3-12-2008

Issues common to Australian critical infrastructure providers SCADA networks discovered through computer and network vulnerability analysis

Craig Valli
Edith Cowan University

DOI: 10.4225/75/57b2803940cc8
6th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 3rd 2008.

Issues common to Australian critical infrastructure providers SCADA networks discovered through computer and network vulnerability analysis

Craig Valli
SECAU Security Research Centre
Edith Cowan University
Perth, Western Australia
c.valli@ecu.edu.au

Abstract

This paper reports on generic issues discovered as a result of conducting computer and network vulnerability assessments (CNVA) on Australian critical infrastructure providers. Generic issues discovered included policy, governance, IT specific such as segregation, patching and updating. Physical security was also lacking in some cases. Another issue was that previous security audits had failed to identify any of these issues. Of major concern is that despite education and awareness programs, and a body of knowledge referring to these issues, they are still occurring. It may be necessary for the federal government to force organisations to undergo computer and network vulnerability assessment from recognised experts on a regular basis.

Keywords

SCADA, security, computer and network vulnerability assessment, process control systems

INTRODUCTION

Traditionally SCADA systems were designed around reliability and safety, and if they were network connected they were connected on isolated internal networks for the purposes of control and management; essentially a closed system. Typically in these situations security was not a consideration due to the isolated nature of the systems and their closed nature. It should be remembered that these systems were implemented also in an era when computing and information technology will also largely conducted in isolated installations or laboratories around the globe (Stouffer *et al*, 2007). The world has now moved on and we are becoming increasingly interconnected and interdependent on these connections for the full functioning of modern society. One of the main conduits and enablers for this has been the rapid expansion of the Internet. Correspondingly, as a result of the growth of the Internet there has been a convergence on the TCP/IP protocol suite as the dominant network protocol for business and industry. This has seen many hardware and software vendors, including SCADA vendors, align their products with this kind of reality (Igure *et al*, 2006). This transition to a level of greater interconnectedness has impacted on the security posture of these systems. Threats and vectors that did not exist prior to this transition are now becoming realisable threats. There is an increasing reliance on public telecommunications networks to link previously separate SCADA systems making them more accessible to attacks. Then be increasing use of published open standards and protocols, in particular Internet technologies, expose SCADA systems to Internet or network borne attacks, that were not realisable for instance on proprietary protocols that were used previously to control such systems. The actual increased interconnection of SCADA systems to corporate networks is a significant threat in itself enabling and making them accessible to undesirable entities e.g. malfeasant insiders (Jackson-Higgins, 2007). Many systems that are in SCADA networks often lack mechanisms to provide confidentiality of communications for example the use of sufficiently strong encryption to protect data during transit. This type ofproblem coupled with a lack of appropriately strong or granular authentication mechanisms and controls in many SCADA systems and the problem becomes manifold even to a security novice. This paper reports on and discusses some generic issues discovered as a result of conducing computer and network vulnerability assessments on Australian critical infrastructure providers.

THE CNVA PROGRAM AND WHY WE NEED IT FOR SCADA

The Computer Network Vulnerability Assessment (CNVA) program is an Australian Government grants scheme developed to help ensure the security of Australia's critical infrastructure (TISN 2008). The program is managed by GovCERT.au – the Australian Government computer emergency readiness team, which is under the umbrella of the Australian Government Attorney-General's Department. The program provides funding of up to 50 per cent of the cost of a vulnerability assessment to private critical infrastructure owners and/or operators, including Government Business Enterprises.

Although not many public stories, there are reports of attacks against critical infrastructure. Sources of attack include vectors both intentional and unintentional. Categories covered by the former include hacking, insider malfeasance, and malware. Unintentional vectors include malware and lack of due diligence. The most infamous of the intentional attacks is the case of Maroochy shire. Their SCADA system was hacked by a person who had been employed to install the system after a request for employment was turned down (Smith, 2001). An example of unintentional malware interfering with SCADA systems is the SQL Slammer worm released in 2003. This worm infected the Davis-Besse nuclear power plant in Ohio, USA, causing operators to lose a degree of control over the system. As a result, the plant safety display system and process control computers were shut down for nearly seven hours (Poulsen, 2003). A more recent incident and an example of lack of due diligence, orintentional consequences of a legitimate activity, was the shutdown of a nuclear power plant. The update of software on a computer on the plants business network caused reset of data on the control system. The safety systems interpreted this lack of data to mean that there was no water in the reservoirs that cool the rods, and shut down the reactor (Krebs, 2008). There has also been public commentary by a CIA analyst that utilities based in foreign countries had been attacked through the internet (Nakashima & Mufson, 2008). It was further reported that these attacks had resulted in power outages in a major city. The same article also indicated that there had been an increase in internet based attacks against utilities in the United States.

SPECIFIC ISSUES INDETIFIED THROUGH THE CNVA PROGRAM

This section discusses the issues that have been discovered as a result of the author's participation in the CNVA program. There were a range of specific issues discovered, with the generic, common issues highlighted in this paper. There are no specific cases discussed here as this would be in violation of various confidentiality agreements.

Connection of SCADA to corporate

This point is not really a surprise, as it is why the CNVA exists. However, despite available advice and documentation (Stoufer *et al*, 2007), and in some cases even in complete contradiction of corporate policy, corporate and SCADA networks are being connected with little, if any, segregation. As mentioned previously, SCADA has a soft underbelly as it was designed to work, with security coming second to functionality. However, when SCADA systems were initially designed, the internet didn't exist, and what elements may have existed was not a threat to systems installed at that time. The issue here is that despite evidence that connection of SCADA to corporate networks without appropriate barriers is an identified risk, and should not happen, it is still occurring.

Governance

All cases had significant issues with effective governance of the critical infrastructure assets. In this case we mean the assets to be both the corporate and SCADA networks of the organisations the authors examined. All organisations demonstrated poor delineation of corporate ownership and responsibility for the SCADA networks and in some cases the supporting information technology infrastructures. Several sessions during the assessments sometimes degenerated into a scene from Martin Scorsese film i.e. "are you talkin to me, are you talking to me?" with the general abrogation of responsibility ensuing shortly there afterwards. Sadly one of the common memes was "Engineers don't know much about security with the counter meme "IT nerds know less about SCADA" often being the first point both parties agreed on. Some fundamental governance questions had not been addressed by any of the organisations.
These were:

- Who was responsible for change management for each of the assets?
- Who is in charge of the IT network, and are they still in charge after it is connected to SCADA?
- What is the escalation process should there be a record of incident?

In some cases, there were even issues relating to the ownership and availability of documentation for corporate networks and computer hardware and software.

Policy

As a result of poor governance structures within the organisations the policy structures also suffered. There was little evidence of any policy review, policy enforcement, policy auditing or existence of any policyimplementation. Review of the policy documentation that was presented during the assessments revealed it was rarely current and was lacking in relevant details. The policy in some instances had not been reviewed or revised for several years. In some cases where there was the existence of a policy there existed approved

procedures which were in direct contravention to the existing policy. These procedures are also often created, produced and implemented by third parties such as contractors. In one case the outsourced contract is for the network infrastructure eventually refused to produce policy documents. The basis for this was that they were not required under the terms of the contract to surrender such documents.

IT SPECIFIC ISSUES

Un-Patched Hardware And Software

All of the assessments conducted found exploitable vulnerability as a result of un-patched hardware and software issues. Of particular concern were perimeter firewalls that had multiple exploitable vulnerability as a result of dilettante patching regimes. These firewall exploits were well known and had been known in the security community for up to four to five years.

Due to legacy nature of SCADA systems all of the underlying supporting computer operating systems had significant vulnerability. Most of the operating systems examined in all assessments had long since become no longer supported by the vendor. Most of the supporting applications in the form of SQL servers, network operating systems or specific SCADA applications were likewise no longer supported by the vendor.

Lack Of Network Segregation And Segmentation

Assessments conducted so far have revealed networks that are severely compromised under the defence in-depth strategy. Several of the network architectures were based on flat 10.0.0.0/8 networks allowing for a reversal of the entire network including corporate and control systems. Penetration of perimeter controls would have allowed complete sight into the enterprises examined. This would allow the easy implantation of malcode such as packet sniffers or keystroke analysers into the network architectures. In one instance the organisation was unsure as to where the connections to a fibre ring they connected to which was used by other organisations actually terminated. Furthermore they were initially unsure and as to what controls and countermeasures were in place to prevent ingress into the network from this network.

Lack Of Sound Authentication Mechanisms

Several of the installations provided generic logins to staff members for example username equals staff password equals staff. All of the systems reviewed had no reliable or monitored audit trial for systems access. That is no coordinated logging of even simple statistics such as logon or log off was conducted. These logins were provided mainly for expediency and were handed out typically as a result of the work environment trusting individuals. Given that 60 to 80% of losses sustained by successful I T. enabled crime or malfeasance is committed by insiders (Richardson, 2008), one could postulate this is an extremely unwise move on the part of management. Furthermore, some of the generic accounts uncovered in the examinations had root or admin level access to the entire IT infrastructure. This would allow any malicious individual the power to corrupt absolutely.

The use of such simple and group based passwords also allows a substantial vector for the disgruntled employee to penetrate the system and wreak havoc with impunity.

Monitoring, logging, auditing

There was a complete lack of any substantive logging of network interactions with attendant monitoring and then subsequent auditing and review. This observation put all organisations in an invidious position with respect to the network based exploit and attack. This leads to the realisation that most of the organisations had no ability to answer fundamental questions such as have we been attacked? We got hacked – how did it happen? Inability to answer even these basic questions makes amelioration or reduction of any network borne threat a relatively impossible task.

In one organisation there was a logging of firewall connections but no actual review of these logs to determine any emergent threat, unauthorised connections or internal malfeasant activity. The net value of this type of logging is a completely negative proposition for the organisation. The organisation is wasting money loggingdata that was never intended to be examined.

It has been proven already due to the nature of SCADA systems that the use of intrusion detection systems and intrusion prevention systems can shutdown communications, which can have potentially catastrophic unintended consequences (Fink *et al*, 2006). If we cannot reliably implement and use intrusion detection systems or intrusion prevention systems to protect networks that run SCADA devices, the use of monitoring logging and auditing are fundamental tools and techniques in providing response against network based attack. In some cases the use of these is the first and last line of defence against attacks that would be perpetrated against networks.

Physical Security

Although not part of a computer system or hardware, physical security is still an important part of computer security, and also part of any properly conducted computer and network vulnerability assessment. For example, are server rooms protected by appropriate fire suppression systems? Are physical access control methods inplace for servers and other equipment?

There were a number of issues relating to physical controls which are of concern, as physical systems can be barriers to casual attacks. One organisation had no restriction on access into the main control room for the SCADA network. Another had servers and other communications equipment stored in a physically vulnerable location. Yet another had no fire suppression system for their SCADA master servers. A remote site visited as part of an assessment had no alarms on doors, unaccounted for keys, rooms that stayed open and unlocked that also had computer terminals. Locked doors were often the only barriers in some cases.

Previous reports and audits

At some of the organisations that were assessed, there were reports on the security that had been conducted by previous groups. It was unclear as to whether these had been conducted as part of the CNVA program, or if they had been commissioned by these organisations in a commendable attempt to increase their security posture. Unfortunately, the reports had missed most of the critical issues identified by the authors in these cases. That is not to say that the authors did not also miss some problems; nobody is perfect. The issue is that these were reports prepared by large organisations who specialise in IT security auditing. It would be of concern if these organisations were part of the CNVA panel, and had been conducting audits on this basis. Given that GovCERT has oversight on the reports produced by CNVA audits, it seems more likely they were not produced as part of the CNVA program. The issue, however, is that security audits are being performed by organisations that do not appear to have the necessary knowledge of specific SCADA IT security issues that must be addressed if security is to be improved.

CONCLUSION

The vulnerability assessments conducted by the authors have left little doubt that there is certainly a need for the CNVA program. It is understandable that safety and risk engineers and managers in the critical infrastructure sector are largely concerned with physical as they either don't understand the nature or the risk from the information technology perspective. The authors have seen on more than one occasion the attitude that "It won't happen to us", or "I have far more to worry about with a faulty valve exploding". There was little perceived risk from the IT vector. However, the reality is that cyber attacks against CIPs are happening around the world, as pointed out earlier in this article. The other upcoming issue is that these CIPs are looking to implement TCP/IP based communication protocols in place of largely unknown legacy protocols such as Modbus and DNP3. This will only introduce further vulnerability, as use of such protocols currently at least provides some sort ofsecurity through obscurity.

Despite the existence in Australia of SCADA communities of interest, despite numerous publications aimed at both management and technical audiences (TISN 2005), and even in spite of the CNVA program, there still appears to be serious issues with recognition of the security issues faced by connecting SCADA networks to the internet. Of concern is that most of the issues reported in this paper are not new, and have been discussed previously in other reports concerning SCADA security (Stamp *et al*, 2003; Fink *et al*, 2006; Igure *et al*, 2006; Stouffer *et al*, 2007). The authors would argue that not only does the CNVA program need to be continued, but that it needs to be expanded. Associated work by the authors has also revealed that hard drives and other computer hardware are being disposed of without being properly erased from CIPs. This adds further weight for a call for all critical infrastructure providers to undergo some form of external computer and network vulnerability assessment or audit on a regular basis.

REFERENCES

Fink, R.K., Spencer, D.F. & Wells, R.A. (2006). Lessons learned form cyber security assessments of SCADA and energy management systems. Retrieved 14th October 2008 from http://www.inl.gov/scada/publications/d/nstb_lessons_learned_from_cyber_security_assessments.pdf

Igure, V.M., Laughter, S.A. & Williams, R.D. (2006). Security issues in SCADA networks. *Computers and Security*. **25(7):** 498-506

Jackson-Higgins, K. (2007). SCADA state of denial. Retrieved 10th October from http://seclists.org/isn/2007/Apr/0068.html

Krebs, B. (2008). Cyber incident blamed for nuclear power plant shutdown. Retrieved 10th October from http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html

Nakashima, E. & Mufson, S. (2008). Hackers Have Attacked Foreign Utilities, CIA Analyst Says. Retrieved 11th October 2008 from http://www.washingtonpost.com/wpdyn/content/article/2008/01/18/AR2008011803277.html

Poulsen, K. (2003). Slammer worm crashed Ohio nuke plant network. Retrieved 10th October 2008 from http://www.securityfocus.com/news/6767

Rishardson, R. (2008). CSI Computer crime and security survey. Retrieved 14th October 2008 from http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf

Smith, T. (2001). Hacker jailed for revenge sewage attacks. Retrieved 10th October 2008 from http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/

Stamp, J., Dillinger, J., Young, W. & DePoy, J. (2003). Common vulnerabilities in critical infrastructure control systems. Retrieved 14th October 2008 from http://www.sandia.gov/scada/documents/031172C.pdf

Stouffer, K., Falco, J. & Scarfone, K. (2007). *Guide to industrial control systems (ICS) security*. USA: NIST Trusted Information Sharing Network (2005). SCADA Security – Advice for CEOs. Retrieved 10th October 2008 from http://www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/(427A90835BD17F8C477D6585272A27DB)~Supervisory_Control+and+Data+Acquisition+(+SCADA+)+-+Security+Advice+for+CEOs.pdf/$file/Supervisory_Control+and+Data+Acquisition+(+SCADA+)+-+Security+Advice+for+CEOs.pdf

Trusted Information Sharing Network (2008). *Computer Network Vulnerability Assessment Program*. Retrieved 11th October from http://www.tisn.gov.au/www/tisn/tisn.nsf/Page/CIPPrograms_ComputerNetworkVulnerabilityAssessment(CNVA)Program

COPYRIGHT