A Survey of Critical Infrastructure Security

William Hurst, Madjid Merabti, Paul Fergus

Chapter 9

A SURVEY OF CRITICAL INFRASTRUCTURE SECURITY

William Hurst, Madjid Merabti and Paul Fergus

Abstract Traditionally, securing against environmental threats was the main focus of critical infrastructure protection. However, the emergence of cyber attacks has changed the focus – infrastructures are facing a different danger that has life-threatening consequences and the risk of significant economic losses. Clearly, conventional security techniques are struggling to keep up with the volume of innovative and emerging attacks. Fresh and adaptive infrastructure security solutions are required. This paper discusses critical infrastructures and the digital threats they face, and provides insights into current and future infrastructure security strategies.

Keywords: Critical infrastructures, security, survey

1. Introduction

The critical infrastructures work together to provide a continuous flow of goods and services, which range from food and water distribution, power supply, military defense and transport, to healthcare and government services, to name but a few [32]. A failure in one infrastructure can directly impact multiple other infrastructures. Beyond the traditional critical infrastructures, non-traditional infrastructures have emerged; these include telephone systems, banking, electric power distribution and automated agriculture. A well-established critical infrastructure network is considered to be the hallmark of an advanced society, and nations are usually judged by the quality of their critical infrastructure networks and the services they provide to citizenry [12]. However, critical infrastructures also represent one of the greatest weaknesses of modern society, due to the fact that a disruption of a critical infrastructure can result in life-threatening and general debilitating consequences to the population, economy and government [40]. As the dependence of society on critical infrastructures

increases, it is vital that the infrastructures are protected and the potential for disasters is reduced to the maximal extent.

Historically, the main focus was on developing infrastructures that would be resilient to environmental conditions [36] and natural disasters. The shutdown of the Torness nuclear power station in Scotland by a large bloom of jellyfish that blocked the water intake system demonstrates the unpredictability of nature and the importance of planning for damaging natural phenomena.

As technology advanced [7], critical infrastructures increasingly came to rely on digital control systems and networking; this has expanded the focus of critical infrastructure protection to include cyber threats as well as environmental incidents and accidents [3]. Critical infrastructure assets are tempting targets for hackers, criminal organizations, terrorist groups and nation states. Remote attacks on critical infrastructures are a new approach for conducting warfare, with the potential to bring about at least as much damage as traditional physical attacks. Cyber attacks make it possible to incapacitate a country and cause harm to its population. Indeed, because of the interconnectivity and interdependence of critical infrastructures across national borders, there is a high risk that a failure in one infrastructure can propagate to other infrastructures, resulting in cascading failures [21] that could affect practically all aspects of society in multiple countries [26].

This paper presents a survey of computer security techniques currently used to protect critical infrastructures. Also, it discusses why effective protection methods are essential for modern critical infrastructures.

2. Motivation

The threat levels that currently face critical infrastructures are higher than ever before. Not only do critical infrastructures have to cope with accidents and changing environmental conditions, but the scope, magnitude and sophistication of cyber attacks are placing great strain on defensive mechanisms. Critical infrastructure protection strategies must continually evolve to keep up with new and emerging threats.

2.1 Cyber Threats

Cyber threats are a major concern to corporations and governments [31]. Former U.S. Secretary of Defense Leon Panetta has compared the potential impact of successful cyber attacks to that of the terrorist attacks of September 11, 2001. In the United Kingdom, the large volume of cyber attacks that target government services and multinational corporations has been the subject of much coverage, including discussion and debate in Parliament. While many of the attacks, such as email messages containing Trojan horses [30], are modest, the sheer volume of attacks is cause for concern.

The malicious email threat is difficult to counter because email contents often appear to be genuine [16]. The malicious messages typically contain links to unsafe websites or contain attachments that, once opened, infect the receivers'

computer systems and networks. During the last few months of 2011, several malicious email attacks were directed at British Government officials. The email messages, which contained viruses, were doctored to look like they had been sent by government colleagues or White House officials.

Phishing attacks are engineered to steal information that is used for identity theft and financial profit. These attacks have many forms, but one of the most common is to direct a user to a fake website that closely resembles a legitimate website. The counterfeit website is often used to collect user names and passwords as well as banking and credit card information [39].

A common but more complex attack involves distributed denial of service [33], in which computer systems are sent large volumes of traffic that consume their resources and cause them to crash. Distributed denial-of-service attacks are effective because legitimate resource requests and bad requests are often practically indistinguishable, making the attacks difficult to block [1]. Another sophisticated technique is a man-in-the-middle attack [34] that interposes malicious code between system components in order to insert fabricated commands and/or responses. A man-in-the-middle attack can have effects ranging from information theft to system disruption; such an attack can be mitigated by employing an authentication protocol to ensure that communications reach their intended recipients [11].

MI5, the British security service, has announced its intention to invest millions of pounds in cyber defense activities to combat system vulnerabilities and counter cyber threats; other government organizations are also focusing on defensive measures [10]. Meanwhile, several other countries have reported steep increases in attacks. China reported that millions of cyber attacks a day were targeted at Beijing Olympic Games venues in 2008 [24]. While an Olympic Games is not an infrastructure, it is an iconic gathering of people from around the world and would be one of the highest profile targets imaginable.

2.2 Physical Consequences

Critical infrastructures are faced with the unexpected when it comes to cyber threats. Attackers have found ingenious ways to cause infrastructure disruptions. Physical parameters, such as temperatures, pressures, speed and flow rates, are measured and controlled digitally, offering tempting targets. Weaknesses that can result in physical failures must be identified and addressed prior to their exploitation.

During the last decade, several successful high-profile cyber attacks have been covered by the media. The most prominent of these is the Stuxnet worm [19]. Designed to target Siemens industrial software and equipment, Stuxnet reportedly disrupted Iran's uranium hexafluoride centrifuges, significantly delaying the progress of its nuclear weapons program. Stuxnet has clearly demonstrated the sophistication of cyber attacks. If it was possible to successfully target what was, arguably, one of Iran's most protected infrastructures, one can only imagine how easy it would be to target vital infrastructures such as information technology and telecommunications systems, water supply

and treatment systems, oil and gas pipelines, and, of course, the electric power grid, which is certainly the most important critical infrastructure to modern society.

3. Critical Infrastructures

The complexity of critical infrastructures and tight demands for services coupled with operational efficiency and reliability have led to the widespread use of control systems in critical infrastructures. However, control systems require extensive networking resources, which introduce numerous vulnerabilities.

3.1 Infrastructure Complexities

Automation has contributed to design complexities in critical infrastructures. An infrastructure may contain thousands of components distributed across a vast area, all of them connected to a control station. Often the individual components are heterogeneous in nature and have to be integrated in order to control operations [37]. The complexity and scale of the infrastructure mean that there are more potential targets for attack. Additionally, increased automation often leads to reduced resilience and new weaknesses due to design complexities and the dependence on computing systems and networks.

The reliance on wireless networking has introduced design complexities as well as other problems [4]. Wireless networks are difficult to protect because they provide numerous potential entry points. Energy requirements of wireless nodes are also an issue; when their energy is depleted, nodes can no longer perform their designated tasks [28]. One way of attacking a wireless sensor network is to identify and exploit nodes with special roles. A node that has a key role in the functioning of an infrastructure is often overburdened; an attacker can increase the probability causing a disruption by targeting the special node as opposed to a random node. One result is the exposure to a weakness-to-sleep attack, which involves denying nodes in an energy-constrained sensor network the ability to sleep; this attack prevents packets (commands) from reaching their destinations. As Zhang, *et al.* [41] emphasize, since critical infrastructures must provide services 24 hours a day, 365 days a year, disruptions of wireless sensor networks used in these infrastructures are unacceptable.

Business operations and supervisory control operations often require real-time access to the same information and computing resources as critical infrastructure assets. This results in critical infrastructure assets being directly or indirectly connected to other networks, including the Internet [5].

The key lesson from Stuxnet is that even the most sensitive system that is heavily secured and strongly air-gapped can be breached indirectly (e.g., using a USB drive). As a result, critical infrastructure protection is now focused on cyber security and human-initiated cyber attacks [14]. Indeed, the destructive potential of cyber attacks could be just as significant as that of a natural disaster, primarily because cyber attacks could be orchestrated to achieve the maximal effects.

Consider, for example, the Fukushima Daiichi nuclear disaster of March 2011. The 9.0 magnitude earthquake destroyed the electric power infrastructure in the region, causing a large-scale power outage. The subsequent tsunami flooded the rooms that housed the emergency diesel generators, rendering them non-operational. Emergency battery-powered systems were able to provide power to the reactor coolant loops. However, they ran out of power a day later, shutting down the active coolant loops and causing the reactors to heat up, ultimately resulting in the meltdown of three of the six nuclear reactors at the facility. While the Fukushima Daiichi disaster was caused by natural events with an extremely low probability, it is clear that the widespread power outage and the destruction of the back-up diesel generators could be caused by coordinated cyber attacks.

3.2 Control Systems

Critical infrastructures use industrial control systems that enable operators to monitor and control components such as valves, pressure gauges, switches and nodes from remote locations [15]. Industrial control systems may be broadly divided into two categories: supervisory control and data acquisition (SCADA) systems and distributed control systems. SCADA systems are typically used in critical infrastructure assets such as oil and gas pipelines and electric power grids that span large geographical regions [9]. Distributed control systems are used in more localized settings such as chemical plants and manufacturing facilities.

A typical SCADA system consists of a network of sensors that acquire physical process data and actuators that manipulate physical processes. SCADA systems include a master terminal unit, remote terminal units and various communications links. The master terminal unit acquires data from and sends instructions to remote terminal units via the communications links. The remote terminal units interface with hardware components and mechanical devices. Communications in SCADA systems occur over fiber optic, microwave, telephone, pilot cable, radio and/or satellite links. Operators use human machine interfaces and engineering workstations to interact with SCADA devices and ultimately with physical processes. SCADA systems also incorporate databases for storing past information (historians) and business information systems.

The connectivity of SCADA systems and distributed control systems and their increasing use of off-the-shelf components renders them more vulnerable to cyber attacks [9]. Recent cyber attacks include Flame and Stuxnet, which targeted SCADA and distributed control systems. Nicholson, *et al.* [23] identify several types of malicious actors that target industrial control systems:

- **Nation States:** Several countries are investing heavily in cyber warfare technologies. Nation state attacks are characterized by their sophistication and their potential to severely impact control systems and the critical infrastructure assets they operate [17].

- **Insiders:** Insider attacks are among the most serious threats to critical infrastructure assets. Insiders, who may be motivated by revenge or greed, are knowledgeable about infrastructure assets and their weaknesses, and often have high-level access privileges or know how to bypass security controls [17].

- **Organized Crime:** Attacks by criminal entities are usually driven by money. Attacks on critical infrastructure assets may be launched for intimidation, ransom or on behalf of third parties on a for-hire basis.

- **Hobbyists and Script Kiddies:** Attacks by hobbyists are typically motivated by curiosity [17]. Attacks by script kiddies, which are executed because of curiosity, for a thrill or to gain attention, are generally unsophisticated, but can still be damaging.

- **Hacktivists:** Attacks by hacktivists are typically undertaken for political reasons or to gain attention [17]. Hacktivist attacks can be very sophisticated. For example, the shadowy group known as Anonymous has conducted several high-profile attacks, including some that targeted law enforcement websites in the United Kingdom.

4. Critical Infrastructure Security

This section describes strategies for securing critical infrastructure assets. In particular, it describes the defense-in-depth strategy, along with conventional and future security approaches,

4.1 Defense-in-Depth Strategy

The impact of a critical infrastructure failure has four dimensions: (i) safety; (ii) mission; (iii) business; and (iv) security. Safety refers to the loss of life, serious personal injury or damage to the environment. Mission refers to the inability of an infrastructure to provide vital services; an example is a water supply failure that would not result in an immediate loss of life, but the consequences of a long-term outage could be devastating. Business refers to significant economic losses. Security refers to the loss, damage or destruction of physical, cyber or human assets.

Because of the potentially high impact of a failure, most critical infrastructure assets adopt a defense-in-depth security strategy. Defense in depth involves the implementation of multiple layers of security with different technologies and intrusion detection systems in each layer to ensure that an attack that penetrates one layer will not automatically bypass the next layer. Kumar, *et al.* [18] note that a defense-in-depth security strategy is most effective when the layers operate independently. A typical defense-in-depth implementation may involve three levels of security: low, medium and high. The low level is designed for general employees who have only basic access to infrastructure assets and related information to perform their tasks, while the medium and high levels

are designed for individuals such as system administrators, managers and key executives who would require access to infrastructure assets and information systems of increasing sensitivity.

A defense-in-depth implementation positions intrusion detection systems in the different layers to detect hostile activities and raise alerts [41]. The intrusion detection systems typically perform anomaly detection and/or signature-based detection. Anomaly detection involves the detection of abnormal system and/or network behavior (e.g., a sudden, unexpected increase in data flow in a certain part of a system). Signature-based detection involves the use of known attack signatures; on its own, this technique is ineffective at detecting new (i.e., zero-day) attacks [20]. For this reason, critical infrastructure assets typically incorporate multiple intrusion detection systems based on different detection modalities to maximize protection.

One of the problems with using intrusion detection systems in critical infrastructures is that their relatively large footprint makes it difficult to implement them on field devices that have limited computing resources. Additionally, the systems are often unable to identify the most serious attacks and they tend to impact system operation (especially, the tight timing requirements of SCADA systems) [8, 38]. Moreover, intrusion detection systems may generate large numbers of false positive errors, resulting in false alerts. Given the scale of critical infrastructures, massive numbers of alerts could be generated [25], potentially misleading operators and masking real attacks [6].

Unified threat management (UTM) systems, which first appeared in 2004, are now widely used to secure large-scale information technology systems [41]. UTM systems use a combination of firewalls, pattern recognition systems, intrusion detection systems and embedded analysis middleware to implement strong protection within the hardware, software and network layers. The utility of UTM systems for critical infrastructure protection derives from their provision of multiple security features within a unified architecture [41].

The benefits of using UTM systems include lower costs because of the reduced number of security appliances. The systems are also easy to deploy, which makes them ideal for organizations with limited technical capabilities. However, one of the main problems with UTM systems is their integration of multiple security technologies (e.g., control interfaces, message formats, communication protocols and security policies), which can complicate administrative and management activities; the result is that applications tend to work independently of each other.

4.2 Conventional Security Approaches

Several solutions have been proposed to address the security problems facing computer networks used in critical infrastructures. Shiri, *et al.* [29] have proposed the use of multiple (parallel) intrusion detection systems. This design increases efficiency by sharing the detection workload, but it does not enhance security performance in terms of the types of attacks that are detected.

Wen [35] has proposed the use of intrusion detection systems involving a combination of technologies to detect intrusions that originate from internal and external sources. The approach, which uses pattern matching and log file analysis to scan internal network activity and incoming network packets for anomalies, helps combat the insider threat as well as external attacks.

Nai Fovino, *et al.* [22] have developed an innovative approach to detect complex attacks on SCADA systems. Their approach combines signature-based intrusion detection with state analysis. The system can be enhanced by incorporating *ad hoc* rules to detect sophisticated attacks on SCADA systems.

In addition to focusing on network intrusions, it is important to address attacks that have successfully breached network security. This is accomplished using host-based monitoring and anomaly detection. The approach requires the careful analysis of normal operating conditions to establish baselines and thresholds for identifying anomalous activities. The baselines and thresholds should be adjusted continually to reduce false positive errors.

Wang, *et al.* [33] have proposed an augmented attack tree model to combat distributed denial-of-service attacks. Their approach creates attack trees to model attacks and guide the development of attack detection and mitigation strategies. While the approach is innovative, specifying attack trees for the multitude of possible attacks is an arduous task. Moreover, the attack models have to be tuned to the specific infrastructure asset being protected.

Schweitzer, *et al.* [27] discuss how one would know if an attack is actually taking place. They posit that an attack would initially involve probes for collecting information about the targeted infrastructure to be used in conducting the attack. Once the main attack is underway, it is necessary to focus on the intruders' movements within the infrastructure. Schweitzer and colleagues emphasize the need to use multiple, independent communications channels, so that if one channel is compromised, an alternative channel exists to signal an alarm. SCADA systems used in critical infrastructures typically incorporate redundant communications channels to ensure reliable operations; this feature can be leveraged to signal attacks as well as to mitigate their effects.

4.3 Future Security Approaches

As critical infrastructure technology evolves, new threats and vulnerabilities continue to emerge. The introduction of smart meters in electrical power infrastructures demonstrates this trend [2]. Smart meters, which are important features of future smart grids, allow two-way communications between electric utilities and consumers. They enable utilities to use power resources efficiently, provide dynamic pricing and reduce power outages; they offer consumers detailed feedback on energy use and the ability to dynamically adjust their usage patterns to lower electric bills. However, one of the key features of a smart meter is that it has a remote off-switch, which is controlled by the utility. Anderson and Fuloria [2] point out that attackers could potentially manipulate these remote off-switches to create massive power outages.

Clearly, the resilience of critical infrastructures is negatively impacted as new technologies are incorporated for reasons of convenience and cost reduction [2]. Consequently, it is imperative to develop innovative defensive mechanisms that replace or augment existing critical infrastructure protection systems. A promising solution is to design protection systems that operate with a broad view of a critical infrastructure and implement coordinated responses to disruptions using behavioral analysis [13]. This approach constructs and leverages a model of correct behavior based on diverse information about computing systems, networks, industrial control devices and physical processes. Indeed, it offers protection that is at once holistic, proactive and resilient – addressing security issues before they become serious problems and helping critical infrastructures respond gracefully when attacks do succeed.

5. Conclusions

Critical infrastructures are becoming more and more indispensable as populations grow and demands are placed for new and increased service offerings. Clearly, modern society cannot function if major components of the critical infrastructure are damaged or destroyed. Despite governmental policy and regulation and massive injections of funding and resources, the vast majority of critical infrastructure assets may not be able to cope with sophisticated and evolving cyber threats. Critical infrastructures are large, complex and expensive assets. Since it is not possible to rebuild these assets from scratch to ensure "baked in" security, the only option is to focus on integrating conventional and innovative security mechanisms in comprehensive defense-in-depth approaches founded on risk management and resilience to ensure that successful attacks do not result in catastrophes.

References

[1] A. Al Islam and T. Sabrina, Detection of various denial-of-service and distributed denial-of-service attacks using RNN ensemble, *Proceedings of the Twelfth International Conference on Computers and Information Technology*, pp. 603–608, 2009.

[2] R. Anderson and S. Fuloria, Who controls the off switch? *Proceedings of the First IEEE International Conference on Smart Grid Communications*, pp. 96–101, 2010.

[3] M. Brownfield, Y. Gupta and N. Davis, Wireless sesnsor network denial-of-sleep attack, *Proceedings of the Sixth Annual IEEE SMC Information Assurance Workshop*, pp. 356–364, 2005.

[4] L. Buttyan, D. Gessner, A. Hessler and P. Langendoerfer, Application of wireless sensor networks in critical infrastructure protection: Challenges and design options, *IEEE Wireless Communications*, vol. 17(5), pp. 44–49, 2010.

[5] K. Claffy, S. Bradner and S. Meinrath, The (un)economic Internet? *IEEE Internet Computing*, vol. 11(3), pp. 53–58, 2007.

[6] L. Coppolino, S. D'Antonio, L. Romano and G. Spagnuolo, An intrusion detection system for critical information infrastructures using wireless sensor network technologies, *Proceedings of the Fifth IEEE International Conference on Critical Infrastructure*, 2010.

[7] L. Coyle, M. Hinchey, B. Nuseibeh and J. Fiadeiro, Guest editors' introduction: Evolving critical systems, *IEEE Computer*, vol. 43(5), pp. 28–33, 2010.

[8] F. Deng, A. Luo, Y. Zhang, Z. Chen, X. Peng, X. Jiang and D. Peng, TNC-UTM: A holistic solution to secure enterprise networks, *Proceedings of the Ninth IEEE International Conference for Young Computer Scientists*, pp. 2240–2245, 2008.

[9] C. Esposito, D. Cotroneo, R. Barbosa and N. Silva, Qualification and selection of off-the-shelf components for safety critical systems: A systematic approach, *Proceedings of the Fifth Latin-American Symposium on Dependable Computing Workshops*, pp. 52–57, 2011.

[10] M. Golling and B. Stelte, Requirements for a future EWS – Cyber defense in the Internet of the future, *Proceedings of the Third International Conference on Cyber Conflict*, 2011.

[11] R. Guha, Z. Furqan and S. Muhammad, Discovering man-in-the-middle attacks on authentication protocols, *Proceedings of the IEEE Military Communications Conference*, 2007.

[12] M. Hashim, Malaysia's national cyber security policy: The country's cyber defense initiatives, *Proceedings of the Second Worldwide Cybersecurity Summit*, 2011.

[13] W. Hurst, M. Merabti and P. Fergus, Behavioral observation for critical infrastructure security support, *Proceedings of the Seventh IEEE European Modeling Symposium*, pp. 36–41, 2013.

[14] M. Kaaniche, Resilience assessment of critical infrastructures: From accidental to malicious threats, *Proceedings of the Fifth Latin-American Symposium on Dependable Computing Workshops*, pp. 35–36, 2011.

[15] D. Kang, J. Lee, S. Kim and J. Park, Analysis of cyber threats to SCADA systems, *Proceedings of the IEEE Transmission and Distribution Conference and Exposition: Asia and Pacific*, 2009.

[16] E. Kartaltepe and S. Xi, Towards blocking outgoing malicious impostor emails, *Proceedings of the International Symposium on a World of Wireless, Mobile and Multimedia Networks*, pp. 657–661, 2006.

[17] P. Katsumata, J. Hemenway and W. Gavins, Cybersecurity risk management, *Proceedings of the Military Communications Conference*, pp. 890–895, 2010.

[18] M. Kumar, D. Mukhopadhyay, H. Lele and K. Vaze, Evaluation of operator actions for beyond design basis events for AHWR, *Proceedings of the Second International Conference on Reliability, Safety and Hazards*, pp. 579–582, 2010.

[19] R. Langner, Stuxnet: Dissecting a cyberwarfare weapon, *IEEE Security and Privacy*, vol. 9(3), pp. 49–51, 2011.

[20] P. Li, Z. Wang and X. Tan, Characteristic analysis of virus spreading in ad hoc networks, *Proceedings of the International Conference on Computational Intelligence and Security Workshops*, pp. 538–541, 2007.

[21] A. MacDermott, W. Hurst, Q. Shi and M. Merabti, Simulating critical infrastructure cascading failure, *Proceedings of the Sixteenth IEEE International Conference on Modeling and Simulation*, pp. 323–328, 2014.

[22] I. Nai Fovino, M. Masera, L. Guidi and G. Carpi, An experimental platform for assessing SCADA vulnerabilities and countermeasures in power plants, *Proceedings of the Third International Conference on Human System Interaction*, pp. 679–686, 2010.

[23] N. Nicholson, S. Webber, S. Dyer, T. Patel and H. Janicke, SCADA security in the light of cyber warfare, *Computers and Security*, vol. 31(4), pp. 418–436, 2012.

[24] S. Pritchard, Securing the 2012 Olympics, *Infosecurity*, vol. 6(6), pp. 12–15, 2009.

[25] S. Roschke, F. Cheng and C. Meinel, A flexible and efficient alert correlation platform for distributed IDS, *Proceedings of the Fourth IEEE International Conference on Network and System Security*, pp. 24–31, 2010.

[26] C. Scarlat, C. Simion and E. Scarlat, Managing new technology projects: Some considerations on risk assessment in the case of NPP critical infrastructures, *Proceedings of the Second IEEE International Conference on Emergency Management and Management Sciences*, pp. 911–915, 2011.

[27] E. Schweitzer, D. Whitehead, A. Risley and R. Smith, How would we know? *Proceedings of the Sixty-Fourth Annual Conference for Protective Relay Engineers*, pp. 310–321, 2011.

[28] W. Seah, A. Zhi and H. Tan, Wireless sensor networks powered by ambient energy harvesting (WSN-HEAP) – Survey and challenges, *Proceedings of the First International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology*, 2009.

[29] F. Shiri, B. Shanmugam and N. Idris, A parallel technique for improving the performance of signature-based network intrusion detection systems, *Proceedings of the Third International Conference on Communication Software and Networks*, pp. 692–696, 2011.

[30] S. Tang, The detection of Trojan horses based on data mining, *Proceedings of the Sixth International Conference on Fuzzy Systems and Knowledge Discovery*, vol. 1, pp. 311–314, 2009.

[31] J. Walker, B. Williams and G. Skelton, Cyber security for emergency management, *Proceedings of the IEEE International Conference on Technologies for Homeland Security*, pp. 476–480, 2010.

[32] C. Wang, L. Fang and Y. Dai, A simulation environment for SCADA security analysis and assessment, *Proceedings of the International Conference on Measuring Technology and Mechatronics Automation*, vol. 1, pp. 342–347, 2010.

[33] J. Wang, R. Phan, J. Whitley and D. Parish, Augmented attack tree modeling of distributed denial of services and tree based attack detection method, *Proceedings of the Tenth IEEE International Conference on Computer and Information Technology*, pp. 1009–1014, 2010.

[34] Y. Wang, H. Wang, Z. Li and J. Huang, Man-in-the-middle attack on BB84 protocol and its defense, *Proceedings of the Second IEEE International Conference on Computer Science and Information Technology*, pp. 438–439, 2009.

[35] W. Wen, An improved intrusion detection system, *Proceedings of the International Conference on Computer Applications and System Modeling*, vol. 5, pp. 212–215, 2010.

[36] T. Wilson, C. Stewart, V. Sword-Daniels, G. Leonard, D. Johnston, J. Cole, J. Wardman, G. Wilson and S. Barnard, Volcanic ash impacts on critical infrastructure, *Physics and Chemistry of the Earth, Parts A/B/C*, vol. 45-46, pp. 5–23, 2011.

[37] S. Wolthusen, GIS-based command and control infrastructure for critical infrastructure protection, *Proceedings of the First IEEE International Workshop on Critical Infrastructure Protection*, pp. 40–50, 2005.

[38] H. Xue, MultiCore systems architecture design and implementation of UTM, *Proceedings of the International Symposium on Information Science and Engineering*, pp. 441–445, 2008.

[39] W. Yu, S. Nargundkar and N. Tiruthani, A phishing vulnerability analysis of web-based systems, *Proceedings of the IEEE Symposium on Computers and Communications*, pp. 326–331, 2008.

[40] F. Yusufovna, F. Alisherovich, M. Choi, E. Cho, F. Abdurashidovich and T. Kim, Research on critical infrastructures and critical information infrastructures, *Proceedings of the Symposium on Bio-Inspired Learning and Intelligent Systems for Security*, pp. 97–101, 2009.

[41] Y. Zhang, F. Deng, Z. Chen, Y. Xue and C. Lin, UTM-CM: A practical control mechanism solution for UTM systems, *Proceedings of the IEEE International Conference on Communications and Mobile Computing*, pp. 86–90, 2010.