Chapter 9

SECURITY STRATEGIES FOR SCADA NETWORKS

Rodrigo Chandia, Jesus Gonzalez, Tim Kilpatrick, Mauricio Papa and Sujeet Shenoi

Abstract SCADA systems have historically been isolated from other computing resources. However, the use of TCP/IP as a carrier protocol and the trend to interconnect SCADA systems with enterprise networks introduce serious security threats. This paper describes two strategies for securing SCADA networks, both of which have been implemented in a laboratory-scale Modbus network. The first utilizes a security services suite that minimizes the impact on time-critical industrial process systems while adhering to industry standards. The second engages a sophisticated forensic system for SCADA network traffic collection and analysis. The forensic system supports the *post mortem* analysis of security breaches and the monitoring of process behavior to optimize plant performance.

Keywords: SCADA networks, security services, forensics

1. Introduction

Industrial control systems, also known as SCADA systems, typically incorporate sensors, actuators and control software that are deployed in widely dispersed locations. SCADA systems originally employed relatively primitive serial protocols and communications infrastructures to link SCADA components and to transport control and data messages. Also, they favored operational requirements over security because SCADA equipment was physically and logically isolated from other networks.

To increase efficiency, enhance interconnectivity, and leverage COTS (commercial off-the-shelf) hardware and software, most major industrial control protocols now include standards for transporting SCADA messages using TCP/IP. The Modbus-TCP and DNP3-over-LAN/WAN specifications are a clear indication that TCP/IP is becoming the predominant carrier protocol in modern SCADA networks. Meanwhile, TCP/IP is also facilitating interconnections

between previously isolated SCADA networks and corporate information technology and communications infrastructures.

This trend raises serious security issues. Most SCADA protocols were designed without any security mechanisms. Therefore, an attack on the TCP/IP carrier can severely expose the unprotected SCADA protocol. Furthermore, attacks on an interconnected corporate network could tunnel into a SCADA network and wreak havoc on the industrial process [4, 6].

The SCADA community has created standards that adapt information technology security solutions to mitigate risk in industrial control environments. The ISA-SP99 Committee on Manufacturing and Control Systems Security has produced two technical reports [11, 12] and is currently developing an ANSI/ISA standard. The American Petroleum Institute has released a pipeline SCADA security standard API-1164 [3], and the American Gas Association has proposed the AGA-12 [1, 2] standard for cryptographic protection of SCADA communications. The United Kingdom's National Infrastructure Security Coordination Centre (NISCC) has released a good practice guide on firewall deployment for SCADA systems and process control networks [5]. Meanwhile, NIST has produced two documents, a system protection profile for industrial control systems [17] and a guide for securing control systems [21].

When SCADA systems are used in critical infrastructure installations, it is important to consider security requirements and to develop security mechanisms and strategies that conform with industry initiatives and standards [7, 10, 13]. This paper discusses two such strategies for securing SCADA networks, both of which have minimal impact on real-time plant operations. The first involves the deployment of a security services suite for serial and multipoint network links that provides risk mitigation facilities in response to identified risk factors and known protocol vulnerabilities. The second strategy engages a forensic system for the capture, storage and analysis of SCADA network traffic. This system supports the investigation of security incidents and assists in monitoring process behavior and examining trends to optimize plant performance.

2. SCADA Network Architecture

SCADA networks range from small home automation systems to vast, distributed networks used in oil and gas pipelines and electric power distribution. Figure 1 presents a reference SCADA network architecture, which we use to discuss the functional design and interconnectivity aspects of SCADA networks.

A SCADA network comprises two major components, a control center and the plant it controls (Sites A through F in Figure 1). The control center and the plant are connected via a SCADA server to sites that are co-located with the control center or are within a short distance of the control center (Sites A, B and C). Remote sites are often connected to the control center by radio or satellite links, leased telephone lines or even the Internet (Sites D, E and F).

The control center is the hub of SCADA network operations. Its components include human machine interfaces (HMIs), engineering workstations, plant data historians, databases and various shared resources. Control center components

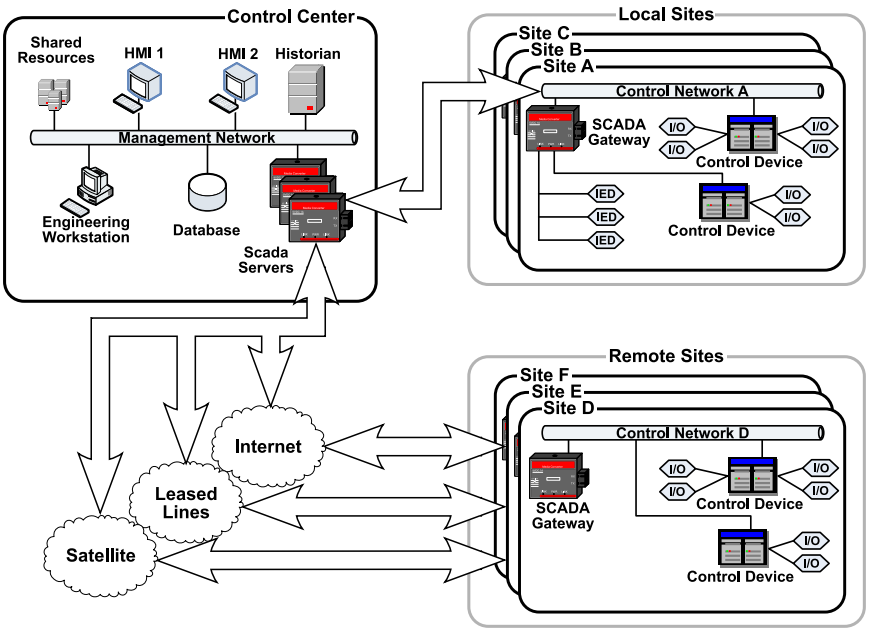

Figure 1. Generic SCADA network architecture.

communicate with each other using the management network, and with the plant (Sites A to F) and other SCADA networks using SCADA servers. Depending on their lower-level protocols, SCADA servers are usually implemented with vendor-specific software and their services are often based on the OPC standard [8].

A control network (e.g., Control Network A) has three types of components: control devices, I/O devices and a SCADA gateway. Control devices, which include programmable logic controllers (PLCs), remote terminal units (RTUs), input/output controllers (IOCs) and intelligent electronic devices (IEDs), implement the process control logic. These devices interface with and manipulate I/O devices (sensors and actuators). Sensors measure specific process parameters (e.g., temperature or pressure). Actuators perform control actions (e.g., open or close a valve) to effect the desired changes to the process parameters.

A SCADA gateway interfaces control network components that cannot communicate directly with the SCADA server. Depending on its functionality, any control device can serve as a SCADA gateway. Special units called front-end processors (FEPs) are commonly used as SCADA gateways in industrial control environments.

Human operators in the control center use human machine interfaces (HMIs) to interact with industrial process systems. Engineering workstation operators, on the other hand, have more authority over the SCADA network; they can reconfigure HMIs and control devices, and modify control algorithms (e.g., ladder logic).

A database housed in the control center records data about process parameters and control actions. Engineering workstation and HMI operators interact with the database to access and modify process data and control variables. Historians archive data about SCADA network activities, including sensor data, control actions initiated by engineering workstation and HMI operators, and management network logs.

The management network contains various shared resources (e.g., printers, fax machines and file servers), but these are typically not considered part of the SCADA network. However, it is increasingly common for corporate networks to interconnect with SCADA networks.

3. SCADA Security Standards

This section outlines the major documents and standards that have been promulgated for SCADA security.

3.1 ISA-SP99 Technical Reports

The ISA-SP99 committee has produced two technical reports on control system security. The first report [11] focuses on security technologies for manufacturing and control systems. It provides a comprehensive survey of electronic security technologies, complemented by usage guidance and security assessments. The second report [12] addresses the integration of security components in manufacturing and control system environments. Elements identified by the first report are used to integrate security in industrial environments using well-defined plans that include requirements, policies, procedures and best practices. The main goal of the report is to provide effective security implementation guidelines for control systems.

3.2 NIST System Protection Profile

In October 2004, NIST released a system protection profile (SPP) for industrial control systems [17], which provides guidance for developing formal statements of functional and security assurance requirements for industrial systems. The NIST document adopts protection profiles as defined by the Common Criteria.

The SPP core specifies functional requirements (login control, role-based access control, data authentication, etc.) and assurance requirements (configuration management, delivery and operation, vulnerability assessment, assurance maintenance, etc.). The NIST SPP also provides guidelines for developing focused protection profiles for various classes of industrial control systems.

3.3 API-1164 Security Standard

The API-1164 Pipeline SCADA Security Standard [3] was released in September 2004. This standard provides guidelines, operator checklists and a security plan template for system integrity and security. The API-1164 standard

provides operators with a description of industry practices in SCADA security along with a framework for developing and implementing sound security practices.

API-1164 guidelines also address access control, communication, information distribution and classification, physical security, data flow, network design, and a management system for personnel. The API-1164 operator checklist is a comprehensive list of measures for evaluating the security status of SCADA systems. Each measure is classified as being required, in-place or not needed. The standard also contains a security plan template that adheres to API-1164 best practices and can be used with minimal modifications.

3.4 AGA-12 Documents

Three weeks after September 11, 2001, the American Gas Association established a working group to recommend protocols and mechanisms for securing industrial control systems from cyber attacks. The working group has produced two documents. The first document, AGA-12 Part 1 [1], addresses policies, assessment and audits. Also, it describes cryptographic system requirements and test planning for security devices. AGA-12 Part 1 requires security devices to comply with NIST FIPS 140-2 (Security Requirements for Cryptographic Modules).

The second document, AGA-12 Part 2 [2], discusses retrofitting serial communications and encapsulation/encryption of serial communication channels. The document describes a session-based protocol with authentication services using symmetric keys (AES and SHA1 are used to implement confidentiality and integrity, respectively). The simple design has minimal impact on latency and jitter and uses sequence numbers to protect against replay attacks. Also, it can encapsulate and transport other protocols, e.g., Modbus and DNP3.

AGA is currently developing Parts 3 and 4 of the AGA-12 documents, which will address the protection of networked systems and the embedding of security in SCADA components.

3.5 NISCC Firewall Deployment Guide

The NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks [5] was developed by the British Columbia Institute of Technology for the U.K.'s National Infrastructure Security Co-ordination Centre (NISCC) in February 2005. It provides guidelines for firewall configuration and deployment in industrial environments. In particular, it describes and evaluates eight segregation architectures from dual-homed computers to VLAN-based network separation. Each architecture is evaluated on the basis of manageability, scalability and security.

The NISCC guide also discusses the implementation, configuration and management of firewalls and other architectural components. Its discussion of future technologies to be used in industrial networks highlights the importance of quality of service, and the need for devices to be aware of industrial protocols.

3.6 NIST SP 800-82 Document

In September 2006, NIST released the first public draft of a guide for SCADA and industrial control systems security (NIST SP 800-82 Document [21]). The NIST document presents a comprehensive treatment of security aspects. In particular, it discusses common system topologies, threats and vulnerabilities, and suggests security countermeasures to be used in mitigating risk. Also, it re-targets management, operational and technical security controls, which were originally specified in the context of federal information systems, for industrial control environments. In addition, the SP 800-82 document discusses other initiatives and efforts focused on developing security best practices for SCADA and industrial control systems.

4. Security Services Suite

We have designed the security services suite as a technical solution for securing industrial networks in accordance with the industry/government standards described in Section 3. The security suite has been implemented in a laboratory-scale Modbus network. It incorporates five approaches that provide security functionality at different levels of the network infrastructure: message monitoring, protocol-based solutions, tunneling services, middleware components and cryptographic key management. The suite also provides security mechanisms compatible with legacy systems, permitting the establishment of trusted and secure communication paths without the need to replace existing equipment.

The five approaches are presented in order of increasing complexity and implementation effort.

4.1 Message Monitoring

The ability to interpret and filter SCADA protocol messages can enhance security while conforming with security standards. The design involves message parsers and a grammar that defines filtering rules and actions to be taken when a SCADA message matches one or more rules in a detection profile.

Message monitoring, which can be implemented in inexpensive field devices, is intended to control traffic directed at specific network components and segments. The monitoring functionality may also be incorporated within RTUs to implement host-based filtering. However, it important to ensure that message monitoring does not impact system performance.

4.2 Protocol-Based Solutions

Security solutions for legacy SCADA systems must conform with protocol specifications and standards. Protocol-based security solutions make this possible by employing standard protocol messages with special codes in unused function fields as the enabling mechanism.

In our prototype implementation, user-defined function codes in Modbus and special data objects in DNP3 are used to convey security-related messages. This

is accomplished by: (i) implementing security functionality via user-defined codes (Modbus [16]) and data objects reserved for future expansion (DNP3 [20]), or (ii) using a subset of the functions currently implemented in field devices.

Regardless of the protocol in use, the two options listed above are abstracted into a security service module placed in the application layer (option (i)) or in the user application layer (option (ii)). Protocol-based solutions allow the implementation of session management, integrity and confidentiality services.

Most industrial control protocols rely on a request/reply mechanism for communication and plant operations. Protocol-based messages extend this mode of operation as the enabling mechanism for implementing challenge-response exchanges and other security primitives. These security primitives serve as building blocks for more sophisticated security services.

Integrity and confidentiality services may be implemented using protocol frames with special fields. These fields contain signatures and, in the case of confidential information, plaintext headers for decrypting data.

The impact on system performance must be considered for both alternatives. For systems where the security module resides in the application layer, incompatibility could occur at the message level if vendors do not use the same semantics for user-defined codes. On the other hand, placing a security module in the application layer only requires field devices to be reprogrammed.

4.3 Tunneling Services

This solution employs simple communication tunnels as wrappers around SCADA protocols to add security functionality in a transparent manner. Note that this approach conforms with methodologies suggested in AGA-12 Part 2 [2] involving secure tunnels with authentication and encryption services over serial links.

Message encapsulation is the primary mechanism for constructing protected tunnels for communicating entities. These tunnels can provide a range of services, including message integrity and confidentiality. Tunneling enables these services to be inserted transparently as an independent layer in field devices or within specialized embedded devices offering services typically associated with gateways.

4.4 Middleware Components

Middleware components provide sophisticated security services in heterogeneous environments. The use of middleware components, which are implemented as protocol sub-layers, differs from the protocol-based and tunneling solutions in that it supports the integration of system components across different networks.

Our approach seeks to develop solutions similar to those provided by IPSec in IP networks. These solutions are integrated at different levels within an

existing SCADA network infrastructure to provide various security services, including authentication, integrity and confidentiality.

The following areas are ideal for applying middleware components as they require sophisticated services in part provided by protocol-based solutions:

- Network access control for SCADA network perimeter defense
- Protocol translation to facilitate device interoperation in heterogeneous environments
- Memory address space mapping to hide internal device memory structure
- Transport and routing of SCADA network packets
- Integration and use of existing information technology security solutions in SCADA networks
- Security, transport and routing for Layer 2 services

4.5 Cryptographic Key Management

Several security services that involve cryptography require efficient key management solutions. Many of the SCADA security standards [1, 12] recognize the importance of key management, but more research is necessary to develop practical solutions.

Creating, distributing, storing and destroying keys without compromising security are challenging tasks. To reduce the risk of key compromise, it is necessary to change keys periodically and to revoke access privileges associated with old keys, which are also difficult tasks.

Consider a fully-connected network of n nodes where a secret key is maintained for each link. As the number of nodes n grows in the fully-connected network, the number of links (and secret keys) increases as n^2. Solutions proposed for addressing this problem include public key cryptography, certificate-based trust chains and special cryptographic protocols that tie the complexity to the number of nodes instead of the number of links. Fortunately, SCADA networks are not fully connected and, in most cases, only the communications between the control center and field devices must be secured (field devices rarely, if ever, communicate with each other). Thus, SCADA network topologies require much smaller numbers of keys and, consequently, involve simpler key management solutions.

We propose three key management solutions for SCADA networks:

- **Hash-Based Key Management:** This solution uses hashing operations for key generation, certification and verification. For example, key generation is performed by hashing the master key specific to a device with other information such as the device ID, timestamp or nonce. In cases where confidentiality is not required, hash values provide integrity guarantees with less processing requirements than other cryptographic primitives.

- **PKI-Based Key Management:** This solution uses a standard PKI that takes into account the unique features of SCADA systems for key lifetimes, and certification revocation list (CRL) verification and distribution procedures. Some of these modifications include making certification lifetimes match the physical maintenance cycles, performing CRL verification sporadically when there is connectivity with the control center, and using normal maintenance operations as opportunities to install new private keys and root certificates.

- **Symmetric Key Distribution:** This solution provides services similar to PKI, except that symmetric key cryptography is used. The prototype implementation uses the Davis-Swick protocol [9] that engages symmetric encryption and symmetric key certificates.

Extending established SCADA protocols (e.g., Modbus) to support the secure transmission and management of keys should be considered as a first approach to minimize system impact. For example, user-defined Modbus function codes could be used to initiate a master secret key exchange protocol to convey cryptographic parameters and handle key expiration and revocation.

5. SCADA Network Forensics

Forensics becomes relevant after a security incident is detected [15]. The goal is to discover the cause of the incident. If the incident is an attack, forensic analysis also seeks to determine the *modus operandi* and identities of the attackers, as well as what went wrong so that the computing system or network can be hardened to prevent future incidents. The following sections describe a forensic architecture for SCADA network traffic collection and analysis [14]. This architecture, which conforms with SCADA security standards, has been implemented in a laboratory-scale Modbus network.

5.1 Role of Forensics

A network forensic system captures and stores network traffic during enterprise operations, and provides data querying and analysis functionality to support post-incident investigations, including incident reconstruction [18, 19]. However, a SCADA network forensics system can also enhance industrial operations [14]. In the context of a SCADA network, the capture and analysis of sensor data and control actions assists in monitoring process behavior and examining trends for the purpose of optimizing plant performance.

Forensics in large-scale information technology (IT) networks is extremely complicated and expensive [18, 19]. On the other hand, SCADA network forensics can be relatively simple. SCADA traffic is routine and predictable, unlike traffic in IT networks, which transport user-generated traffic with complex communication patterns. Traffic uniformity and low traffic volumes in SCADA networks make it possible to log relevant process/control data associated with every message and to subsequently analyze the data in forensic investigations

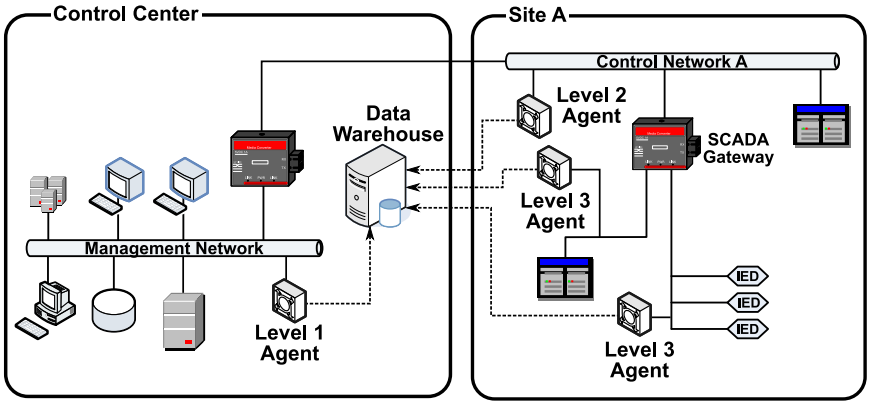

Figure 2. SCADA network with forensic capabilities.

and plant performance evaluations. In fact, our architecture makes use of the regularity of traffic in SCADA networks to minimize the volume of data collected for forensic analysis and incident response.

5.2 Forensic Architecture

Figure 2 presents a forensic architecture that supports the capture, storage and analysis of SCADA network traffic. The architecture employs "forensic agents" at strategic locations within a SCADA network to systematically capture state information and network traffic [14]. These agents forward relevant portions of network packets ("synopses") to a central location for storage and subsequent retrieval. A complete history of SCADA operations may be obtained by the stateful analysis and reconstruction of network events from the stored synopses.

The forensic architecture incorporates multiple agents and a data warehouse. An agent captures SCADA traffic in its local network segment and forwards a synopsis of each packet [18, 19] to the data warehouse. The data warehouse analyzes each packet synopsis and creates a data signature, which it stores along with the synopsis in a storage area designated for the sending agent. The data warehouse also supports queries on the stored data. An isolated network is used for all communications between agents and the data warehouse.

A SCADA network typically has several types of agents. A Level 1 agent is connected directly to the management network. Level 2 agents are located on the control networks. Level 3 agents are positioned downstream from SCADA gateways.

Industrial operations often involve multiple interconnected SCADA networks, which makes it necessary to log traffic across different SCADA networks. This is accomplished by positioning Level 0 agents between SCADA networks and employing a Level 0 data warehouses (not shown in Figure 2). To facili-

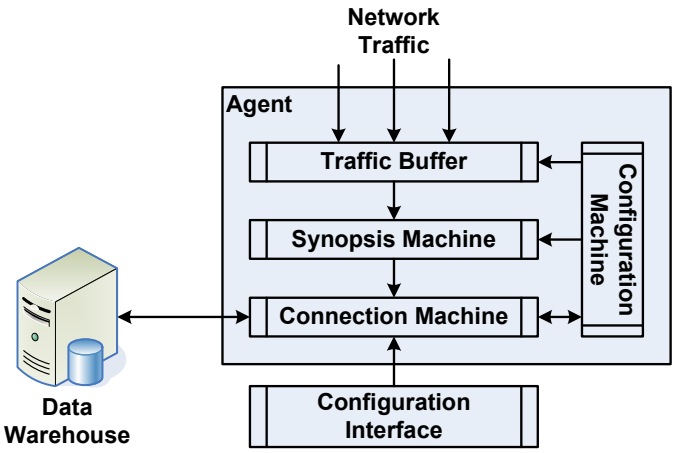

Figure 3. Synopsis generation.

tate robust querying, a Level 0 data warehouse must be connected to the data warehouses of the individual SCADA networks using an isolated network.

5.3 Forensic Agents

Forensic agents capture SCADA traffic and create synopses of network packets that contain information relevant to forensic analysis [18, 19]. An agent incorporates a network traffic buffer, synopsis machine, connection machine and configuration machine (Figure 3).

The traffic buffer stores unprocessed network traffic. It employs a multithreaded implementation of the standard producer/consumer algorithm and a bounded buffer.

The synopsis machine is the core of a forensic agent. It examines packets in the traffic buffer and generates packet synopses according to its configuration rules. Partial synopses are produced for each encapsulating protocol, e.g., agents configured for the OSI model might produce Layer 3 (network) and Layer 4 (transport) synopses. The partial synopses are combined with location information and timestamps to produce synopsis objects that are forwarded to the data warehouse.

The connection machine facilitates communication between agents and a data warehouse. Secure communication is achieved by requiring architectural components to register with an authentication engine. Access control lists (ACLs) are used to implement mutual authentication.

The configuration machine provides mechanisms for regulating agent operation. External devices attempting to configure an agent must be registered with the authentication engine and must use a common configuration interface. Some security settings are similar to those employed in IT networks; others, such as synopsis settings, are unique to this architecture.

Proper configuration of an agent's synopsis engine is important because of its role in the architecture. Two methods may be employed: level-based configuration and manual configuration. The level-based method configures agents according to their location, allowing agents to be configured with pre-defined synopsis algorithms. Agents are configured as Level 0 (between SCADA networks), Level 1 (management network), Level 2 (control network) and Level 3 (behind a SCADA gateway). Pre-defined synopsis algorithms minimize the size of synopses generated by outgoing requests and incoming replies to agents, while increasing synopsis size as agent level decreases (i.e., Level 3 agents have larger packets while Level 1 agents have smaller packets). Manual configuration of agents may be performed to fine tune agent behavior and packet analysis. Synopses contain timing information, but agent and data warehouse timing synchronization is assumed to be handled using methods external to the forensic architecture (e.g., network time protocol (NTP)).

Note that multiple SCADA protocols are often used in industrial environments. Moreover, in addition to standard protocols, e.g., Modbus and DNP3, some environments implement variations of standard protocols or proprietary protocols. The requirement to deal with diverse SCADA protocols has motivated the design of modular agents with configurable synopsis engines.

5.4 Traffic Storage and Querying

Forensic agents submit their SCADA traffic synopses to a designated data repository for storage. The design uses a relational database and query mechanisms to support forensic investigations. The traffic storage and querying facility incorporates a connection machine, data buffer, analysis machine, storage machine, query interface, query processor and agent configuration interface (Figure 4).

The connection machine supports communications between data warehouses and registered agents. Connections between a data warehouse and registered agents are used to receive synopses and configure agents. Connections to other data warehouses facilitate the processing of queries that span multiple SCADA networks.

Synopses submitted by agents for storage are placed in the data buffer and passed to the analysis machine using a producer/consumer algorithm. The analysis machine creates signatures associated with synopses that are used for event reconstruction and for analyzing and correlating SCADA traffic patterns. Signatures reduce storage requirements while maintaining forensic capabilities. For example, if a PLC communicates with certain field devices, only those device addresses must be stored and associated with the PLC. The corresponding device-based signature is generated by correlating synopses from all the agents that observe traffic associated with the PLC.

Pattern analysis capabilities may be developed for the forensic architecture. For example, PLCs often execute repetitive control loops with well-defined communication patterns. These patterns can be analyzed to produce network-based signatures for forensic investigations and anomaly detection.

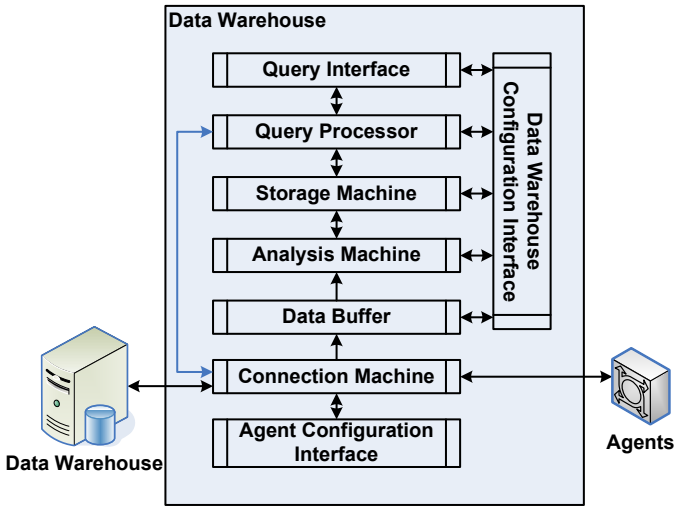

Figure 4. Traffic storage and querying.

The storage machine uses hash tables and a relational database. Each registered agent has a set of hash tables, which are used to index repetitive signature data associated with an agent. For example, partial synopses generated during communications between two devices with largely static-address-oriented data need not be stored more than once. Instead, a pointer to the entry is used as the signature (stored in the database) for identifying the communication. The number of tables associated with an agent depends on the types and quantity of synopses generated by the agent.

The query interface supports incident reconstruction, system checking and process trend analysis. The interface provides two SQL-based querying mechanisms. One uses a GUI and pre-defined options for routine analysis. The other provides a console that gives analysts more freedom to specify queries. Results are presented in reports augmented with graphical information about the SCADA network, including its component systems, devices and agents.

The query processor fields queries received from a local query interface or from another SCADA network via the connection machine. The processor determines whether or not the resolution of the query involves information from another SCADA network. If this is the case, a query is sent to the appropriate data warehouse, which in turn dynamically generates and processes a query whose response is returned to the sender.

6. Conclusions

The security strategies discussed in this paper are promising because they balance assurance and performance while adhering to SCADA protocols and standards. The security services solution can be systematically integrated into process control networks as part of a risk management process without nega-

tively impacting plant operations. The forensic solution supports investigations of SCADA security incidents as well as process trend analysis and optimization. Both solutions are flexible and scalable, and are capable of handling multiple protocols and interconnected SCADA networks.

Acknowledgements

This work was partially supported by the Institute for Information Infrastructure Protection (I3P) under Award 2003-TK-TX-0003 from the Science and Technology Directorate of the U.S. Department of Homeland Security.

References

[1] American Gas Association, Cryptographic Protection of SCADA Communications; Part 1: Background, Policies and Test Plan, AGA Report No. 12 (Part 1), Draft 5, Washington, DC (www.gtiservices.org/security/AGA12Draft5r3.pdf), 2005.

[2] American Gas Association, Cryptographic Protection of SCADA Communications; Part 2: Retrofit Link Encryption for Asynchronous Serial Communications, AGA Report No. 12 (Part 2), Draft, Washington, DC (www.gtiservices.org/security/aga-12p2-draft-0512.pdf), 2005.

[3] American Petroleum Institute, API 1164: SCADA Security, Washington, DC, 2004.

[4] M. Berg and J. Stamp, A reference model for control and automation systems in electric power, Technical Report SAND2005-1000C, Sandia National Laboratories, Albuquerque, New Mexico, 2005.

[5] British Columbia Institute of Technology, Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks, National Infrastructure Security Co-ordination Centre, London, United Kingdom, 2005.

[6] E. Byres, J. Carter, A. Elramly and D. Hoffman, Worlds in collision: Ethernet on the plant floor, *Proceedings of the ISA Emerging Technologies Conference*, 2002.

[7] E. Byres, M. Franz and D. Miller, The use of attack trees in assessing vulnerabilities in SCADA systems, *Proceedings of the International Infrastructure Survivability Workshop*, 2004.

[8] E. Byres and T. Nguyen, Using OPC to integrate control systems from competing vendors, *Proceedings of the Canadian Pulp and Paper Association Technical Conference*, 2000.

[9] D. Davis and R. Swick, Network security via private key certificates, *Operating Systems Review*, vol. 24, pp. 64–67, 1990.

[10] J. Graham and S. Patel, Security considerations in SCADA communication protocols, Technical Report TR-ISRL-04-01, Intelligent System Research Laboratory, Department of Computer Engineering and Computer Science, University of Louisville, Louisville, Kentucky, 2004.

[11] Instrumentation Systems and Automation Society, Security Technologies for Manufacturing and Control Systems (ANSI/ISA-TR99.00.01-2004), Research Triangle Park, North Carolina, 2004.

[12] Instrumentation Systems and Automation Society, Integrating Electronic Security into the Manufacturing and Control Systems Environment (ANSI/ISA-TR99.00.02-2004), Research Triangle Park, North Carolina, 2004.

[13] D. Kilman and J. Stamp, Framework for SCADA security policy, Technical Report SAND2005-1002C, Sandia National Laboratories, Albuquerque, New Mexico, 2005.

[14] T. Kilpatrick, J. Gonzalez, R. Chandia, M. Papa and S. Shenoi, An architecture for SCADA network forensics, in *Advances in Digital Forensics II*, M. Olivier and S. Shenoi (Eds.), Springer, New York, pp. 273–285, 2006.

[15] K. Mandia, C. Prosise and M. Pepe, *Incident Response and Computer Forensics*, McGraw-Hill/Osborne, Emeryville, California, 2003.

[16] Modbus IDA, MODBUS Application Protocol Specification v1.1a, North Grafton, Massachusetts (www.modbus.org/specs.php), 2004.

[17] National Institute of Standards and Technology, System Protection Profile – Industrial Control Systems v1.0, Gaithersburg, Maryland, 2004.

[18] K. Shanmugasundaram, H. Bronnimann and N. Memon, Integrating digital forensics in network architectures, in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, New York, pp. 127–140, 2005.

[19] K. Shanmugasundaram, N. Memon, A. Savant and H. Bronnimann, Fornet: A distributed forensics system, *Proceedings of the Second International Workshop on Mathematical Methods, Models and Architectures for Computer Network Security*, 2003.

[20] M. Smith and M. Copps, DNP3 V3.00 Data Object Library Version 0.02, DNP Users Group, Pasadena, California, 1993.

[21] K. Stouffer, J. Falco and K. Kent, Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security – Initial Public Draft, National Institute of Standards and Technology, Gaithersburg, Maryland, 2006.