes.

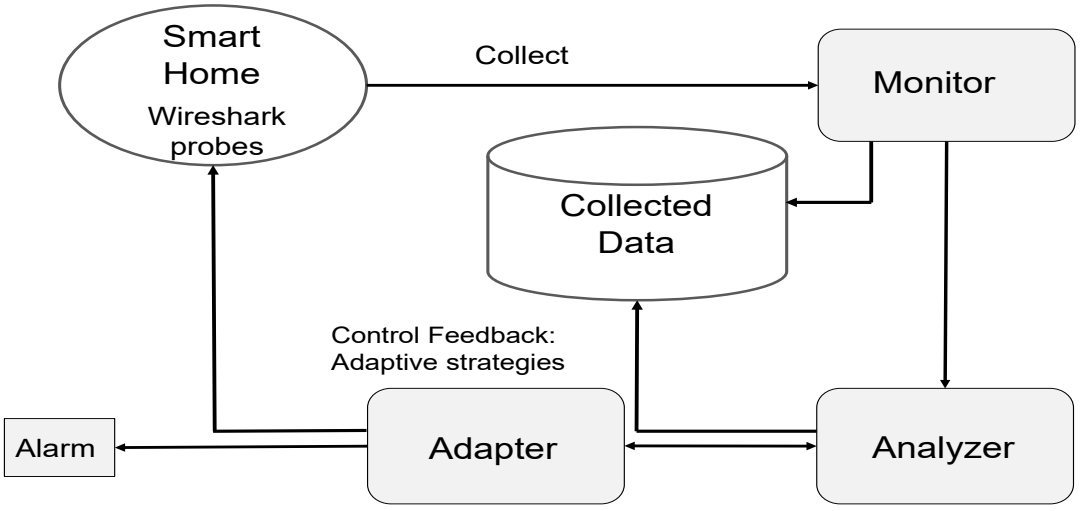

Figure 2 - Adaptive Data Collection Framework

The analytic algorithms selected for evaluation include:

For light-weight analytics

- Support Vector Machines (SVM)
- K-Nearest-Neighbors (KNN)
- Naive Bayes (NB)
- Decision Tree (DT)
- Random Forest (RF)

For identification of complex risks and attack patterns

- Long-short term memory network (LSTM)
- Artificial Neural Network (ANN) (with multi-hidden layers perceptron)
- Deep Belief Network and Probability Neural Network (DBN and PNN) and DL

The publicly available Datasets KDDCup-99 dataset, CICIDS2017 dataset, and UNSW-NB15 dataset were used for validation with close to 99% accuracy.

The Rest of the report describes the key findings and published results.

Paper 1 [1]: **Risk-Based Adaptive Authentication for Io T in S mart Home**

This paper addresses the major security concerns to efficiently utilize the services of IoT-based healthcare. One of the means that helps us to maintain system security is authentication. We, therefore, proposed a novel risk-based adaptive authentication model for IoT in Smart Home to identify the activities of the user and to verify the validity of the sensor nodes. The model uses a naïve Bayes machine learning algorithm to classify the channel characteristics variation between sensor nodes and their gateway. According to the observed variation of channel characteristics, the model assesses the risk to determine the probability of the device in question being compromised. Based on the risk score obtained from the assessment the model selects an authentication decision suitable for the particular risk score. Furthermore, the selected authentication decision resource need is compared with the available resource of the authenticator device and in case of scarcity in the available resource, the authentication process is offloaded to a device with available resource.

Paper 2 [2]: **An Evolutionary Game for Integrity Attacks and Defences for Advanced Metering Infrastructure**

In this paper, we address the problem of protecting integrity of the messages in an Advanced Metering Infrastructure (AMI), which is a component of IoT-enabled Smart Grids. We applied evolutionary game theory to a resource constrained security game model of AMIs. The AMI is modelled as a tree structure where each node aggregates the information of its children before passing this information on to its parent. The aim of this work is to explore the space of possible behaviours of attackers and to develop a framework where the AMI nodes adaptively select the most profitable strategies. Using this model, we simulated the evolution of a population of attackers and defenders on various cases resembling the real-life implementation of AMI. The results of the simulation indicate how to enhance security in AMI using evolutionary game

theory either by a priori analysis or as a tool to run dynamic and adaptive infrastructure defence.

Paper 3 [3]: **Adaptive Cybersecurity Framework for Healthcare Internet of Things**

In this paper, we studied dynamic and adaptive modelling of cyber security attacks and defences for healthcare critical infrastructures, with an emphasis on smart homes. The main components of a dynamic cyber security framework for protection of healthcare IoT infrastructures were defined. We applied evolutionary game theory to assist the security framework for the healthcare ecosystem. The framework has been evaluated using simulations. The results of this simulation represent the best possible response of the defence to dynamic and adaptive attacks.

Paper 4 [4]: **Cognitive Cybersecurity for CPS-IoT Enabled Healthcare Ecosystems**

This paper addresses the increasingly sophisticated attack methods in the Cyber Physical Systems (CPS)-Internet of Things (IoT)-enabled healthcare services and infrastructures. The CPSIoT-enabled healthcare services improve human life, but they are vulnerable to a variety of emerging cyberattacks. Cybersecurity specialists are also finding it hard to keep pace of the increasingly sophisticated attack methods. There is a critical need for innovative cognitive cybersecurity for CPSIoT enabled healthcare ecosystem. This paper presents the conceptualization and description of a cognitive cybersecurity architecture for simulating the human cognitive behaviour to anticipate and respond to new and emerging cybersecurity and privacy threats to CPS-IoT enabled healthcare ecosystems. To achieve this, it combines artificial intelligence, cognitive methods, forensics, and innovative security mechanisms as cross-cutting services. It is structured in four layers, collaborative, perception and knowledge, data collection and actuation, and infrastructure. This architecture is developed based on different concepts developed in different projects and it will enable processing of increasing volume of data by interpreting, diagnosing and adapt to the environment without the need for human intervention.

Paper 5 [5,6]: **Evolutionary Game for Confidentiality in IoT-enabled Smart Grids**

In this paper, we address the problem of protecting AMI infrastructure against attacks on confidentiality. To do this, we modelled confidentiality attacks and defences as an evolutionary game and analysed the behaviours of the attacker and the defender of the AMI system. By applying evolutionary game theory to this problem, we introduced an important dynamic and learning capabilities in the behaviour of both attackers and AMI nodes, to explore the space of strategies, and to select the optimal set of solutions. The AMI is modelled as a tree structure where each node aggregates the information of its children before encrypting it and passing it on to its parent. As a part of the model, we developed a discretization scheme for solving the replicator equations. We used the replicator equation to show the evolution of utilities for both type of players. Further, we outlined how the evolutionary game model can used to evaluate the security threats in AMI systems. In our simulation scenarios, we show that the solution converges to ESS for all investigated cases. The simulations also show that the behavior of the replicator dynamic depends not only on incentives but also on the network configuration and

proportions of the protected assets. It is important that the outcomes of this work give us the best possible defence strategy against evolving attacks. It allows the defender to continuously stay ahead of the attacker in defending the AMI nodes.

Paper 7 [7]: **Risk-driven security metrics for an Android smartphone application**

This paper addresses the challenge of security management in Android smartphone platforms. Android smartphone is used in various application areas such as public safety, mobile networks, smart homes, smart grids, etc. Therefore, overcoming this challenge is important. This article systematically develops risk-driven security objectives and controls for Android smartphone applications and determines how to offer enough evidence of its security performance via metrics. It also includes conceptualisation and description of adaptive security for an Android platform which can improve the flexibility and effectiveness of these security controls and end-user's confidence in service providers.

The paper also argues that the successful deployment of mobile applications depends on ensuring security and privacy that need to adapt to the mobile devices' processing capabilities and resource use. This can be achieved through the development of adaptive and context-aware security for the next generation of digital ecosystems. It used the biological and ecosystem metaphors that provide interesting parallels to the conceptualisations and descriptions of the adaptions, self-adaption and responses which can be at a macroscopic ecosystem level (e.g., system or species) or a microscopic biological level (e.g., molecular, cellular), or at hybrid levels. The self-adaptive component achieves its goal through the following properties:

- **Autonomy**, which allows it to operate without the direct intervention of humans or others and to have control over its actions and internal state.
- **Social ability**, which allows it to interact with other agents (possibly humans).
- **Reactivity**, which allows it to perceive its environment and respond in a timely fashion to changes that occur in it (the environment)
- **Pro-activeness, learning, and adaptiveness**, which allow it to exhibit goal directed behaviour by taking the initiative, to learn when reacting and/or interacting with its external environment, and to modify its behaviour based on its experience.

The paper contributes to the security of smart home applications that may use Android phones such as eHealth related devices, energy management system, automated transportation, smart closed-circuit television (CCTV), home networks, mobile apps, security applications, and environmental monitoring.

In addition, two master's Theses were conducted and written in the following two areas:

Risk based Adaptive Authentication for IoT in Smart Home eHealth [9]: The research work developed a risk risk-based adaptive authentication mechanism which continuously monitors the channel characteristics variation, analyzes a potential risk using naive Bayes machine learning algorithm and performs adaptation of the authentication solution. The solution validates both the authenticity of the user and the device. In addition, it evaluated the resource need of the selected authentication

solution and provide an offloading functionality in case of scarce resource to perform the select ed protocol. The approach is novel because it defines the whole adaptation process and methods required in each phase of the adaptation. The paper also briefly describes the evaluation use case - Smart Home eHealth. The main results have been published in [1].

Semantic Description of IoT Security for Smart Grid [10]: This research work proposed, developed and evaluated IoT Security ontology for smart home energy management system (SHEMS) in smart grids. The ontology description includes infrastructure, attacks, vulnerabilities and counter measures for the main components of SHEMS such as Smart Meter, Smart Appliance, Home Gateway, and Billing data. The ontology extends the SAREF energy management ontology with security features. We have two main reasons for selecting SAREF ontology to base our work on. First, SAREF is standardized by ETSI. Second, it is specifically designed for energy management and efficiency. We checked the correctness of our ontology by running SWRL rules and SPARQL queries. Our test results showed that our ontology is useful to analyse and infer IoT security for smart home and can be extended to more complex reasoning of IoT security features.

In summary, Figure 3 depicts our contributions to the overall goal of the IoTSec project which is safe and secure IoT-enabled smart power grid infrastructure.

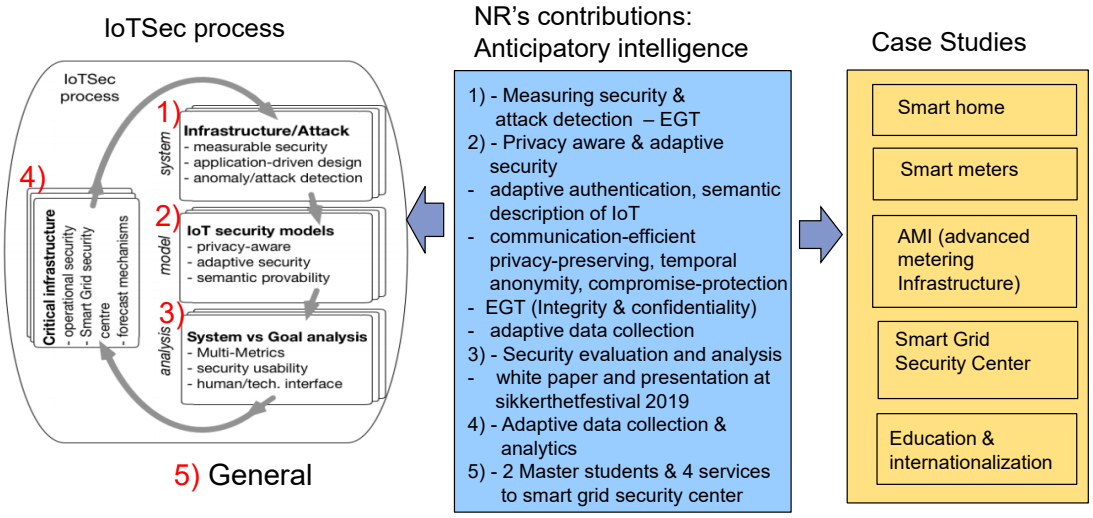

Figure 3 - Safe and secure IoT-enabled smart power grid infrastructure

References

[1] Mattias Gebrie, Habtamu Abie, Risk-based Adaptive Authentication for Internet of Things in Smart Home eHealth, ECSA '17 Proceedings of the 11th European Conference on Software Architecture, Pages 102-108, Canterbury, United Kingdom, September 11-15, 2017, ACM New York, NY, USA

[2] Svetlana Boudko and Habtamu Abie, An Evolutionary Game for Integrity Attacks and Defences for Advanced Metering Infrastructure. In 12th European Conference on Software Architecture: Companion Proceedings (ECSA'18), September 24-28, 2018, Madrid, Spain. ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3241403.3241463

[3] Svetlana Boudko and Habtamu Abie, Adaptive Cybersecurity Framework for Healthcare Internet of Things, In the Proceedings of the IEEE 13th International Symposium on Medical Information and Communication Technology (ISMICT 2019), Oslo, Norway, 8-10 May 2019

[4] Habtamu Abie, Cognitive Cybersecurity for CPS-IoT Enabled Healthcare Ecosystems, In the Proceedings of the IEEE 13th International Symposium on Medical Information and Communication Technology (ISMICT 2019), Oslo, Norway, 8-10 May 2019

[5] Svetlana Boudko, Peder Aursand, Habtamu Abie, Evolutionary Game for Confidentiality in IoT-enabled Smart Grids. Preprints 2020, 2020110002 (doi: 10.20944/preprints202011.0002.v1).

[6] Boudko S, Aursand P, Abie H. Evolutionary Game for Confidentiality in IoT-Enabled Smart Grids. Information. 2020; 11(12):582. https://doi.org/10.3390/info11120582

[7] Reijo M. Savola, Markku Kylänpää, Habtamu Abie, Risk-driven security metrics for an Android smartphone application. In Int. J. Electronic Business, Vol. 15, No. 4, 2020, pp 297-234. https://doi.org/10.1504/IJEB.2020.111059

[8] Habtamu Abie, Anticipatory adaptive security models for IoT-enabled Smart Grids, D 2.2.1, 2020

[9] Mattias Tsegaye Gebrie, Risk based Adaptive Authentication for IoT in Smart Home eHealth, Master's Thesis, University of Politecnico Di Torino, Nov 2017

[10] Getinet Ayele Eshete, Semantic Description of IoT Security for Smart Grid, Master's Thesis, University of Agder, Faculty of Engineering and Science Department of Information and Communication Technology June 2017