Towards a SCADA Forensics Architecture

Tina Wu, Jules Ferdinand Pagna Disso, Kevin Jones and Adrian Campos
EADS Innovation Works Quadrant House Celtic Springs
Coedkernew, Newport NP10 8FZ UK
{Tina.Wu, Julesferdinand.Pagna, Kevin.Jones, Adrian.Campos}@eads.com

With the increasing threat of sophisticated attacks on critical infrastructures, it is vital that forensic investigations take place immediately following a security incident. This paper presents an existing SCADA forensic process model and proposes a structured SCADA forensic process model to carry out a forensic investigations. A discussion on the limitations of using traditional forensic investigative processes and the challenges facing forensic investigators. Furthermore, flaws of existing research into providing forensic capability for SCADA systems are examined in detail. The study concludes with an experimentation of a proposed SCADA forensic capability architecture on the Siemens S7 PLC. Modifications to the memory addresses are monitored and recorded for forensic evidence. The collected forensic evidence will be used to aid the reconstruction of a timeline of events, in addition to other collected forensic evidence such as network packet captures.

Digital Forensics, SCADA Forensics, Critical Infrastructures, PLC, Process Control, EnCase, Forensic Architecture

1. INTRODUCTION

Attacks on critical infrastructures have increased over the years with reports by ICS-CERT in 2012 showing 198 attacks against utility industries and other infrastructure facilities Team (2012). These types of attacks are becoming more sophisticated with the aim to commit espionage and sabotage in addition to cybercrime. Most recently, malicious malware was used to commit cyber espionage on the U.S energy sector with the intention of collecting sensitive information Ryan (2013). A further sophistication of cyber-attacks is the destruction of infected machines making it difficult for forensic analysis Paganini (2012).

The initial designs of critical infrastructures did not incorporate security features as the focus. At the time SCADA systems were isolated and the focus was to provide availability of the data rather than confidentiality and integrity, and at the time SCADA systems were isolated. In recent years SCADA systems have moved onto open networks such as Ethernet and TCP-IP leaving SCADA systems vulnerable due to a lack of security mechanisms. Many critical infrastructures are outdated, still run Windows XP and 2000, combined with a lack of updated patches, and have auto run features enabled making easy targets for infections.

These major vulnerabilities in a SCADA system enabled a cyber-attack in July 2010 on Irans nuclear program caused by the Stuxnet virus. Stuxnet was the first identified malware specifically aimed at critical infrastructure. This was a complex multi layered attack against several vulnerabilities found in Siemens S7 PLCs, software and systems operating on the Windows operating system Kushner (2013). Since then there has been an increase in attacks on critical infrastructures with new malware strains known as Flame and Duqu using similar techniques as Stuxnet. These new viruses targeted systems running Windows operating systems left vulnerable due to a lack of patching Dalziel (2013).

2. IMPORTANCE FOR DIGITAL FORENSICS IN SCADA

It is critical after an incident to carry out a forensic investigation as soon as possible, to prevent the loss of forensic artefacts. The investigation should be carried out with a strategy in place. The aim of the investigation should be to identify how the the attack occurred its perpetrators and harden of the system against further attack. A forensic investigation is vital after any cyber incident and in every scenario different questions need to be answered, for example the SCADA malware Stuxnet worm was used to compromise a system,

causing the system to malfunction. A forensic investigation will be able to aid an investigation to answer the following questions:

- It was found that the worm could steal sensitive information: what information was stolen?
- It was found that an infection cause the malfunction: what was the cause and is the system still compromised?
- How far has the infection spread through the system?

This paper presents an overview of the typical attack methods on SCADA systems and the increasing threats of new attacks due to technological developments. Next, a SCADA digital forensic process will be examined and the importance of digital forensics in a SCADA system outlined. The current challenges forensic investigators are facing in SCADA forensic investigations are identified with the limitations of existing research in SCADA forensics. A SCADA forensic architecture will be experimented to provide a forensic capability before an incident. This is using Step 7 watch table for real-time monitoring of the memory addresses on the Siemens S7-PLC. If any modifications are made to the memory addresses this would indicate an attack on the PLC. The values will then be output to a forensically sound storage to aid forensic investigations.

2.1. Typical models of attacks on SCADA systems

There are many different types of threats against critical infrastructures. These are examined in more detail by Zhu et al. and Nicholson et al (2011) (2012) with the most common types of attacks targeting SCADA hardware; software and communication stack. Cyber-attacks can escalate through various vectors such as a corporate network, directly through the internet or remote access on a customer's site or through an engineers laptop via infected USB sticks. A frequent source of infected USB stick is through contracted engineers bringing them onsite with the most recent infection affecting a power generation plant Finkle (2013), Paganini (2013). There are many cyber threats against SCADA systems with sophisticated malware attacks, SQL injection, cross-site scripting, and buffer overflow attacks being the most common type of vulnerability. Disclosure of vulnerabilities in various CNI in 2012 were found to have sharply increased Frei (2013).

The increasing development of technology has led to more sophisticated attack methods on SCADA systems using mobile devices such as tablets and mobile phones. A possible entry of attack is when an operator has connected to a rogue wireless access point allowing access to the SCADA system Schad (2012).

With the increasing popularity of cloud computing some researchers suggest partially implementing a SCADA system onto the cloud. Instead of having to install local servers, data is stored, processed and maintained in the cloud. As this can provide many benefits such as cost savings, system redundancy, low maintenance and uptime of running their own servers. Implementing a SCADA system in the cloud causes more potential security risks to a system that is already vulnerable. The challenges of performing a forensic investigation on a SCADA system implemented in the cloud are also increased along with the current challenges facing cloud forensics such as the preservation and availability of forensically relevant metadata Wilhoit (2013), Zawoad and Hasan (2013), Inductive Automation (2011).

3. SCADA DIGITAL FORENSIC PROCESS

Digital forensics is an important part of an incident response strategy in an IT forensic investigation following an incident and will provide an effective response in a forensic manner Imtiaz (2006).There are several steps to conduct a digital forensic investigation with basic steps being; preservation, identification, extraction and documentation of digital evidence. The purpose of the digital forensic process model is to demonstrate in the court of law that the evidence has been collected in the correct manner and following legal procedures with scientific backing. Currently a SCADA forensics model identified by Radvanovsky and Brodsky (2013) has the following investigative steps:

3.1. Step 1 Examination

Identify the potential sources of evidence, including the systems, the network and connected devices. In addition to these sources an investigation should examine other systems that have a relationship to the SCADA system such as access terminals, servers and routers.

3.2. Step 2 Identification

Identify the type of systems to be investigated, this includes operating system, the manufacturer including the serial numbers and model types of PLCs, the network design and implementation. Once the operating system has been identified it is important to note a system could be running more than one operating system such as a Linux variant. Many SCADA systems run a child system over a base OS. During the identification process several areas can assist, including manufacturers

documentation, design specifications, network diagrams, and the HMI (Human Machine Interface).

3.3. Step 3- Collection

Collect potential evidence from the memory systems that are suspected to be part of the SCADA system being investigated. It is critical that volatile and dynamic information across various network cards and controller units be collected first to prevent any loss of data from network connections. Network traffic is also captured to discover anomalous traffic.

3.4. Step 4- Documentation

In this step it is critical to keep accurate documentation of the investigation to ensure chain of custody. Records need to be kept of potential evidence as well as case numbers and the time when the evidence was collected. Many investigators will photograph the entire investigation process including the systems that could be connected to the SCADA system or that are presently connected, to ensure that the examiner will be able reconnect them if needed later. A detailed report would need to be produced of the whole digital forensic process to include the captured system throughout the collection process. The last stage is to gather all the information together and store in a secure and safe location.

4. PROPOSED SCADA FORENSICS PROCESS MODEL

The purpose of proposing a new SCADA forensic process model is that the exisiting processes lacks any detail in carrying out a full forensic investigation of a SCADA system. The suggestion of an SCADA forensic investigative process model using combination of incident response and cyber forensics investigative model. The following phases have been identified, and are shown in Figure 1:

- Phase 1- Identification and Preparation
- Phase 2- Identifying data sources
- Phase 3- Preservation, Prioritising and Collection
- Phase 4- Examination
- Phase 5- Analysis
- Phase 6- Reporting and Presentation
- Phase 7 Reviewing results

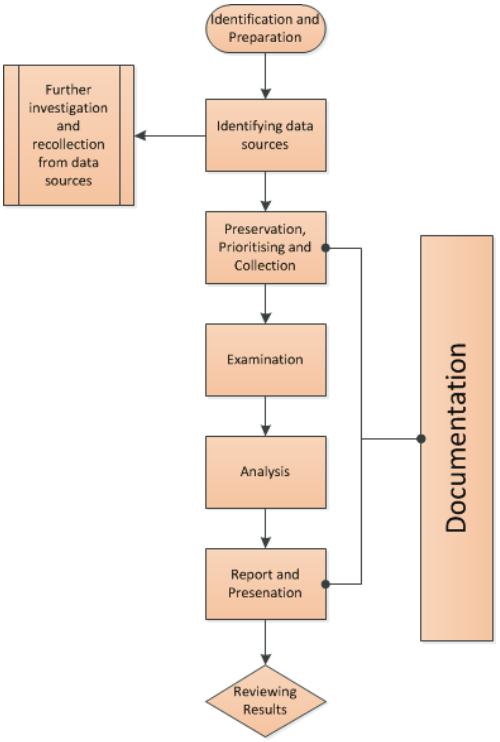

Figure 1: *Incident response forensic process*

4.1. Phase 1- Identification and preparation

This phase takes place before the investigation, aimed at understanding the architecture of the SCADA systems, the network, and possibly understanding the type of incident that has occurred. An appropriate strategy would need to be developed taking into consideration the systems, the type of incident and time constriants including the requirements that SCADA systems be operational for 24/7. This is the collection of documentation by gathering information from various resources and parties including vendors, software, hardware providers and contractors.

4.2. Phase 2- Identifying data sources

Documentation is required from phase 2 to phase 8 so at the end of the forensic investigation a report can be complied to provide a conclusion of the findings from the investigation and demonstrate that the chain of evidence has been met. Identifying the point of entry by looking at possible entry points or if a device has been used to access the SCADA system. This could be by various possible points of entry including a small mobile device, access through a wireless link, or 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 camera monitoring a remote device on a SCADA network. This will be the phase to identify data sources based on the type of incident, that may have come in contact with the incident and have potential evidential data. In this phase identification of SCADA systems operating

systems, and the devices on the network can be used to compile a forensic toolkit e.g. hardware and software devices required to take as an incident response kit. Developing a plan is a vital part of a forensic investigation because there are multiple data sources. The plan must incorporate a prioritisation of the data sources, establishing the order in which the data should be acquired. To decide on the prioritisation several factors need to be considered:

- Potential value of the data source
- Volatility of the data once the system has been powered off, this could cause a loss of potential volatile data such as physical RAM that could lose live connections, current running processes etc. Volatile data would be given priority over any non-volatile data
- Amount of effort required: The amount of effort to acquire different data sources differs in each forensic investigation. Consideration needs to take in the time spent acquiring and the cost of equipment. The problem that SCADA systems have many field devices such as PLCs. Decision need be made to determine which devices to acquire data from and whether they have potential forensic artefacts, this would depend on the asset value of the field device. The key components that potentially collect data following an incident will be examined in more detail. Further analysis will be carried out on each component to determine whether data stored in these devices collect any potential forensic evidence. These are:

    - Engineering workstation
    - HMI
    - PLC (Programmable Logic Controller)
    - OPC (Open Process Control) Clients:SQL Server

4.3. Phase 3- Prioritising, preservation and collection

The purpose of prioritising and preserving volatile data is that in a SCADA systems intermingling of data and huge amounts of process data is normally created, with data is being overwritten or being compromised. The procedure for collecting from data sources on the SCADA system depends on the volatility of the data. This would require the forensic investigator to take steps to preserve and prioritise in the collection methods.

- The collection of volatile evidence: Acquiring volatile data of the physical RAM of memory, that would normally be lost when power cycled.

    - PLC and RTU RAM memory
    - Workstation
    - Database, Servers
    - Wireless devices
    - Routers
    - Switches

- The collection of Non-volatile evidence: This phase involves collection of evidence from non-volatile devices such as flash memory, SD cards from PLCs, USB sticks. If a mobile device is connected to a workstation (HMI) data must also be acquired from this. With the increasing open connectivity of critical infrastructures consideration must be given to the investigation of any mobile devices that may be connected to the system.

4.4. Phase 4- Examination

This stage involves the forensic examination of the collected evidence by specialist trained forensic examiners. This part of the process is an important part of the forensic investigation to provide an answer to questions raised before the investigation. The collected data from a SCADA system will normally be huge volumes therefore this is the part of breaking down the evidence into manageable loads for forensic analysis. In the form of data filtering, removal of known files, pattern matching and searching through known hash values, keyword searches based on the intelligence provided before the incident. This is the phase of data recovery and to to identify systems that have been tampered and modifed. It is during this phase that a forensic investigator may find forensic artefacts that may be attached to another SCADA process and may need to revisit the site for further collection from data sources.

4.5. Phase 5- Analysis

This is the phase of finding relationships between the recovered forensic artefacts and piecing the evidential data together to develop a timeline of the incident This makes it possible to reconstruct the events in a test enviroment, to help answer questions as part of the forensic investigation.

4.6. Phase 6- Reporting and Presentation

After the examination and analysis phase the results must be complied into a report to be viewed by various audiences. This should include any conclusions found from the examination and analysis phases and answer any questions about the incident. The report should include the following:

- Background of the forensic examiner such as expertise, training and certifications.
- Detailed description of the forensic software and hardware tools methodologies.
- Chain of custody documents.

4.7. Phase 7- Review results

The final stage is reviewing the results from the examination and analysis phase. A forensic investigation may not answer all questions in the investigation. If forensic artefacts create more than one explanation the forensic investigator should either prove or disapprove these explanations. A report that is presented in the court as evidential material should have detailed description of all the phases of investigation, and possibly evidential copies of the collected data. A report presented to an engineer would require a detailed report of network traffic and details of identified possible vulnerabilities in the system that requires attention. Where a conclusion has not been met during the forensic investigation possible further data may be collected. For example, a list of network connections with further investigation could provide answers to gaps in the investigation. During this phase of the investigation, vulnerabilities in the SCADA system should be rectified to prevent further attacks.

5. LIMITATIONS OF USING TRADITIONAL IT FORENSIC PROCESSES

Using traditional IT digital forensic process is unsuitable for SCADA systems. This is because currently there are no forensic processes to collect from embedded devices on the SCADA systems such as Programmable Logic Controllers (PLC) and Remote Telemetry Unit (RTU). SCADA system use MODBUS and Distrubuted Network Procotol (DNP3) that are different communication protocols not normally found in IT networks. Some SCADA systems also use traditional networking protocols such as TCP/IP, and typical forensic methodologies and approaches can be applied where an IT network has conventional servers and computers. In a SCADA system embedded devices such as PLCs and RTUs would require specialised processes as these devices are often deployed in different locations making it difficult to determine where data is held. Although a forensic capability would be easier to implement in a SCADA network than a normal IT network because in an IT environment the communication traffic is generated by users: making traffic unpredictable. Network traffic on SCADA systems provides process data without much variation therefore making it easier to identify any anomaly patterns. A forensic investigation in a large scale IT network can be complex and expensive, however in a SCADA network a forensic investigation may be considerably simpler depending on the critical infrastructure. In an IT network there may be a high volume of traffic when compared to a SCADA network making it possible to log relevant process control data and subsequent methods to analyse the data Olivier and Shenoi (2006).

6. CHALLENGES FOR SCADA FORENSICS: IT VS SCADA SYSTEMS

Currently forensic investigators face complex SCADA environments which prevent them from applying contemporary forensic techniques and tools. The challenges facing investigators are outlined below:

6.1. Live forensics and integrity of data

Due to safety, costs and time requirements even after an incident a SCADA system is required to be operational. Live forensics is required and it is vital that this takes place as soon as possible after the incident, to prevent further loss of volatile data. Live forensics is becoming more useful in forensic investigations where potential forensic artefacts would be lost if the system was shut down. Live acquisition would potentially capture an image of the running system, preserving memory, process and network artefacts. A live system is a dynamic environment therefore live forensic acquisition is problematic because volatile RAM cannot be verified and will be forensically unsound. Unlike traditional acquisition methods where data can be verified with a hash algorithm such as MD5 that produces a 128-bit hash value Vacca and Rudolph, (2010)

Ladder logic in many field devices will rarely alter although some network configurations may change the resident memory. It is best practise for a forensic investigator to create a baseline hashing algorithm of the ladder logic that could be potentially useful further on in the forensic investigation. The hash algorithms should be stored with read-only access and offsite in a secure unit. In the event of an incident a comparison of the existing logic inside the device would provide a comparison to the known hash that was previously calculated. Although baseline measurements for example ladder logic baseline would need to be updated regularly to verify the devices integrity Grobler and von Solms (2009).

6.2. Lack of compatible forensic tools for field devices

Currently there are no methodologies or data acquisition tools to extract data from embedded devices such as PLCs. This is because there is a lack of demand for forensic acquisition vendors to

incorporate compatibility with SCADA devices or produce hardware or software to be used for SCADA forensic data collection Olivier and Shenoi (2006), Fabro and Cornelius (2008)

Field devices such as PLCs have been targeted by cyber attackers such as Stuxnet aimed at Siemens S7 PLCs. Therefore it is vital that potential forensic artefacts can be retrieved from PLCs, as they have limited amounts of memory and short retention of data and it is unlikely that an attack would be detected straightaway therefore any forensic artefacts within a PLC could have been overwritten. Even though the retention time of the data within a PLC is short, there is data in the RAM and flash memory that would be useful for a forensic investigation. The following are suggested requirements for a forensic data acquisition tool specifically for PLCs, because of the limits on acquiring the data they may need to be deployed in various locations:

- Network acquisition- The tool should have the capability to remotely acquire data from a suspect computer to a forensic investigators workstation. Currently there are many different forensic network acquisition tools such as EnCase Enterprise, F-Response and ProDiscover. EnCase Enterprise allows the forensic investigator workstation to acquire harddisk and RAM data through an encrypted authentication to the suspect computer. Encase Enterprise is a remote program called a servlet, that is installed passively onto the suspect machine. Although it was used Cassidy et al (2007) to collect forensic artefacts from HMI and server. Acquiring data on legacy SCADA systems will be slower, due to the use of modems and the limitations of bandwidth with modems having estimated speed of 300-1200 bit per second (bps) Kalapatapu (2004), Kent et al. (2006).
- The tool should feature Live forensic capabilities as acquisition will be carried out on the field device while it is still running, but in situations where the device has malfunctioned an engineer will power cycle the field device resulting in a loss of RAM artefacts.
- The tool should be lightweight to prevent causing too much noise on the SCADA network.
- Must be compatible with a field devices unique with PLCs operating system such as VxWorks, INTERGRITY and MQX, or often integrated with a vendors own operating system (Linux Variant). Therefore a forensic data acquisition would need to be developed that was compatible with the various file systems on PLCs Byres (2011).
- A tool that create the least footprint without making modifications to the original data source.

There are data acquisition tools compatible with some field devices with the use of cables and flashing equipment, although this type of equipment is usually used for system servicing and repairs. This makes it difficult to obtain less common models of PLCs and RTU and forensically sound access to the RAM and ROM on these devices is difficult to achieve without first turning the device off Radvanovsky and Brodsky (2013).

6.3. Lack of forensically sound storage

In a typical SCADA system the following are the types of devices available for data storage:

- OPC Clients- This is software used for communicating with the OPC Servers an example of a OPC Client is a SQL Database DataHub (2010).
- Historian- This database that stores audit-logs of all activities on a SCADA network NcNamee and Elliott (2011).

These devices are used for specific purposes therefore the data stored within them may not be forensically sound. For example data stored in a Historian is normally used for data trending and can be accessed through external systems that could be compromised. Although McNamee and Elliott (2011) have found that using a Trusted Service Engine (TSE) that allows remote access to Historian data. NcNamee and Elliott (2011) believes this will improve the security of a Historian by isolating it from the SCADA network. Historians collect large amounts of process data used for long term storage, therefore intermingling of data is high and sorting the data will be a time consuming forensic process Inductive Automation Horizons (2013).

6.4. Identifying data sources on a SCADA system

SCADA systems have a complex architecture (see Figure 2) with multiple layers of data communication making it difficult to determine the types of data sources that would be helpful for a cyber-forensics investigation. Separating the type and location of forensic artefacts for collection can be problematic, this can be resolved by collection of a large sample. Although sorting the data would be a time consuming task because of having to separate the malicious data and data unrelated to the incident. In a SCADA network there are several layers of connectivity. This makes it difficult to carry out a forensic investigation.

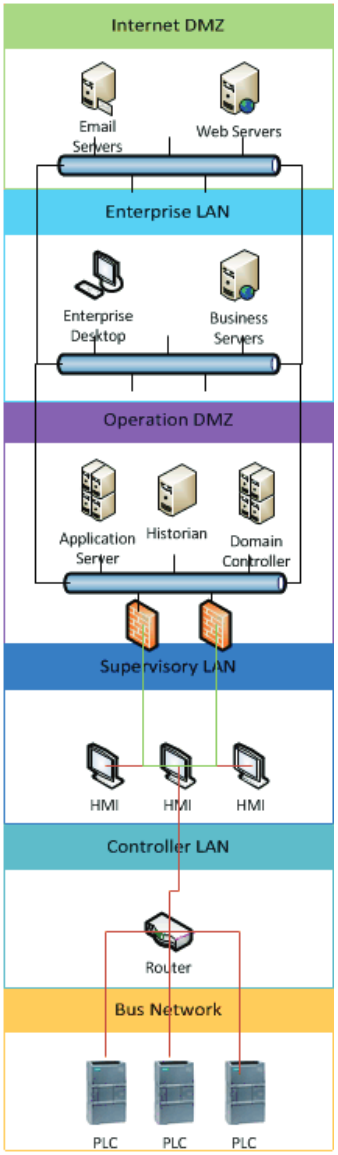

Figure 2: *Network connectivity on a SCADA system*

6.5. Increase of sophisticated attacks

The SCADA forensics acquisition process can be a combination of hardware and software to acquire flash and RAM memory. This can be challenging because of increasing sophisticated attack methodologies. With recent cyber-attacks having the ability to execute malicious code using shellcode through buffer overflow attacks, this allows not infect the storage system or the flash memory; this adds problems to the complexity of the forensic process [23].

7. EXISTING TOOLS TO SUPPORT SCADA FORENSICS

A limited amount of work has been reported to date that deals with the forensic recovery of artefacts from a SCADA system. The following are existing research in SCADA forensics:

7.1. Hex dumps of the file system

Hexadecimal dumps are known as flashing and is often use on mobile devices to dump the phone memory into a format of either hexadecimal or binary. This is to extract the memory contents of the phone in order to recover hidden or deleted data Harrington (2007). A hex dump of the system is the physical acquisition of the systems memory. The majority of devices such as mobile phones require specialist flasher tools. The specialist support tool is designed for repairing and servicing SCADA hardware or field devices such as RTUs and PLCs. The hex dump is important to obtain if the PLC or other embedded system is suspected to be infected during a cyber-attack and network traces have not remained. With the gathered information a standard forensic analysis may be conducted and in many cases file systems can be checked for known malware signatures, and compared against expected file signatures to determine changes to the file system. The benefit of using this tool is that it allows the dumping of the system memory, although this method will be different depending on the make and model of the field device. This type of forensic acquisition on a PLC and RTU would be impractical as it varies between make and model of PLC and RTU. Therefore it could be difficult to locate a specific flashing tool [23].

7.2. Network monitoring

Network monitoring captures the real-time network traffic and state information. It should be implemented into the SCADA architecture to support the use of network forensics which can be useful and more efficient for forensic investigation. The solution is a Security Incident Event Management (SIEM) providing a unified platform of security software that offers real-time security analysis and alerting. Netresec have a SCADA network monitoring tool called Network Miner 1 that supports ICS protocols. Network miner is used to monitor the SCADA network by implementing sniffer agents into multiple zones on the SCADA network allowing easy network forensics the attacker to run the code in the memory without installation on the target machine. The code does investigations following an incident. The flaw in this architecture is that all network traffic is collected creating a large dataset which will be difficult to sort in a forensic investigation Ahmed et al. (2012).

Olivier and Shenoi (2006) has proposed an architecture that supports post-mortem analysis of SCADA network traffic. This focuses only on providing the collection of network packets from the

[1] 1 http://www.netresec.com/?page=NetworkMiner

management network of the HMI and database and the control network of the field devices. Agents are installed on the data warehouse at secure isolated locations in the management network. The agents collect the network packets and forward them to the data warehouse. The flaws in this architecture is the network communication between the agents and the data warehouse are assumed to be isolated. SCADA systems are increasingly becoming connected to the internet and it is impossible to say whether the agents have been compromised during an cyber-attack, and that the collected network packets are forensically sound.

7.3. Remote Network Acquisition

Cassidy et al. (2007) carried out an experimentation of remote network acquisition using commercial forensic tool Encase Enterprise. Their assumptions are that a forensic analysis has to be conducted on a live SCADA system. Onsite analysis of SCADA systems is impractical due to the location of some SCADA devices. Therefore, forensic acquisition must be carried out from a central location with minimal workload to the SCADA system. This experimentation used Encase Enterprise, created customised EnCase scripts tested by collecting from HMI, application server and Historians. Results from Cassidy et al. (2007) experimentation found that the Servlet has no noticeable impact on the overall system with the scripts and imaging of the HMI, Historian and application server having only a limited amount of memory, network traffic and CPU utilisation.

7.4. Fault logging

All networking devices log security events to help detect attacks and provide an audit trail for security incident investigations. Currently many PLCs and other field devices have very limited security logging. Digital Bond have identified limitations of security logging features on Rockwell Automation ControlLogix PLC. This is overcome by creating ladder logic to purposely record security events. This method was tested using RSLogix 5000 to record security events moving fault log data to a data historian, but found that the fault log was only capable of monitoring four variables. The four system variables recorded are:

- MajorEvents
- MajorFaultBits
- MinorEvents
- MinorFaultBits

Currently these ladder logic variables are created to alert an engineer of faults on a PLC or HMI. Additional ladder logic variables should be created to record security events and monitor any modifications of the ladder logic and store securely in a data historian. Therefore this is assumes that that the data stored in the Historian is forensically sound and cannot be accessed from external sources.

7.5. Forensically sound storage

AlienVault created by Ossim have a Security Information and Event Management (SIEM) a unified security solution that is specially aimed for the use on ICS/SCADA systems. In Ossim's commercial version they provide a forensic storage of the security events generated by the SIEM. The data is digitally signed to confirm the integrity of the data during transport and provides Advanced Encryption Standard (AES3DES) by applying the algorithm three times in succession with three different keys to the traffic to ensure chain-of-custody Singh and Supriya (2013).

Although Afzaal et al. (2012) have found that Ossim have implemented forensic storage using only RSA classic algorithm to only digitally sign important security events. There are weaknesses in the RSA classic algorithm that uses private and public keys, that can easily be compromised by searching the hard drive for secret keys, the signed events would then be inadmissible in court. Afzaal et al. (2012) have designed their own forensic storage and through tests shown that their solution ensures integrity of data even in the presence of attacks.

8. EXPERIMENTATION

The purpose of this experimentation is to prove that the proposed forensic capability architecture will provide forensic artefacts for collection after a incident. Our experimentation is based on a traffic light scenario created using the Siemens S7 PLC. After compiling the ladder logic, we then downloaded it unto the PLC. In our attack scenario, we sent a crafted network packet that turned all the traffic lights green. This is materialised in the program by a change of memory variable values. We use the Siemens programming software to monitor the changes that occur in the memory as the attack is happening. This type of security monitoring on a PLC will be useful after a cyber-attack for forensic investigations if the changes to the systems are forensically recorded. The setup of experimentation shown in Figure 3 requires the following components:

- Siemens S7 PLC
- Siemens STEP7 (ladder logic software) used to create a PLC programme for a traffic light system.

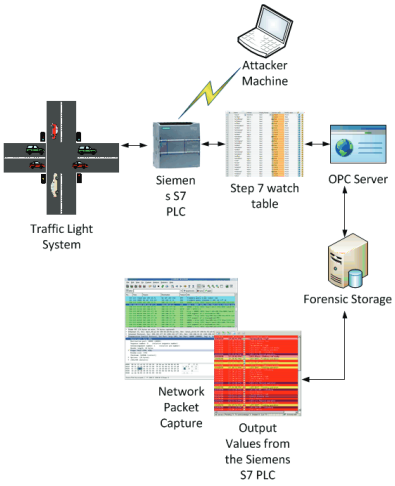

Figure 3: *Experimentation enviroment*

9. RESULTS

Results are shown in Figure 4 and 5 of a watch table on Siemens S7 PLC monitoring the memory addresses in real-time. Table 1 shows the watch table and the contents in each of the columns:

A	Name	shows the memory name given by the user.
B	Address	This displays the memory address of the stored tag of the memory of the Siemens S7 PLC.
C	Display Format	This displays the type of memory that is stored,
D	Monitor Value	This displays the actual value of the monitored memory address in real-time. When the value is TRUE the memory is in use and FALSE when not in use.
E	Modify Value	This displays the actual value of column D has been modified. When this value is FALSE no modifications have made and if TRUE the memory address has been modified.

Table 1: *Step 7 watch table*

The memory addresses in the PLC are rarely modified and column E will stay FALSE this is shown Figure 4. If modifications are made in the memory addresses this will be displayed in column E as TRUE shown in Figure 5 indicating an attack on the PLC. The changes in these value would be a useful forensic artefact when output into a forensic storage to use later in the forensic investigation for timeline reconstruction. From this experiment we have proved that it is possible to utilise OPC Server using a variable logging mechanism to support incident response in a forensically sound manner. Thus, preserving volatile data to improve cyber investigation intelligence.

	Name	Address	Display format	Monitor value	Modify value
1	"S1"	%I0.6	Bool	FALSE	
2	"S2"	%I0.7	Bool	FALSE	
3	"Red"	%Q0.0	Bool	FALSE	FALSE
4	"Yellow"	%Q0.1	Bool	FALSE	FALSE
5	"Green"	%Q0.2	Bool	TRUE	FALSE
6	"Pedrestians_Red"	%Q0.3	Bool	TRUE	FALSE
7	"Pedrestians_Gree.	%Q0.4	Bool	FALSE	FALSE
8	"START"	%M0.0	Bool	TRUE	
9	"STATE0"	%M0.1	Bool	TRUE	
10	"STATE1"	%M0.2	Bool	FALSE	
11	"STATE2"	%M0.3	Bool	FALSE	
12	"STATE3"	%M0.4	Bool	FALSE	
13	"STATE4"	%M0.5	Bool	FALSE	
14	"STARTP"	%M0.6	Bool	TRUE	
15	"BUTTON"	%M0.7	Bool	FALSE	
16		<Add new>			

Figure 4: *Screenshot of Step 7 watch table before an attack on the ladder logic before an attack*

	Name	Address	Display format	Monitor value	Modify value
1	"attack"	%M200.6	Bool	FALSE	FALSE
2	"M1TRED"	%M1.0	Bool	FALSE	TRUE
3	"M1TORANGE"	%M1.1	Bool	TRUE	FALSE
4	"M1TGREEN"	%M1.2	Bool	FALSE	FALSE
5	"M1PRED"	%M1.3	Bool	TRUE	TRUE
6	"M1PEDGREEN"	%M1.4	Bool	FALSE	TRUE
7	"M2TRED"	%M1.5	Bool	TRUE	FALSE
8	"M2TORANGE"	%M1.6	Bool	FALSE	FALSE
9	"M2TGREEN"	%M1.7	Bool	FALSE	FALSE
10	"M2PRED"	%M2.0	Bool	FALSE	FALSE
11	"M2PGREEN"	%M2.1	Bool	TRUE	FALSE
12	"M3TRED"	%M2.2	Bool	FALSE	FALSE
13	"M3TORANGE"	%M2.3	Bool	TRUE	FALSE
14	"M3TGREEN"	%M2.4	Bool	FALSE	FALSE
15	"M3PRED"	%M2.5	Bool	TRUE	FALSE

Figure 5: *Screenshot of Step 7 watch table before an attack on the ladder logic after an attack*

10. CONCLUSION

This paper provides an experimentation of using the Step 7 software that provides real-time monitoring of the memory addresses on the Siemens S7 PLC. Memory addresses in the PLC rarely change any modification would indicate an attack on the PLC, this would output a value that can be used as forensic evidence but only if the value is stored in a forensic storage. Further research will be required to store the values in a forensically sound manner. This paper also provides an improved SCADA forensic process, that will be used to support incident response.

11. FURTHER RESEARCH

This is an on-going research project further research will be required to produce a full forensic capability for a SCADA system. The aim of this research is to implement a forensic capability architecture that will allow a forensic investigation after an incident. The architecture is using the output values that are created when there are modifications to the memory addresses on the PLC. The output values will be used to aid a forensic investigation and to create a timeline of events of the incident. A security logger on the PLC would provide the best security monitoring solutions to record all events and modifications to the memory addresses. The drawback to this solution is that it will be impractical for current SCADA systems that may have vast amount of variables to tag and could take a large amount of

memory on the PLC. Further research will need to be carried out in storing these values in a forensic storage similar to Ossim forensic storage and the development of a visulisation tool to detect any patterns and modifications to the memory addresses in the PLC.

REFERENCES

Afzaal, M. et al. (2012) A resilient architecture for forensic storage of events in critical infrastructures. In: *HASE*. Omaha, NE, USA. Oct. 2012. 48–55.

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

Byres, E. (2011, May) *PLC security risk: Controller operating systems*. Tofino. Available from http://www.tofinosecurity.com/blog/plc-security-risk-controller-operating-systems

Cassidy, R. F. et al. (2007) Remote forensic analysis of process control systems. In: *Critical infrastructure protection*. Berlin, Germany: Springer-Verlag. 223–235.

Dalziel, H. (2013, Feb.) The four amigos: Stuxnet, flame, gauss and DuQu.

DataHub, O. (2010) What is OPC?

Fabro, M. and Cornelius, E. (2008, Aug.) Recommended practice: Creating cyber forensics plans for control systems.

Finkle, J. (2013, April). Malicious virus shuttered power plant: US government.

Frei, S. (2013, Feb.) Vulnerability threat trends.

Grobler, M. and von Solms, B. (2009) A best practice approach to live forensic acquisition. In: *ISSA*. 3–13.

Harrington, M. (2007). Hex dumping primer.

Imtiaz, F. (ed.) (2006, Dec.) Enterprise computer forensics: A defensive and offensive strategy to fight computer crime. In: *Proceedings of the 4th Australian Digital Forensics Conference*. 1–10.

Inductive Automation (2011) Cloud-based SCADA systems: The benefits and risks. *White Paper*.

Inductive Automation Horizons (2013) Data acquisition, trending, and historians.

Kalapatapu, R. (2004, Oct.) SCADA protocols and communications trends.

Kent, K. et al. (2006, Aug.) *Guide to integrating forensic techniques into incident response*. Gaithersburg, MD, USA: NIST.

Kushner, D. (2013, March) The real story of Stuxnet. *IEEE Spectrum*.

NcNamee, D. and Elliott, T. (2011, June) Secure historian access in SCADA systems. Galios. *White Paper*.

Nicholson, A. et al. (2012) SCADA security in the light of cyber-warfare. *Comput. Secur.*, 31 (4). 418–436.

Olivier, M. and Shenoi, S. (2006) *Advances in digital forensics II*. 222. Berlin, Germany: Springer. 364.

Paganini, P. (2012, Sep.) Cyber espionage on energy sector, Chinese hackers are not the only.

Paganini, P. (2013, Jan.) New attacks against SCADA, old vulnerabilities, very old issues.

Radvanovsky, R. and Brodsky, J. (2013) *Handbook of SCADA/control systems security*. Boca Raton, FL, USA: Taylor & Francis Group.

Ryan, M. (2013, January). *Energy sector remains the main target of cyber attacks*. Available from http://www.bizjournals.com/houston/blog/nuts-and-bolts/2013/01/energy-sector-remains-the-main-target.html. (16 Jan. 2013).

Schad, C. (2012, July) *A new era of mobility using mobile devices for SCADA*. Schondorf, Germany: Industrial Ethernet Book.

Singh, G. and Supriya (2013, Apr.) Article: A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. *Int. J. Comput. Appl.*, 67 (19). 33–38.

Team, I. C. S. C. E. R. (2012, Dec.) ICS-CERT monitor.

Vacca, J. and Rudolph, K. (2010) System forensics, investigation, and response. In: *Information systems security & assurance series*. Burlington, MA, USA: Jones & Bartlett Learning.

Wilhoit, K. (2013). SCADA in the cloud - A security conundrum?

Zawoad, S. and Hasan, R. (2013). Cloud forensics: A meta-study of challenges, approaches, and open problems.

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, ITHINGSCPSCOM '11*. Washington, DC, USA, Piscataway, NJ, USA: IEEE Computer Society. 380–388.