Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

Note

Optimized Anticipatory Adaptive Security Models for IoT-enabled Smart Grids

Deliverable D2.2.4

Note no.	DART/10/20
Authors	Habtamu Abie
Date	21. okt. 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.

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>

Title	**Optimized Anticipatory Adaptive Security Models for IoT-enabled Smart Grids**
Authors	**Habtamu Abie**
Quality assurance	<Insert quality assurance responsible here>
Date	21. okt. 2020
Year	2020
Publication number	DART/10/20

Abstract

The objective of this deliverable is to improve the accuracy of the adaptive mechanisms for different IoTs processing capabilities by applying high-level optimization using machine learning and AI approaches. In adaptive security models, the properties of feedback control loops affect the system design and architecture, besides making the control loops explicit, the control loops' properties must be made explicit and optimized as well.

Keywords	Artificial Intelligence, Machine learning, Cognitive Security, Adaptive security models, healthcare ecosystem
Target group	Research Council of Norway and Partners
Availability	Public
Project number	320548 (248113/O70)
Research field	Anticipatory Adaptive Security Models for CPS-IoT-enabled ecosystems

Number of pages	2
© Copyright	Norsk Regnesentral

Grant Agreement Number: **248113/O70**

Project acronym: **IoTSec**

Project full title:

Security in IoT for Smart Grids

D 2.2.4

Optimized Anticipatory Adaptive Security Models for IoT-enabled Smart Grids

Due delivery date: M48

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 2.2.4
Deliverable responsible:	Habtamu Abie
Work package:	WP2
Editor(s):	Habtamu Abie

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

Document Revision History			
Version	**Date**	**Modifications Introduced**	
		Modification Reason	**Modified by**
V01	10.01.2019	Initial input	Habtamu Abie
V02	10.05.2019	Cognitive Cybersecurity for CPS-IoT Enabled Healthcare Ecosystems	Habtamu Abie
V1.0	21.10.2020	Final	Habtamu Abie

1 Optimized Adaptive Security Models

The objective of this deliverable is to improve the accuracy of the adaptive mechanisms for different IoTs processing capabilities by applying high-level optimization using machine learning and AI approaches.

Figure 1 depicts the adaptive security models developed in another deliverable [3]. As the properties of feedback control loops affect the system design and architecture, besides making the control loops explicit, the control loops' properties must be made explicit as well.

The Monitor (Check) model starts with the collection of relevant data from environmental sensors and other sources that reflect the current state of the system. It answers questions such as:

- What is the required sample rate?
- How reliable is the sensor data?
- Is there a common event format across sensors?

The Analyze (Plan) model analyzes the collected data and answers questions such as:

- How is the current state of the system inferred?
- How much past state may be needed in the future?
- What data need to be archived for validation and verification?
- How faithful is the model to the real world?
- Can an adequate model be derived from the available sensor data?

The Adapt (Decide & Act) model decides about how to adapt in order to reach a desirable state and implements the decision, the system must act via available actuators and effectors. It answers questions such as

- How is the future state of the system inferred?
- How is a decision reached (e.g., with off-line simulation or utility/goal functions)?
- What are the priorities for adaptation across multiple control loops and within a single control loop?
- When should the adaptation be safely performed?
- How do adjustments of different control loops interfere with each other?
- Does centralized or decentralized control help achieve the global goal?
- Does the control system have sufficient command authority over the process - that is, can the action be implemented using the available actuators and effectors?

The purpose of this deliverable is to optimize these central mechanisms for Cyber-Physical System (CPS)-Internet of Things (IoT) processing capabilities by applying optimized machine learning and AI approaches.

Paper 2 optimizes risk-based adaptive authentication mechanisms using naive Bayes machine learning algorithm by continuously monitoring the channel characteristics variation, analysing a potential risk, and performing adaptation of the authentication solution. 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 assess 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 1 attempts to optimize the model depicted in Figure 1 by introducing a cognitive architecture for modelling humans' cognitive behaviour to anticipate and respond to new and emerging security and privacy threats as shown in Figure 2. As the properties of feedback control loops affect the system design and architecture, besides making the control loops explicit, the control loops' properties must be made explicit and optimized as well.

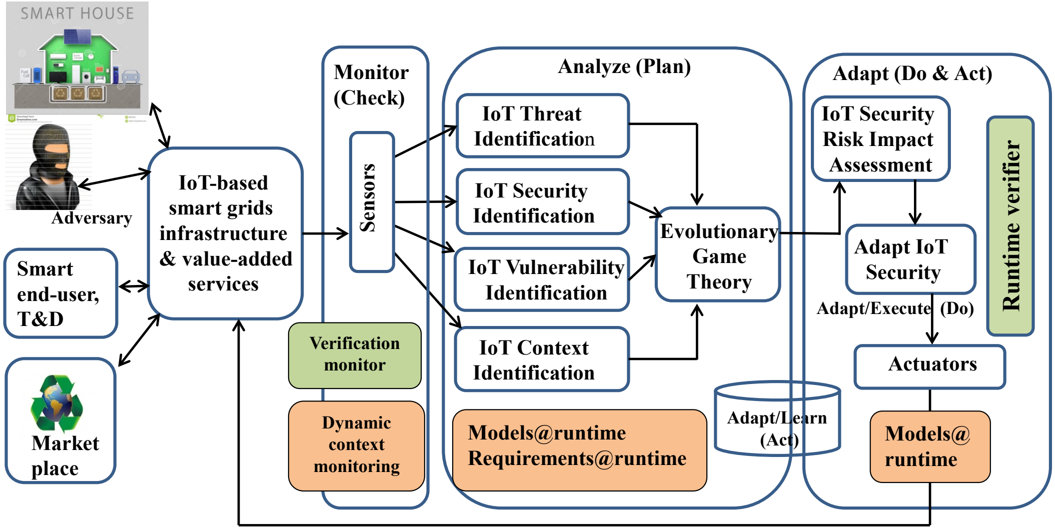
SMART HOUSE
Adversary
IoT-based smart grids infrastructure & value-added services
Smart end-user, T&D
Market place
Monitor (Check)
Sensors
Verification monitor
Dynamic context monitoring
Analyze (Plan)
IoT Threat Identification
IoT Security Identification
IoT Vulnerability Identification
IoT Context Identification
Evolutionary Game Theory
Models@runtime Requirements@runtime
Adapt/Learn (Act)
Adapt (Do & Act)
IoT Security Risk Impact Assessment
Adapt IoT Security
Adapt/Execute (Do)
Actuators
Models@ runtime
Runtime verifier

Figure 1 - Anticipatory adaptive security and semantic provability

More recently, Cyber-Physical System (CPS)-Internet of Things (IoT) (CPS-IoTs) are being developed with the capability to learn, reason, and understand both physical and social worlds by themselves, simulating the cognitive behaviour of humans – a cognitive CPS-IoT. “In knowledge-intensive environments, the smartest uses of the IoT will be those that enable the ingrained capabilities of human thinking to take centre stage.". However, all this introduces new challenges:

(i) increasing cognitive complexity of CPS-IoTs can lead to unexpected emergent behaviour;

(ii) cognitive CPS-IoT will suffer from traditional CPS-IoT vulnerabilities and threats, and new threats related to their inherent cognitive functionalities; and

(iii) CPS-IoT's ubiquity will present a significantly expanded attack surface making the public safety risks higher for critical infrastructure through its interfaces and improved flexibility of access to services and information.

Therefore, CPS-IoT Security, the integration of computer networks with the physical environment – raises a whole new class of concerns about security, forensics, safety, and privacy. The dynamic nature of the threats to CPS-IoT requires the ability to anticipate, detect, respond, and predict attacks, and effectively recover from attacks. CPS-IoT 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. Advanced situation awareness allows us to maintain a tactical advantage over dynamic cyber-physical threats such as addressing moving target, persistent and evolutionary threats, and adversarial environments, and not least to integrate with human users.

The main aim of the proposed approach in **Paper 1** and depicted in **Figure** 2 is to provide a methodology for defending against dynamic and adaptive attacks to the CPS-IoT-enabled healthcare ecosystem. This will be achieved through

(1) a cognitive architecture for modelling humans' cognitive behaviour to anticipate and respond to new and emerging security and privacy threats,
(2) trade-offs and other contributing factors to get ahead of attackers' cognitive decision cycle accounting for uncertainties, and optimizing temporal feedback loops,
(3) integrate innovative mechanisms for security, privacy, metrics, and dynamic security knowledge base to enhance threat prevention, threat detection, incident response and mitigation of impacts,
(4) privacy-aware collaboration, computational techniques, adaptive data collection and actuation, and
(5) integrating cross-cutting techniques such as AI predictive analytics, machine learning approaches, run-time verification, evidence collection and tracing for evidence-based risk management and dynamic forensics.

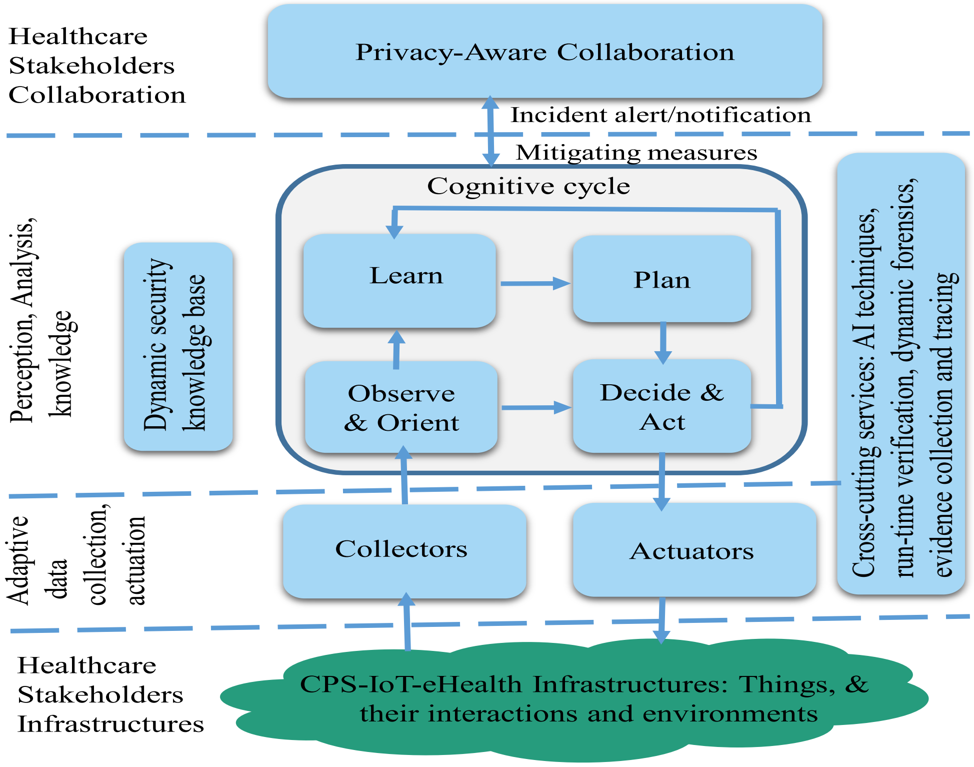
Healthcare Stakeholders Collaboration
Privacy-Aware Collaboration
Incident alert/notification
Mitigating measures
Perception, Analysis, knowledge
Dynamic security knowledge base
Cognitive cycle
Learn
Plan
Observe & Orient
Decide & Act
Cross-cutting services: AI techniques, run-time verification, dynamic forensics, evidence collection and tracing
Adaptive data collection, actuation
Collectors
Actuators
Healthcare Stakeholders Infrastructures
CPS-IoT-eHealth Infrastructures: Things, & their interactions and environments

Figure 2 - Cognitive Cybersecurity Architecture for CPS-IoT-enabled Healthcare Ecosystems

Figure 2 depicts the overall architecture of our cognitive cybersecurity for CPS-IoT enabled healthcare ecosystems with the building blocks in four layers: Healthcare Stakeholders Collaboration layer, Perception and knowledge layer, Adaptive Data Collection and Actuation Layer and Healthcare Stakeholders Infrastructures layer.

Cognitive cybersecurity, thus, aims to simulate human thinking and behaviours to anticipate and respond to new and emerging security threats, adapt constantly to changing security conditions including human participations, tasks and roles, and dynamically learn from experience and dynamic conditions. To achieve this, cognitive cybersecurity applies AI technologies patterned on human thinking processes to detect threats and protect cyber systems.

Artificial Intelligence/ Machine learning algorithms for cybersecurity make it possible for cognitive systems to constantly mine data for significant information and acquire knowledge through advanced analytics. Cognitive systems learn to anticipate threats and generate proactive solutions through continually refining methods and processes. This ability to process and analyse huge volumes of structured and unstructured data allows cognitive security systems to identify connections among data points and trends that would be impossible for a human to detect. Deep learning, which is the evolution of neural networks, enables the identification of complex attack patterns. ML techniques include artificial neural networks, support vector machines, clustering, explanation-based learning, induction, reinforcement learning, genetic algorithms, nearest neighbour methods, and case-based learning.

AI techniques are thus appropriate and effective solutions to meet the numerous characteristics of communications networks. These characteristics are relevant to CPS-IoT enabled services and infrastructures and include:

- ***Dynamicity***: AI techniques for planning under uncertainty make choices that will be appropriate even as the domain changes.
- ***Partially-observable***: AI techniques are good at inferring missing data and generalizing a situation so that decisions make sense for current conditions.
- ***Ambiguous observations***: AI techniques are good at recognizing ambiguity or low confidence and can either gather more information to discriminate or make decisions appropriate for both conditions.
- ***Resource constrained***: AI techniques are effective at scaling a solution to the platform they are operating on and designing tasks that manage available resources effectively.
- ***Diverse***: AI techniques consider diversity a benefit, as it allows resources to be managed in different ways.
- ***Massive scale***: Data mining and ML techniques are effective even on massive datasets; moreover, incremental planning and learning techniques.
- ***Complex access policies***: Knowledge engineering techniques can represent policies as constraints, and then constraint reasoning techniques can find satisfying solutions quickly incorporate new information efficiently and rapidly).

In sum, cybersecurity solutions utilizing AI and ML/deep learning can greatly reduce the amount of time needed for threat detection and incident response and can alert anomalous behaviour in real time.

References

[1] 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

[2] 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

[3] Habtamu Abie, Svetlana Boudko, Anticipatory Adaptive Security for IoT-based Smart Grids Infrastructure and Value-added Services, Deliverable D2.2.2, DART/09/20, 21. Sep. 2020