CyNetPhy: Towards Pervasive Defense-in-Depth for Smart Grid Security

Mohamed Azab[1(✉)], Bassem Mokhtar[2], and Mohammed M. Farag[2]

[1] The City of Scientific Research and Technological Applications, Alexandria, Egypt
Mohamed.m.azab@gmail.com, mazab@vt.edu
[2] Electrical Engineering Department, Alexandria University, Alexandria, Egypt
{bmokhtar,mmorsy}@alexu.edu.eg

Abstract. Security is a major concern in the smart grid technology extensively relying on Information and Communication Technologies (ICT). New emerging attacks show the inadequacy of the conventional defense tools that provision isolated uncooperative services to individual grid components ignoring their real-time dependency and interaction. In this article, we present a smart grid layering model and a matching multi-layer security framework, CyNetPhy, towards enabling cross-layer security of the grid.CyNetPhy tightly integrates and coordinates between a set of interrelated, and highly cooperative real-time defense solutions designed to address the grid security concerns. We advance a high-level overview of CyNetPhy and present an attack scenario against the smart grid supported by a qualitative analysis of the resolution motivating the need to a cross-layer security framework such as CyNetPhy.

Keywords: Smart grid · Smart grid security · Pervasive monitoring and analysis · Autonomic management · Elastic computing · Privacy-preserving

1 Introduction

The smart grid is a cyber-physical system that tightly integrates control, computation, and communication technologies into the electrical power infrastructure. Smart grid has emerged as the next generation power grid aiming at enhancing the efficiency, reliability, and resilience of legacy power systems by employing information and communication technologies (ICT) [7]. To establish the smart grid global vision, widespread sensing and communication between all grid components are established via communication networks and managed by cyber systems. Extensive deployment of and reliance on ICT inevitably exposes the smart grid to cyber security threats increasing the risk of compromising reliability and security of the electrical power infrastructure [6]. Scale and complexity of the smart grid network create several vulnerabilities providing numerous attack entry points. Inadvertent infiltration through infected devices, network-based intrusion, and a compromised supply chain are examples of such attacks.

C.G. Panayiotou et al. (Eds.): CRITIS 2014, LNCS 8985, pp. 275–282, 2016.
DOI: 10.1007/978-3-319-31664-2_28

Liu *et al.* presented a detailed overview of relevant cyber security and privacy issues in smart grids [5]. Authors showed that every aspect related to cyber technology in the smart grid has potential vulnerabilities due to inherent security risks in the classical cyber environment.

The proliferation of increasingly sophisticated cyber threats with massive destructive effects, necessitates that smart grid security systems must systematically evolve their detection, understanding, attribution, and mitigation capabilities. Unfortunately, most of the current security systems fall short to adequately provision security services while maintaining operational continuity and stability of the targeted applications especially in presence of advanced persistent attacks. Most of these security systems use uncoordinated combinations of disparate tools to provision security services for the cyber and physical domains. Such isolation and lack of awareness of and cooperation between security tools may lead to massive resource waste due to unnecessary redundancy, and potential conflicts that can be utilized by a resourceful attacker to penetrate the system. Recent attacks against the power infrastructures such as Stuxnet have highlighted vulnerabilities and inadequacy of existing security systems. The Stuxnet worm infects the cyber domain (computers and workstations), spreads via networks and removable storage devices, and exploits four zero-day attacks to manipulate the physical equipment. The primary target is believed to be an Iranian nuclear power plant, and likely caused a 15 % drop in production of highly enriched uranium [3]. Defense against complex cyber threats such as Stuxnet, requires coordination between various security domains to address strict security concerns.

Figure 1 depicts a hierarchical model of the smart grid as a set of correlated interacting layers where each layer has a complete hierarchical layering model. At the top of the model is the grid users and system operators with direct access to the physical domain of the grid. The next layer represents the physical systems and components participating in the generation, transmission, distribution, and consumption sectors. The physical domain is managed and controlled by a cyber-base that provides the needed computation and communication services facilitating local control and processing operations and inter- and intra-communication between the physical and the cyber domains. The physical domain is tightly coupled to the cyber domain via a cyber-network represented by a network layer encapsulating both data and control traffics.

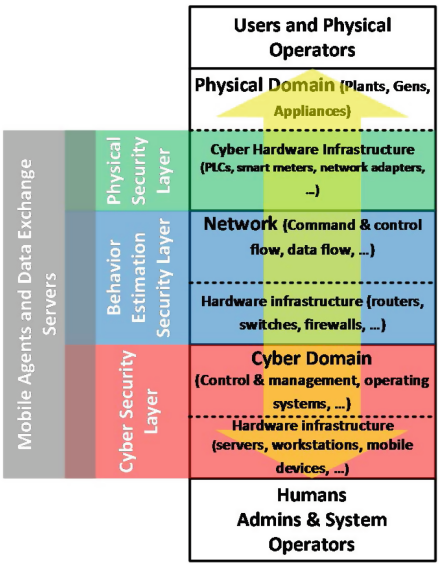

Fig. 1. Smart grid hierarchical model and layers interaction with CyNetPhy

The cyber domain is represented by two sub-layers, the cyber or the application sub-layer where the management and control logic resides, and the hardware sub-layer hosting such logic and providing the needed interfaces for data exchange. The high-level system management resides in the upper two layers, the Cyber layer where the management and control application and software are running on top of a hardware layer and operated by a set of operators and administrators.

Each layer in the presented model denotes a broad hierarchical model encapsulating interrelated sub-layers. For example the network layer in the smart grid model is a representation of the hierarchical OSI model. Most security systems addresses security of a single layer or sub-layer neglecting security concerns of other layers and interaction between interrelated layers. The smart grid with its large scale, complexity, and importance is an easy target for such at-tacks exploiting the lack of collaboration between security tools at different layers.

We advance an integrated security framework, termed CyNetPhy, supported by three main pillars namely, the Cyber Security Layer (CSL), the Behavior Estimation Layer (BEL), and the Physical Security Layer (PSL) collaborating towards enhanced smart grid security. Figure 2 illustrates The CyNetPhy multi-layer architecture.

In this article, we present a high-level description of the CyNetPhy security framework and introduce an attack scenario supported by a qualitative analysis showing the need to the CyNetPhy cross-layer security framework. For further details about the CSL,BEL, and PSL please refer to [1,2,4,8]. The remaining of this paper is organized as follows: Sect. 2 provides a brief overview of the CyNetPhy framework. An attack scenario and a qualitative analysis of the resolution is introduced in Sect. 3. Conclusions and future work are portrayed in Sect. 4.

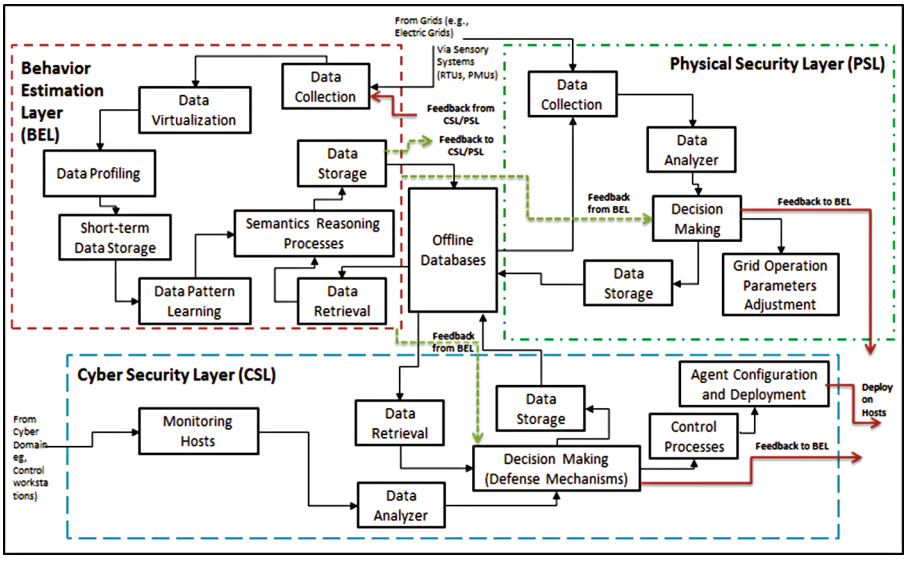

Fig. 2. The CyNetPhy architecture

2 CyNetPhy Framework Overview

The BEL monitors, analyzes and learns patterns of grid data and control flows independently extracting semantic feedback about the behavior of each grid component. The independent feedback by the BEL relies on deploying distributed dynamic reasoning models in order to fine-granulate semantics extraction processes to build efficient dynamic behavior models regarding normal/abnormal behavior of various grid components. Data profiling and dimensionality reduction techniques are used to enable efficient data storage and pattern learning. Analyzing the data flow independently from the control flow enables the BEL to spot accidental/deliberate human errors. The BEL is the intelligent part of CyNetPhy with the ability to read between the lines and initiate proactive measures to counter potential cyber threats in collaboration with the PSL and CSL.

The CSL is responsible for monitoring the cyber layer using a set of smart distributed mobile agents, pervasively crawling the systems cyber and physical domains searching for possible attack indications. In addition to the smart utilization of the agents in provisioning on-demand conventional defense services to the cyber hosts, the CSL collects host-oriented real-time feedback from its agents investigating various aspects that might to be an indication for a malicious behavior not detectable by regular techniques. The CSL is a responsible for information sharing between the three CyNetPhy security layers.

The PSL is responsible for monitoring and securing individual cyber systems with direct access to the physical domain. The cyber layer comprises a set of application-specific embedded systems and devices with clearly defined functionality and objectives. Usually cyber-attacks against this layer aim at misleading the upper layers of the grid or disrupting the underlying physical systems by compromising the operation of the cyber components. Clarity of objectives for both cyber systems and associated threats facilitates deriving security policies and specifications to protect cyber systems in the physical domain. Security policies are derived from the system physical characteristics and component operational specifications, and translated into security monitors and components that can be implemented in either hardware- or software-based platforms. Hardware-based security is preferred due to the hardware immunity against software attacks and high-performance offered by hardware [4]. The PSL collaborates with the BEL and CSL by exchanging relevant data, delivering accurate measurements about particular systems, and applying adequate measures in the physical domain.

The inter layer interaction is established through a set of circulating CSL mobile agents collecting high-level feedback from the three layers and feeding it to the data exchange servers. These servers are considered as the memory for the BEL. Patterns of maintained data in those servers are learned by the BEL for behavior estimation and semantics extraction. The security framework has three phases of operation: real-time monitoring, anomalous event investigation, and proactive actuation. In the monitoring phase the three security systems monitor and analyze real-time data and operation of the under-lying protected layers and pass abstract reports to the BEL to be analyzed at a higher abstraction level. Upon detecting anomalous or malicious behavior, the concerned layer initiates

the investigation phase where the three security layers exchange relevant data to ascertain about the event and initiate the resolution procedures. In the actuation phase the concerned layer applies a set of actions and measures to resolve detected attacks. Countermeasures include raising alarms to system operators and isolating and finding suitable alternatives for infected systems.

3 Attack Scenario

To further motivate our research and to illustrate the effectiveness of CyNetPhy in achieving its mission we utilize the following working scenario depicting a hypothetical Smart Grid attack named the BlackWidow (BW) attack. The main players are a resourceful malicious organization XYZ trying to sabotage infrastructure assets for a neighbor country. The victim in this attack is the country's smart grid, namely the power distribution section. The BW is designed to split into a set of code parts and spread in different directions and locations to decrease the probability of detection. The distribution of parts and the interconnection between them in different hosts weave a large web. This web is bi-directionally traversed to send any harvested data from the attacked target and to update the malware with new tools and missions. The BW is designed to be as generic as possible; it is not oriented to any specific application. By constructing the BW web the attacker can start to task the BW towards its designated mission based on the attackers target. BW tasks might be remotely assigned through internet or preprogrammed in internet-inaccessible locations.

The attack is designed to be stealthy by hiding from the security system sensors searching for attack signatures. The attack will target an intermediate host machine that shall host the BW command and control channel communications. In order to do so, the BW is designed to not harm the host or change any of its settings that might raise the anti-malware alerts. The malware will use minimal resources and will work in a very slow fashion not to alert the security systems of its existence. The BW uses stolen digital certificates to authenticate its existence in the host machine in the form of drivers. The only way to detect this malware is through deep analysis and investigation for the entire system component behavior, this includes both Cyber and physical components. Current oblivious defense tools that shares the same host resources with its targets cannot realize such level of awareness. Additionally, most of the physical components are always assumed to be secured by perimeter defenses with no/limited consideration to the other security measures. The attacker utilizes these limitations to his advantage as illustrated later. The malware is intended to be targeted, but due to the intentionally random deployment method, the code works in two modes as follows: (1) Benign mode where the malware infects other machines that do not belong to the target space. Those machines might be used later in case of target change, or as a base for future attacks; and (2) Malicious mode, where the BW works only on the target host systems.

3.1 Attacker Assumptions

1. The security and management system shares the same network or host with the target of attack/security system. [Note: security system might be exposed to attack by compromising the Target of Security (ToS). Additionally, stolen passwords can simply be used to modify rules of IDS, routers,firewalls, proxies, etc].
2. The ToS or major parts of it uses COTS and signature based security products.
3. The system is computationally incapable of being fully situation aware of all its components in a massive-scale network, in real-time.
4. Cyber security is oblivious of and is not coordinated with physical security to protect the target cyber- physical system.

3.2 Attack Procedures (in Air-Gapped Target)

The attacker uses phishing attack or an insider to inject the malware seed into the grid computers. The BW is programmed to search the network for connected computers then it starts using one of the zero days exploits to clone itself into these computers. The attack victims will receive parts of the malware. Each of these parts will contain a fraction of the designated mission and a simple communication module. The communications module will be used to open a direct channel with the attacker and to search and establish communication with other parts. Directions to other parts locations might be sent by the attacker to minimize the search time.

The attacker uses malware fractions to construct logical executable entities in the form of mobile software agents targeting different objectives. The first objective will be to search and infiltrate the network for data stores. The malware will sniff the network traffic searching for predetermined signatures for such locations. The second objective will be to attack such data stores using the zero day exploits and the stolen certificates to locate the power distribution planer and the RTU command and configuration credentials. The malware will frequently update the attacker of its findings based on a predetermined update methodology. After successful reception of this data, the attacker will use it to transfer the BW to the grid Command and Control Center (CCC) using a compromised RTU hocked on the grid. The CCC controls the entire grid by real-time configuration of the distributed RTUs managing the operation of the distribution centers.

The drastic effect of the attack begins when the BW use the stolen configuration credentials to reprogram the RTUs to include a set of programmed blackouts across the nation among a series set of power overloads on the transmition lines causing them to breakdown. The attacker can launch data injection attacks that propagates through the network and send fake power shortage and network overload indications. Such attacks cause imbalance between the generation and demand power which can directly result in a major financial lose.

4 Conclusions

We have presented a multi-layer model of the smart grid and a matching cross-layer remote defense and management framework, termed CyNetPhy. CyNetPhy integrates and coordinates between three interrelated and highly cooperative real-time defense systems crossing section various layers of the smart grid cyber and physical domains. We presented a complex synthetic attack scenario to illustrate the limitations and challenges of the current SG defenses. In this section, we shall discuss how CyNetPhy invalidates the attacker assumptions, the pillars that supports that attack. The first two assumptions assumed that the defense platform shares the same host with the ToS and uses a signature based COTS defense products giving the attacker the chance of disabling or even tricking the defense system. CyNetPhy presents a smart isolation of defense and control concerns into a set of stacked self-managed interconnected layers of hierarchical distributed management. CyNetPhy operates from a remote secure cloud-like platform isolating the computational needs of the defense platform from the resource constrained grid hosts. CyNetPhy delivers its monitoring and defense services through a circulating mobile agents hiding the platform heterogeneity from the defense and control. It delivers tailored defense services to each host when needed and where needed. These features invalidates the first two assumptions. CyNetPhy Layers are highly cooperative, each layer exchange its defense related feedback with the other layers through CyNetPhy brain that process such feedback and provide directed guidelines to each layer taking into consideration the current state to the other layers. Such level of global awareness invalidates the last two assumptions and the entire attack. Our future work includes building network and security threat models for CyNetPhy. These models can be used to construct a complex large-scale simulation scenario for various smart grid cyber and cyber-physical attacks, showing the effectiveness of the comprehensive CyNetPhy's subsystems in detecting and mitigating such attacks.

Acknowledgment. This work is supported by the SmartCI Research Center, Alex., Egypt.

References

1. Azab, M., Eltoweissy, M.: Defense as a service cloud for cyber-physical systems. In: 2011 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), pp. 392–401. IEEE (2011)
2. Azab, M., Eltoweissy, M.: Bio-inspired evolutionary sensory system for cyber-physical system security. In: Hassanien, A.E., Kim, T.-H., Kacprzyk, J., Awad, A.L. (eds.) Bio-inspiring Cyber Security and Cloud Services: Trends and Innovations. ISRS, vol. 70, pp. 39–69. Springer, Heidelberg (2014)
3. Chen, T.M., Abu-Nimeh, S.: Lessons from stuxnet. Computer **44**(4), 91–93 (2011)
4. Farag, M.M.: Architectural Enhancements to Increase Trust in Cyber-Physical Systems Containing Untrusted Software and Hardware. Ph.D. thesis, Virginia Polytechnic Institute and State University (2012)

5. Huang, Y.F., Werner, S., Huang, J., Kashyap, N., Gupta, V.: State estimation in electric power grids: Meeting new challenges presented by the requirements of the future grid. Signal Process. Mag. IEEE **29**(5), 33–43 (2012)
6. Kopetz, H.: Real-time systems: design principles for distributed embedded applications. Springer, Heidelberg (2011)
7. Liu, Y., Ning, P., Reiter, M.K.: False data injection attacks against state estimation in electric power grids. ACM Trans. Inf. Syst. Secur. (TISSEC) **14**(1), 13 (2011)
8. Mokhtar, B., Eltoweissy, M.: Hybrid intelligence for semantics-enhanced networking operations. In: The Twenty-Seventh International Flairs Conference (2014)