Critical Infrastructure Cyber Threat – A Case Study

Y Wangdi, D Veal, S P Maj⁎,

Edith Cowan University, Perth, Western Australia

Summary
Critical infrastructure is considered to be any facilities or technologies that if degraded or rendered unavailable for an extended period would significantly impact on national economic and social well being. Hence in some countries there are government driven and led initiatives to provide critical infrastructure resilience. These initiatives require critical infrastructure owners and operators to manage foreseeable risks to ensure operational continuity even when subject to cyber attacks. This paper is a case study of the communications system of the national power generating company in an Asian country. Despite the importance of this company to the entire country it was found that network security measures were significantly lacking. Hence a secure network infrastructure was designed and is currently being implemented.

Key words:
Critical infrastructure, cyber threats, network security.

1. Introduction

Modern societies are a complex interdependence of hospitals, transport systems, power generation and supply systems, manufacturing etc. This infrastructure is critical to the normal operation of society within a given country. One definition of critical infrastructure is:

Those physical facilities, supply chains, information technologies and communications networks which, if destroyed, degraded or rendered unavailable for an extended period would significantly impact on the social or economic wellbeing of the nation or affect Australia's ability to conduct national defense and ensure national security. [1]

This infrastructure is substantially dependent on IT systems which in turn are progressively subject to cyber attack. According to McAfee and the Centre for Strategic and International Studies (CSIS) report there are massive increases in cyber attacks and sabotage on unprepared critical infrastructure systems. Furthermore, there are now sophisticated forms of malware such as Stuxnet which is specifically designed to sabotage critical infrastructure IT systems [2].

It should be noted that Stuxnet affords the perpetrators no financial benefit and is designed purely to sabotage industrial Supervisor Control and Data Acquisition (SCADA) systems. SCADA networks are universally used in the control of wide range infrastructures. Other key findings in this report are that some countries are lagging behind in their security measures.

2. Company background

A case study was conducted of a national power generating company in a developing country. For the purposes of this paper the company will be referred to as XYZ. XYZ is responsible for power supply to the entire country. As such the company consists of multiple power generation sites with four centralized departments located in the capital city that include: Finance, Operations & Maintenance, Human Resources & Administration and Projects. XYZ is mandated to operate and maintain all existing power plants, and also to play a leading role in building new power projects.

However, this case study is based specifically on the network communications systems of XYZ and its three subsidiary power plants each located over 1000km apart. These three power plants will be referred to as PP1, PP2 and PP3. Each of these plants has over 100 PCs; switches; routers and wireless access devices which form the basis of their communication systems. The total number of staff employed by XYZ was nearly one thousand.

3. Business impact analysis

There is a need for a comprehensive cyber security framework for critical infrastructure [3]. A range of quantitative methods and layered security architectures have been proposed [4], [5], [6]. However in this case it was found that only basic security measures were employed such as: restricted access to buildings and room and the use of passwords. Surprisingly there were no company policies on passwords such as; minimum length, and number and type of character; change frequency etc. When considering only the communications network it was found:

- None of the network devices were hardened
- Encryption was not used
- Virtual Local Area Networks (VLANs) were not used

Manuscript received June 5, 2011
Manuscript revised June 20, 2011

- Virtual Private Networks (VPNs) between remote sites were not used
- Secure Shell (SSH) was not used
- No scalable Authentication, Authorization and Accounting (AAA) systems were used
- No device redundancy (for reliability)
- No communication channel redundancy (for reliability)
- No firewalls

Hence it was sufficient to apply a simple Business Impact Analysis (BIA) with respect to the effect on significant down-time on operations, finance and the associated legal implications. BIA ratings of 1 (negligible) to 5 (very high) were used. BIA is a business continuity process used to analyze mission-critical business functions and hence both identify and quantify functional loss on an organization. The results of this simple BIA (tables 1 to 3) were sufficient to vindicate that a comprehensive security plan was needed.

Network Issues	Impact rating
Lack of router security	5
Lack of switch security	5
Lack of wireless security	5
Lack of device redundancy	5
Lack of communication channel redundancy	5
No firewall	5

Table 1: Network security

IT policies	Impact rating
Lack of comprehensive network usage policies	4
Lack of comprehensive network audit policies	4
Lack of staff password policies	5

Table2: IT policies

Physical security	Impact factor
Environmental factors	4
Theft	4

Table 3: Software security

Cleary even though the risk of sabotage could be low the potential consequences are considerable. Power loss even for a relatively short time would have serious implications for commerce, industry and all aspects of life dependent on power.

4. Secure network requirements

Given that the XYZ and associated sites of PP1, PP2 and PP3 all had connections to the Internet, in the first instance it was deemed important to design, configure and hence implement a secure network infrastructure as this represented the most immediate and pressing security problem. This was also the opportunity to design and a more scalable network. A requirements specification including the following was recommended:

Security

- Network device hardening (login warning banner, enhanced username password security, password encryption, SSH, multiple administrative roles with different privileges, NTP, Syslog etc)
- Secure network device administrative access
- Secure OSI layer 2 device configuration (portfast, BPDU guard, storm control, root guard etc)
- Secure site to site Virtual Private Networks (VPNs) between networks using the IPSec standards framework
- Firewalls between PP1, PP2, PP3 and the Internet
- Secure, scalable administrative access using AAA
- Virtual Local Area Networks (VLANs) for each department
- SSH only for remote device connection
- Intrusion Prevention System (IPS) along with updates IPS signatures
- Virus scanning with regular updates
- Regular network device operating system updates
- Security policy development and deployment

Scalability

- Link aggregation between switches – providing both reliability and scalability
- Systematic allocation of IP addresses

Reliability

- Link aggregation between switches – providing both reliability and scalability
- Routine, documented backups
- Uninterruptable power supplies

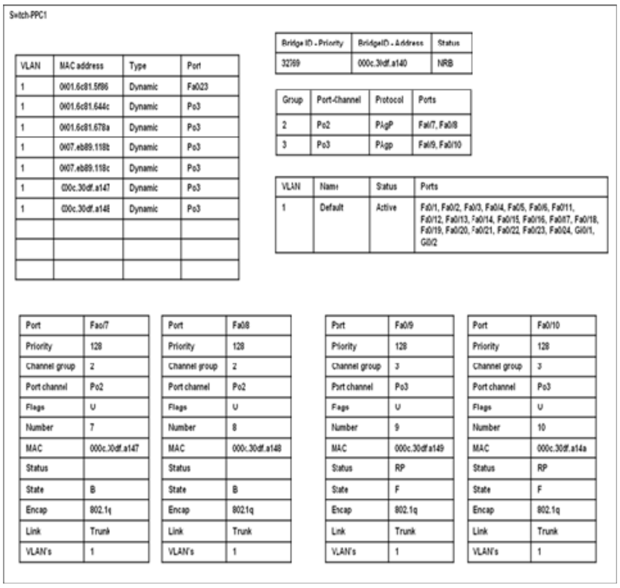
The security policy consisted of three main areas: governing policies, end-user policies and technical policies. In this phase of the project the main focus was on the technical policy

Fiber optic connectivity has the potential advantages of security, scalability and reliability and was recommended. However this was discounted on the basis of cost. Similarly the use of an Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) were both recommended but for operational reasons not included.

Significantly the cost, other than development and testing time, was negligible. Previously firewalls were typically dedicated devices. However for Cisco based networks the recommended method of firewall implementation is on a standard router with the appropriate Internet Operating System version.

A fully scaled test network was configured and tested - the tested configurations then being deployed to the operational devices. This has the advantage of significantly fewer configuration errors and reduced down time during the change-over to the new system.

State Model Diagrams (SDMs) were found to be useful for documentation and testing routers and switches but were of particular value for the more complex security protocols [7], [8], [9], [10]. Hence an intrinsic aspect of the technical documentation (of the fully scaled network) was SMD representation of every device and associated protocols. Significantly, using SMDs it is possible to model multiple protocols operational on a single device. It is then possible to selectively interrogate each protocol by simply opening the corresponding state tables. It is then possible to clearly observe not only protocol states but interactions between different protocols (figure 1).



Switch-PPC1

VLAN	MAC address	Type	Port
1	0001.6c81.5f86	Dynamic	Fa023
1	0001.6c81.644c	Dynamic	Po3
1	0001.6c81.678a	Dynamic	Po3
1	0007.eb89.118b	Dynamic	Po3
1	0007.eb89.118c	Dynamic	Po3
1	000c.30df.a147	Dynamic	Po3
1	000c.30df.a148	Dynamic	Po3

Bridge ID - Priority	BridgeID - Address	Status
32769	000c.30df.a140	NRB

Group	Port-Channel	Protocol	Ports
2	Po2	PAgP	Fa0/7, Fa0/8
3	Po3	PAgp	Fa0/9, Fa0/10

VLAN	Name	Status	Ports
1	Default	Active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gi0/1, Gi0/2

Port	Fao/7
Priority	128
Channel group	2
Port channel	Po2
Flags	U
Number	7
MAC	000c.30df.a147
Status	
State	B
Encap	802.1q
Link	Trunk
VLAN's	1

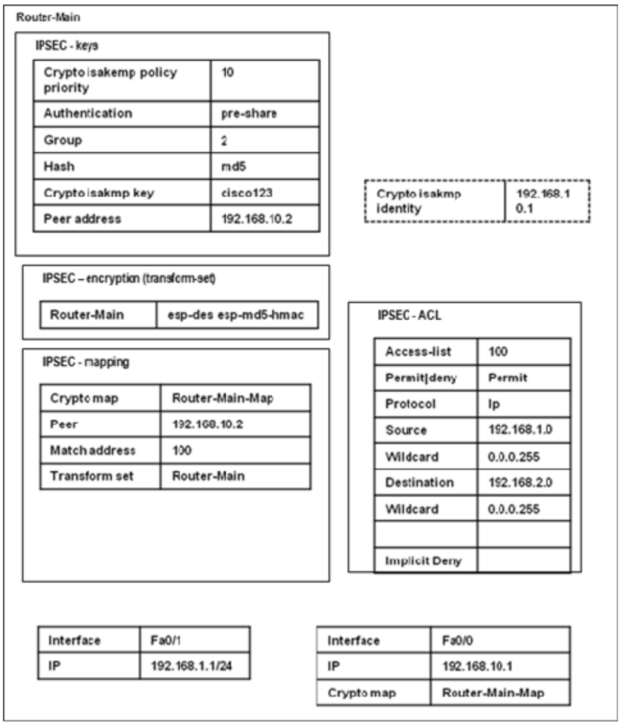
Port	Fa0/8
Priority	128
Channel group	2
Port channel	Po2
Flags	U
Number	8
MAC	000c.30df.a148
Status	
State	B
Encap	802.1q
Link	Trunk
VLAN's	1

Port	Fa0/9
Priority	128
Channel group	3
Port channel	Po3
Flags	U
Number	9
MAC	000c.30df.a149
Status	RP
State	F
Encap	802.1q
Link	Trunk
VLAN's	1

Port	Fa0/10
Priority	128
Channel group	3
Port channel	Po3
Flags	U
Number	10
MAC	000c.30df.a14a
Status	RP
State	F
Encap	802.1q
Link	Trunk
VLAN's	1

Figure 1: Switch with multiple protocols

For example this switch is configured for: trunking, port aggregation, VLANs (default VLAN1) and Spanning Tree Protocol (STP). It is possible to readily observe that, for example interfaces fa0/7 and Fa0/8 are both members of port aggregation channel 2 employing the Port Aggregation Protocol (PAgP). Furthermore both interfaces are in VLAN and are blocked by the Spanning Tree Protocol.



Router-Main

IPSEC - keys

Crypto isakmp policy priority	10
Authentication	pre-share
Group	2
Hash	md5
Crypto isakmp key	cisco123
Peer address	192.168.10.2

Crypto isakmp identity	192.168.1 0.1

IPSEC – encryption (transform-set)

Router-Main	esp-des esp-md5-hmac

IPSEC - mapping

Crypto map	Router-Main-Map
Peer	192.168.10.2
Match address	100
Transform set	Router-Main

IPSEC - ACL

Access-list	100
Permit|deny	Permit
Protocol	Ip
Source	192.168.1.0
Wildcard	0.0.0.255
Destination	192.168.2.0
Wildcard	0.0.0.255
Implicit Deny	

Interface	Fa0/1
IP	192.168.1.1/24

Interface	Fa0/0
IP	192.168.10.1
Crypto map	Router-Main-Map

Figure2: Router-Main

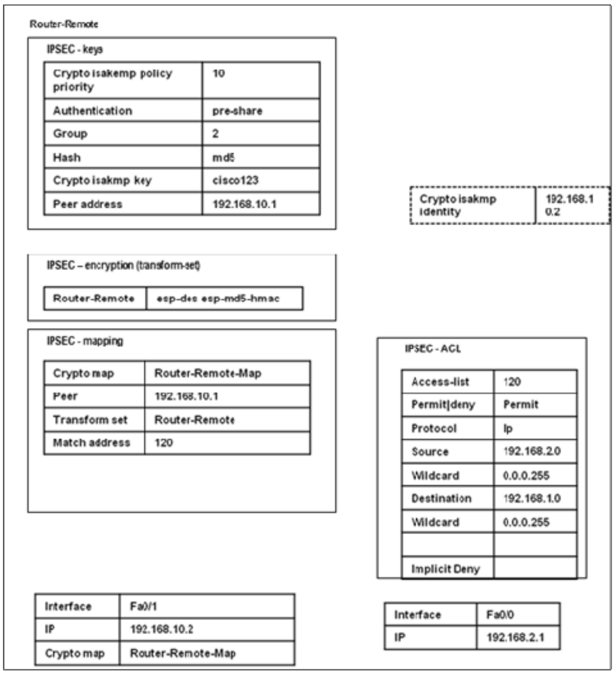
Using the SMD representations of IPSec VPNs it was a simple procedure to cross-check the following parameters:

- Peer IP address
- Access Control List asymmetry
- Transform set encryption standard
- Isakmp policies (authentication, encryption, hash, key)

The VPN configuration parameters in for example Router-Main (figure 2) could very easily be cross checked against the configuration parameter of the associated Router-remote (figure 3).

3. Conclusions

Critical Infrastructures must be guarded against possible cyber attacks. The potential excuse that, for some types of infrastructure perpetrators cannot receive financial gain is erroneous. Sabotage can be purely mischievous. Though the risk may be low the consequences are considerable. It has been shown that for minimal cost a network can be considerably hardened against potential attacks. If possible it is recommended that a fully scaled test bed is used to develop the device configurations. This has the advantage that fully tested configurations can then be deployed thereby minimizing down-time.



Router-Remote

IPSEC - keys

Crypto isakemp policy priority	10
Authentication	pre-share
Group	2
Hash	md5
Crypto isakmp key	cisco123
Peer address	192.168.10.1

Crypto isakmp identity	192.168.1 0.2

IPSEC – encryption (transform-set)

Router-Remote	esp-des esp-md5-hmac

IPSEC - mapping

Crypto map	Router-Remote-Map
Peer	192.168.10.1
Transform set	Router-Remote
Match address	120

IPSEC - ACL

Access-list	120
Permit|deny	Permit
Protocol	Ip
Source	192.168.2.0
Wildcard	0.0.0.255
Destination	192.168.1.0
Wildcard	0.0.0.255
Implicit Deny	

Interface	Fa0/1
IP	192.168.10.2
Crypto map	Router-Remote-Map

Interface	Fa0/0
IP	192.168.2.1

Figure 3: Router-remote

References

[1] Government, A., Critical Infrastructure Resilience Strategy. 2010: Barton, ACT.

[2] McAfee, In the Dark. Crucial Industries Confront Cyberattacks. 2010, Centre for Strategic & International Studies.

[3] Ten, C., Liu, C., Govindarasu, M., Cyber-Vulnerability of Power Grid Monitoring and Control Systems, in Cyber Security and Information Intelligence Research Workshop, F. Sheldon, Editor. 2008, ACM: Oak Ridge, Tennessee, USA.

[4] Verendel, V., Quantified Security is a Weak Hypothesis, in New Security Paradigms Workshop, A. Somayaji, Editor. 2009: Oxford, UK.

[5] Blackwell, C., A Multi-layered Security Architecture for Modelling Complex Systems, in Cyber Security and Information Intelligence Research Workshop, F. Sheldon, Editor. 2008, ACM: Oak Ridge, Tennessee, USA.

[6] LeMay, E., Unkenholz, W., Parks, D., Muehrcke, C., Keefe, K., Sanders, W. H., Adversery Driven State-Based System Security Evaluation, in Security Measurement and Metrics. 2010, ACM: Bolzano-Brozen, Italy.

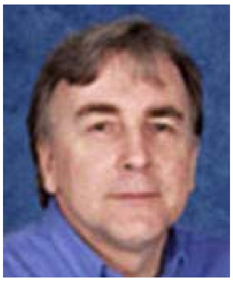
[7] Maj, S.P., Makasiranondh, W., Veal, D., State Model Diagrams - a universal runtime network management tool. Modern Applied Science, 2010. 4(12): p. 26-35.

[8] Maj, S.P., Makasiranondh, W., Veal, D., An Evaluation of Firewall Configuration Methods. International Journal of Computer Science and Network Security, 2010. 10(8): p. 1-7.

[9] Maj, S.P., Veal, D., An Evaluation of State Model Diagrams for Secure Network Configuration and Management. International Journal of Computer Science and Network Security, 2010. 10(9): p. 66-72.

[10] Maj, S.P., Veal, D., Using State Model Diagrams to Manage Secure Layer 2 Switches. International Journal of Computer Science and Network Security, 2010. 10(9): p. 141-144.

Yeshey Wangdi is a master's candidate in Computer and Network Security at the Edith Cowan University, Perth, WA. He was awarded the prestigious Golden key award in 2010 for his outstanding performance in academia. He is currently IT Manager for Druk Green Power Corporation, Bhutan.



Dr. David Veal is a Senior Lecturer at Edith Cowan University. He is the manager of Cisco Network Academy Program at Edith Cowan University and be a unit coordinator of all Cisco network technology units. His research interests are in Graphical User Interface for the visually handicapped and also computer network modeling.

A/Prof S. P. Maj has been highly successful in linking applied research with curriculum development. In 2000 he was nominated ECU University Research Leader of the Year award He was awarded an ECU Vice-Chancellor's Excellence in Teaching Award in 2002, and again in 2009. He received a National Carrick Citation in 2006 for "the development of world class curriculum and the design and implementation of associated world-class network teaching laboratories".