2005

Integrating Open Source Protections into SCADA Networks

Craig Valli
Edith Cowan University

Integrating Open Source Protections into SCADA Networks

Craig Valli
School of Computer and Information Science
Edith Cowan University
Email: c.valli@ecu.edu.au

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. There are a range of open source tools that now offer functionality that can be used to secure SCADA networks from intrusion or compromise. This paper explores some of the issues with current SCADA deployment trends from a network security perspective and then examines open source countermeasures that could be used to help mitigate some of these risks.

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

INTRODUCTION
SCADA Systems are increasingly mentioned as weak points in critical infrastructure in various Government reports. The reports from various agencies see SCADA systems as highly vulnerable to attack or compromise that would result in catastrophic failure of national critical infrastructure. Many of these systems are used to run 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. Compromise or even disruption to these systems could have catastrophic consequences resulting in massive economic impact or loss of life.

Many of the older proprietary systems are now being upgraded to open platform systems that utilise open protocols such as Distributed Network Protocol 3 (DNP3). Many of the newer SCADA systems also use modern open standard communications networks to provide access to the SCADA systems that then talk to the underlying control systems. These networks even if totally private will almost atypically run the TCP/IP range of protocols and supporting services. Consequently, some of this traffic may actually travel on or rely upon open networks such as the Internet to provide these conduits. Of greater risk is that some of these systems utilise wireless systems for system control conduits.

This paper will examine the threats to SCADA systems as result of the decreasing use of proprietary protocols and related equipment and their move to open protocol based systems. The paper will also outline available open source countermeasures to some of these threats. The paper will not deal with the Programmable Logic Controllers (PLC) found withing SCADA systems but the egress of packets to and from these devices.

OPEN IS NOT ALWAYS SECURE
SCADA is one set of systems where it could be argued the use of open source or protocols significantly impacts the security of the systems. SCADA systems are moving to the DNP3 protocol away from other control protocols, these are delivered wrapped in a TCP/IP transport or actual raw DNP3 packets across the chosen media. The logic behind having a "common" protocol across these systems is so that each platform or vendor device can interact at a network or system level. This logic seems complete enough and one that makes economic sense i.e. economies of scale, one protocol, one lot of training etc. From a security perspective this is not true as a mono-culture tends not to be resilient as others i.e break one, break all.

So one has to ask what is the security benefit in moving away from proprietary protocols running on closed systems to open protocols running across open networks? Common protocols have been proven to be problematic already in network defence particularly if the flaw is inherent. If we take WiFi or

802.11 equipment as a recent example, if it meets the standard for 802.11b it is regardless of manufacturer susceptible to a wide range of protocol based attacks (Baird & Lynn, 2003; Bellardo & Savage, 2003). These protocol based attacks are effective and essentially unstoppable without further countermeasures or extension of the 802.11b protocol. What could occur if DNP3 or ModBUS or a similar SCADA specific protocol was found to have the same level of exploit?

Even closed or supposedly private networks that use wireless infrastructure are increasingly exposed as open to attack (Valli & Wolski, 2004). Take the fact that many modern SCADA systems have http enabled management consoles that are accessed via a web browser and use either direct wired or wireless connectivity to achieve connection and you will have significant security problems already associated with this mode of network transport. 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 enables the transmissions to be susceptible to denial of service at a physical layer with wireless jamming devices (Hoad and Jones, 2004). These physical attacks are in addition to known exploits against particular wireless protocols which are numerous (Baird & Lynn, 2003; Bellardo & Savage, 2003; Osborne, 2003;). Even if the wireless communications use encryption or VPN to protect the transmission there are numerous tools that can break, intercept or even inject into these types of network countermeasures (Airjack, 2004).

Even though SCADA has been flagged as a problem for at least 5 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 (NISCC, 2005). This hinders the development of enterprise initiatives as alternative products or 3rd party plugins must be adopted often with varying levels of integration success into a network infrastructure.

OPEN SOURCE COUNTERMEASURES

The typical countermeasures that are utilised for securing Ethernet/TCP/IP based networks apply to SCADA networks in theoretically the same way. These tools would include typically include a firewall, intrusion detection systems and some method of protocol analysis. This section of the paper examines briefly open source offerings that are currently available for SCADA systems that provide these features.

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 protocols in commercial software is scant at best (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:

1. Function code – filtering is based on single or multiple function codes
2. UnitID – filter on specified ID
3. Reference Number – filtering on a specified reference number
4. 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.

As this type of firewalling is a kernel level activity the amount of logging that can be afforded these particular filtering functions is extensive. This allows for a rich picture of network activity and any associated problems to be developed using appropriate analysis tools.

Intrusion Detection Systems

There are commercial offerings that have limited support for intrusion detection on SCADA based protocols but this is steadily increasing and should be a major part of any defensive strategy.

The open source Snort IDS has the ability to allow for the creation of custom rulesets and one of the supported sets available for SCADA comes from DigitalBond. The rulesets cover both DNP3 and

ModBUS and cover buffer overflows, unauthorised commands and variety of other functions that need monitoring or trapping. The rulesets also have a network capture file that can be played back to verify the functioning of the rulesets before deployment of SCADA aware IDS. 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 sight into the SCADA networks of an enterprise providing valuable feedback to network and security administrators.

One of the principal conduits for SCADA systems are wireless systems. The use of the Snort Wireless extensions from http://www.snort-wireless.org provide some protections or at least warning that systems are being attacked. As Valli(2004) 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 Water Services case the use of a wireless intrusion detection system could have resulted in early detection of the attacks.

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 were not aware of active and on-going attacks on SCADA systems (Pothamsetty & Franz, 2004)

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 Ethereal does filtering and decodes on DNP3, ModBUS TCP (Ethereal, 2005). 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 Ethereal allows for the 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 for subsequent actioning.

CONCLUSION

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

The use of Ethereal 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 Snort rulesets or the honeypot to provide a robust and tailored solution for the particular enterprise.

The lack of a suitable firewalling is an issue that needs urgent research and development in SCADA networks. 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. The ModBUS firewall implementation provides some basic protections for these types of network however, DNP3 and other networks are afforded minimal protections.

As SCADA network protocols become more open and widely know the potential for exploits will also increase. Urgent research is needed now to combat cyber attacks that for the first time could have deadly and permanent consequences.

REFERENCES

Baird, R. and Lynn, M. (2002) *Advanced 802.11b Attack*, In Blackhat Briefings 2002, Caesars Palace, LasVegas, Nevada.

Bellardo, J. and Savage, S. (2003) *Disassociation and De-auth attack*, In 2003 USENIX Security Symposium USENIX

Ethereal (2005) Ethereal: Display Filter Reference, http://www.ethereal.com/docs/dfref/

Gracia, S. (2004) Snort Wireless Patches, http://www.snort-wireless.org

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

NISCC, (2005) *NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks*, National Infrastructure Security Co-ordination Centre, British Columbia Institute of Technology

Osborne, M. (2003) FATAjack, http://www.loud-fat-bloke.co.uk/.

Pothamsetty, V. & Franz, M (2004) *SCADA HoneyNet Project: Building Honeypots for Industrial Networks*, http://scadahoneynet.sourceforge.net/

Stock, S. and Beames, K. (2002) FakeAP, Black Alchemy Enterprises.

Valli, C. and Wolski, P. (2004) *802.11b Wireless Networks Insecure at Any Speed*, In SAM'04(Eds, Arabnia, H. R., Aissi, S. and Mun, Y.) CSREA Press, Las Vegas, pp. 154-158.

Valli, C. (2004) *Wireless Snort – WIDS in progress*, 2nd Australian Computer, Network and Information Forensics Conference, Fremantle, Western Australia

COPYRIGHT