2009

# SCADA Security - Slowly Circling a Disaster Area

Craig Valli
*Edith Cowan University*

Andrew Woodward
*Edith Cowan University*

# SCADA Security – Slowly Circling A Disaster Area

**Craig Valli and Andrew Woodward**
secau – Security Research Centre
School of Computer and Security Science
Edith Cowan University
Mount Lawley WA, Australia

**Abstract** - *SCADA (Supervisory Control And Data Acquisition) networks control much of the industrialised nations production and supply complexes. Various government reports and investigations have highlighted the vulnerability of these systems. Many of these systems are on private networks which are increasingly being connected to systems that are accessible from other networks such as the Internet.*

*SCADA systems have unique security and operational requirements. However, many of the most basic security measures are missing in these networks. This examines some of these issues and proposes some technologies that could help secure these networks from attack.*

**Keywords:** SCADA, infrastructure, countermeasures, open source, IDS, firewall, honeypots

## 1 Introduction

Critical infrastructure is largely controlled by the use of automated control systems and in particular supervisory control and data acquisition (SCADA) systems. SCADA systems are being identified in various Government reports and the media as systems that are increasingly coming under attack [1-3]. The reports from various agencies rate SCADA systems as highly vulnerable to attack or compromise that would result in catastrophic failure of these systems.

Many of these systems are used to run the modern industrial complexes that supply modern Western nations with many of the services and goods that they take for granted. These systems are to be found in but not limited to: petroleum complexes, power generation grids, water supply networks, sewerage networks and most other complex systems that require constant computer-based monitoring or control.

Failure or even disruption to these systems could have catastrophic consequences resulting in supply chain collapse, with resultant economic impacts and even loss of life directly or indirectly. As a recent example, disruption of gas services as a result of an industrial mishap in Western Australia alone in 2008 almost saw that States economy grind to a halt [4]. The loss of capacity at ~ 40% was sufficient to have considerable downstream effects that for instance caused laundry for hospitals to be shipped in from other Australian states until increased supplies of gas could be obtained. A cyber based attack that could disrupt supply in the same manner could have similar effects.

SCADA/control devices and resultant systems are built to run, monitor or control a particular process, typically as a part of combined automated process that results in a product. Many of these devices and systems in which they operate are intended to run for the life of the project, life of an ore body in a mine, or product cycle which can be decades not weeks. As a result, SCADA systems have a larger than expected level of legacy hardware and software installed, the old engineering adage if it is not broken do not fix it, was and remains a meme in many of these systems. This *modus operandi* was a perfectly acceptable operational paradigm in which to operate when many of these companies/entities did not connect to any network except their own, and the production or engineering network was never connected to the corporate network that connected to the Internet. This *status quo* has now changed for a number of reasons, namely, the increasing ubiquity of the Internet and its associated technologies and protocols and interconnection with business processes. The drivers are not always technological: smaller companies merge and combine to become bigger entities, particularly as the pressure of globalisation and economic rationalisation increase. This trend leads toward network infrastructures that are often comprised of different and disjointed legacy network systems and infrastructures. Further adding to the entropy with respect to the security and technical stability, is the attachment to the corporate network and increasing use of Internet technologies such as http to reach into these SCADA and control networks. In addition, it is not uncommon to have a third party entity in charge of the SCADA network and systems, and possibly even an additional third party IT outsourcing company in charge of corporate networks.

Many of the older SCADA and control systems were proprietary systems with protected protocols and processes. As a result, these systems had a reasonably high level of security through obscurity and limited knowledge of their design and operation. When these SCADA and control systems are upgraded, they are being moved to open platform systems that utilise open network protocols such as Distributed Network Protocol 3 (DNP3) or ModBUS, and increasingly, TCP/IP based control systems.

Atypically, older systems infrastructures were controlled via tied lines or privately controlled proprietary wired or proprietary wireless networks. New generation SCADA and control systems also use modern open standard communications networks to provide access to the SCADA

systems for control and command. These newer networks even if totally private will almost atypically run the TCP/IP range of protocols and supporting services for backbone and control. Many providers are as previously mentioned also replacing dedicated hard physical links to control/command interfaces with links that may actually travel on or rely upon open public networks such as the Internet for data transport, due to either telecommunications provider enforced changes, or due to financial pressure. Of greater risk is that some of these systems utilise open protocol wireless systems such as 2.4 GHz WiFi for these command and control functionalities.

This paper will examine the threats to, and countermeasures for SCADA systems as a result of the decreasing use of proprietary protocols and equipment, and their move to open protocol based systems and the use of the Internet as a backbone. It should be noted that the hacker community is increasingly aware of SCADA networking issues, with serious exploits now being available in the Metasploit framework for use by anyone who can use a mouse and connect to the Internet.

## 2 SCADA – Slowly Circling A Disaster Area

Unlike conventional Ethernet networks that run business enterprises, SCADA and control networks typically need to have consistent connection to devices that control industrial processes. SCADA and control systems work by receiving data from instruments or data points and also sending commands or instructions to devices. These instructions or data could be to check flow rates of toxic chemicals, or open valves or start pumps to avert overflow of a fluid storage facility. The system is set to poll or respond over a given interval of time back to a controller or master. A break in this polling as a result of a simple disruption of these monitored processes can in turn cause these systems to go into failsafe modes or implement shutdown procedures or worse fail. These procedures are designed to provide maximum safety for the particular process being run, and in some cases these shutdowns or failsafe procedures are mandated by regulation and law. Therefore, it is reasonable to assume that disruption or denial of service on a SCADA network could have catastrophic consequences and is a highly undesirable event in these systems.

SCADA and control systems are one set of systems where it could be argued the use of open source or protocols significantly impacts the security of these systems, and a wide range of interconnected systems and critical infrastructures. There is little doubt there is significant value in secret knowledge or compartmentalisation of knowledge for critical systems otherwise we would all have access to nuclear missile launch codes.

As mentioned previously SCADA and control systems are moving to open source/open community protocols such as DNP3, and away from other proprietary systems protocols. The logic behind having a common protocol and platform across these systems so that each platform or vendor devices can interact at a network or system level would be one that seems complete and one that makes good economic rational sense *i.e.* economies of scale, one protocol, one training provider *etc*. It could also be argued that it makes good technical sense as well to have a single unified environment with common hardware and software interacting. That is however, where any benefit stops, particularly from a security perspective. The use of like equipment can see an entire facility be vulnerable as part of a larger exposure in the equipments core. Cisco is without question the market leader in provision of network hardware and software, yet even it has system wide vulnerability that allowed complete compromise of a network that was using its equipment. Furthermore the use of a single platform in a network environment particularly for egress and ingress of network packets goes against a basic tenet of security, which is defence in depth.

Common protocols have been proven to be problematic in networks, particularly if the flaw is patent and inherent in the design. Even closed or supposedly private networks that use wireless infrastructure are increasingly exposed as open to attack [5]. If we take WiFi or 802.11 equipment as a recent well known example, if the wireless equipment meets the IEEE standard for 802.11 it is regardless of manufacturer susceptible to a wide range of protocol based attacks [6, 7]. These protocol based attacks are devastatingly effective and unstoppable without further countermeasures or extension of the 802.11 protocol. What could occur if DNP3 or ModBUS or a similar SCADA specific protocol was found to have the same level of exploit?

Wireless based networks use a wide range of protocols and rates of transmission and some even use half duplex transmission to overcome low speed issues, but nonetheless the irrefutable fact is that they are transmitting across a commonly accessible media *i.e.* the atmosphere. This accessibility enables the transmissions susceptible to denial of service at a physical layer with wireless jamming devices [8]. The bad news is that this attack at the physical layer is almost impossible to defend against and can be hard to trace. These physical attacks are in addition to known exploits against particular wireless protocols which are numerous and well documented [6, 7, 9]. Even if the wireless communications use encryption or VPN technologies to protect transmission, there are numerous tools that can break, intercept or even inject into this type of network countermeasures [10] and the aforementioned physical attacks bypass these anyway. These vulnerabilities in wireless and associated transmission protocols are also not limited to WiFi or the 2.4 GHz spectrum simply

because they are radio based: they can also apply to other wireless frequencies and transmission protocols.

The use of open source protocols is also problematic as many modern SCADA systems have http enabled management consoles and use either direct wired or wireless connectivity to achieve connection and you will have significant security problems already associated with normal network transport.

SQL and database technologies are an invaluable tool for storing and retrieving data from appliances, and they are also widely used in configuration management for SCADA and control systems. They provide the ability to relay or receive commands, gather outputs or readings from various apparatus and store them for later use or processing, for example the generation of customer billing. The historian is an integral part of a SCADA or control system, and also replies upon these database technologies. The use of SQL systems all leave the window open for SQL injection and other exploit of database systems to occur as well in SCADA and control networks. Compromise and control of the SQL elements in a system can have catastrophic effects as was evinced in the 2003 SQL Slammer incursion into a nuclear power plant [11] .

Even though SCADA has been flagged as a problem for at least the past 10 years, most commercial Ethernet centric firewalls and network security countermeasures are focussed on the resolution of problems with TCP/IP protocols and still largely ignore SCADA relevant protocols [12]. This hinders the development of enterprise initiatives as alternative products or 3rd party plugins must be adopted often with varying levels of integration and consequent success.

A paper by [13] highlighted a range of security issues found in some of Australia's critical infrastructure. These issues can be summarised as follows.

General Issues:

- Connection of SCADA to corporate networks
- Governance
- Policy
- Physical Security

IT Specific issues:

- Un-patched hardware and software
- Lack of network segregation and segmentation
- Lack of sound authentication mechanisms
- Lack of monitoring, logging and auditing

Of concern here is that an examination of any report or document relating to SCADA security, or recommendations to secure SCADA lists most of the above as being areas that must be concentrated on (Stamp *et al* 2003; Fink *et al* 2006; Stouffer *et al* 2007). Furthermore, it should be noted that these documents have been freely available since at least 2003.

# 3 COUNTERMEASURES?

The typical countermeasures that are utilised for securing Ethernet networks apply to SCADA and control networks in theoretically the same way. These tools would include typically include a firewall, intrusion detection systems and some method of protocol analysis. There are however, subtle nuances in the way these would be utilised for instance it would be irresponsible to have an IDS halt/deny routes in SCADA/control network.

**Firewalls**

Firewalls are a primary defensive mechanism for any network situation and through stateless or stateful inspection will allow or disallow egress of network packets through a gateway device or control point. Support for SCADA and control system protocols in commercial software is improving but the take up is slow (NISCC, 2005, p.31). However, the open source community has developed a firewall for the ModBUS protocol that runs on Linux using extensions to the kernel netfilter firewalling (REF modbusfw). The filtering occurs on four header values these are:

- Function code – filtering is based on single or multiple function codes
- UnitID – filter on specified ID
- Reference Number – filtering on a specified reference number
- Length – Filter on size greater than, less than or equal too.

This level of filtering allows for a reasonable degree of protection and ability to make rulesets that for instance would be able to trap buffer overflow attempts, incorrect or malformed commands, out of range packets or probative packets. This allows for a rich picture of network activity and any associated problems to be developed using appropriate analysis tools.

Of course modern firewalls can have custom rule sets written and in fact some sources of these rulesets now exist for use. These rule sets however tend to suffer from one fatal flaw they are only as good as the person writing them and as robust as the person(s) testing them. Furthermore as these rule sets are often customised and run outside of the compiled or core firewall system they can have a significant performance impact on the firewall. Stateful packet inspection is a necessary and useful firewall technology that is becoming an almost default feature for TCP/IP based firewalls. There are still few firewalls capable of decoding SCADA protocols available, hence stateful packet inspection at this level can be at best problematic or at worst non-existent.

**Intrusion Detection Systems**
There are commercial offerings that have limited support for intrusion detection on SCADA and control based protocols it should be noted that this is steadily increasing. Commercial and open source IDS has the ability to allow for the creation of custom rulesets. One of the supported ones available for SCADA comes from DigitalBond group and is designed mainly for Snort. The rulesets cover both DNP3 and ModBUS and cover buffer overflows, unauthorised commands and variety of other functions that need monitoring. These rulesets although rudimentary in nature provide a sound basis for building an IDS capability that deals with DNP3 and ModBUS protocol traffic in an enterprise network situation. Combined with other Snort utilities and extensions such as Snort Wireless, SnortReport, ACID or Base this type of system could provide valuable sight into the SCADA networks of an enterprise providing valuable feedback to network and security administrators.

One of the conduits for SCADA and control systems control are wireless systems. The use of the for instance the Snort Wireless extensions from http://www.snort-wireless.org provide some protections or at least warning that systems are being attacked. As [14] points out, the effectiveness of these systems in preventing attacks are limited but some protections or at least alerts are better than none. In the often quoted Maroochy Shire Council in Queensland [15] case of sewerage overflow the use of a simple wireless intrusion detection system could have resulted in early detection of the attacks.

One method used by conventional IDS is also to deny routes automatically based on some preset threshold in a ruleset. This may be desirable for TCP/IP networks but is not desirable for SCADA due to failsafes activating any such ability in IDS should be turned off by default.

All IDS allow for the capture of packets in a network stream to a file for later analysis. It is the authors contention that in an enterprise network at key junctures that there should always be a recording packet capture occurring preferably to a hard disk. This allows for the replay of incidents and more importantly the forensic analysis of what actually went wrong. This is particularly relevant in that the network borne exploit may not be a known and this one way of at least capturing it.

**Honeypot systems**
It is well documented in the literature that honeypot systems have proven their worth in being able to trap, contain or waste resources of persons or malcode with malicious intentions. Their purpose varies based on the intent of the deploying entity however, the common tenet is the emulation of a service/function within a network to effectively deceive the attacking entity that they are in fact attacking or probing a real system.

There is an extension for the open source honeyd honeypot to provide emulation of PLC and SCADA technologies. The project files are a series of enhancement and additions to the existing honeyd architecture that enable mimicry of ModBUS and a PLC. The level of emulation is medium with OS fingerprints provided for a range of commonly available PLC devices plus supporting scripts to emulate the ModBUS protocol.

This, like the Snort IDS rulesets, provides the basis for development of a sound, customised enterprise defensive approach. The scripts are customisable and allow an organisation to provide a customised and purpose designed system. The outputs from this type of system could be used to effectively detect inside malfeasance and also attempted penetration of systems from outside. It should be noted that the developers of the honeypot noted that the system would be best deployed near a real system but at the time of production were not aware of active and on-going attacks on SCADA systems [16]. There have been several other honeypot designs made for SCADA with DigitalBond [17] being one of them.

**Protocol Analysis**
One of the key diagnostic tools for any network administrator is the use of a protocol analysis tool that allows analysis of network traffic at the packet level. The open source tool Wireshark formerly known as Ethereal does filtering and decodes on DNP3, ModBUS TCP. This allows for network monitoring to occur even if the current firewalls and other countermeasures are currently insufficient in coverage and scope. The use of filters in Wireshark allows for the realtime monitoring of the enterprise network. For example monitoring could occur for the hex string 02040506090A0F12 which is an unauthorised write request to a PLC which could then generate an alert or log entry. True you could use an IDS for this but the use of Wireshark in this case is as a diagnostic tool. As previously mentioned the use of packet capture at key points in a network is a prudent choice. Wireshark is one such tool that is capable or capturing network streams to disk for later forensic investigation.

# 4 Conclusion

There are problems with commercial systems not fulfilling or even supplying network countermeasures that are at least aware of SCADA or control system protocols. Open source solutions offer some partial remedy to the enterprise deployment of countermeasures and monitoring for SCADA systems.

The use of Wireshark as a defensive mechanism within enterprise networks would currently allow for a highly granular approach to implementation of surveillance into SCADA based networks. This network intelligence in turn could be used to develop or extend IDS rulesets or the

honeypot to provide a robust and tailored solution for the particular enterprise.

Firewalls are the primary and often only defence in a networked environment. They are primary filters of malcode and unauthorised transmission across a network interface. Yet support for stateful packet inspection and other technologies employed in conventional Ethernet based firewalls is still very much an immature technology in this space.

As SCADA network protocols become more open and widely known the potential for exploits will also increase, ubiquity breeds vulnerability. Recent developments with existing penetration and testing tools being enhanced to target SCADA and control system vulnerabilities is of concern.

Governments are starting to recognise the need for research to combat cyber attacks. However the focus of much of this research is looking at ameliorating threat in web services and end user products, there is not as of yet concentrated efforts on SCADA and control systems. This is an area that governments and others should be directing research energies into because if you do not have power, water or telecommunications whether your browser works or not is essentially a moot point.

# 5 References


[1] T. Claburn, "CIA admits cyber attacks blacked out cities, ," in *informationweek*, 2008.

[2] S. Gorman, "Electricity grid in US penetrated by spies," The Wall Street Journal, 2009.

[3] E. Nakashima and R. J. Smith "Electric utilities may be vulnerable to cyber attack," in *Washington Post*, 8th April 2009 ed Washington, 2009.

[4] E. Gosch, "West Australian gas shortage to continue all year," perthnow.com.au, 2008.

[5] C. Valli and P. Wolski, "802.11b Wireless Networks Insecure at Any Speed," in *SAM'04*, Las Vegas, 2004, pp. 154-158.

[6] R. Baird and M. Lynn, "Advanced 802.11b Attack," in *Blackhat Briefings 2002*, Caesars Palace, Las Vegas, Nevada, 2002.

[7] J. Bellardo and S. Savage, "Disassociation and De-auth attack," in *2003 USENIX Security Symposium*, 2003.

[8] R. Hoad and A. Jones, "Electromagnetic (EM) threats to Information Security - Applicability of the EMC directive and Information Security Guidelines," in *3rd European Conference on Information Warfare* University of London, Royal Holloway College, Egham, UK: MCIL, 2004.

[9] M. Osborne, "FATAjack," http://www.loud-fat-bloke.co.uk/, 2003.

[10] Abaddon, "Airjack," http://802.11ninja.net/airjack/, 2003.

[11] K. Poulsen, "Slammer worm crashed Ohio nuke plant network," SecurityFocus, 2003.

[12] NISCC, "NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks," National Infrastructure Security Co-ordination Centre, British Columbia Institute of Technology 2005.

[13] A. Woodward and C. Valli, "Issues common to Australian critical infrastructure providers SCADA networks discovered through computer and network vulnerability analysis," in *6th Australian Digital Forensics Conference*, C. Valli and A. Woodward, Eds. Edith Cowan University, Mount Lawley, Western Australia: SECAU - Security Research Centre, 2008, pp. 206-210.

[14] C. Valli, "Wireless Snort – A WIDS in progress," in *2nd Australian Computer Network & Information Forensics Conference*, Esplanade Hotel, Fremantle, Western Australia, 2004, pp. 112-116.

[15] T. Smith, "Hacker jailed for revenge sewage attacks.," 31st October ed: The Register, 2001.

[16] V. Pothamsetty and M. Franz, "Virtual SCADA Honeynet," in *KEMA CyberSecurity Confererence*, 2003.

[17] Anonymous, "Digital Bond - SCADA Honeynet." vol. 2009: Digital Bond, 2009.