The Development of a Generic Framework for the Forensic Analysis of SCADA and Process Control Systems

Jill Slay and Elena Sitnikova

Defence and Systems Institute, University of South Australia
Mawson Lakes SA 5095 Australia
Jill.slay@unisa.edu.au

Abstract. There is continuing interest in researching generic security architectures and strategies for managing SCADA and process control systems. Documentation from various countries on IT security does now begin to recommendations for security controls for (federal) information systems which include connected process control systems. Little or no work exists in the public domain which takes a big picture approach to the issue of developing a generic or generalisable approach to SCADA and process control system forensics. The discussion raised in this paper is that before one can develop solutions to the problem of SCADA forensics, a good understanding of the forensic computing process, and the range of technical and procedural issues subsumed with in this process, need to be understood, and also agreed, by governments, industry and academia.

Keywords: SCADA, process control systems, security, forensics.

1 Introduction

A Supervisory Control and Data Acquisition (SCADA) system is used for gathering real time data, monitoring and controlling process equipment from automated systems in geographically distributed locations. They can be used to automate processes such as:

- Electricity power generation, transmission and distribution,
- Oil and gas refining and pipeline management,
- Water treatment and distribution,
- Chemical production and processing,
- Railroads and mass transit.

There is continuing and ongoing interest in researching generic security architectures and strategies for managing SCADA and process control systems. A major aspect of this type of approach [1] is the use of proprietary forensic computing tools [2] or specially developed network forensic architectures [1] to analyse network traffic at the packet level so as to be able to collect evidence after a potential event. Other researchers work at the junction of security and forensics examining intrusion detection and event logging in SCADA networks running specific protocols with the aim of providing

M. Sorell (Ed.): e-Forensics 2009, LNICST 8, pp. 77 – 82, 2009.

solutions that may reduce the risk of a catastrophic event should a system be breached and also providing electronic evidence that might eventually allow the perpetrator to be taken to court.

Documentation from various countries on IT security does now begin to recommendations for security controls for (federal) information systems which include connected process control systems. Thus we do recognise the maturity (even in our own work [3], [4]) of the development of general and generalisable security architectures and frameworks which then provide a foundation for the development of technical solutions and administrative processes around which sound SCADA and process control systems security can be built and assured. However, little or no work exists in the public domain that takes a big picture approach to the issue of developing a generic or generalisable approach to SCADA and process control system forensics.

The assertion in this paper is that before one can develop solutions to the problem of SCADA forensics, a good understanding of the forensic computing process, and the range of technical and procedural issues subsumed within this process, need to be understood, and also agreed, by governments, industry and academia. This paper then examines systematically:

- What is forensic computing?
- What evidence should be collected from SCADA and process control systems and where might this evidence be located?
- How can an enterprise be prepared for a possible forensic investigation?

2 What Is Forensic Computing in a Control System Context?

This question has been asked many times in academic literature but still needs to be considered in a SCADA and process control system context. We have asserted previously [5] that forensic computing (electronic evidence collection, digital evidence collection) has developed out of a demand for service from the law enforcement community and has typically developed in an ad hoc manner rather than a scientific one. It has since developed into a discipline that crosses the corporate, academic, legal, and scientific as well as the law enforcement domains and it is developing both as a discipline and as a forensic science.

If we take a holistic perspective we see that forensic (meaning 'for the court') computing is about collecting evidence that can be presented to a court after a crime has taken place. This means that we only need to be able to collect enough of the right kind of evidence to provide conclusive proof that a crime has been committed. In our definition, there is a distinct difference between the process of forensic computing investigation and that of incident recovery and response. Incident response and recovery is an essential feature of the security of SCADA and process control systems, and it would be hard to find a SCADA or control system that was part of the national critical infrastructure which did not have established procedures for response and recovery. These systems, as opposed to commercial or corporate information systems, are built with [6] redundancy and minimum mean time to repair with a primary focus on availability since they control the major national utilities, or major industries such as oil, mining, commodity production and transport.

Although there is no single accepted standard, there is a basic computer forensic methodology including rules and procedures forensic computing investigators should follow. McKemmish [7] has four rules for forensic computing investigations: *"minimal handling of the original, account for any changes, comply with the rules of evidence and do not exceed your knowledge"*. He also identifies and details the four stages of a forensic investigation: *"identification of digital evidence, preservation of digital evidence, analysis of digital evidence and presentation of digital evidence"*.

Chain of custody is another aspect that is integral to a computer forensic investigation. Chain of custody is the process of tracking evidence to ensure it is of the highest integrity when presented in court. Without a properly executed chain of custody, a defence lawyer could argue that the evidence may have been tampered with or not looked after properly. The chain of custody needs to record all persons who handled or had access to the evidence and what actions were performed on the evidence.

Forensic computing, if seen as a specialty within computer science, is different from other branches of computing as the output must be derived from a process that is legally acceptable [7]. Forensic computing is still a developing branch of IT, however, there are many practices and methods that have been developed and have been accepted by experts in the field. These methods are also accepted in a court of law because they have been shown to be reliable and produce accurate results. Using unknown or untested third party software for forensic analysis is not generally acceptable and could mean the conclusions drawn from analysis are regarded with low integrity or not admissible at all [7].

3 SCADA and Control Systems

The implementation of Control Systems up to 20 years ago gave no thought to the defence or security issues that could be faced in the operation of these systems. Aging systems with little processing power and network strength, bedded on adapted windows operating systems, have been connected to the internet for efficiency and cost effectiveness. These systems now face threats from an un-trusted network connection as well as the human errors in the control of these systems.

Systems consist of numerous technologies ranging from legacy to state of the art systems with the processing power to match. In his paper on Control Forensics, Fabro [8] makes a distinction between three possible system architectures. They are:

- Modern / Common Technologies – which have modern computing capabilities and are still sponsored by the vendor;
- Modern / Proprietary Technologies – which have been created in the last ten years and are fully supported and understood by the vendors and owners;
- Legacy / Proprietary Technologies – systems have been deployed further than ten years ago and have moderate capabilities.

Legacy systems are commonly PLC based systems with computers used to control the output and display to the HMI.

Modern systems have often been modified to suit operational requirements in other organisations. Modern control systems have more than enough processing power to monitor and process information as well as controlling the systems that they are

designed for. The problem still remains that remote locations rely on sending information back to the control site. The networks that carry this information have increased in bandwidth, so the conjecture of slowing the network due to the transfer of more information is not warranted. However, an attack that controls the information that is transmitted across that medium could go unnoticed until it is detected further down the line by its effects.

4 Evidence from SCADA and Control Systems

Internationally, we discover the usage of legacy SCADA systems which were built on proprietary protocols and operating systems. These have over the years been interconnected using Ethernet- based protocols, and with the addition of COTS software too. More recently, remote control via various forms of communication link has allowed efficient monitoring of field devices over the public internet.

This means that we have complex SCADA systems and control Ethernet LANS, inter connected with utility corporate networks, regulator networks, vendor networks and often with essential employee mobile device and home computer network access. Thus we find that, while SCADA is often presented as a simple network of remote devices working on simple protocols in real-time, there is an intricate web of IP and Ethernet networks surrounding these devices.

In some regard, this understanding of the complexity surrounding SCADA systems is of help in establishing what evidence we might collect and how. We can leverage much of the more general research in forensic computing and electronic evidence collection, to gain an understanding of the type of electronic evidence we might be looking for in a SCADA or process control system. If we assume that there has been an attack on a SCADA or process system and we have to plan how to investigate, then we start with the knowledge that some device would have been used to access the system. This access might have been via a small mobile device, access through a wireless link, access through a Denial of Service attack on a wired network, an attack on a PC running an insecure application or an attack on a web cam monitoring a remote device on the SCADA network. So we would assert that SCADA and process control system forensics cannot exist in a vacuum but the application of digital forensic approaches to SCADA and Control Systems however is new and quite complex in its approach.

5 Forensic Challenges

Traditional forensic challenges consist of the retrieval of data from volatile memory and network devices as well as storage devices. It often relies on incident response after the event, observing the recorded data from the attack because of inadequate logging and inappropriate administrational processes. Control systems further hinders the collection and analysis of information due to the nature and environment of these systems.

Traditional retrieval consists of the removal of the device and imaging of the data source. This can not be done in a control environment due to the real time environment and the inability to shut down specific zones.

The intermingling of data due to control systems producing huge amounts of information that is used in the control of the system in the form of set points and monitoring alarms and sensors. This information is stored on control servers that could also be trusted to store any forensic information. The process of filtering any relevant information from these huge amounts of data is both time consuming and limiting.

The volatility of the data due to the fact that enormous amounts of data are being logged for the operation of the system, data is often overwritten on some devices, commonly remote terminal units and field devices.

Legacy systems have very little computational power available for the analysis or recording and sorting of data that is produced in conjunction with control data. Any network connections are for the monitoring of production and set points. The systems are backed up frequently, with all information stored on servers that contain information that dates back to the start of operation. This information is recorded for the operation of the systems and provides evidence of previous and current set points. Accessing back up tapes for information would not hinder the operation of the systems, and would provide a life time of operation records, but mingled control and forensic data would have to be filtered to get valuable information.

Law enforcement investigators who might be called upon in the case of a breach of a SCADA system have a very good understanding of the computer and network data which needs to be provided to them by an organisation in the case of forensic investigation. However, they are often hampered in this work because Australian enterprises are not aware that they should collect computer and network data, log files and records in a systematic manner. This means that when a system breach occurs, or computer crime is suspected, the potential evidence is not available for law enforcement investigators to analyse, and in some cases has never been collected. Currently the IT management, and particularly the security management, of Australian organisations is largely governed by a series of national and international standards which are based on process models created before the widespread growth of computer crime. These lack any real and explicit focus on Forensic Readiness or the potential need to work in such a way that systems are designed and built to collect evidence.

6 Conclusion

Just as there is a need to develop generic security models for SCADA and process control systems, so there is a parallel need for a generic forensic framework for the same kind of systems. This framework needs to provide for the development of Forensic Readiness in an organisation, particularly one that is part of the national critical infrastructure. It also needs to provide an environment where well-established Forensic Computing functions can be carried out by law enforcement.

References

1. Chandia, R., Gonzalez, J., Kilpatrick, T., Papa, M., Shenoi, S.: IFIP International Federation for Information Processing. In: Goetz, E., Shenoi, S. (eds.) Critical Infrastructure Protection, vol. 253, pp. 117–131. Springer, Boston (2008)

2. Cassidy, R.F., Chavez, A., Trent, J., Urrea, J.: IFIP International Federation for Information Processing. In: Goetz, E., Shenoi, S. (eds.) Critical Infrastructure Protection, vol. 253, pp. 223–235. Springer, Boston (2008)
3. Slay, J., Miller, M.: A Security Architecture for SCADA Networks. In: Proceedings of the17th Australasian Conference on Information Systems, Adelaide, December 5-6 (2006)
4. Slay, J., Miller, M.: The Maroochy Water SCADA Breach: Implications of Lessons Learned for Research. In: Advances in Critical Infrastructure Protection, pp. 73–82. Springer, Boston (2008)
5. Beckett, J.J., Slay, J.: Digital Forensics: Validation and Verification in a Dynamic Work Environment. In: HICSS-40, Hawaii, January 3 (2007)
6. Miller, A.: Trends in Process Control Systems Security. In: IEEE Security and Privacy, pp. 57–60 (September/October 2005)
7. McKemmish, R.: What is Forensic Computing, Australian Institute of Criminology (1999)
8. Corporate & Technology Group of Freehills 2001, Cybercrime Act 2001 (Cth), FindLaw.com, viewed 27/03 (2006), http://www.findlaw.com.au/article/1408.htm
9. Fabro, M.: Recommended Practice: Creating Cyber Forensics Plans for Control Systems, Department of Homeland Security (2008)