DOI: http://dx.doi.org/10.14236/ewic/ICS2015.5

A Forensic Taxonomy of SCADA Systems and Approach to Incident Response

Peter Eden
Information Security Research group
School of Computing and Mathematics
Department of Computing, Engineering and Science
University of South Wales
Pontypridd, CF371DL UK
peter.eden@southwales.ac.uk

Andrew Blyth
Information Security Research group
School of Computing and Mathematics
Department of Computing, Engineering and Science
University of South Wales
Pontypridd, CF371DL UK
andrew.blyth@southwales.ac.uk

Pete Burnap,
Yulia Cherdantseva
Computer Science and Informatics
Cardiff University, Queen's Buildings
5 The Parade, Roath
Cardiff CF24 3AA, UK
p.burnap@cs.cardiff.ac.uk, y.v.Cherdantseva@cs.cardiff.ac.uk

Kevin Jones,
Hugh Soulsby
Airbus Group Innovations
Quadrant House Celtic Springs
Coedkernew
Newport NP10 8FZ, UK
kevin.jones@eads.com, hugh.soulsby@eads.com

Kristan Stoddart
Department of International Politics
Aberystwyth University
Penglais, Aberystwyth
Ceredigion
SY23 3FE, UK
kds@aber.ac.uk

SCADA systems that monitor and control Critical National Infrastructure (CNI) are increasingly becoming the target of advanced cyber-attacks since their convergence with TCP/IP and other networks for efficient controlling. When a SCADA incident occurs the consequences can be catastrophic having an impact on the environment, economy and human life and therefore it is essential for a forensic investigation to take place. SCADA system forensics is an essential process within the cyber-security lifecycle that not only helps to identify the cause of an incident and those responsible but to help develop and design more secure systems of the future. This paper provides an overall forensic taxonomy of the SCADA system incident response model. It discusses the development of forensic readiness within SCADA system investigations, including the challenges faced by the SCADA forensic investigator and suggests ways in which the process may be improved.

Keywords: SCADA forensics, digital forensics, incident response, SCADA architecture, ICS forensics, critical infrastructure

1. INTRODUCTION

SCADA (Supervisory Control and Data Acquisition) systems are responsible for the monitoring, automation and control of many of the world's critical national infrastructure. They are common amongst distribution systems and industrial control systems found in oil refineries, power grids, nuclear plants and water distribution, as well as transportation in areas such as rail, airlines and traffic lights. Many of these SCADA systems were designed and implemented decades ago, on closed networks, with a focus on making data available but not necessarily secure or confidential. Today, these SCADA systems are interconnected with corporate networks and the Internet, communicating over TCP/IP, wireless IP and Bluetooth, to allow for a more efficient monitoring and control process. Given the role that these SCADA systems play within critical infrastructure it is essential for them to operate continuously, without interruption, 24-7. As a result many of these systems are yet to evolve with the modern environment in

© *Eden et al. Published by BCS Learning & Development Ltd.*

which they operate making them vulnerable to external attacks.

Although recorded attacks on SCADA systems date back as far as 1982, where a Trojan Horse was responsible for the Trans-Siberian gas pipeline explosion, over recent years we have seen a dramatic increase in the number of dedicated attacks on SCADA systems. Stuxnet, described by some as the world's first cyber-weapon, was an eye-opener to all but there have been many since. Duqu, Flame, Gauss and Wiper are just a few examples of sophisticated attacks designed to sabotage the operation of specific SCADA systems (Miller and Rowe 2012). In recent years there has been a focussed effort to improve the awareness and development of cyber-security within ICS and SCADA systems with projects such as CockpitCI (Cruz et al. 2014) and VIKING (Björkman 2010), as well as developments in ICS security standards and recommendations such as ISA-99 and IEC 62443.

Whenever there is a cyber-attack or an incident occurs on critical infrastructure or industrial control systems it is essential that a forensic response takes place. However, traditional computer forensic methodologies cannot simply be applied to SCADA systems as their attributions are very different. Therefore, there is a requirement to develop a SCADA forensic incident response plan in order to provide remediation when events do occur.

2. CONCEPTUAL ARCHITECTURE OF A SCADA SYSTEM

SCADA system architecture consists of various hardware components that will effectively become data sources in a forensic investigation. These components communicate across various zones using an array of SCADA protocols.

2.1. Components

Components can be categorised into two main sections within a SCADA system; Field Sites; and Control Centre (Ahmed et al. 2012). There can be many field sites spanning huge geographical areas, which act as the nerve endings in a SCADA system. The components found here are PLCs, RTU and IEDs, and are attached to physical processes and field instruments such as motors, switches, thermostats etc. The Control Centre collects information about the state of its field devices and physical processes. PLCs and RTUs will continually transfer data regarding their status to a central control centre. Its main components consist of an HMI (Human Machine Interface), Historian, MTU (Master Terminal Unit).

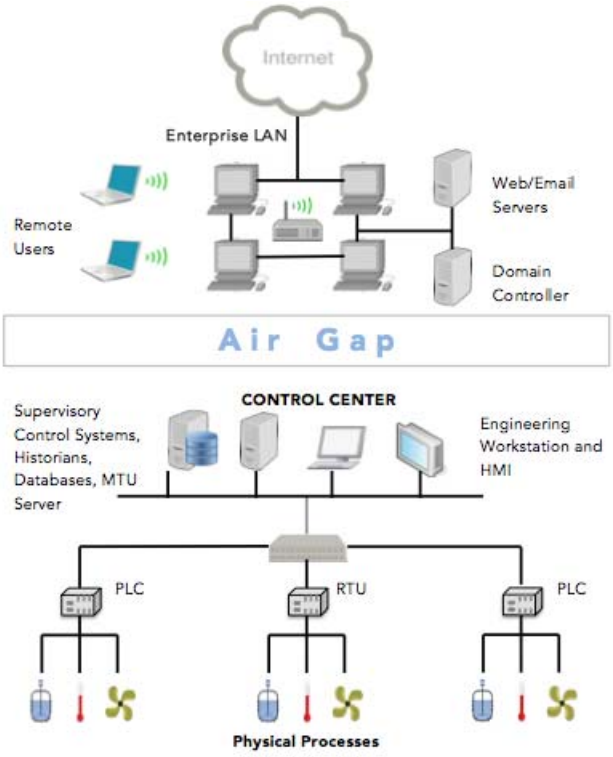

Figure 1: *Conceptual SCADA architecture*

2.1.1. PLC (Programmable Logic Controller):
PLCs are computerised devices connected to sensors and are used to control automated processes.

2.1.2. RTU (Remote Terminal Unit)
An RTU is very similar to a PLC and performs virtually the same function. Generally speaking, RTUs have faster CPUs and a much larger support for communication. They also tend to be a bit more rugged and reliable in tough environments (Boyer 2009).

2.1.3. IED (Intelligent Electronic Device):
IEDs allow for monitoring and control functionality as well as electrical protection and perform upper level communication completely independently without having to rely on any other devices.

2.1.4. HMI (Human Machine Interface)
In order to interpret and visualise data that is transferred to the control centre SCADA systems use an HMI. The HMI not only provides a way to visually present the data that is processed but also allows for human interaction with the system as a way of controlling its overall state. Depending on what the SCADA system is controlling will ultimately depict the size and design of the HMI interface. This can range from a large-sized, computerised control panel at a nuclear plant to a small computer or even an application on a mobile phone.

2.1.5. Historian:
The Historian is the Database Management System that stores and archives data that is sent to the control centre and provides audit logs for all activity across a SCADA network (Dylan McNamee 2009).

2.1.6. MTU (Master Terminal Unit):
The Master Terminal Unit, sometimes referred to as the SCADA server, is responsible for receiving and processing all the data transmitted to the control centre from the field devices as well as providing communication with those devices. It may pre-process data before sending it to the Historian and also provides a graphical representation of the information stored in it to be transferred and displayed on the HMI(Stouffer and Kent 2008).

2.2. Network and Communication

Modern SCADA systems have evolved considerably, since their original flat network architecture, due to their interconnectivity with other networks (corporate, Internet etc.) and as a result the network structure can be separated into four zones, defined by the information that is communicated, their access, and their locations:

1. External Zone - Internet DMZ allowing for connectivity from remote users.
2. Corporate Zone - Enterprise LAN used for corporate communication and consisting of enterprise/web/email/DNS servers
3. Data Zone - Consists of operational traffic, such as monitoring and control over DMZ and contains data acquisition servers and historians as well as management devices.
4. Control Zone - HMIs on a supervisory LAN communicating via a switch to multiple PLCs/RTUs/IEDs

To increase security within the network, SCADA systems perform their most critical communications within the lowest zones(Keith Stouffer 2011). Because connectivity within a SCADA network has multiple layers the forensic acquisition of the necessary data can often be difficult to trace(Wu et al. 2013).

2.3. Protocol Utilization

Although there is a wide range of protocols, both proprietary and non-proprietary, that could be used within a SCADA system, there are a select few that are becoming standard or more common than others. These are MODBUS, DNP3 and PROFIBUS. Others include RP-570, Conitel,IEC 60870, PROFINET IO and many more.

2.3.1. Protocol Vulnerabilities
The collection of protocols being used today within modern SCADA environments was originally intended to run on isolated networks but as a result of the developments in technology over the years these protocols are now being transported across TCP/IP making SCADA systems more vulnerable to outside attacks. It is clear there is a distinct lack of security-integrated mechanisms within ICS protocols. Implementing security features into protocols can add latency between communications and could disturb operations and critical processes. However, simply securing SCADA networks at the perimeter using firewalls, IDS, IPS is not enough. SCADA protocol manipulation and lack of security mechanisms can result in;

- packet modification
- packet replay
- packet deletion
- latency
- eavesdropping
- spoofing

3. A FORENSIC TAXONOMY OF SCADA SYSTEM INCIDENT RESPONSE

3.1. Traditional Forensic Triage and SCADA

A forensic investigation of a traditional IT system will involve the gathering of forensic artefacts from both volatile and non-volatile data sources within that network or environment. Although the same can be said for the SCADA forensic process there are many attributes that deny the use of traditional forensic tools and techniques being applied to SCADA systems.

One of the reasons for this involves proprietary and legacy equipment. The rate of change for a traditional IT system might be, for example, 3-5 years. During this period software, hardware and communication networks are likely to have been replaced and updated in relation to business needs and new technology. In a SCADA system the rate of change is a lot slower. Systems that were designed and implemented decades ago have been left to run continuously untouched and unpatched. The reasons behind their immaturity being that interfering with the running system could cause latency and critical processes to fail. As a result many SCADA systems contain legacy components that are no longer supported and that are communicating via proprietary protocols instead of more widely used open standard protocols that have been adopted

over more recent years (McCarthy and Mahoney 2013). Therefore, conventional methods and forensic tools used to acquire data from traditional IT systems may not be compatible with many SCADA environments and if compatibility was not the issue then latency and interference introduced by running the tool could be. The requirement for continuous operation, zero-tolerance on latency and interference, together with varying legacy components and technology is enough to separate SCADA from 'normal' IT systems and warrant a requirement of dedicated SCADA forensic tools and methodologies.

3.1.1. Challenges for the SCADA Forensic Investigator

There are certain challenges, including those currently documented by Ahmed (Ahmed et al. 2012) and Fabro, (Mark Fabro 2008) facing the SCADA forensic investigator. These include:

- Live Forensics - The majority of SCADA systems cannot simply be switched off and analysed due to their role in critical processes. Therefore a live forensic analysis is needed while the system and devices are running. An order of volatility must be followed in order to minimise the changes to data in memory and also to reduce interference that may cause latency to operations(Mark Fabro 2008).
- Rapid Response - Forensic evidence will be at its peak the time an incident occurs. As time passes potential evidence may be overwritten by new processes so it is vital to respond promptly (Taveras 2013). This may be difficult when one SCADA system covers thousands of square miles with hundreds of field sites locations.
- Integrity and Validity - Digital evidence is normally verified by matching the hash value (calculated by applying a hashing algorithm to the data) of the original evidence against its acquired copy. The challenge of data validity within SCADA systems exists because as the system remains live and data is continuously being updated the state of the data can change from the start of the copying process to the completion of a calculated hash, resulting in the hash being unusable.
- Incident relevant logs and effective storage - Effective logging can assist significantly in a forensic investigation and help piece together a timeline of events. According to Fabro, it is not uncommon for systems with logging and audit functionality to be deployed with these functions disabled or have such small storage capacities that relevant logs do not last long before being overwritten (Mark Fabro 2008). It is vital that when logging features are absent or insufficient in a system that network traffic be logged to help understand device communication at the time of an incident.
- Lack of SCADA Forensic Tools - Research shows a clear absence of data acquisition tools and methodologies designed specifically to incorporate SCADA system, including their protocols and proprietary log formats(Ahmed et al. 2012). This may be, partly, due to the transparency of the effect such tools can have on live SCADA services as well as many other issues that may have prevented the production of such tools already.

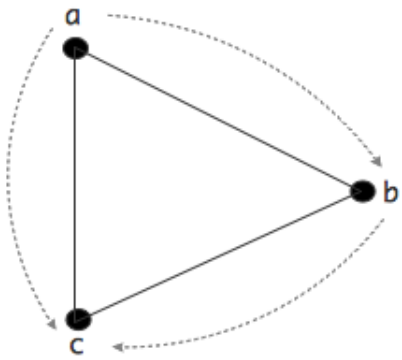

Figure 2: *SCADA artefact existence levels*

3.2. Forensic Readiness

3.2.1. A SCADA Forensic Artefact

A forensic artefact to an investigator is anything that helps piece together the cause of the problem and to identify the current state of the system at which the problem occurred. A forensic artefact could exist in many different formats and on a variety of data sources within the SCADA environment. We can describe a SCADA forensic artefact as a piece of information, where that information can exist conceptually at 3 levels:

1. Enterprise level - The information has business content and is designed for a particular goal i.e. logging protocols, routing table, sending a command etc.
2. Information level- The information has a structure, a specific length that can be used to help calculate an artefact's half-life.
3. Physical level - The information will exist on one or more specific physical components.

The key for the forensic investigator is to be able to narrow down the type of artefact needed based

on the type of incident that has occurred, and then acquire that artefact. Figure 2 describes the levels at which a SCADA forensic artefact can exist, where a = enterprise level, b = information level and c = physical level, and the route the investigator may take to retrieve it.

When a particular artefact is identified at an enterprise level (a) it will have a logical structure (b) and exist on one or more physical assets (c). If the logical structure is unknown the investigator may go straight to the physical assets and retrieve everything (a-c), however, if the investigator is able to understand the logical structure of the artefact it will define exactly what information is needed and from which particular assets (a-b-c).

3.2.2. Half-life of a SCADA forensic artefact

Assuming that the investigator knows the type of artefact he/she wants and the physical asset it is located upon, they will also need to know how long that artefact will last before it is overwritten and replaced by a newer process on that device. Given the complex nature, sheer scale of possible data sources, and various interconnected networks within a typical SCADA system, calculating the half-life of data for an entire system would be impossible as it would change dramatically from one system to another and be dependant upon the type of incident that has occurred and the devices running. For example, data would last longer in a historian than it would in an engineers workstation, which in turn would last significantly longer than data stored in a PLC. Therefore, The half-life of data should be identified at a lower level, for each specific component within that particular SCADA system. It can be achieved by understanding the SCADA artefacts at the information level together with the physical asset it is stored upon. This will help to influence a prioritisation list of data sources in which to examine.

3.2.3. Asset Classification

The classification of an entire SCADA system would be hard to achieve as different sections of the environment would have varying criticality levels. We can, however, look to classify specific components within a SCADA system, as described in Table 1. This will inform the investigator exactly which areas/devices can be interrogated, those that can be switched offline and those that must be investigated live. It also identifies the components that simply cannot be disturbed. The classification of assets will assist the investigator in reacting appropriately and carrying out a safe and accurate forensic response.

Device Classification	Description
Safety-Critical (Process)	Failure of the component can result in loss of life, injury or damage to the environment
Safety-Critical (Timed)	Failure of the component can result in loss of life, injury or damage to the environment after a specific length of time
Safety-Critical (Location)	Access to the component for interrogation or repair can result in injury or loss of life.
Mission-Critical	Failure of the component can result in failure of some global directed activity
Business-Critical	Failure of the component can result in high economic losses

Table 1: *Classification of SCADA System Assets*

3.2.4. Asset Prioritisation

The asset classification list together with the half-life of information on specific devices will ultimately provide the investigator with a priority list that will help to maximise the amount of potential evidence that can be recovered. Suggestions for calculating a priority list have already been described by (van der Knijff 2014). Knijff's approach applies a formula using certain factors to calculate an asset's priority, such as evidential value, the volatility of that evidence, and asset accessibility. Combining Knijff's approach with pre-calculated asset half-lives will provide a more accurate response plan and increase the potential recovery of SCADA forensic artefacts.

3.3. Implementation of SCADA Forensic Hardware

Due to the classification of certain live devices physical access to certain assets may be restricted, meaning the investigator is unable to interrogate them. It may also be that a specific device of interest is located thousands of miles away but the device's half-life of information compared to the response time would mean the forensic artefacts would be overwritten by the time it was reached.

To overcome each of these scenarios, a forensic hardware wrapper could be implemented on each desired device in order to improve the availability and recovery of information, much like an aircraft's black box is used in a disaster investigation. A typical SCADA system could potentially contain thousands of PLCs and deployment of such a device could result in the cost outweighing the benefit. However, these devices could be deployed

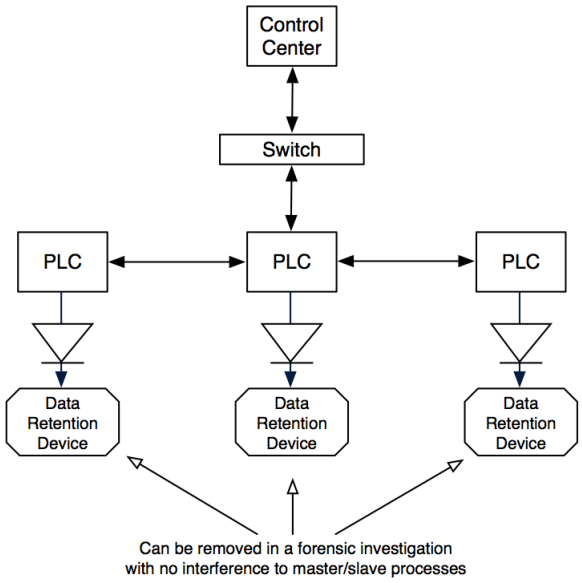

Figure 3: *Implementation of forensic hardware wrappers for incident response*

on specific field devices of interest, such as those controlling particular safety-critical processes or those with significantly shorter half-lives.

The wrapper could act as an inline hardware-based data-recording device and could be, for example, attached to a PLC to collect and store PLC data, such as memory status, modifications and issued commands. The device could be developed from an SBC (single-board computer), such as a Raspberry-Pi, and could be configured with a much larger storage area of that in the PLC to increase half-life length.

As some field devices are quite robust to withstand the terrain in which they operate the same would have to be said for the wrapper. Therefore an SSD or SD card would be optimal over a hard-disk drive as there are no moving parts. For example, a 128GB SSD could be used, implementing a data-diode to ensure the unidirectional flow of data and to eradicate the risk of interference or traffic from the hardware back to the PLC. Using an SD card would result in a more cost-effective approach to implement over SSD but would require more attention to overcoming file-system consistency issues across different platforms.

When an incident has occurred the additional hardware device could then be detached or SD card simply removed for data extraction and forensic analysis without the need to interact in any way with the PLC. To reduce the risk of interference with the wrapper or a network tap being placed between the field device and wrapper the additional hardware

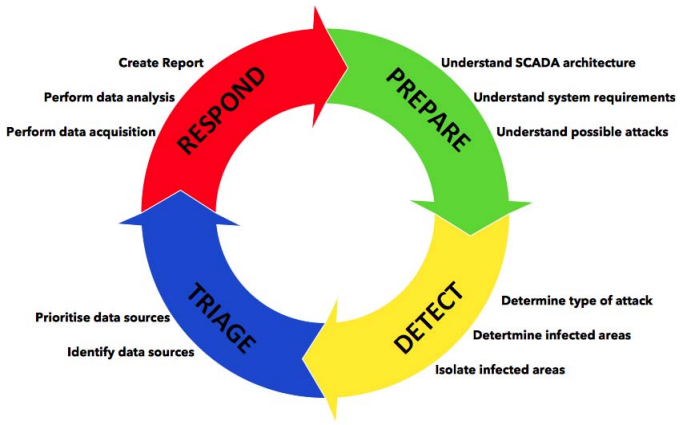

Figure 4: *SCADA Forensic Incident Response Model*

should be placed as close to the field device as possible.

A similar concept, the SSU (Shadow Security Unit), has recently been put forth by T. Cruz(Cruz et al. 2015), which implements a hardware device in parallel with SCADA field devices allowing for continuous assessment of their security and operational status. The SSU is a solution for improving the security within SCADA systems at the PLC level, whereas the forensic hardware wrapper proposed in this paper is more focused on the forensic recovery and increased data retention of field device artefacts post-incident.

4. A SCADA FORENSIC INCIDENT RESPONSE METHODOLOGY

The SCADA forensic process should not just take place after an incident has occurred but also before and during an incident. The more detailed information the investigator has access to regarding a SCADA system under investigation the more it will increase the level of forensic evidence recovered. Below is a proposed forensic incident response model implementing four main stages; Prepare;Detect;Triage; and Respond. The final stage helps to improve the preparation for the next time an investigation is needed.

4.1. Stage 1: PREPARE

The first stage in a SCADA forensic response should occur before an incident takes place and should consist of planning and understanding every type of scenario to inform how to react and respond to a given event. For this to occur we first need to understand the architecture of the SCADA system being investigated.

4.1.1. Understand SCADA Architecture
As systems will vary from one to the other it is important for each SCADA system to have detailed documentation regarding its network architecture, components and requirements. This should include all hardware being used including manufactures, makes and models, all software running on each device across all zones, and all entry points into the networks. Accurate geographical documentation regarding locations of field devices and device half-life etc. should also be available to an investigator on request.

4.1.2. Understand System Requirements
Special requirements should also be documented for the specific SCADA system. This should include information such as what systems/devices need to remain running, those that can be either powered down and those that can be switched to a back-up. The forensic investigator should be made fully aware of the classification of SCADA System devices under investigation ie business-critical, safety-critical etc.

4.1.3. Understand possible attacks
As well as an understanding of architecture and requirements it is essential for an investigator to be aware of what types of attacks can occur and how they can infiltrate a SCADA network. According to Zhu, and further discussed by Stirland *et al*, given the components of a typical SCADA system the manipulation and types of attacks that can occur can be classified into three categories. These are hardware, software and the communication stack. More detailed information relating to these types of attacks can be found at (Zhu et al. 2011) and also at (Igure et al. 2006).

Hardware Attacks Hardware attacks can involve an unauthorised user gaining access to field devices and SCADA assets through unauthenticated remote access. If successful, they could then begin to manipulate threshold boundaries and cause a device to behave unsafely or shut down. It is already evident in the light of Stuxnet that specially designed malware can target the operation of specific hardware components in a SCADA network. These actions could have catastrophic consequences if the targeted device is relied upon for continuous and accurate operation of a critical process. An attacker gaining unauthorised access who is able to reprogram device logic may also be able to control alarms and alerts so that an operator is unaware of an event.

DOS: One type of hardware attack could be in the form of a Denial of Service attack on a PLC. If an attacker had unauthenticated remote access to SCADA field devices and was able to send data to it then they could potentially flood its bandwidth rendering the PLC inoperable. In 2013 it was Solera Networks discovered that specially crafted packets could be sent to a Nano-10 PLC causing a denial-of-service for that device (ICS-CERT 2013).

Software Attacks Some software, common among SCADA systems, can be vulnerable to buffer overflow attacks, integer overflow, SQL injections as well as memory exploits in PLCs using RTOS (Real Time Operating System). Zhu emphasises the distinct lack of privilege separation in some PLC embedded OS's such as in VxWorks resulting in poorly protected memory (Zhu et al. 2011).

Buffer Overflow: A buffer overflow is when a process or program attempts to store more data in a buffer than it was designed to handle, overrunning the buffer boundaries and overwriting memory. There are two areas within a SCADA system that could be the subject of a buffer overflow attack. The first is the servers and workstations of the external, corporate and data zones. In 2011 a vulnerability was discovered in a popular industrial automation software used to manage historian servers called Kingview HistorySrv. It was identified that Kingview was vulnerable to a heap-based overflow by using generic shellcode to send specially-crafted requests to the HistoryServer.exe process. By creating a buffer overflow on the software an attacker could execute arbitrary code or cause the system to crash (ICS-CERT 2011).

The second area susceptible to a buffer overflow attack is any field device within the control zone that is reliant upon a real-time operating system (RTOS). RTOS used in embedded devices such as PLCs issue fixed memory allocation time to real-time processes which is critical to SCADA systems. It is not uncommon for field devices to run continuously for many years without rebooting which leads to accumulated memory fragmentation and can ultimately lead to program stalls (Zhu et al. 2011).

SQL Injection: A result of SCADA systems migrating to TCP/IP and allowing for communication over the Internet is that the open themselves up for SQL injection attacks. The parts of the SCADA network vulnerable to this type of threat are the web and database servers. An SQL injection takes advantage of poorly constructed web applications where an attacker inputs specific data, such as a malicious SQL statement, into an entry field that the web application fails to sanitise. This is then executed and can cause malicious changes to database information resulting in massive damage. Zhu highlights the risk that if a "command shell" store procedure was to be enabled an adversary could hypothetically gain complete control of a database

and execute commands across the system (Zhu et al. 2011).

Communication Stack/Protocol attacks Attacks occurring at the communication stack can exploit vulnerabilities in SCADA protocols such as DNS forgery at the application layer and SYN flood attacks at the transport layer (Stirland et al. 2014) as well as packet modification, deletion, and fabrication. Igure *et al* emphasises the weaknesses in SCADA protocols, such as the lack of cryptography, that, if attacked, could potentially compromise the integrity of transmitted data resulting in packet manipulation or modified threshold values preventing alarms going off when certain set points are reached (Igure et al. 2006)

Man-in-the-middle (MITM:): Protocols that include source and destination addresses in their packet frame format, such as DNP3, could be manipulated in a man-in-the-middle attack to;

- switch off reporting causing interference with process specific alarms
- spoof response packets from field device to HMI describing false information and causing the engineer to issue incorrect commands
- instruct disruptive operations by restarting devices or halting their CPUs.

Lee describes how it is possible to sniff and modify packets given that an attacker has already gain access to the SCADA system. Their experiment involves using Ettercap to perform MITM, ARP poisoning and packet forwarding attacks. After creating an attacker tool to sniff for DNP3 packets using libpcap they were able to divide an intercepted packet into its separate layers. They were then able to modify requested packets to always show safe water level readings when actual readings were critical (Dongsoo Lee 2014).

Spoofing: Protocols that do not contain any authentication security mechanisms could be susceptible to PLC spoofing attacks especially where a particular PLC has a slow response time. For example, in a PLC spoofing attack an attacker could alter the thresholds of safety parameters before a valid PLC response is sent resulting in disruption to the SCADA system. An MTU spoof attack could involve an attacker sending inappropriate commands to a PLC such as to shutdown a process or close a valve while a pump is still activated (Dongsoo Lee 2014).

Packet Manipulation: The lack of security features within SCADA protocols leaves systems vulnerable to packet manipulation attacks such as;

- Packet Fabrication - Type of protocol attack where an attacker with access to the SCADA network inserts counterfeit objects such as forged network packets.
- Packet Modification - Type of man-in-the-middle attack where an attacker with access to the SCADA network modifies the packet being sent between master and slave or modifies the route of the packet.
- Packet Deletion - Type of protocol attack where an attacker with access to the SCADA network deletes packets being sent from one device to another either randomly or selectively.

4.2. Stage 2: DETECT

4.2.1. Determine Type of Attack

Attempt, if possible, to determine the type of attack that has/is taking place by assessing what events and anomalies have occurred.

4.2.2. Determine potential infected areas

Narrow down the SCADA system into potential infected areas. This will aid the next phase when identifying possible data sources.

4.2.3. Isolate infected areas, if possible

If infected areas can be highlighted an attempt can be made to segregate those areas by isolating networks and devices depending upon their requirements of operation within the SCADA environment.

4.3. Stage 3: TRIAGE

4.3.1. Identify Data Sources

Using documentation from the planning stage together with information regarding the possible type of the attack, if known, a list of potential data sources can be compiled to investigate, including; device location within the network; device make, model, serial number; and nature of device ie. process critical (Wilhoit 2013).

4.3.2. Prioritise Data Sources

When data sources of forensic value have been identified they need to be prioritised in an order that reflects their value, volatility and accessibility in order to maximise the amount of evidence that can be recovered from them (van der Knijff 2014). Prioritisation will also depend upon the type of event that has occurred and the needs of the business or company involved. Turnaround time of such a priority list would be a huge factor in overall response time, especially when there are potentially hundreds of assets to investigate, as the time taken to simply produce could run the risk of losing evidence stored in memory of certain assets.

4.4. Stage 4: RESPOND

This stage will consist of forensically acquiring the data from relevant data sources and analysing results and relationships of data into a final report.

4.4.1. Perform Data Acquisition
In SCADA systems forensic evidence can come from two main data sources; data that is stored in the various devices across the SCADA system; and data that is communicated through the network (van der Knijff 2014).

Data stored within SCADA components need to be extracted using forensically compliant methods in order to stand up in court. This will include memory dumps, disk imaging and chip imaging. For the engineering workstations, servers and historians normal IT forensic methodologies and tools can be applied to perform the data acquisition but this is not the case for the more specialised process control devices like PLCs and RTUs. For these embedded devices flashing software may be required from the manufacturer to extract a raw memory dump using JTAG ports and ensuring that no affect is made to the operation of the device if required to remain operational (Stirland et al. 2014). There would need to be clear guidelines as to how to approach each type of asset. Each component would have to have its own tailored forensic methodology and would be dependent upon an accumulation of information gathered in the previous stages such as;

- Does the component need to remain live within the SCADA system?
- If performing live memory acquisition what is the order of volatility for that component?
- If the component can be switched off and taken away for analysis, or switched to a back up, does volatile memory need to be acquired first?
- What is the half-life of evidence on the component after start of incident? Is the potential evidence likely to be present or is it likely to have been overwritten?

The data acquisition stage should also include network data whether this is from network taps intercepting packet flow using tools like Wireshark to capture data in transit or from network flows and logs. For a list of traditional forensic tools that can be applied at the acquisition stage please refer to (Stirland et al. 2014).

4.4.2. Perform Data Analysis
This procedure will involve analysing and correlating relationships between all recovered artefacts. The use of various forensic tools and software will help to carry out this stage, create a timeline of events and help to understand the overall effect on the SCADA system.

4.4.3. Create Report
Finally, a report should be compiled regarding results and findings with inferences made between relationships of data gathered. This should include validation and integrity of data records such as chain of custody reports. It should also include any recommendations towards the development or patching of the SCADA system.

5. CONCLUSION

A forensic investigation of a SCADA system can be seen as a jigsaw puzzle. The puzzle is complete at the time an incident occurs but as time goes by pieces of the puzzle are removed and it becomes harder to see the whole picture. The point at which a cyber-attack occurs is the point that the most evidence is present and available in that SCADA system. From there on an existing process in memory may be overwritten by a newer process, removing that piece from the puzzle. Developing a forensic readiness plan for SCADA systems is far from straight forward and can be a very lengthy process due to each system being so very different from the next. Nevertheless, despite its complexities, if a SCADA system responsible for the safe operation of critical national infrastructure is going to run for many decades without change, it is worth the time and effort to develop the forensic readiness as accurately and as detailed as possible for each system.

This paper has outlined the SCADA forensic triage process, highlighting the challenges of carrying out a forensic incident response on a SCADA system and including how it differs from traditional systems. It has also suggested ways the process may be improved in the future by calculating asset half-lives and the implementation of added forensic hardware wrappers into SCADA systems to assist the incident response process.

6. FURTHER RESEARCH

This paper is part of an ongoing SCADA Cyber Security Lifecycle Research Program co-funded by Airbus Group and the Welsh Assembly Government through Foundation Wales. The program's research is being carried out collaboratively by Airbus Innovations, the University of South Wales, Cardiff University and Aberystwyth University. Further research will look at developing a more defined forensic triage methodology and to build on the

forensic readiness of the SCADA incident response process. It will also look at developing forensic hardware to aid in a SCADA forensic investigation.

REFERENCES

Ahmed, I. et al. (2012) SCADA systems: Challenges for forensic investigators. *Computer* 45 (12), 44–51.

Björkman, G. (2010) The viking project–towards more secure SCADA systems. In: *FirstWorkshop on Secure Control Systems (SCS)*

Boyer, S. A. (2009) SCADA: Supervisory control and data acquisition. *International Society of Automation*

Cruz, T. et al. (2015) Improving network security monitoring for industrial control systems. In: *14th IFIP/IEEE Int. Symposium on Integrated Management (IM 2015)*

Cruz, T. et al. (2014) Improving cyber-security awareness on industrial control systems: The CockpitCI approach. In: *13th European Conference on Cyber Warfare and Security ECCWS-2014 The University of Piraeus*. Piraeus, Greece, 59.

Dongsoo, L. and HakJu, K. P. D. Y. (2014) Simulated attack on DNP3 protocol in SCADA system. In: *The 31st Symposium on Cryptography and Information Security* The Institute of Electronics and C. Engineers, Eds. The Institute of Electronics, Information and Communication Engineers.

Dylan M. T. E. (2009) Secure historian access in SCADA systems.

ICS-CERT (2011) *WellinTech KingView buffer overflow*. Available from https://ics-cert.us-cert.gov/alerts/ICSALERT-11-011-01

ICS-CERT (2013) *Triangle research NANO 10 PLC denial of service*. Available form https://ics-cert.us-cert.gov/advisories/ICSA-13-189-02

Igure, V. M., Laughter, S. A., and Williams, R. D. (2006) Security issues in SCADA networks. *Comput. Secur.*, 25 (7), 498–506.

Keith S. and Joe F. K. S. (2011) *Recommendations of the national institute of standards and technology* NIST, Tech. Rep.

Mark F. E. C. (2008) *Recommended practice: Recommended practice: Creating cyber forensics plans for control systems*. Department of Homeland Security, Tech. Rep.

McCarthy, J. and Mahoney, W. (2013) SCADA threats in the modern airport. *IJCWT* 3 (4), 32–39. Available from http://dx.doi.org/10.4018/ijcwt.2013100104

Miller, B. and Rowe, D. (2012) A survey SCADA of and critical infrastructure incidents. In: *Proceedings of the 1st Annual conference on Research in information technology*, ACM, 51–56.

Stirland, J. et al. (2014) Developing cyber forensics for SCADA industrial control systems. In: *Proceedings of the International Conference on Information Security and Cyber Forensics*, SDIWC Digital Library.

Stouffer, K. F. J. and Kent, K. (2008), *Guide to industrial control systems (ICS) security*. Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology, Tech. Rep.

Taveras, P. (2013) SCADA live forensics: Real time data acquisition process to detect, prevent or evaluate critical situations. *European Scientific J.*, 9 (21).

van der Knijff, R. (2014) Control systems/SCADA forensics, what's the difference? *Digital Investigation*, 11 (3), 160–174.

Wilhoit, K. (2013) ICS, SCADA, and non-traditional incident response. In: *The 2013 SANS Digital Forensics and Incident Response Summit*. Austin, Texas.

Wu, T. et al. (2013) Towards a SCADA forensics architecture. In: *Proceedings of the 1st International Symposium for ICS & SCADA Cyber Security Research*. 12.

Zhu, B., Joseph, A., and Sastry, S. (2011) A taxonomy of cyber attacks on SCADA systems. In: *Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*. IEEE Computer Society, Washington, DC, USA, 380–388.