Interoperating Smart Grid Cyber Security Systems: Adaptive Risk Management across Unified OT and IT Domains

Partha Datta Ray, Ranjit Kumar, Christopher Reed, Atul P. Agarwal

Albeado, Inc.
18640 Casa Blanca Lane, Saratoga, CA 95070
partha.dattaray@albeado.com

Keywords: interoperating pervasive smart grid security, distributed and adaptive security risk management, unified OT and IT systems security risk control, context and situation aware power system security, automated risk model with self-similar security analysis and control elements

Abstract

Convergence of Utility Business Information Technology (IT) and Power System Operation Technologies (OT) are bringing new protocol, analysis and performance challenges for interoperable end to end security risk management systems. Successful solutions should exploit grid and information system domain contexts so that security postures of the grid can adapt to the situational awareness based on near real time security state and events of power and information systems. Security analysis and control systems should also leverage the interplay of security, reliability and stability in the smart grid through unified vulnerability models and threat analyses for the OT and IT domains.

We present essential characteristics and properties for Interoperating Smart Grid Cyber Security Systems that are functionally pervasive, topologically distributive yet flexible in supporting traditional and emerging smart grid characteristics (e.g., distributed renewables integration, pervasive monitoring and control for automated decision intelligence). Such systems need to balance the challenges of different security postures that the OT system warrants where availability and data integrity is paramount vis-à-vis the IT system where confidentiality takes priority. Such solutions should be aware of the differing safety and cascading impacts that external attacks, malicious insider breaches, or erroneous operations could have on the power grid or the information systems.

1. INTRODUCTION

The electric power grid is slated to evolve into a significant force of economic value creation by ushering in a paradigm shift in ways electricity is produced, traded and consumed. The evolving Smart Grid is based on visions of modernization of the electricity generation and delivery systems to enable integration of diverse generation and storage options, to create and support newly imagined markets and operations, to invite richer customer participation, and to enhance resiliency of the power grid – all while improving unified [1]cyber security risk management [1,2] of the OT and IT systems. This integration in turn would involve diverse, interoperating, interdependent and adaptive functions and applications to enhance grid reliability and stability, improve capital and operational efficiency and ensure improved security of the electric grid.

In contrast with the current mix of traditional and renewable resources, the smart grid is envisioned to be ultimately based on very large penetration of renewable resources with end-to-end direct transactions between producers, wholesalers, retailers and consumers as well as diverse opportunities for trading among them. Such transactions will be facilitated market service providers and connectivity providers much the same way e-commerce and other online business transactions and interactions are enabled by internet and e-commerce service providers (SPs) like eBay, Amazon or AT&T Such service providers will likely offer all necessary infrastructure for transmission and distribution of energy as well as the relevant information and data exchanges. Trading of power and various services based on allied information will enjoy internet- enabled market transparency and ease of execution [3].

Such future imperatives along with today's competitive market forces make utilities rely heavily on a robust business information environment that requires interconnections among the control and business information system domains, the external internet, supplier and other peer organizations. Integrating operational information like equipment status, phasor measurements, distributed generation and storage status with business level information such as consumer preferences and energy usage and market prices allows organizations to improve overall enterprise productivity through higher end to end business

[1] Some of the materials presented here are covered by multiple pending patents

and operational efficiency analysis while reducing grid stress and vulnerability.

As a result, the power grid operational system is evolving from relatively isolated clusters of computers running stand alone applications on a proprietary (thus "secure through obscurity") platform to a highly interconnected and interdependent system of local and wide area information and communication systems. Consequently, it is being exposed to new and emergent vulnerabilities and risks which are very different in size, scope, likelihood and frequency of occurrence than what traditional system and risk analysis would suggest.

The power grid operation systems have unique performance and reliability requirements. Repurposing security mitigations commonly effective in the IT domain for use in the grid operations domain is rendered much more challenging by limited availability of computation and communication capabilities in legacy system platforms. Examples of such limitations include legacy Intelligent Electronic Devices (IED), the slow serial links through which communications among substations, control centers and field equipments take place and clear text communication protocols like Supervisory Control & Data Acquisition (SCADA) over Modbus or Distribution Network Protocol (DNP3).

Convergence of Utility Business Information Technology (IT) and Power System Operation Technologies (OT) are bringing new protocol, analysis and performance challenges for interoperable end to end security risk management systems [4, 5, 6].

It has also been observed that leveraging the interdependency of security, reliability and stability of the power grid in a virtuous coordination enhances the overall operation and efficiency of the solution. For example, domain aware analysis of data (phasor measurements, IEDs, meters) could provide telltale signs of certain breaches of security in the IT System and detection of certain intrusions in the IT System could be used to harden OT resources for improved resilience of the power system.

As the OT and IT systems integrate more, security control solutions are also evolving to address the emerging vulnerability and threat impact. Unified IT and OT security risk analysis and control systems will leverage traditional security measures which are often point or perimeter solutions applied to each target system - be they computers, networks or applications. Today, these methods (e.g., Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS), end point device security, firewall protection of LAN) usually lack the correlated domain and situational awareness needed to analyze events and inputs. As a result they are not in a position to respond with right-sized situational security by adapting their security postures to evolving situations and transitions. Pervasive monitoring and control, as presented here, will be able to provide automated risk analysis in appropriate domain and situational context. That in turn will enable distributed security control to coordinate and evolve with changes in operational and security state and events thus making not only the IT system but the integrated IT and OT system both robust and resilient to attacks, accidents and operational errors.

A critical requirement to build the security risk management system presented here is the interoperability of diverse data collection devices (e.g., meters and sensors), various analysis programs correlating them with other power system and customer data and of course all the security risk control elements. These devices and programs, possibly provided by different vendors, will need to interactively coordinate to provide such functionally pervasive yet context aware security risk analysis and control systems. Interoperability among them is a critical requirement to unleash the innovation, competition and emergence of a sustainable ecosystem for integrated security and risk mitigation. That in turn will usher in systemic treatment of security risks and help move the state of the art beyond ad-hoc point and perimeter security solutions.

Interoperability is best supported by layered architecture approaches. Organizing IT system infrastructures into various layers has enabled the explosive growth of the internet with unprecedented value creation for businesses, individuals and societies by greatly enhancing the "plug and play" interoperability between equipments of different vendors and in fact between different networks using diverse physical and link layer protocols like Ethernet, Fibre Channel, WiFi, WiMax, LTE and so on. The resulting innovation and competitive cost-reduction have largely been the driving force behind the internet build-up of the last two decades. Technical issues in one layer are largely insulated within that layer so that the implementation choices of one layer are independent of the implementation of other layers. This layered architecture also allows for future extension of layers without making earlier layers obsolete.

The layers of two architectural models, GWAC (GridWise Architecture Council) and OSI (Open Systems Interconnection) are shown in Figure 1. The technical issues of basic connectivity, network level interoperability and part of syntactic interoperability (first 3 GWAC functionalities) are typically addressed in the first 4 OSI layers designated as physical, data link, network and transport layers. Basic informational protocol issues (next 2 GWAC functionalities) are addressed in the next 3 OSI layers designated as session, presentation and application layers.

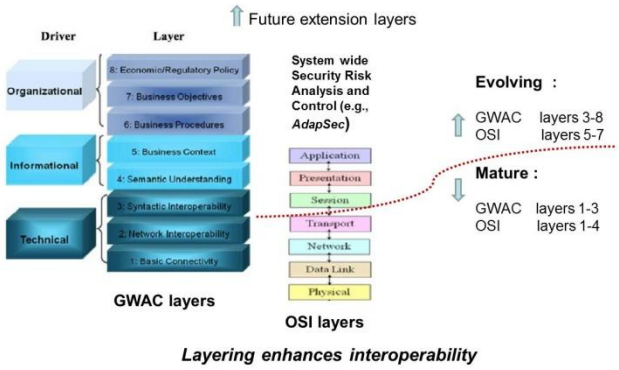


Fig.1: GWAC and OSI: Experience in Interoperability

Layered implementation also best enables evolutionary development of higher levels of abstraction in additional informational and organizational layers described in the GWAC stack such as Business procedures, business objectives and economic/regulatory policies.

Traditional information security measures can take on many forms like (a) perimeter, host or application security based on passwords and digital certificates for authorization and authentication checks at an entry point (e.g., gateway to a network, port of a computer, remote call to an application) (b) host, storage and application security based on scanning for signatures of known malware (e.g., viruses, worms, etc.) either at the entry point or after the fact scan of various memory and storage elements (c) perimeter security based on filtering out unwanted sources and destinations (d) data security based on cryptographic measures and key managements. But these point or perimeter solutions applied to host computers, networks or applications often work with little knowledge of each other's functions and capabilities. Lacking the correlated domain and situational awareness needed to analyze events and state inputs, they fail to respond with right-sized situational security and often overwhelm administrators with deluge of messages without helpful contexts. Also, their influences are generally limited to OSI layers 1-3 and GWAC layers 1-2

.

Plethora of solutions exist for layers 1 – 4 of OSI model and all end to end SG security frameworks will need to be flexibly built on them. The focus of this paper is technologies necessary for improving cyber security at higher levels (OSI layers 5-7 or GWAC levels 4-8). Evolving cyber security solutions (e.g., AdapSec [7]) will also need to leverage mature risk management approaches, including automated risk analysis by correlating situational and domain contexts captured in GWAC layers 3 and below and processed at layers 4 and above. Risk governance artifacts like security blueprint, security policies, security processes and security rules could be used to determine appropriate risk mitigation and security postures. Thus the higher layer GWAC information and procedures will work with monitored inputs to generate the security controls.

In order to be truly successful for the Smart Grid (SG) domain, such systems should exploit grid and information system domain awareness so that security postures of the grid can continuously adapt to the situational context based on near real time security state and to events across the integrated OT and IT domains of the electric utilities. Such frameworks will allow an evolving "intelligence" to "right size" the end to end security depending on component level security, and available resources. Conceptually such framework could encompass data centers and IEDs as well as emergent infrastructure and processes. They could also address integration of legacy systems using robust security wrappers.

To be successful, security postures of the grid need to adapt to the OT and IT state and events in nearly real time, based on unified risk assessment methods which are aware of the interplay of security, reliability and stability of the end to end Smart Grid (SG). A slower paced adaptation responding to changes in threat profile, emergent vulnerabilities, security audit, resource availability etc. drives the security process or blueprint changes.

Profiles of threats against the power OT system functions, where integrity of data and availability of information are paramount, differ significantly from those against IT functions such as utility customer billing where confidentiality is a greater concern – hence warranting a different security posturing. The security systems should balance the challenges of these differing security postures. Such solutions should be aware of the differing safety and cascading impacts an attack or erroneous operation could have on the power grid or the information systems.

2. OVERVIEW OF UNIFIED SMART GRID CYBER SECURITY

A schematic representation of a typical enterprise-wide IT infrastructure is depicted in Figure 2. The network infrastructure consists of several clusters of computers (servers and clients) connected to one or more communications networks. Typically a "client" sends a "request" for information to the "server" via the communication network. The "server" provides the requested information to the "client" via the network. The designation of any given computer as a "server" or "client" is not absolute and can change depending on its role in the

transaction at hand. Depending on the main function of a "Server" it may be designated by various names such as "Application Server", "Database Server", "Web Application Server", "Data Acquisition Server", "Web Server", "Proxy Server", "Enterprise Message Server" etc. The communication network can comprise of one or more of elements commonly known as Internet, Intranet, LAN, WAN, etc. These networks may use various protocols to manage the exchange of messages (i.e., "requests" and "responses") between the appropriate source and destination computers. The computers should be capable of sending and accepting messages in the relevant protocols.

Computers within each cluster can communicate with each other through infrastructures like an Enterprise Service Bus (ESB). Each ESB may be connected to the global internet either directly or indirectly through an enterprise-wide ESB. A computer (server or client) may be a real computer or a virtual computer. A computer may have numerous peripheral devices for various functions (e.g., input, output, communication, data storage, etc.). Each computer may host a number of computer programs (e.g. applications) which interact with each other through various messages which could be as large as the largest file being exchanged and as small as a command code containing only a few bits (e.g. to turn a breaker on or off).

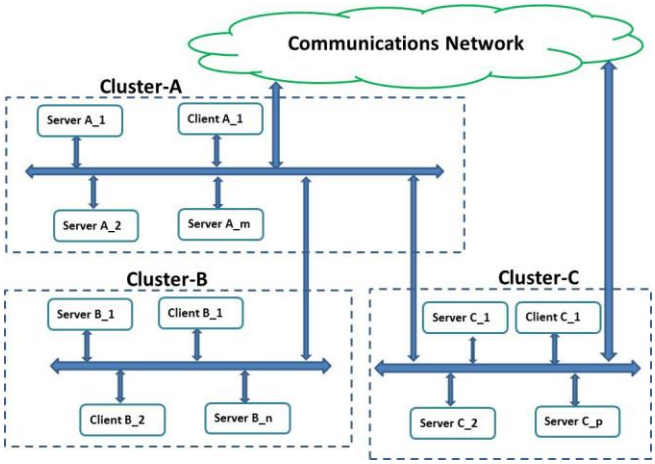
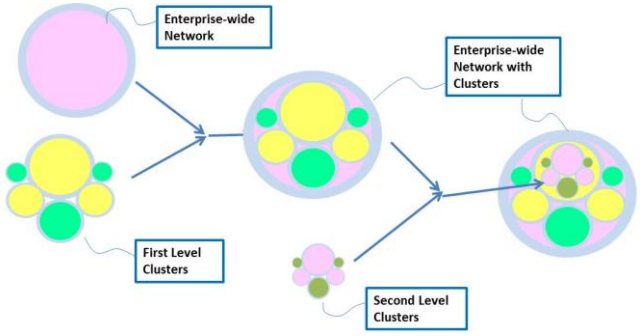


Fig. 2 Enterprise-Wide Computer Network Architecture

An enterprise-wide information system network composed of OT and IT network itself can be seen as a component of a larger network of many such networks representing various enterprise domains, suppliers, customers, regulatory agencies and other stakeholders. Similarly, each cluster and subnet of computers, networks and applications in the network can itself be seen as an extremely complex network of diverse components. Thus the IT network can be seen as a hierarchical composite system of pervasively distributed self-similar elements.

Therefore a unified smart grid cyber security system should also be distributed pervasively throughout the enterprise-wide OT and IT systems of an electric utility as depicted in Figure 2.

Fig. 3 is a schematic diagram showing the functional pervasiveness and structural self-similarity of the solution domain over various hierarchical levels of the network. The largest all encompassing circle represents an enterprise-wide computer network to be protected. It can be seen conceptually as embedded in a computer network of a larger global set of enterprises (not shown in Fig 3) and protected by a perimeter from external malicious agents. It also encompasses smaller circles representing clusters of subsystems within the enterprise. Some subsystems are large and others are small. Each subsystem encompasses other yet smaller circles representing lower level subsystems and individual computers and so on. The computers in turn encompass other smaller monitored and controlled elements (MCE). This hierarchical representation can be carried down to as many levels as necessary to include all MCEs and the underlying business processes.



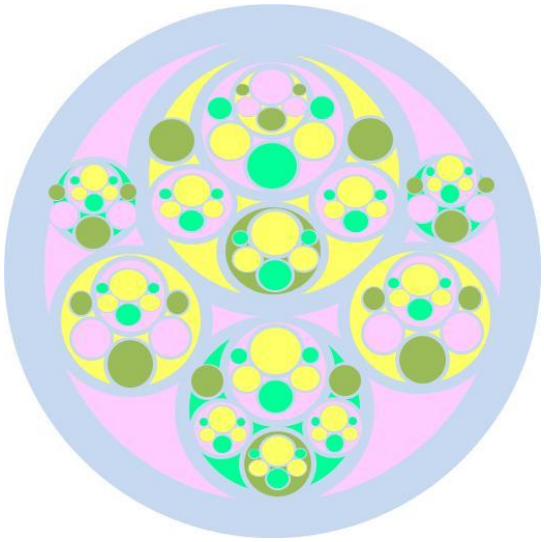


Fig. 3- Functionally and Structurally Pervasive Architecture

FIG 4 shows the control hierarchy associated with the monitored and controlled elements (MCE) of the enterprise-wide network. The capability for monitoring, analyzing, and adjusting security postures is pervasively implemented. The entire enterprise-wide network is at the highest level of the control hierarchy. This Enterprise MCE monitors and analyzes the collection of all information exchanges going through a designated Enterprise Service Bus (ESB) including messages to and from external computer network systems (e.g. partners, customers, regulatory authorities, markets, etc.) through dedicated networks or the internet.

At lower levels of the hierarchy lie the individual computers, applications and local networks (e.g, "Server Security Engine, SE" in Fig 4). The Server SE monitors, and analyzes the collection of all information exchanges going through the various ports of the computer including all the inputs and outputs including reads and writes to its databases.

Each of the monitored and controlled elements (MCE) at the lower hierarchy levels of applications, databases and messages can have their own security engines (SE) for monitoring and analyzing all relevant information and providing the security control postures.

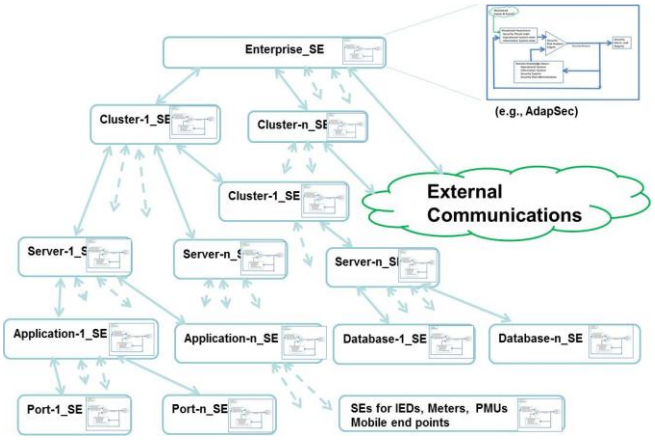


Fig. 4 System Security Monitoring & Control Hierarchy

An overview of the architecture of the unified OT and IT domain aware adaptive security system is illustrated through figures 5 and 6. Both the real time operational interactions among its various components and updates of longer periodicity are described below.

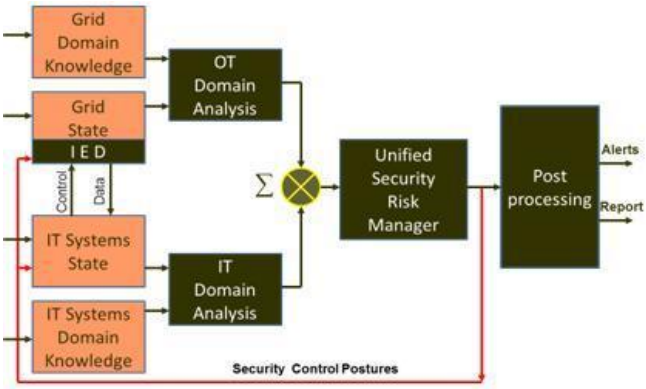


Fig. 5 Real time Adaptive Security System

Figure 5 shows how the security control posture changes in near real time (order of milliseconds to hours) in response to changes in the power and/or information system state changes due to security, reliability, stability related incidents or events. The block labeled IED (Intelligent Electronic Devices) represents the aggregate information system embedded in the field equipment at substations and central power stations as well as transmission lines and distribution feeders.

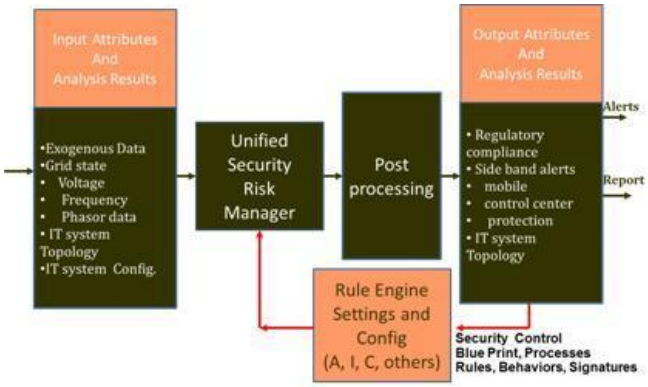


Fig. 6 Longer Periodicity Adaptive Updates

The objectives of adaptation include:

- Increasing or decreasing the security levels associated with various grid components and IT system components according to the threat environment inferred from various grid and information system states and other inputs
- Right sizing security by balancing costs against benefits. In the real-time context, this involves the allocation of available IT resources for processing security related functions versus business related functions. For example, when the power system is undergoing certain changes, the volume and variety of grid information related transactions may increase and if necessary, some of the low priority security related transactions may have to be curtailed. In the maintenance/upgrade mode, "right sizing" involves balancing the life-cycle costs of security against the grid-related benefits.

3. SECURITY RISK MODELS

To evaluate security (or other) risks in a large enterprise one has to employ a systematic methodology to cover all assets of the enterprise. Such methodology should consist of the following steps:

- Identify all assets that are important to the business goals of the enterprise
- Assess vulnerabilities of each asset
- Analyze all potential threats that can exploit the identified vulnerabilities
- Identify appropriate security control mechanisms against each threat
- Determine optimum security postures for each asset

Each of the above steps should focus on arriving at a description of the assets, vulnerabilities, threats, security control mechanisms and security postures that can facilitate automated analysis to arrive at unambiguous actionable results. Such descriptions should be based on comprehensive sets of qualitative or quantitative metrics. Various security metrics are being defined in the industry for general purpose IT Systems [8,9]. They can serve as a starting point for the development of metrics necessary in the Security Risk Manager (SRM). However quantitative metrics are essential for implementing fine grade adaptation capabilities while qualitative metrics may be sufficient for coarse grade adaptation.

For most systems, dependable numerical values for quantitative metrics are not available. However a properly designed SRM can start with proxy values initially and over time collect the historical data that can help in fine tuning those values.

Some of the metrics can be useful as a parameter specification for designing an SRM. For example, the parameter mean-time-between-attacks depends on the motivation and opportunity of hackers to attack. However a reasonable range of value(s) can be used to determine how often a security scan should be performed and the corresponding quantity of IT resources to be allocated for such scans. This in turn will help in assessing the associated costs and benefits even if no specific real-world value for the metric is known.

Some of the metrics should reflect the performance quality of the SRM in a simulated test environment or in the real world. Examples of such metrics include percent of attacks detected, mean-time-to-detect, mean-time-to-quarantine, mean-time-to-service-restoration.

Other metrics can be indicators of the impact of an attack. The impact can be in terms of damage to equipment, loss of revenue, consequential losses of customers and other stakeholders, and damage to public relations.

Metrics should represent various aspects of the power grid OT and IT domains at an appropriate level of granularity. For example, in designing the SRM, if the smallest breach of security is represented by the same value as the most severe, and the impact of the smallest loss of service on a distribution system by the same value as a large-scale blackout, then the resulting SRM would be prohibitively expensive.

Some example metrics are discussed in Section 4.

4. SG CYBER SECURITY METRICS

Since an exhaustive list of metrics relevant to the cyber security of a smart grid is too large to be included in this paper, the following subsections provide only a glimpse into the considerations that go into defining a comprehensive set

of metrics in a unified consideration of the OT and IT domains.

4.1. Assets and Services

Metrics to model assets and services could represent their impact on the revenues and costs to enterprise, to customers and other stakeholders. The assessment of the impact should include consideration of the periods of normal operation, disruption of normal operations and time to restore normal operations. Typically use of redundant equipment will minimize the impact of loss of service from a single asset.

4.1.1. Power Systems

Power system and IT system equipment essential for maintaining the stability of the grid and/or IT system should be given high importance. The equipment relevant to service quality should be treated as of mid-level importance. Equipment relevant to energy efficiency can be treated as of a lower-level importance.

Power system service impacts vary by the nature of the impacted loads. In general, facilities containing life support systems should be treated as of the highest level of importance. Hospitals, traffic lights and certain preregistered residences are examples of such facilities. Public safety facilities should be ranked based on their scope. Examples include City Police Office, precinct level police station, fire station, main thoroughfares, air and other transport centers etc.

4.1.2. Information Systems

Typically, IT systems are organized by hierarchical zones with each zone having its own security level. Contact between the zones should be handled through designated gateways. There should be redundancy of the gateways so as to minimize the adverse impacts in cases of malicious attacks or other failures.

Each IT system component should be assigned its importance based on the impact of its failure on the business objectives.

4.2. Vulnerabilities

Vulnerabilities are intrinsic to either individual equipment or groups of equipment. Both physical and informational vulnerabilities have to be assessed.

4.2.1. Power Systems

Examples of power system vulnerabilities that affect security postures include:

- Weather (probability of lightning or fire along a transmission right-of-way)
- Loading levels (higher transmission loading levels make the system prone to instabilities)
- Risks to energy supplies (frozen waterways, broken gas or oil pipelines, political unrest along transportation routes, etc.)

4.2.2. IT Systems

Examples of IT system vulnerabilities that affect security postures include:

- Tampered data in control signals (e.g. open or close breakers)
- Tampered operational data (e.g. leading to incorrect operation of control)
- Risk of fire in the data center
- Risks to communication links(storm, fire, political unrest along transportation routes etc.)

4.3. Threat Models

Threats should be assessed in the context of the vulnerabilities that could be exploited. Both intentional attacks by miscreants as well as accidental adverse events should be considered.

4.3.1. Motivation

Monetary gain as a motivation can be quantified based on the value of the specific attack target and the difficulty of attack against the specific target.

Motivation of belligerent states and terrorists depends on the importance of the target to the national infrastructure or as a symbol of national identity. It can vary in time based on the political climate.

Motivational levels of disgruntled insiders can be fairly intense, usually for short periods of time.

Motivation associated with opportunity to boast about an attack depends on the value of the target as a symbol of invulnerability and the difficulty of the attack

Motivation level associated with inadvertent security incidents should be assigned a small value commensurate with the observed rate of such incidents.

4.3.2. Attack paths

Methods of attack are a function of the motivation and the vulnerabilities of the associated target as well as the technical capabilities of the attacker. For the purposes of the SRM, they can be quantified based on the ease of execution and importance of the target and probability of success of the method. The impacts of attacks can vary significantly based on the nature and scale of attacks.

Attacks on power systems may include direct attacks on the power system hardware or rights-of-way or other energy supply routes. This may include:

- Tampering with switching devices at Distribution Networks
- Tampering with switching devices at Transmission Networks

Attack paths targeting IT systems may include the following:

- Tampering with Meter Reading and other measurements data
- Tampering with electricity pricing data
- Tampering with usage data (time of usage etc.)
- Tampering other operating data

4.4. Security Controls

Security controls should be assessed in the context of the threats that need to be averted. It may be necessary to use more than one security control mechanism to thwart one threat, and conversely a single security control can thwart several threats. There are no fool-proof security solutions that can guarantee security indefinitely. Therefore metrics for modeling security solutions should be time based. Examples of the metrics include:

4.4.1. Time to detect attacks

Time to detect an attack depends on the nature of the attack as well as the monitoring capability of the SRM. This metric can be used as a design objective. The time to detect can be minimized by increasing the frequency of security scans and/or by other means such as "honey pots" (i.e. fake targets to trap potential attacks and attackers). Using multiple independent detection schemes can increase the probability of detection and consequently decrease the time to detect.

4.4.2. Time to respond

Time to respond is determined by the nature of the response. The response could be as simple as dropping suspect data packets or terminating the suspect session. It can be more involved as in quarantining data packets, computers, security zones, etc. for further analysis.

4.5. Security Postures

Security postures should be determined in the overall context of the importance of the target assets, severity of their vulnerabilities, probability of the occurrence and success of the threats that exploit those vulnerabilities and the effectiveness of the security control measures against those threats. An optimization process could consider the total enterprise-wide cost of all security postures to be implemented against the total enterprise-wide benefits.

4.5.1. Implementation of Security postures

Security postures can be physical or informational. Examples of physical postures are security guards and patrols, fences, gates, physical locks, remote cameras, etc. Informational security postures include enhanced encryption levels, auditing of process related messages (actual versus theoretical, recent past versus historical), etc.

4.5.2. Performance Impact

"Right sizing" security requires an appropriate balance between the two types of processes: security and business. Each security solution (detection, prevention, recovery) impacts the turnaround times of both these types of processes. Most of these processes are periodic (security scans, analysis of grid state, etc.). Therefore the performance impact of a security process should be based on a cycle time appropriate for that process and other business processes relevant to that time scale [9].

5. DATA MONITORING

Traditionally, the physical state of the power grid has been monitored extensively. However the IT systems monitoring the grid have not been monitored as thoroughly. In a smart grid it is imperative that the IT systems be monitored thoroughly also.

5.1. Real Time – Power System

Traditionally, data relevant to the power grid state has been collected every few seconds for automatic generation control as well as for breaker statuses in the transmission system. Data concerning transmission line loading has been collected every few minutes. Similar information at the distribution level is not available in most systems.

However, in the SG environment similarly detailed picture of the distribution system will be available. In addition, transmission system data will be available on a sub-second basis for at least the most important components, if not for all [10]. The scan rate corresponding to each power system component or power system application can be treated as an indicator of the importance of the relevant component or application.

It is possible to assess the importance of the power system components in a given real-time operating condition based on this data. For example, a transmission line in a group of three transmission lines supplying energy to an area may be more important than a similarly loaded line in a group of four lines supplying to another area. SRM should take into account such real-time importance of grid components while determining the appropriate security posture relevant to those components. In times of IT system stress, security scan rate for less important grid components can be decreased.

5.2. Real Time – Information Systems

In traditional power systems (and in typical industrial control systems), the voluminous IT system logs are not analyzed on a real-time basis. In many cases the disparate logs from the numerous IT components may not be available in a centralized database for a unified analysis.

However, in the context of SG, all data will be made available for a unified security analysis. Examples of this data include the IT system logs concerning both successful and unsuccessful attempts to access, time and source of requests for various information/data transactions, time of updates of software and data in each IT component, and so on. Activities associated with control actions should be meticulously recorded.

5.2.1. Messages

An essential requirement of SRM is the ability to perform a unified analysis of messages communicated among the various IT components. In this context an IT component can be a computer or a dedicated IED representing a power system component or a software application.

Unusual occurrence (or absence) of certain messages can be a clue essential for timely detection of an attack. A message can be unusual in many ways, including when and where it occurs (or does not occur) as well as the source and destination of the message.

Examples of messages relevant to SRM include:

- Heartbeat messages from various software and hardware components of automated meter readers, SCADA system, Energy Management Systems, and other enterprise-wide systems, external partner systems, etc. Heartbeat messages from various components of SRM should also be monitored and analyzed.
- Grid messages regarding the state of the power system (SCADA) should be analyzed for content.
- IT System Messages regarding the state of the IT components including time and location of software and data updates along with corresponding changes in disk space and memory allocations, etc.

It is essential to minimize false positives that overwhelm users.

6. CONCLUSIONS

Market driven convergence of Utility Business Information Technology (IT) and Power System Operation Technologies (OT) are bringing new protocol, analysis and performance challenges for end to end security risk management systems. To be scalable across the enterprise, the solutions should be based on interoperable components pervasively distributed. Successful solutions should exploit grid and information system domain contexts so that security postures of the grid can adapt to the situational awareness based on near real time security state and events of power and information systems. Security control systems should also leverage the interplay of security, reliability and stability in the smart grid through unified vulnerability models and threat analyses for the OT and IT domains.

This paper presented essential characteristics and properties for Interoperating Smart Grid Cyber Security Systems that are functionally pervasive, topologically distributed yet flexible in supporting traditional and emerging smart grid characteristics. Such systems neede to balance the challenges of different security postures that the OT system warrants where availability and data integrity is paramount vis-à-vis the IT system where confidentiality takes priority. Such solutions should be aware of the differing safety and cascading impacts external attacks, malicious insider breaches, or erroneous operations could have on the power grid or the information systems.

An architectural model for pervasive implementation of domain and situational aware adaptive cyber security system has also been presented. The system is intended to provide adaptive security postures in the face of evolving threats and vulnerabilities of the unified OT and IT systems of the smart grid.

We conclude that diverse data collection devices, various analysis programs correlating them with other power system and customer data and control elements from possibly different vendors will need to interactively coordinate to provide such functionally pervasive yet context aware security risk analysis and control systems. Interoperability among them is a critical requirement that ensures that innovation and competition offer customers a sustainable ecosystem for integrated security and risk mitigation solutions.

References

[1] U.S. Department of Energy, Office of Electricity Delivery & Energy Reliability, “Smart Grid Research & Development: **Multi-Year Program Plan (MYPP)** 2010-2014”, March, 2010

[2] Annual Energy Review 2009, August 2010, U.S. Energy Information Administration, Office of Energy Markets and End Use, U.S. Department of Energy, Washington, DC 20585

[3] Ranjit Kumar, Partha Datta Ray, Chris Reed, “Smart Grid: An Electricity Market Perspective”, IEEE Innovative Smart Grid Technology Conference, January, 2011

[4] Partha Datta Ray et. al, "Smart Power Grid Security: A Unified Risk Management Approach", Proceedings for the 44th IEEE International Carnahan Conference on Security Technology (ICCST),San Jose, CA, October 5th – 8th, 2010.

[5] Partha Datta Ray, “The Smart Grid’s Singular Security Challenge”, POWERGRID INTERNATIONAL, vol.16, No.05, pp 58-60, May 2011.

[6] Jeff Katz, “Smart Grid Security and Architectural Thinking”, White Paper, http://www.ibm.com/smarterplanet/global/files/us__en_

us__energy__smartgridsecurity_and_architecturalthinking_katz.pdf
[7] Partha Datta Ray et, al. Patent pending
[8] Wayne Jansen, "Directions in Security Metrics Research", NISTIR 7564, April 2009
[9] "The CIS Security Metrics: Consensus Metric Definitions V1.0.0", Center for Internet Security, May 2009
[10] K. Moslehi, R. Kumar, "A Reliability Perspective of the Smart Grid", IEEE Transactions on Smart Grid, Vol1, Issue 1, pp.57-64, , June 2010.

Biographies

Partha Datta Ray has 26 years of industry experience and served in multiple business and technology management roles including Vice President at GDA Technology (acquired by Larsen and Toubro) handling engineering and strategic marketing, TeraBlaze (a networking start up acquired by Agere), LSI Logic, Telerate (acquired by Dow Jones), Silicon Compiler (acquired by Mentor Graphics) and AT&T Bell Laboratories.

He currently leads the Information Security Work Group for the IEEE P2030 Smart Grid Standards Committee. He held the chairmanship of the RapidIO BFM Working Group, an interconnect standard widely deployed in wireless communications and is a senior member of the IEEE Communication Society. In the past, he led or served on various industrial and trade groups on Communications Protocols, Simulation, and Modeling.

Partha holds a BSEE and MSCS from Rutgers and conducted advanced post graduate research work at leading academic and research institutes.

He holds multiple patents in areas of circuit and network optimization and has multiple pending patents in areas of cyber security control and automated risk management. He has been invited keynote speaker at CIO Utilities Summit and most recently has presented at IEEE International Security Conference, IEEE Innovative Smart Grid Technology Summit and many other industry events.

Ranjit Kumar brings wide domain knowledge of the engineering and business aspects of the power industry to Albeado. His contributions in a variety of applications related to optimal design and operation of power systems and electricity market management systems along with his extensive experience in power systems applications, such as Network modeling, State Estimation, Dispatcher Power Flow and Contingency Analysis uniquely qualifies him to lead the Power System Application development effort at Albeado. He is known around the world for his publications in the areas of self-healing power grids, constrained energy resource optimization , power system stability analysis and use of expert systems in power system applications and automation over more than three decades.

He received his Ph.D. from the University of Missouri at Rolla (now known as Missouri University of Science and Technology). He started his career as an academic taking on teaching and research roles at Michigan Tech. Later he moved to the industry and has served in multiple business and engineering roles at Harris Control (now GE Harris Energy), ABB, and SAP. His past clients include CAISO, ERCOT, NYPP, PG&E and EPRI. He is the Chief Power Application Architect at Albeado Inc.

Christopher Reed has served in senior leadership roles in service organizations at companies ranging from startups to Fortune 500 including Nokia, Borland and Intellisync. Chris has built and lead teams distributed around the globe that provided integration and development services, custom engineering and educational support. He currently leads the Enterprise Solution Engineering and Services at Albeado.

Chris attended University of California, Santa Cruz & earned his BSEE at San Jose State University and is currently leading the Information Modeling Subgroup for IEEE P2030 standards committee. He actively participates in other industry consortiums like MultiSpeak, CIM & others. He is nearing completion of his JD degree.

Atul P. Agarwal has 23 years of experience in building complex software systems both in technology and enterprise business domains. He currently heads a team of about 10 engineers building a Java/J2EE framework for easily and securely integrating applications based on various Smart Grid standards like MultiSpeak, CIM and others. Atul has earlier founded and successfully grown Apt Software a software product and services company in India which provides software development and product engineering services to organizations around the world in diverse areas like energy exploration and operation, mobile platforms and applications for commerce and entertainment, semiconductor design and services. He has worked with many technology startups in the Silicon Valley and is currently heading the Albeado India Design Center.

He earned his Bachelor of Technology (Computer Science), degree from Indian Institute of Technology, Kharagpur and MS in Computer Science from Rutgers University, USA. Atul is the founder of the Apt Group and is associated as board member of various organizations. He has earlier worked with National Semiconductor, Santa Clara where he developed software for computer aided design of VLSI circuits.