Securing Supervisory Control and Data Acquisition Systems: Factors and Research Direction

Full Paper

Emmanuel Ayaburi
The University of Texas at San Antonio
emmanuel.ayaburi@utsa.edu

Lucia Sobrevinas
The University of Texas at San Antonio
andsav@gmail.com

Abstract

SCADA systems before their current generation were seen as mostly centralized and isolated monolithic structures that relied on proprietary network, hardware and communication protocol and were thus were considered insulated from cyber-attacks. However, with the recent advancement in network and communication technologies SCADA systems are now connected to corporate intranet and the internet. While this change has increased the ease of management and integration, it has also exposed SCADA systems to a myriad of cyber vulnerabilities. This research examined key factors that support secure assessment and operation of SCADA systems, the methods and techniques used to implement best practices and security controls within these systems, and finally it identified areas of currently ongoing and future research within this field.

Keywords

SCADA, security, vulnerability, assessment, threat.

Introduction

Supervisory control and data acquisition systems (SCADA) are used to provide remote human monitoring and automatic control of real world processes. There are approximately three million SCADA systems used around the world (Hildick-Smith 2005) and securing these systems has become a national priority in the US. Publicly announced SCADA system vulnerabilities have increased from one in 2005 to ninety eight in 2012 representing over a 9000% increment (Positive Technologies, 2012). The security of SCADA systems have been at the center of research at institution such Sandia, standardization organizations such as National Institute of Standards and Technology (NIST) and American Gas Association (AGA) for the last several years. Some known vulnerabilities of SCADA systems include buffer overflow, remote code execution, local privilege escalation, denial of service attacks (DoS), data integrity and authentication / key management. These vulnerabilities are found in devices made by major vendors all over the globe such as Siemens, General Electric and Schneider Electric (Positive Technologies, 2012). While there are many organizations such as NIST, OPC Foundation and AGA currently involved in an effort to standardize security of SCADA systems, most systems are not yet properly secured from a managerial and technological perspective (Igure et al. 2006).

The increased deployment of SCADA systems will undoubtedly give rise to complex challenges due to factors such as the human behavior, commercial interest, regulatory policies and political interest. There is a pressing need to understand the factors that can lead to insecure SCADA systems. Therefore research should focus on the motivation, capability and objectives of an attack on a SCADA system.

The primary purpose of this paper is to outline from past literature the factors that affect secured operations of SCADA Systems and identify researchers’ salient findings. The paper reviews recommendations from perspectives including intrusion detection systems, network and data transmission, operating system, standardization, architecture of SCADA systems such as the move toward
the cloud and app based controls, analyzing the resiliency of SCADA systems against targeted attacks (both internal and external), and reviewing security controls systems such as alert management, user access controls, intrusion detection systems, intelligent traffic routing and management and security management. Finally, the paper intends to point out directions for future research in security of SCADA systems.

The organization of the rest of the paper is as follow: at the conclusion of the introduction of this paper there will be a discussion of the basic concepts of cyber physical systems and system vulnerabilities. The discussion of SCADA vulnerabilities and future research directions will be next. Finally, the paper concludes with a call as to why there is the need to more deeply explore the vulnerabilities to SCADA systems.

Concepts

Supervisory Control and Data Acquisition systems

Supervisory control and data acquisition systems (SCADA) describe a collection of systems that measure, report, and change in real time both local and geographically remote physical process (William T. Shaw, 2006, Pg. XVIII). The basic capabilities of a SCADA system includes acquisition of data from sensors and users, command of physical process through controllers or users, communication network and control through actuators. Some major components of SCADA include field devices, operating equipment, local processors, communications network and host computers. Some field devices include programmable logic controllers (PLC), remote terminal units (RTU) and intelligent electronic devices (IED) such sensors, motors, circuit breakers and console light that have microprocessor in them (Nicholson et al. 2012). Signals from an operator, RTU or PLC can make IED take control actions on physical processes. These systems are connected together with SCADA systems through the usage of different transmission mediums including: ethernet, fiber-optic cabling, telephone lines (copper), microwave, satellite or radio. These connection points and in particular the wireless connectivity makes them more prone to cyber-attacks.

The increase use of SCADA system in an ever growing list of diverse areas include critical infrastructure such as power generation, medical operation, telecommunication, transportation, banking, finance, water supply, emergency services, government services, agriculture and aviation have made them a suitable and desirable target not only for cybercriminals but even for state sponsored cybercrimes. The Presidential Decision Directive 63 document initiated by President Clinton in 1997 established the framework to protect the critical infrastructure and the Presidential document of 2003, the National Strategy to Secure Cyberspace stated that securing SCADA systems is a national priority in the US (Hentea 2008).

SCADA systems differ from typical IT systems in a variety of ways particularly in terms of its risk and operational requirements management. SCADA systems have a deep and far-reaching demand on continuous availability and reliability in addition to other security properties such confidentiality and integrity. The field devices such as RTUs and PLCs have an immensely important role in many of these critical control systems as they can directly impact human life. Legacy issues with SCADA software and hardware, protocols, large and distributed physical base, computational requirements of edge devices and wide interface between digital and analog signals make securing SCADA system a atypical and complex IT task (Zhu et al. 2011).

Vulnerabilities

Vulnerability is defined as the measure of a system’s susceptibility to a likely threat or attack opportunity (Cai et al. 2008). As cyber-security threats have impacted IT networks on a global scale, it has become increasingly apparent that the air gap isolated security mentality that the SCADA community had for so long relied upon is no longer applicable. The oftentimes outdated network infrastructure including dial-in modems and legacy hardware along with proprietary protocols and applications make SCADA networks vulnerable to numerous types of security breaches both from external attackers as well as from internal incidents. About 70% of security incidents in SCADA system are from external sources while 30% are from either internal or accidental sources (Byres and Lowe 2004). In an effort to update the SCADA environment, researchers have contributed numerous policy, procedural, and theory-based solutions to
harden the system. Most SCADA systems are vulnerable because vendors are reluctant to have users patch their systems without their approval due to the potential for incompatibility errors and its resulting system downtime. SCADA systems operate on time sensitive data such that an antivirus processing delay might turn out to be ineffective. Most traditional firewalls were designed and configured to filter SCADA packets at the application layer (Cai et al. 2008). For instance, organizations typically use firewalls to protect their LAN against external attacks, but what is in place for monitoring of the internal network? For many organizations, this is an area in which they are highly lacking and extremely vulnerable to a security breach—particularly in the case of an insider attack. Among adversaries that SCADA systems are vulnerable to include state sponsored hackers, terrorists, organized crime, insider threat, hobbyists, script kiddies, activist hackers and legitimate penetration testing (Nicholson et al. 2012). In order to better combat this movement more advanced firewalls is needed in addition to well configured and monitored IDS and IPS systems, access controls, and better monitoring of internal network traffic.

**SCADA Vulnerability**

SCADA Systems and Cloud Computing

While cloud computing offers improved efficiency and optimization of network resource usage, the implementation of the smart grid backed by the cloud infrastructure also provides an environment that allows all elements of the SCADA smart grid to communicate with one another: RTUs, operators, sensors and SCADA applications. The VS-Cloud would manage the alarms and incident alerts through the use of specialized intermediary nodes that have the necessary computational and processing resources needed to compute and analyze the varying message formats in the system. The three major components of this system are: a SCADA transmission component which is charged with transmitting any operational information to the SCADA system, a redundancy component which is responsible for replicating the aforementioned operational information with the VS-Cloud, and finally an advanced search component which manages dynamically resolving any queries according to a strict set of parameters. What researchers are referring to as the VS-Cloud or the virtual SCADA cloud would be a virtual backbone for the control system by not only inter-connecting all components but by also providing redundancy by storing all pertinent data recorded by the system including: alerts/alarms, measurements, permissions, and executed actions and processes generated by the system (Alcaraz et al. 2011). The redundancy offered by this solution would allow the entire system to recover any affected parts by allowing other functional areas to directly access the VS-Cloud to gather all the evidence that occurred before the anomalous event.

An important element of any information system is the element of security. The VS-Cloud model would implement security controls using numerous distinct models such as searchable encryption. This form of encryption allows a server to execute queries without having to decrypt any of the data and thus preserving the confidentiality of the data. The solution also includes private information retrieval which allows a client to retrieve information from the database without revealing anything about the nature of the data being queried to the server.

**Network and Data Transmission**

As mentioned earlier, as a growing number of SCADA systems are beginning to implement the standard TCP/IP protocol suite, the shift brings along with it numerous advantages such as an improved ability to design and maintain the communication infrastructure. Unfortunately, there is a tradeoff as the implementation of this commonly used protocol suite also brings its set of disadvantages via exposure through the Internet to malicious attacks. Furthermore, while TCP/IP is more properly suited for the network infrastructure of most enterprises, its “best effort” approach is not enough for SCADA’s strict reliability and timeliness requirements for data delivery. In order for TCP/IP to deliver data to the standard demanded by SCADA systems, significant routing configurations have to be implemented.

To address this situation Avallone et al. (2010) propose a routing mechanism that will both provide for the resiliency requirement for a SCADA communications infrastructure to both node/link failures as well as attacks. The idea proposed by the authors consists of splitting the packets belonging to a data flow onto two node disjoint paths. Avallone et al. (2010) explain that the advantage provided by this technique is that if an attacker has been able to somehow compromise a node, they will still be unable to intercept all of the data packets since the data flow is being split among two nodes. Consequently, the attacker will be
unable to build the entire information flow. Additionally, once the compromised node is identified, all other packets will be re-directed to another node via the splitting technique described earlier—where in this case the splitting is disabled so that traffic can only be directed to a single uncompromised node. Once the compromised node has been controlled and the threat(s) neutralized, the splitting can be re-enabled. In order to handle this sort of traffic re-routing and prioritization, the network infrastructure will need to implement MPLS edge routers. Any potential attacker wanting to attack a SCADA network with this architecture would face the enormous challenge of completing all of the following tasks in order to compromise the network: (1) gain access to traffic flowing across every network path in the MPLS cloud, (2) have awareness of the splitting criterion being used, and (3) be able to identify the set of layered service provider selected to carry a specific traffic aggregate from the ingress to the egress edge of the cloud.

While TCP/IP may have originally been designed to transport data packets in the fastest way possible without any guarantees other than that of a “best effort”, quality of service routing algorithms can be used to minimize jitter, delay, and packet loss among other factors and thus allow the protocol suite to provide the required levels of reliability needed by critical SCADA systems. This routing algorithm would not only compute a path to meet the necessary flow requirements but also simultaneously make the best use of available system resources through network optimization. The shift from serial communications in earlier SCADA systems to using internet technologies and broadband communication is also posing a challenge in planning and operating secured SCADA systems (Khurana et al. 2010). SCADA systems do not typically support any cryptography (Igure et al. 2006) due to unique characteristics of the type of network such as the already mentioned limited computational capacities of RTUs. This makes any communication among RTUs and between RTU and control systems vulnerable to cyber-attacks. With advancement in designing intelligent RTUs, future research can look at the effectiveness of applying cryptography used in regular IT networks into SCADA systems. Even with cryptography, however, key management will be an important issue for research in SCADA data transmission. The reason is that since RTUs are located in isolated places without proper physical protection making any key stored in them an issue (Igure et al., 2006).

**Operating System**

One of the critical software architectures that have enabled widespread deployment of SCADA systems is the operating systems. Two of the dominant operating systems used in SCADA are Linux and Microsoft Windows which have their own set of vulnerabilities (Hentea, 2008). One major source of concern is the massive number of lines of code for an operating system. Recent studies of software reliability estimate that while a Linux kernel may have approximately 15,000 bugs from 2.5 million lines of code, Windows XP has at least double the number of vulnerabilities. Most real-time operating systems (RTOS) are susceptible to DoS (denial of service) attacks. It is critical to establish a robust patching strategy for SCADA operating systems to include rigorous development and testing of these patches and updates prior to their deployment in a production environment. However the availability and timely response requirement of most SCADA makes these systems vulnerable to unpatched vulnerabilities. One suggested solution is to have multiple operating systems integrated into the SCADA system (Fernandez and Fernandez 2005). There is the need for more research in the security of the interaction between the operating systems of the control software and embedded operating system (Igure et al., 2006).

**Standardization**

Most protocols for communication in SCADA systems are Modbus, ICCP and DNP. Modbus as well as ICCP have no authentication built into them making them lack any form of true integrity checking features (Nicholson et al. 2012). There is a drive by OPC Foundation for developing open interconnectivity in industrial systems using open standards. With the birth of 64 bit microprocessor and advances in networking capabilities, most SCADA systems have adopted open system architecture instead of proprietary architecture. Some SCADA systems connect to corporate intranet/internet using TCP/IP which (as mentioned earlier) is known to have numerous vulnerabilities such as spoofing or man in the middle attack. Other more relatively secure protocols such as DNP3 is not currently supported by all vendors. As most vendors begin to use standard protocols this leads to building of systems that are less secured. Future research could look at vulnerabilities due to improper implementation protocols and
those inherent in the protocol itself as well as any recommendation on how to remedy the situation (Igure et al., 2006).

**Trust system architecture**

As the trend in the move toward cloud migration continues, there are those who foresee a future in which an Internet-like utility intranet will be used to manage and control a SCADA network. This framework will allow for more frequent polling between RTUs and the master control station as well as higher and improved bandwidth to accommodate greater data transmissions. Essentially, this utility intranet would harness the scalability of the cloud alongside the flexibility and standardization provided by the Internet to improve upon the grid’s reliability and efficiency.

SCADA systems are typically managed using a trust system architecture which can be defined as a communication security device with a firewall and intrusion detection capabilities which is designed to be used with time-critical network systems (Coates et al. 2010). This type of architecture is useful in a SCADA setting due to the fact that it uses both an active networking architecture. Naturally, since many SCADA systems have many legacy items attached to the infrastructure, piecemeal upgrades are significantly preferred over major hardware upgrade overhauls. In essence, the goal of the trust system is to both intercept and to react to status messages and commands from the network nodes which in turn are transmitting data to the master control station as well as other nodes spread out throughout the network. It is the duty of the trusted system to not only validates any input, but to also identify any relevant risks and bad data along with any necessary alarms or alerts triggered by them.

Applying the typical IT security mechanisms (which focuses on standalone products) does not translate well into the tightly integrated SCADA environment. In reality, what would be more appropriate in this type of setting would be a solution that took advantage of applying the standalone products such as intrusion detection system, firewall, access control list and combined them all into what Coates et al., 2010 refer to as a “coordinated security paradigm.” This arrangement would in turn create an infrastructure where all components are aware of all relevant network activities. The network would become more flexible and adaptive to its environment as would the now application-aware solutions. The following are three distinct forms of implementing the trust system described above into a SCADA system infrastructure: 1) passive mode, 2) half-active mode, and 3) active mode are proposed by Coates et al., 2010. When implemented in passive mode, a trust device is connected to a hub or switch between the SCADA master control station and the rest of the nodes that it controls on the utility’s intranet. In this passive mode, the system examines or sniffs packets as they come across. It saves a copy for analysis and issues an alert if an established security or trust rule violation is detected. The downside to this implementation mode is that it can only detect the malicious packets that it comes across, however it is unable to prevent them from reaching their intended recipient. In the half-active mode implementation, the trust system interacts directly with a separate firewall or router access control list to block further packets by source IP, interface, transport protocol, and message type combinations. In this mode the downside is that this analysis will add some delay and potentially allow one or more malicious packets to be delivered to their destination before other such similar packets are detected and blocked. Finally, in active mode, this implementation is entirely online with all the communication between the SCADA network and any additional communication on the Utility Intranet. This mode is able to block or prevent attacks as they are detected. One of the major disadvantages of this form of implementation is that it has a single point of failure on the communication link; however, if other redundant technologies are implemented alongside this mode this issue can be circumvented.

**SCADA Human Computer Interaction technology**

SCADA applications and their respective user interface presentations have also been evolving over time. The trend in the design of the SCADA system graphic user interface (GUI) is not only for them to offer users more powerful control and cohesive viewing options, but they also need to harness the power offered through rich web-based visualization environment which in turn offers an unbroken integration of control and monitoring systems. A system of this kind could be quickly and easily deployed giving organization’s easy access to their automated processes, controls, alarms, and trends analysis and reporting needs. It also would make it easier of information technology administrators to maintain and integrate information from various distinct sources which would converge in a detail-rich and interactive
digital dashboard. Consequently, operators would be able to more efficiently monitor operational conditions and performance of the distributed SCADA systems and their respective assets all through a single web-browser environment. An additional benefit of implementing this type of solution is that it would provide the company with a fully web-based server/client architecture that would be loosely coupled with distinct operating systems and would also provide easy remote access management to allow for configuration settings and security enhancements (Eduard, V. L., 2010). In fact, this technology is transparent in nature and because of its loose coupling is able to better handle load sharing between the server and clients as well as improve IT administrators’ ability to implement strict security control settings and parameters.

**SCADA survivability**

The traditional intrusion detection systems (IDS) used by enterprise networks do not work as well for SCADA systems due to a lack of information and compatibility across these two distinct systems. One of the biggest encountered issues when trying to design an intrusion detection system for SCADA systems stems from the lack of a comprehensive database of attack signatures. The reason for this being that few if any organizations that have had their SCADA systems compromised are willing to make this publicly known. An additional incompatibility between enterprise IT systems and SCADA systems is that the former are generally secured by a combination of either host based IDS or perimeter based IDS that detect malicious code and viruses. These type of solutions cannot be implemented because they cannot be applied in many of the legacy (and resource limited) SCADA field and embedded devices (Queiroz et al. 2010).

Instead, what the researchers recommend is a system that analyzes the entire system and assesses its survivability potential. Here, survivability is defined as a discipline that focuses on the performance of essential services within a system by analyzing additional components such as security, fault tolerance, reliability, and overall performance. The overall objective of a survivable system is that it is able to ensure essential services and tasks are performed prior to a complete system shutdown. From a quantitative perspective, the researchers define survivability as the ratio between the system performance when under attack and the performance in normal state. Additionally, each of the services is given a specific weight which is determined based on its respective importance. Another measurement to determine is the worst degree of survivability that the system is able to tolerate before ceasing to operate. It is important to establish the service breakdown used for this model: field and enterprise. These services are then further broken-down based on three attributes: operation type, processing capacity, and reliability level. Field services typically require low processing power and hardware resources and as such are deterministic in nature and have a high degree of reliability. Enterprise services, on the other hand, are the exact opposite and their services demand much higher levels of processing power, memory, and faster disks. The tight interconnection between components in a SCADA and the close monitoring of all parts of the system can be carefully managed and the evaluation of these same services will, according to Queiroz et al., (2010), offer the best approach to capturing a snapshot of the system’s current state as well as to detect and possible points of failure. From these weights and values end organizations can then optimize the values and make more informed decisions that will results in improving the robustness and hardening of the system.

SCADA systems encounter two distinct types of faults or errors in their typical day-to-day operations: the first type is called benign faults which are typically due to things such as hardware crashes, power failures, and network disruptions. The second type of encountered fault is referred to as malicious cyber-attacks in which an attacker intentionally targets components on a SCADA system in an effort to cause either a disruption of service or improper reaction through the system. The downtime resulting from either of these types of faults is referred to as the system exhibiting an availability gap—which is a window that leaves the systems vulnerable to downtime. Many improvements have been made in today’s SCADA systems that make them significantly more resilient to benign faults; however, their ability to overcome cyber-attacks is still very much limited. To further complicate matters, since SCADA systems have moved away from the isolated private network and instead share interoperability and connection with enterprise IT networks, isolation is lost which results in them not only inheriting the latter’s security vulnerabilities, but also makes SCADA systems much more vulnerable to an even larger variety of attacks.
In order to address this serious concern, researchers are attempting to not only design, but to also implement and monitor what they refer to as the first “survivable SCADA system”. In this case, the term survivable means that the SCADA system is able to “operate correctly and with minimal performance degradation even if malicious attacks compromise part of the system (Kirsch et al. 2014). Proper shutdown is essential especially for critical infrastructure that utilizes SCADA systems such as nuclear power plants and electrical/utility companies where the inability to properly shutdown or terminate a process can result in the loss of lives as well as significant environmental damage.

To achieve this objective, Kirsch et al., (2014) proposed system employs intrusion-tolerant replication. Essentially, it operates by running in parallel several valid copies of the SCADA master application; however, all of the copies collectively behave as a single logical SCADA Master. This single logical SCADA master provides consistent and timely service as long as “less than a threshold fraction of the copies is compromised.” In this manner, the application is allowed to serve as its own firewall and consequently continues to provide a level of protection even if the system’s security perimeter has been compromised. A graphical representation of this operation is shown below. This system also implements an extra layer of security by introducing diversity to the system by deploying a unique private key for each replica. In this manner, even if an attacker is able to compromise one of the replicas, it will be unable to send any communication without knowledge of its respective private key. Naturally, there will have to be a key management process in place in order to ensure that the keys are not lost or compromised in any way. An additional attractive feature of this proposed solution is that the replicas do not need to have prior knowledge of attack signatures and behaviors in order to provide their guaranteed level of security and service.

**Security Management**

The current security management practices in normal IT operations such as NIST “general accepted principles and practices for securing information technology system” might not be applicable in SCADA environment (Igure et al., 2006). SCADA systems have more emphasis on the availability of the system than other security indicators such as confidentiality and integrity. This leads to more calls for research into developing a metric to assess the security of SCADA network. Some control systems are built to control process without any provisions in place for tracking the processes for future audit purposes. This practice makes carrying out any digital forensics on SCADA systems a challenge since most devices lack persistent memory (Nance et al. 2009). In the event of a security breach, firms are expected to investigate and establish the source and cause of such breaches. Thus, digital forensics in SCADA system is an area needing further research.

Additionally, detecting and preventing attacks on SCADA is very important to avert any financial damage, environmental damage or loss of life. Due to their time sensitive nature and the critical nature of SCADA systems monitoring and control, there is growing interest in further developing and deploying intrusion detection systems that can better alert system operators and prevent any incoming attacks. The use of artificial immune algorithms in a control network to detect patterns, unique features and their distributive nature is on the rise but there are challenges with dynamically generating different immunity cell agents (Cai et al., 2008).

**Security Assessment**

Information system security management is a continuous process requiring satisfying cycle of phases such as risks assessment, policy development, implementation, training and auditing. The assessment phase is the process and results of analyzing assets, identifying vulnerabilities, potential risk, and countermeasures. However, several methods have been developed to automate the risk assessment process ((Montanari et al. 2009 and Ten et al. 2008) but none seem to be able to fully identify all of the vulnerabilities in SCADA system. There is the need to therefore strive to develop a standard metric or series of metrics for the assessment of the security posture of any SCADA system.

**Conclusion**

In this paper, SCADA systems and the factors that determine their successful deployment as well as the vulnerabilities that make the deployment an issue from both the technical and business perspectives have
been outlined. The increased use of SCADA system in numerous areas and industries including critical infrastructure such as in power generation, medical operation and aviation have made them a suitable target for cybercriminals. There is growing threat of cyber warfare after reported attacks on corporate and SCADA infrastructure (Nicholson et. al, 2012). Therefore, nations, vendors and consumers should act in concert to prevent the possibility of any attack. Only a combination of best technological and human practices can make SCADA systems safe. Therefore research should look at architectures of SCADA systems, administrative policies and platform security mechanisms for secure SCADA operation. Some of the identified directions for future research into SCADA include but are not limited to: cryptography and key management for SCADA data communication, protocol standardization, digital forensics in SCADA systems, and finally the development of a security assessment metric or metrics for evaluating and improving upon the security of SCADA networks.

REFERENCES


Shaw, William T., (2006), Cybersecurity for SCADA systems Tulsa, Okla.: PennWell Corp.,