

## NETWORK SECURITY RISKS IN POWER SYSTEM AND GATHERING ADMISSIBLE EVIDENCE ISSUES

A.Sankaran\*

---

### *Abstract—*

Computer network is playing an active role in modern business management in power system. Nowadays, information power industry develops rapidly, highlighting the growing importance of information security, and the challenges are increasingly serious. This paper analyzes security risks in power enterprise network and proposes specific corresponding strategies. Thus, this paper critically describes and analyses emerging security challenges in the investigation of that interface with computer systems. The review will be functionally useful to researchers, vendors, security professionals and IT end users in general.

*Keywords- trusted computing; TPM, trusted booting; credible I/O control; ultra-dependable; real time operating system; embedded system; isolation safeguard; error handling; Sensor networks, Business impact analysis, failed attacks, security policy, network forensics..*

---

\* P.G Scholar, Department Of Computer Science And Engineering, Indira Institute Of Engineering And Technology.

## INTRODUCTION

The development of computer network technology provides advanced technologies and services means for their own development. Power data communication network links power grid enterprises at all levels to achieve inter-enterprise information system interoperability and resource sharing. With the development of computer technology, communication technology and network technology, internal information network of power system is gradually established, and network services and applications become more and more, so that network and information security is facing huge challenges.

Attacking activities such as virus, malicious code and unauthorized access pose a great threat on network and business information systems. Therefore, a lot of power enterprises strengthen hardware and software construction of power information network authentication, anti-virus and anti attack security system [1-3].

On the other hand, management of power industry information security lacks unified planning and standards, as well as effective monitoring and inspection mechanism, resulting in delays of starting construction work of infrastructure in information security. In addition, the market urgently needs security solution adapted for various power systems. Within the network of power system at all levels, problems such as loose access control, late discovery of network abnormality, lack of warning means and security risk detection still exist.

## II. ANALYSIS OF SECURITY RISKS IN POWER ENTERPRISES

### A. Less Security Strength of Network

EMS systems in many power companies deploy common firewall, which is traditional logic-based control mechanism firewall. For applications in general terms, these measures are adequate. But for core control system in secret agencies, such as military, government, electricity, finance, etc., because the firewall is based on common logical entity, which itself may also be manipulated, the security control is limited, and the adaptability is not enough for a variety of communication protocols, what's more, a high degree of data security can not be met. Due to this, confidential can not only depend on the probability of protection, an absolute security gate must be established to ensure that the information from confidential

network is not betrayed and damaged.

***B. No Overall Protection Plan***

Network security is a kind of system engineering, with a long-term. On the one hand, with the increasingly open networks and computer applications in production control system, security of data in networks is becoming more and more important, production control system is becoming bigger and bigger, and their security is relative fragile. On the other hand, computer technology changes daily and hacker tools developed rapidly, so effective security policy firewall or isolation device may be out of date tomorrow. Therefore, we must rely on technological progress to constantly update and improve security measures, and timely response, block possible loopholes before they occur .

**III. LACK OF NETWORK MANAGEMENT TOOLS**

***A. Less Security Strength of Network***

*Table 1*

*Assessment of Electric Power Information*

<i>Process Area</i>	<i>Assessment Content</i>	
	<i>Risk Evaluation</i>	<i>assessment of the impact on the whole power system from the security of information network</i>
		<i>assessment of current risk existing in information system</i>
		<i>assessment of current threat of power information network</i>
		<i>assessment of current vulnerability of power information network</i>
	<i>Engineering Management</i>	<i>management of security monitoring strategies of power information network</i>
		<i>coordination of security operation of power information</i>

		<i>network</i>
		<i>monitoring of security situation of power information network</i>
		<i>provide security input of power information network</i>
		<i>confirm and explain security requirement of power information network</i>
<b>Security Process Area</b>	<b>Assurance</b>	<i>establish security assurance for power information network</i>
		<i>verification of security for power information network</i>
<b>Project Engineering Area</b>		<i>guarantee the quality of power information network</i>
		<i>management of security deployment for power information network management</i>
		<i>monitoring of technology work for power information network</i>
		<i>scientific plan technology for power information network</i>
<b>Organization Process Area</b>		<i>definition of system engineering process for power information network</i>
		<i>improvement of system engineering process for power information network</i>
		<i>management of evolution process for the production of power information network</i>
		<i>management of engineering support environment for power information network</i>
		<i>provide skills and knowledge for sustainable development of power information network</i>
		<i>coordination of provider related with power information network</i>

Building information security system focuses on security and stability. Mature technologies and products should be adopted, novelty can not be too perfectionist. Training of information security professionals and enhancing information security management should be carried out with the construction of information security protection system, in order to play the role of protection. According to SSE CMM ideas, combining with the assessments of electric power information network security,

security engineering process can be divided into 3 basic process areas, and content of each process area is determined.

### ***B. Configuration of Preventing Hacker***

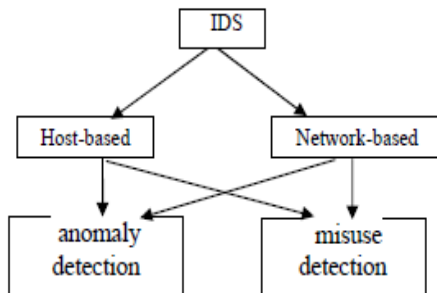
Hackers are monitored through information detection, attack detection, network security analysis and operating system security analysis. Firewalls can block unauthorized data packets, shielding the illegal attacks against the network and block hacker intrusion. Under normal circumstances, the firewall can

cause a significant delay of information transmission. Therefore, in real-time power system, a special firewall component is recommended to reduce impact of delay brought by common firewall software.

### ***C. Intrusion Detection System***

IDS is a kind of network security technology to protect themselves from security attacks. As a reasonable complement of firewall, intrusion detection technology can help system against network attacks, enhancing the capacity of the system administrator's security management, including safety audit, monitoring, attack recognition and response, which improve the integrity of the information security infrastructure. It collects information from a number of key points in computer network and analyzes the information. Intrusion detection is considered to be the second security gate after firewall, and can monitor network without prejudice of network performance.

In accordance with the different sources of information collection methods, intrusion detection system can be divided into host-based IDS and network-based IDS. According to analysis methods, it can be divided into anomaly detection and misuse detection. The classification scheme is shown in Figure 1:



**Figure 1. Classification Scheme of IDS**

#### **D. Anti-virus System**

In power system, computer information network system has covered all of the enterprise production, operation and management positions. Internet users may be subject to virus attacks when conduct a variety of data exchange. Contacting by e-mail services is highly vulnerable to viral infections, and has spread within the enterprise network. Information must guard against all aspects of the network in order to effectively prevent and control viruses. Anti-virus technology must have features of real-time monitoring, support and services for multi-platform, in order to prevent and control new virus effectively. For the external network and internal network, a distributed solution is used to achieve the unity of virus protection in the whole network. Anti-virus technology runs in the background, and it gets control right before virus. In addition, it practices real-time monitoring towards system, and if suspicious signs appear, operation of illegal procedures is stopped, and some specialized identification techniques are used to judge the programs, and then remove it.

#### **IV. RELATED WORK**



Single Intrusion Detection System (IDS) can be installed on a segment or gateway of computer networks to promptly analyze each packet and to isolate normal activities from abnormal activities. IDS users may also install multiple Intrusion Detection Systems (IDSs) at different segments of the same network to safeguard their computer resources. These mechanisms are robust in capturing, alerting and logging evidence of abnormal activities on computer disks for analysts to be able to carry

out further review of the incidences [12]. Some malicious attacks may not be detected at the network level. Attacks that target the application level may be different from attacks that target operating system of targeted networks. Hence, there are different categories of IDSs.

#### IV. INDUSTRIAL STANDARDS

The efficacy and validity of industrial best practices for safeguarding standalone computers, information resources, computer networks and their peripherals are not frequently evaluated in the domain of computer network security and network forensics. The main reason is that industrial best practices are mostly propounded by globally recognized body of experts such as American National Standards Institute (ANSI), National Institute of Standards and Technology (NIST), British Standards Institute (BSI), Standard Organization of Nigeria (SON), Institute of Electrical and Electronics

Engineers (IEEE), International Standards Organization (ISO) and Information Systems Audit and Control association (ISACA) [14, 19].

While industrial standards are constantly being updated and new disposable devices are being manufactured from time to time, we are unsure whether the new versions of each standard is sufficient enough to adequately provide the necessary guidelines that network forensics experts and IS auditors would use to effectively discharge their duties.

##### A. Outsourcing of IT operations

Outsourcing of IT functions is becoming the best IT practices in the industry. The rate of change in customer requirements, computer crimes across the globe are also on the increase [12-14]. IT auditors

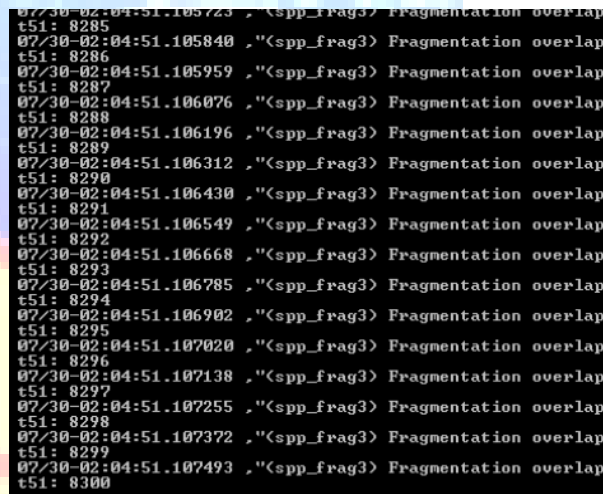
must continually evaluate third party applications, selection of vendors; profiles of access assigned to vendors and Business Contingency Planning (BCP) procedures of their organizations

to ensure strict compliance with best practices and to lessen downtime. There is a growing rate of complexity on how to actually conduct purposeful Business Impact Analysis

(BIA) and penetration testing across multiple outsourced IT operations in order to anticipate potential vulnerabilities of computers and cloud resources that can be exploited by malicious users and hackers. There are numerous unidentified stealthy attacks and techniques to evade detection that may not be covered by the present industrial best practices known to the BIA team. Consequently, current best industrial practices and the results of most BIA are highly subjective.

### ***B. Redundant intrusions and redundant alerts***

IDSs fundamentally generate numerous alerts while in operation to detect potential attacks. From that fact, conceptual discussions of redundant intrusions and redundant alerts can generate controversies in some cases. basically, redundant intrusions such as in Figure 2 below are similar intrusions that are reoccurring over time. Statistically, some alerts are related, some are partially related and others may not correlate altogether.



```
07/30-02:04:51.105723 . "<!-- spps_frag3 --> Fragmentation overlap
t51: 8285
07/30-02:04:51.105840 . "<!-- spps_frag3 --> Fragmentation overlap
t51: 8286
07/30-02:04:51.105959 . "<!-- spps_frag3 --> Fragmentation overlap
t51: 8287
07/30-02:04:51.106076 . "<!-- spps_frag3 --> Fragmentation overlap
t51: 8288
07/30-02:04:51.106196 . "<!-- spps_frag3 --> Fragmentation overlap
t51: 8289
07/30-02:04:51.106312 . "<!-- spps_frag3 --> Fragmentation overlap
t51: 8290
07/30-02:04:51.106430 . "<!-- spps_frag3 --> Fragmentation overlap
t51: 8291
07/30-02:04:51.106549 . "<!-- spps_frag3 --> Fragmentation overlap
t51: 8292
07/30-02:04:51.106668 . "<!-- spps_frag3 --> Fragmentation overlap
t51: 8293
07/30-02:04:51.106785 . "<!-- spps_frag3 --> Fragmentation overlap
t51: 8294
07/30-02:04:51.106902 . "<!-- spps_frag3 --> Fragmentation overlap
t51: 8295
07/30-02:04:51.107020 . "<!-- spps_frag3 --> Fragmentation overlap
t51: 8296
07/30-02:04:51.107138 . "<!-- spps_frag3 --> Fragmentation overlap
t51: 8297
07/30-02:04:51.107255 . "<!-- spps_frag3 --> Fragmentation overlap
t51: 8298
07/30-02:04:51.107372 . "<!-- spps_frag3 --> Fragmentation overlap
t51: 8299
07/30-02:04:51.107493 . "<!-- spps_frag3 --> Fragmentation overlap
t51: 8300
```

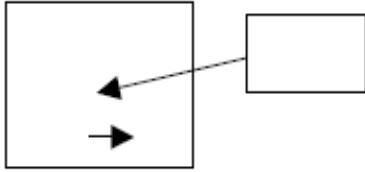
***Figure 2 Alerts from redundant intrusions***

In other words, it is difficult to determine how closely two alerts triggered by IDS covary. It is also difficult to separate alerts that form perfect negative correlation, no correlation or those that form perfect positive correlation.

Human factor in analyzing intrusion logs is relevant in the context of administration of IDS especially whenever attackers launch attacks that cause NIDS to trigger alerts with the aim of exhausting capabilities of the analysts.

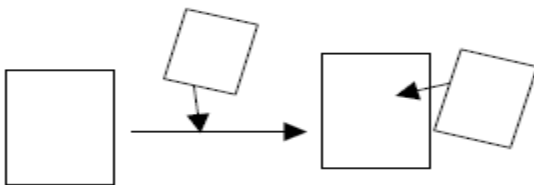


The issue here is that some analysts might not notify their management or their strategic managers on the need to deploy additional hands to cooperatively analyze swamped alerts for the fear of being fired. Accordingly, many attacks go unnoticed despite series of warnings from the IDS in use. Several factors can cause alerts swamping and intrusion redundancy.



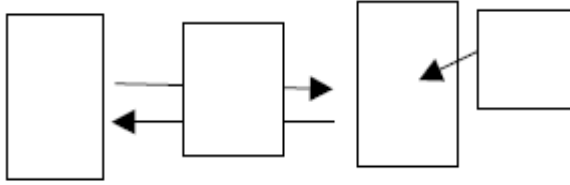
**Figure 3 Attack on a standalone computer system**

Figures 2 to 5 illustrate that configurations of a standalone computer system can completely different from configurations of computers in a set of computer networks. The basic fact is that an attack on a standalone computer system has the same source and destination address unlike an attack that involves computers networks such as in Figure 3. Essentially, Figure 3 shows one IDS (Q) that mediates between two computer networks A and B and another IDS (M) that is installed on a computer in network B. Figure 4 illustrates the complexity in the installation of IDSs shown in Figure 3. Figure 4 therefore shows an attack that originates from a computer machine or a device (S) towards another computer system or a device (T). There are IDS in the target system (T) and another IDS (NIDS) that mediates between the source of the attack and its destination. Users often deploy multiple IDSs to maximally detect network intrusions. Homogeneous, hetero-generous or semi-heterogeneous IDSs can be deployed in this regards. Homogeneous IDSs are similar IDSs such as in the deployment of Snort in multiple segments in an organization.



*Figure 4 Attack across different computer networks*

Heterogeneous IDSs comprise of different categories of IDSs. It may signify the deployment of NIDS (such as Snort for monitoring computer networks) and host-based IDS (such as OSSEC for monitoring the integrity of internal components of computing systems in an organization).



*Figure 5 Attack within the same computer networks*

However, in an attempt to rigorously safeguard computer systems and cloud resources from intruders, design flaws are indirectly built into them.

#### IV. CONCLUSION

Power is a basic industry related to the life of people and a nation, and has a strong requirement of information security. In order to achieve interoperability within the network, and connection between internal network and the Internet, a network with definite authority, improving service is needed to be established. Because of inevitable connection with external network, virus threats from external hackers must be prevented. In order to maintain power information security and to ensure stable and reliable information network systems, construction of network security system is extremely important.

**REFERENCES**

- [1] Watts D J, Strogatz S H. Collective dynamics of small-world' networks [J]. Nature, 1998, 393 (6684): 440-442.
- [2] Arabási A L, Albert R. Emergence of scaling in random networks[J]. Science, 1999, 286(5439): 509-512 .
- [3] J. D. Howard, "An Analysis of Security Incidents on the Internet", PhD thesis, Carnegie Mellon University, August 1998.
- [4] Computer Security Institute and Federal Bureau of Investigation, "CSI/FBI Computer Crime and Security", Survey, Computer Security Institute Publication, March 1999.
- [5] Y. Chen. "Toward a quantitative understanding of DoS". Class Proposal, University of California, Berkeley, USA, [http://www.cs.berkeley.edu/~yanchen/course /261\\_proposal.html](http://www.cs.berkeley.edu/~yanchen/course /261_proposal.html), 2000.
- [6] D. Moore, G. Voelker, S. Savage. " Inferring Internet Denial-of-Service Activity", In Proceedings of the 10th USENIX Security Symposium, pages 9-22, August 2001.
- [7] Jiri Kutha, "Comparison of Service Creation Approaches for SIP", International SIP conference, March 2000.
- [8] V. Paxson. "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks". White Paper, AT&T Center for Internet Research at ICSI, International Computer Science Institute Berkeley, USA, 2001.
- [9] J. Damas, F. Neves, "Preventing Use of Recursive Nameservers in Reflector Attacks", Category: Best Current Practice , <http://www.ietf.org/rfc/rfc5358.txt>, October 2008.
- [10] Glenn C., George Kesidis, G. Brooks, R. R. and Suresh Rai, "Denial-of-Service Attack-Detection Techniques" IEEE Internet computing 2006.
- [11] Peng.T, Leckie.C and Kotagiri. R, "Survey of Network-based Defense Mechanisms Countering the DoS and DDoS Problems", Journal: ACM Computing Surveys, volume 39, issue 1, 2007, article no.3.
- [12] Mirkovic.J, Sven Dietrich, David Dittrich, Peter Reiher, "Internet Denial of Service: Attack and Defense Mechanism", First Edition, Prentice Hall, 2004.

## Authors Profile



**A.Sankaran** received the Diploma in electronics and communication engineering from Adhiparasakthi Polytechnic College in 2007, **B.E.** degree in Computer Science engineering from Adhiparasakthi Engineering College, Chennai, India, in 2010. Currently doing **M.E.** in Computer Science engineering from Indira Institute Of Engineering And Technology, India. His research interest includes wireless communication (**WiFi, WiMax**), Mobile Ad hoc networks, Sensor Networks, Neural Networks and fuzzy logic, Communication networks. And Publications are.

- [1] **“Computer Network Database Attacks Security From Threats And Hackers,”** International Conference On Intelligence Computing (ICONIC’12) Sponsored By DRDO, pp 18 ISBN 978-93-80757-90-2.
  - [2] **“Start-up and I/O Access Control of Embedded Linux Based Real Time Operating System,”** International Conference On Recent Trends In Computer Science And Engineering (ICRTCSE’2012), 05/2012, ISBN 978-81-9089-8072.
  - [3] **“A Sensing Platform To Support Smartphone’s Accessing Into Wireless Sensor Networks,”** International Conference On Recent Trends In Engineering & Computer Application (INRTIEMC-12), 24/02/2012.
  - [4] **“Vehicle Security From Terrorists And License Checking Using Camera In Traffic,”** National Conference On Signal Processing And Communication Technology (NCSC’10).
  - [5] **“Nano Drug And Gene Delivery In An Anti-HIV tool,”** Published by Center For Nanotechnology Education, Research & Applications (CENTRA). Sullivan University College Of Pharmacy Louisville, KY, pp 84-93, ISBN 1-4392-5489-3.
  - [6] **“Nano In Anesthesiology- A Pain Killer,”** VI Mantra 2008 Project contest, Bangalore.
- “Security for computer network database attacks,”** National Conference On Technical Advancement Computer Technology (NCTACT-12), 17/03/2012, pp 64-69.

[7]“**Mobile Multimedia Sensor Using Peer-To-Peer Networks Architecture And Routing,**” National Conference On Technical Advancement Computer Technology (NCTACT-12), 17/03/2012, pp 86-90.

[8] “**Mobile Multimedia Sensor Using Adhoc Networks: Architecture And Routing,**” National Conference On Innovative Trends on Advanced Computing(NCITA-12), 29/02/2012.

[9]“**Smartphone Sensing Using Peer to Peer Computing Wireless Networks,**” National Conference On Innovative Trends on Advanced Computing(NCITA-12), 29/02/2012.

