A Trust System Architecture for SCADA Network Security

Gregory M. Coates, Kenneth M. Hopkinson, *Member, IEEE*, Scott R. Graham, *Member, IEEE*, and Stuart H. Kurkowski, *Member, IEEE*

***Abstract*—This paper discusses the use of a communications network security device, called a trust system, to enhance supervisory control and data-acquisition (SCADA) security. The major goal of the trust system is to increase security with minimal impact on existing utility communication systems. A previous paper focused on the technical operation of the trust system by augmenting routers to protect User Datagram Protocol (UDP)-based traffic. This paper concentrates on placing the trust system into a broader context, creates new trust system implementations to increase its flexibility, and demonstrates the trust system using TCP traffic. Specifically, the article expands on previous work in the following ways: 1) the article summarizes major threats against SCADA systems; 2) it discusses new trust system implementations, which allow the trust system to be used with a wider array of network-enabled equipment; 3) it discusses key SCADA security issues in the literature and shows how the trust system responds to such issues; 4) the paper shows the impact of the trust system when widely prevalent TCP/IP network communication is used; and 5) finally, the paper discusses a new hypothetical scenario to illustrate the protection that a trust system provides against insider threats.**

***Index Terms*—Computer network security, computer networks, power system security, supervisory control and data-acquisition (SCADA) systems.**

I. Introduction

A TRUST system is a communication security device, with firewall and intrusion detection capabilities, designed for use with time-critical network systems [3]. A trust system can perform at or near the real-time requirements that the supervisory control and data acquisition (SCADA) network requires even with the overhead of TCP/IP and UDP/IP communications, Internet Protocol Security (IPSec) encryption, firewall rules, format check, and access control functions. The goal is to both enhance security in traditional systems and to facilitate information sharing between regional utilities. A final consideration is whether a gradual upgrade path exists for a SCADA network. A secure system that requires that all existing devices be replaced is unlikely to be implemented in existing utilities. The trust system uses an active network routing architecture to allow utilities to add it to key inter-domain or backbone communication systems without requiring that the upgrades be done all at once.

The research described in this article extends previous trust system work in a number of key ways. First, previous work concentrated solely on the technical aspects of the trust system. This article tries to place it into a broader system or systems context by describing utility concerns that have appeared in the literature followed by a discussion of how the trust system can help address such concerns.

The article also expands the scope of the trust system. Earlier work concentrated on the trust system's use in communication between utilities, such as in the Wide Area Measurement System in the Western United States. Our new research concentrates on the trust system's use within utilities, by strengthening SCADA security and other protection and control communication using next-generation equipment such as that conforming to IEC 61850.

With the shift to IP-standards and common control system operating systems (e.g. Windows, Linux, UNIX), SCADA systems are becoming more vulnerable to both skilled and amateur attackers familiar with IP-based exploits, techniques, and attack tools downloadable from the Internet [4]. With Utility companies using more commercial off-the-shelf (COTS) components, their networks will increasingly resemble modern IT networks. The trust system uses leading IT security mechanisms and standard IP protocols while meeting SCADA needs, such as the need to allow increased cooperation and information sharing in protection and control systems without disrupting their operation. To illustrate this, one of the two new experimental scenarios concentrates on the trust system's ability to guard against insider threats.

The original trust system only had an active mode router-based implementation. This article introduces passive mode, half-active mode, and tunnel/gateway mode trust systems to greatly add to the range of situations where security can be added to existing SCADA systems. The new trust system implementations allow firewall and intrusion detection security to be embedded through tunneled connections when SCADA traffic must pass through the Internet or other unsecured networks. Passive and half-active implementations also allow for trust systems in environments where router replacements or direct modifications are not possible.

Finally, earlier trust system work concentrated on its ability to minimally impact UDP-based utility traffic. Given its prevalence, a new experimental scenario looks at the performance impact of the trust system using TCP/IP. New results show that the

Manuscript received December 03, 2008; revised July 06, 2009. First published December 08, 2009; current version published December 23, 2009. The views expressed in this document are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government. Paper no. TPWRD-00867-2008.

The authors are with the Department of Electrical and Computer Engineering, Air Force Institute of Technology, Wright-Patterson Air Force Base, OH 45433-7765 USA (e-mail: gregory.coates@afit.edu; kenneth.hopkinson@afit.edu; scott.graham@afit.edu; stuart.kurkowski@afit.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TPWRD.2009.2034830

TABLE I
SOURCES AND MOTIVATIONS FOR UTILITY DISRUPTIONS AND ATTACK [1]

Source	Reason
Industrial sabotage or theft	Financial advantage in insider trading or competing vendor partnerships
Concentrated physical and cyber attack	Destruction, terror, or activism
Vendor compromise	Easier to target the supplier than the defended infrastructure itself [2]
Technical design error or environmental influence	Hardware or code; network design, installation and configuration; or interferences from other technologies in the environment
Natural disasters	Earthquakes, tornadoes, volcanoes, fire, thunderstorms, and snow storms
Operator error	Misjudgment, misconfiguration, or failure to remember operational details, resulting in dangerous or costly results

trust system introduces minimal delay with TCP. This is fortunate since previous studies have shown that TCP is particularly sensitive to delay and packet loss [5].

II. LITERATURE REVIEW

A. Supervisory Control and Data-Acquisition Overview

SCADA central or distributed system that monitors and controls a single site or one spread out over a long distance [6]. SCADA systems are found throughout the public utility industry and are integral to operation of critical infrastructure including oil and gas pipelines, electric power generation facilities and transmission grids, and air traffic control towers [2], [7]. Due to the mission critical nature of SCADA systems, attacks could result, directly or indirectly, in massive financial and sensitive data losses, facility destruction, or loss of life.

B. Threat to Utility Operations

1) Threat Sources: Potential sources for cyber attacks and operational disruptions to SCADA systems are listed in Table I.

2) Specific Threats: Theoretical scenarios abound; however, many businesses and engineers are incredulous or simply lack the resources or technical expertise to plan and maintain security upgrades that might reduce profits or affect performance. There is also an "if it ain't broke, don't fix it" mentality that can be found when modifying control system operations and cyber security implementations. The security threats to power SCADA systems are wide-ranging and include outdated or misapplied security patches, electronic access lockouts, malicious code, denial of service attacks, data and control message spoofing, and unauthorized access or data sniffing [8].

3) Open Source Intelligence: There is often an assumption that legacy SCADA systems, which do not conform to common standards, have security through obscurity. Even for legacy control systems, the knowledge to cause a widespread power blackout is readily available on the Internet, where SCADA vendor websites post manuals, software, and source code for major applications [9]. It has been found that "over 90% of major SCADA and automation vendors have all of their technical manuals and specifications available on-line to the general public" [9].

Many corporate websites list training materials and operating manuals, vulnerabilities, firewall policies, network diagrams, configuration files, and protocol documentation [9].

4) Real-World Incidents: There have been several real-world incidents affecting SCADA systems, and many others never publicized, that clearly illustrate critical infrastructure vulnerabilities [2].

1) During the Cold War, the U.S. provided Trojan firmware to the Soviet Union, causing a pipeline to explode in one of the world's largest non-nuclear explosions [2]. SCADA software, hardware, or firmware can be maliciously produced and sold to U.S. companies by foreign or domestic entities with the intent to destroy the power supply to a region.
2) In 2001, hackers hacked CAL-ISO, California's primary power grid operator, and were not discovered for 17 days [7].
3) In 2003, the Slammer Worm took Ohio's Davis-Besse nuclear plant safety monitor offline for five hours [2].

Cyber attacks have the potential to affect supplies of gasoline, electricity, or water, impacting global stock prices.

C. Changes in the SCADA Environment

The restructuring of the utility industry has increased competition while driving the need for more efficient operations and better utility coordination. The first element of restructuring is regulatory. Power grids, historically, were centrally controlled. Regulatory changes now encourage independent ownership of generators and favor competitive mechanisms for bilateral or multilateral power generation contracts. The second element involves changes in the large-scale operation of the grid. In the past, this was a centralized task. In the restructured climate, competing power producers must coordinate their actions through independent service operators. Restructuring has occurred incrementally. In its earliest stages, large utilities that might have owned beginning-to-end power production and delivery were broken into smaller companies with typically specialized roles in only generation, transmission, or distribution. At the same time, there have been a growing number of long-distance contracts.

D. Current State of SCADA System Protection

The old paradigm was to install a system, run it unattended, and replace it in five years or more. For newer PC-based systems, utilities have to cope with more dynamic operating procedures and financial planning (i.e. install a system, patch it weekly, perform backups and virus scans, upgrade or replace incremental capabilities each year, and train personnel) without impacting 24/7 operations or profits [2].

On the positive side, the SCADA constituency is becoming increasingly aware of their systems' vulnerabilities and there

is increased emphasis on SCADA information systems security. Standards organizations are developing guidelines for the security of SCADA systems. National laboratories have established SCADA test beds to evaluate the most effective security measures. Organizations such as the National Institute of Standards and Technology (NIST) have initiated programs focusing on SCADA security [8]. The negative side is that these measures have not been universally applied due to a lack of funds, management apathy, or other competing issues [8].

Conventional IT security approaches generally focus on standalone products (i.e. firewalls, IDSs, router ACLs, etc.) associated with individual network devices. This point-oriented approach is vulnerable to attacks that circumvent the one particular security control. In addition, other parts of the network might be unaware of an attack. A coordinated security paradigm is needed that takes advantage of the capabilities of devices such as routers that are cognizant of large-scale network activities. What is necessary is to develop adaptive network and application-aware solutions that address security as a collaboration of defense mechanisms operating as a system to identify threats and respond accordingly [8].

The future power grid will begin to support higher levels of integration and federated systems services [10]. The trust system concept supports the goals for current and future SCADA systems. These goals include the ability to be self-healing, dynamic, predictive rather than reactive, distributed in terms of the assets and information, able to integrate with legacy systems, and to increase system security [1], [8], [10].

III. Trust System

A. A Future Utility Intranet

Many researchers anticipate that an Internet-like Utility Intranet dedicated to the power grid and mostly isolated from the public Internet, will emerge in the future [4]. SCADA is likely to migrate to a Utility Intranet is due to the higher polling rates that will be possible with the increased bandwidth available in the new network [5]. Given the stricter response thresholds of SCADA systems, securing this new environment presents an extreme challenge where connections to the Internet (whether known or not) are almost certain to exist, providing a tempting avenue for cyber attacks.

The power industry is turning towards next-generation communications systems to meet the increased demands on the power grid. These standards point toward the future adoption of a private Utility Intranet based on Internet technology to improve the grid's efficiency and reliability. The Utility Intranet is likely to begin as an effort to improve upon the monitoring, protection, and control of individual utilities and to then to connect between utilities over time. The introduction of a Utility Intranet has many potential benefits such as increased information sharing, greater protection and control of the grid, and the enhanced ability to share power in complex situations such as bilateral load following. However, care is needed to ensure that network capacities, communication protocols, security, and quality of service (QoS) are managed to meet utility requirements [5].

Traditionally, SCADA systems and corporate IT systems have focused on very different information assurance priorities. Whereas IT system priorities are confidentiality, authentication, integrity, availability, and non-repudiation, SCADA systems emphasize reliability, real-time response, tolerance of emergency situations, personnel safety, product quality, and plant safety, usually to the exclusion of any security mechanism that might hinder these.

Now, with the compatibility and overlap of the two networks, both SCADA and corporate IT will have to develop complementary security models. Current issues such as dial-in modems connected to one system compromising the other, the possibility of unprotected, rogue corporate Internet connections exposing the SCADA network, the real-time deterministic requirements of SCADA systems, and 24/7 operations require deconfliction of the disparate cultures of SCADA and IT [8]. A good example of this is the routinely scheduled downtime for IT organizations to upgrade, patch vulnerabilities, perform backups, and so on [8]. Such downtime cannot be tolerated for most SCADA systems [8].

Throughout this transition to a Utility Intranet, SCADA system networks must be well defended yet maintain the same level of service required by their customers [7]. Blindly layering standard IT security mechanisms on top of SCADA networks will not work without accounting for their unique requirements and time constraints. therefore, it is important to first understand current and future SCADA architectures and operational philosophies.

B. Trust System Concept

1) What the Trust System Is: The concept of a trust system is to provide a non-proprietary system, system of systems, or software agents that plug into an existing network, somewhat transparently, to perform the functions of correlating data and identifying risk levels for corresponding events and status updates that point to negative impacts on utility services. The core of the trust system is a software agent performing active security analysis and response. In a network where nodes have sufficient unused hard drive capacity, memory, and processing power, the agent would be loaded directly onto the node and provide an active interface between incoming messages and the node's code, data, and applications, similar to other software firewalls.

2) What the Trust System Does: The trust system intercepts and reacts to status messages and commands from network nodes destined for the master control station and other nodes in the network. For companies with some legacy SCADA nodes and other types of communicating equipment, this would require protocol gateway plug-ins for the trust system to interpret and analyze packets delivered in different protocols and formats.

The trust system validates input, identifies risks and bad data, and initiates appropriate alerts. It then assigns data types for the good data elements in each packet. It next determines if the recipient is authorized to read all of the data types in the message, especially when the recipient is external to the company. If the message is not authorized, the system sanitizes the parts of the message that are not allowed to be passed to the recipient or it simply deletes the message. Finally, the good data elements

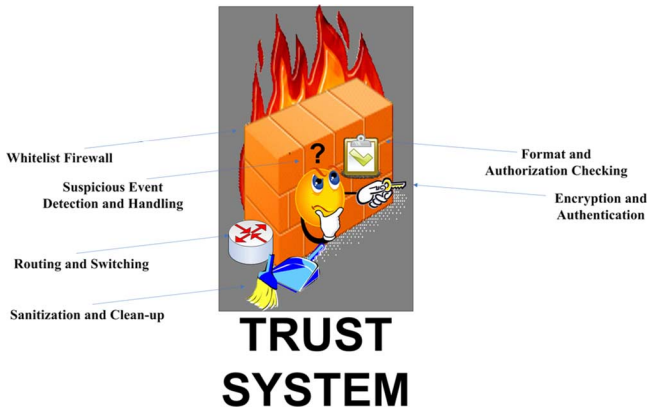

Fig. 1. Trust system logo with capabilities summary.

(i.e. those that pass all checks) are transferred to database systems for archiving for historical and trend analysis and then it is passed to intranet display. The data that gets archived is viewable and accessible by someone with appropriate privileges. The SCADA network should never be connected to other company networks if possible.

IV. Trust System Implementation

A. *Flexibility in Implementation*

The trust system can be implemented in a variety of ways. This is one of the main strengths of the trust system as most current legacy SCADA do not have the hardware to support software agents. Furthermore, the trust system can be implemented, depending on the current architecture and needs, without jeopardizing existing control functions.

Since every utility company's network will be different, each individual company must perform its own individual network needs assessment and simulation to determine security and financial feasibility to identify weak points and points of failure in its own network design. It is then up to that company to implement the best network design with the level of redundancy and defense-in-depth that is economically feasible and corresponds to due diligence in protecting national infrastructure and utility services. The trust system's cost-effective, modular acquisition and employment options are well suited for meeting a wide range of implementation requirements. A logo and summary for the functions supported by the trust system is depicted in Fig. 1.

1) Passive Mode Implementation: In passive mode, a trust device is connected to a hub or switch on the link between the SCADA master control station and the nodes it controls between the company's SCADA network and its outgoing connection to the rest of the Utility Intranet, as depicted in Fig. 2. The passive trust system sniffs packets as they pass by, saves a copy to analyze, and alerts if a security or trust rule has been or may potentially be broken. The advantage of passive mode is that the trust device is not in-line with the communications, so a failed trust system does not block the communications link. A disadvantage is that the trust device can only report malicious packets it detects. It cannot prevent them from reaching the intended recipient.

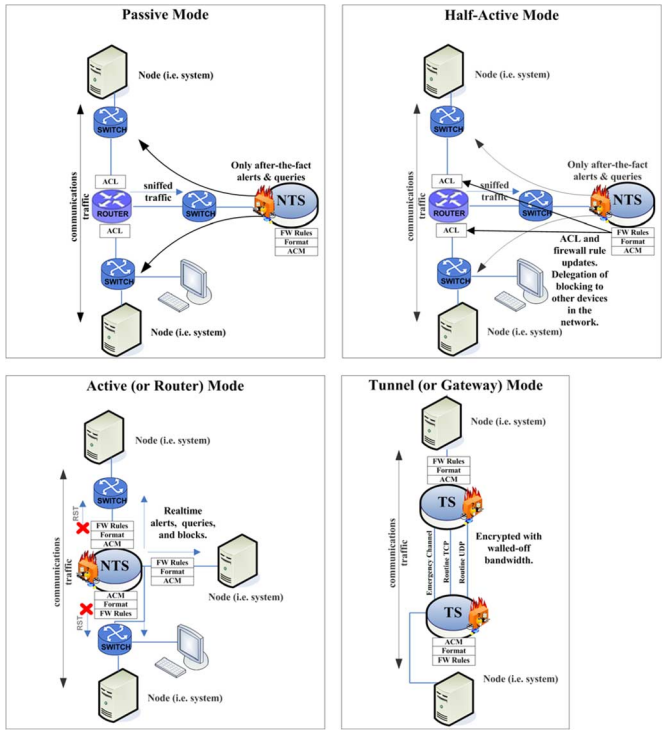

Fig. 2. Trust system modes and configuration options.

2) Half-Active Mode Implementation: A way to implement blocking with a passive mode implementation is for the trust system to interact with a separate firewall or router access control lists (ACL) to block further packets by source IP, interface, transport protocol, and message type combinations. The advantage is that passive monitoring is combined with a way to halt malicious traffic. The disadvantage is that there will still be some delay and a chance that one or more malicious packets will be delivered to their destination before other similar packets are blocked.

3) Active Mode Implementation: The article's experiments used a trust system in active mode to show its blocking functionality. A trust system is in active mode when hardware is inline with all of the communication between the SCADA network and any connections to the rest of the Utility Intranet, as shown in Fig. 2. This device may be a specialized trust box or a trust-enabled router which is also responsible for routing all packets on the link. One of this design's strong points is that it is able to block attacks and other potentially harmful packets as they are detected. An attack is blocked when a "denied" entry is added to the firewall rules or a lowered trust level and effective Access Credentials Control Number (ACCN) is set for a specific user. One of the disadvantages to active mode is if there is a single point of failure on a link, the trust system fails, but this can be alleviated with alternate or redundant routes.

4) Tunnel (or Gateway) Mode Implementation: In case some nodes cannot be loaded with nodal trust agents or afford the CPU cycles for encryption, the trust system may be implemented in either passive or active *gateway mode*, as depicted in Fig. 2. In gateway mode, trust system boxes or routers provide firewall and other security features for the nodes behind them. They also create an encryption gateway between themselves to pro-

tect communications between trust systems. This mode can also be called *tunnel mode*, since IPsec would be implemented in IPsec tunnel mode. The advantage of the Tunnel implementation is that traffic can be protected and encrypted when traveling outside of a utility's network. Malicious traffic must also pass through the trust system whenever entering from outside the utility network. The disadvantage is that tunneling between trust systems adds overhead and delay for packet encryption and decryption.

B. Real-World Applications of the Trust System: Intercompany and Interarea Protection

While not the norm in present day SCADA architectures, a Utility Intranet can make possible unprecedented situational awareness between utility companies, control and engineering centers, and neighboring utility control areas. Sharing of automatic status updates will enable near-real-time situational awareness for trusted ISOs, control authorities, and reliability coordinators who can, in turn, direct actions to prevent catastrophic overloads or underloads and ensure equity of resources within their areas of responsibility and oversight.

The trust system, when placed at strategic locations such as connections between adjacent utility companies, outgoing connections from utility companies to area control and engineering centers, ties lines between control and transmission areas, specifically between control centers, engineering centers, and between reliability coordinators in different ISOs provides low-cost network security to traditional SCADA networks with their mix of legacy, proprietary systems and protocols and newer standards-based solutions. Fig. 3 illustrates the fact that the trust system can be arranged in both master-slave, which would be typical within utilities, as well as in peer-to-peer arrangements, which would be likely in communication systems connecting utilities together. Obviously, an understanding of appropriate and inappropriate information flows (e.g. who, what, when, where, and how) is critical to network security planning and design in general but more so in the design and configuration.

Just as status updates in electric power utilities are sent from field equipment via Intelligent Electronic Devices (IEDs), Remote Terminal Units (RTUs), or Programmable Logic Controllers (PLCs) and on to SCADA master control stations every few seconds, either the same updates, a subset of those updates (i.e. only significant changes from the previous update), or a summary report can be easily forwarded on to connected control area authorities and adjacent electric utility companies on the Utility Intranet. When substation automation applications do not support this forwarding, the trust system can be configured to initiate this on their behalf whenever it sees a qualifying message cross its path.

Situational updates shared between adjacent utility companies will facilitate automatic recognition of changing conditions that might affect their levels of generation or transmission. Neighboring companies that receive reliable status updates will have earliest warning of creeping load changes versus current power generation levels. Early warning and impact assessment will prompt timely decisions on the right combination of load shedding and generation adjustment necessary to compensate

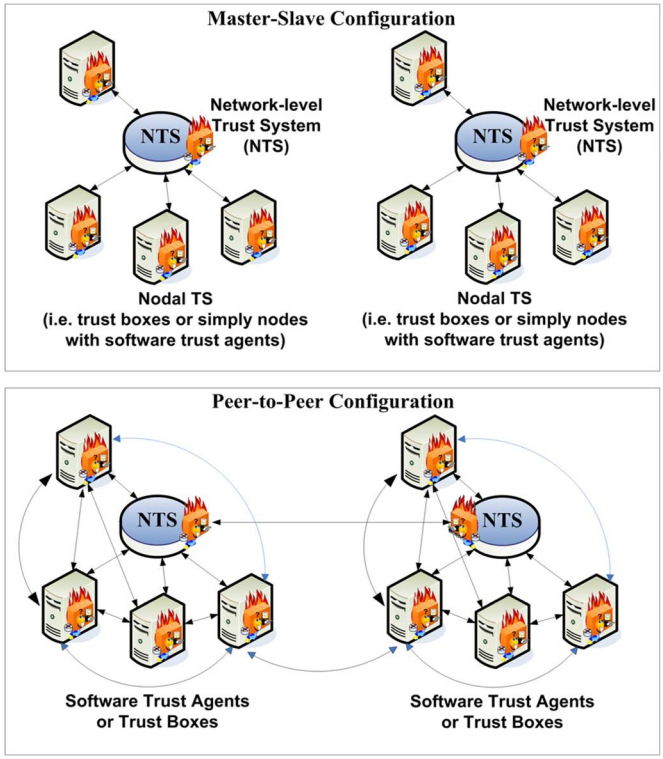

Fig. 3. Trust system configurations.

for rapid changes in power flows from adjacent companies. This will aid private companies in preserving service to their own customers while preventing blackouts, alleviating the associated financial costs, and loss of public trust that can result from outages.

Monitoring systems in neighboring utility company operations centers can then automatically update their operational picture with a wider perspective of power capabilities and emergencies in the immediate area while area controllers, ISOs, and reliability coordinators would have a complete picture of currently segmented utility operations owned by private companies. Control areas can forward area-wide status updates and emergency notifications to a regional utility operations center and to their adjacent area operations centers for improved regional situational awareness.

The trust system can facilitate this message forwarding right now between utility company networks and control areas for which numerous existing SCADA applications do not cooperate in this manner. When the trust system inspects and then reassembles a packet, it can check its own access control matrix (ACM) for the list of recipients external to the company network who are authorized to receive that message type, translate the message into a new packet with the proper format understandable by those receivers, and then forward the original message internally, as normal, and the new message to those external destination IP addresses.

In the event of a neighboring company noticing a spike or increasingly dangerous situation, in what amounts to a macroscopic version of the local neighbor_trip, backup_trip, and intertrip messages that are proposed to occur through embedded software agents within a single company, a similar trip message

might be generated from an adjacent neighbor company to ensure the owning company is aware of the impending emergency and can approve or disapprove the requested action, even if its own systems are malfunctioning.

The Northeast Blackout of August 14, 2003, the largest blackout in North American history, illustrated this very scenario. Due primarily to malfunction, accidental shutdown, and internal miscommunication, systems failed to report problems to the control center within one company, which later denied any need for concern when it received phone calls from a neighbor company warning they had indications of abnormal readings along their shared borders of the transmission grid [11]. The controllers continued to operate, blind to the actual situation, for hours before the cumulative affect (there were also power lines that had sagged in the heat to where they contacted overgrown trees) created a system-wide point-of-no-return. A series of cascading transmission line outages traveled through Ohio, around the Great Lakes in Michigan, through Canada, and into New York State in only ten seconds [5]. Once it began, the blackout that cascaded from Cleveland to the Northeastern United States took just seven minutes [5]. Nearly 10 million people in the province of Ontario (one-third of the Canadian population) and 40 million people in eight U.S. states (one-seventh of U.S. population U.S.) were without power. The financial losses due to the outage were estimated between $4 and $10 billion [11].

In a highly reliable and secure environment, trip messages from one company to another, especially from a trusted partner that has the interests of both companies at heart, might be trusted to automatically trip breakers in another company. This would require a complete culture change from the way electric utilities are currently operated. Today such company-to-company initiated actions would likely be rejected for fear of false trips due to technological or human errors, outside hackers/crackers/attackers, or corporate sabotage/espionage. This is where the trust system will assist in validating traffic and providing assurance to utility managers.

Those companies hesitant to allow automatic actions to their systems by neighbor companies would be more amenable to the option to approve or deny the trip requests first or to allow neutral ISOs and reliability coordinators the ability to send commands to company SCADA systems or breakers in reaction to a growing power outage seen within their control area. It is also conceivable that the control area authorities that recognize such a situation could contact the company to direct actions and, if granted proper permissions, initiate breaker trips remotely when the required reaction time does not allow for coordination. Either way, shared electronic status readings are more credible than word of mouth, and a master control station receiving conflicting reports from its own substations. The neighbor's control center could alarm to warn the operator and would have prevented the 2003 blackout.

In the future, security mechanisms, such as those investigated in the trust system simulations, when layered over ever-increasing bandwidth and connectivity between utility organizations, would enable the creation of regional utility operations (or control and security) centers. These centers could ensure power-grid integrity and fair use. Centers could also provide utility-specific capabilities for network security responses, technical assistance, and could serve as law enforcement liaisons within their regional spans of control.

V. Specific Challenges to SCADA Security and Recommended Solutions

A. Per-User Authentication and Access Control

1) SCADA Security Issues: In the SCADA environment, a control operator might need to enter a password to gain access to a device in an emergency. If the operator types in the password incorrectly a few times, a conventional IT security paradigm will lock out the operator. Locking out the operator can lead to disaster in real-time control environments [2].

Many SCADA systems require no authentication at all. When user accounts do exist, username and password information is almost always sent in the clear in both human-to-machine and machine-to-machine applications [2]. In practice, SCADA systems or consoles tend to be configured with the same username and password or with standard defaults, such as console, administrator, or anonymous.

Remote terminal unit (RTU) test sets, to issue commands to RTUs, are commonly available on the market. The systems do not authenticate and have little to no data validity checking.

2) Recommendations From Literature: For operators on local control devices, passwords might be eliminated or made extremely simple [8]. In situations where the passwords might be subject to interception when transmitted over networks, encryption should be considered to protect the password from compromise.

Access controls should be implemented for all SCADA systems. Role-based access controls might be used at the supervisory level of SCADA operations [8].

In addition, access might also be restricted based on two-factor authentication and digital certificates or challenge-response tokens [8]. Options include biometrics, smart card identification, and other authentication technologies.

Procedures should be implemented to monitor access controls for authorized access, un-authorized access, and unsuccessful un-authorized access attempts.

3) Objections and Questions From Utilities: Biometrics are not completely reliable. There may be many false rejections or false acceptances. Issues are possible with throughput, human factors, or system compromises.

Given SCADA's real-time nature, could password policies prevent lockout in emergencies? How would rights be managed for people with multiple, changing roles?

It is costly to keep ACLs of who should connect to whom up-to-date as the network evolves over time. It may not be practical to reconfigure all monitoring systems rapidly when a problem arises unless there are automated communications to push updates to each affected node in the network [4].

4) Trust System Solutions: The trust system interacts with an existing authentication mechanism, such as a logon server, to enforce multi-level, role-based access based on the success or failure of credentials provided. For this article, the most restrictive policy was assumed and is suggested, requiring initial logon of every new user as well as every system that is coming back

online. By tracking the time, conditions, and status of all logons and monitoring, correlating, and even blocking suspicious logon activity (tracked by username, IP address, credentials, and distance), the trust system provides comprehensive logon state and security situational awareness.

The trust system can perform data and validity checks on incoming commands and messages on behalf of field equipment (i.e. from an RTU, power line communication (PLC), or intelligent electronic device (IED) test set or admin laptop); however, access control at the SCADA field equipment, first, and then authentication at the network logon server (i.e. network-level logon) is preferred before further communication with the SCADA node. This can be facilitated by the trust system. Authentication by a device connected to an IED requires an IP port on the SCADA field device and an IP-enabled test set or laptop (preferably using encryption) capable of supplying authentication credentials.

Distribution of trust agents throughout the network allows a much more decentralized and efficient implementation of this authentication scheme and all other trust system functions.

B. Prevention of Data Interception or Alteration

1) SCADA Security Issues: Traditional RTUs, PLCs, and IEDs are designed for efficiency to prioritize task execution using microprocessors with limited memory and computational capacity, stringent real-time constraints, low bandwidth links, and minimal attention to security policies [12]. They typically send information without transmission security and many use wireless connections susceptible to interception [8].

Packet-based SCADA protocols usually provide message integrity checking at the data link layer to find errors caused by electrical noise and other transmission errors [12]. Since these checks do not include encryption and their algorithms are well documented and publicly available, they only provide protection against inadvertent packet corruption caused by hardware or data channel failures [12].

2) Recommendations From Literature: Digital certificates and cryptographic keys should be used for encryption and digital signatures in SCADA systems [8]. Transmission errors are best detected close to the source or physical medium (i.e. at the data link layer) while protection from network content alteration is best achieved close to the application layer (i.e. at the network layer or above) [12].

When packets are routed through a LAN or Utility Intranet, message IP addresses must be visible to each router and switch to appropriately route a packet to its destination. Traditional security solutions at the network layer or above are usually proprietary VPN schemes or standards-based (e.g. IPsec) protection schemes [12]. For these public-key cryptosystems, key management, including certification that a key belongs to the person named, is a critical issue to be handled by the organization. Such keys can also require relatively long processing times that may be incompatible with the real-time requirements of SCADA control systems [8].

As a result, symmetric-key cryptosystems, which can perform much faster, may be more suitable for SCADA environments; however, key management becomes more difficult. Although, symmetric-key cryptography has not yet been widely applied to SCADA systems, it is applicable to data transmitted over a long-distance SCADA network and could be added to protect its most critical portions [8].

3) Objections and Questions From Utilities: Older systems cannot support the computational burden of block encryption [12]. Encryption, configuration control, and other security measures make SCADA management more difficult. Complexity is the bane of efficiency.

IP already adds nearly 30% more overhead to SCADA communication. Encryption will add too much latency.

The TCP security model, SSL, permits a client of a server to authenticate and then encrypt sensitive data such as a credit card number, but that capability does not account for varying levels of trust between mutually suspicious operators [4].

4) Trust System Solutions: Research in [13] indicates that IPsec public key encryption can be used for non-real-time communications and has the potential, with faster processing, to reduce latency so it can be applied to real-time communications.

For legacy systems and applications that do not, or cannot, provide encryption at the IP-level or above, the trust system in gateway-configuration, with IPsec tunnel mode, can act as an encryption gateway. This can occur by encrypting unencrypted incoming packets, adding an IP header with destination address of the next trust system on the way to the destination. When the packet is received by the trust system closest to the destination, it strips the address, decrypts the packet, and forwards it, unencrypted, to the destination.

For systems that can be loaded with software trust system agents, agent middleware can interact to package data with IPsec encryption at the host before it is transmitted.

IPsec delay is highly processor-dependent. Until improvements are made in the SCADA hardware in utility networks to allow fast enough processing and less queuing delay, standalone symmetric key hardware can be added to the network to encrypt packets after they leave the source, switch, and possibly the first router, at the physical layer, and decrypt the packet before passing it to the destination router, switch, and recipient. In that case, the basic IP-to-IP *firewall rules* checks of the trust system could still be performed on a packet in transit and fixed-length message-types could be deduced. However, unless the trust system itself implemented the symmetric key encryption, the trust system's *format module* and some *access control matrix* checks would be negated due to encrypted packets, including message types. Once the data was decrypted, full trust system checks could be performed at the host level, catching at delivery instead of stopping malicious activity closer to the source.

C. Cybersecurity Priorities

1) SCADA Security Issues: Cyber-security is a low priority to many utilities because of long-held misconceptions of invulnerability. There is industry denial about the level of SCADA-Internet connectivity and there is an increasing trend in connections from the corporate network to the SCADA network for activity and performance reports. The same corporate offices are connected to the Internet for e-mail and web access. Remote login over the Internet and telephone lines for monitoring

and administration of SCADA systems has also grown in popularity. Earlier, control systems were less visible than IT systems and many were not connected to external networks. Their components required detailed technological knowledge to implement and operate, so the myth of security-through-obscurity had some basis in fact, but that is not so anymore.

A press release, dated April 7, 2002, stated that, according to an FBI survey, most large corporations and government agencies have been attacked by computer hackers, but more often and more frequently they do not inform authorities of the breaches. The survey found about 90% of respondents detected computer security breaches within the previous year but only 34% reported those attacks to authorities. Many respondents cited fear of bad publicity. There is much more illegal activity in cyberspace than corporations admit to their clients, stockholders, or to law enforcement [9].

2) Recommendations From Literature: Education of decision makers in the industry is key to dispelling the myths. Vulnerability assessments have already demonstrated unauthorized access to SCADA and Distributed Control Systems. Examples from contracted penetration testing, indicate the level of naivety among SCADA users. A common misperception among SCADA operators and managers is that "the threat is low because outsiders know nothing about our systems" [2]. They were appalled to learn that teams were able to, in a matter of minutes, gain access to the SCADA control network through unsecured Wi-Fi access, unknown and unprotected dialup lines, and the Internet. Although organizations were adamant about the fact that their operations network was not connected to the Internet, teams more often than not identified a connection between production and office networks, with no airgap, and the office network then connected to the Internet. In many cases, the teams discovered flawed network diagrams and laptops, not tracked or accounted for, allowed to connect to the production network from the outside (spreading viruses and worms) [2].

A combination of scheduled vulnerability assessments to include remote and internal scans, human engineering analysis (i.e. looking for written passwords, accessible network equipment, phishing techniques, etc.), and operational security assessments (i.e. searching for sensitive information from public websites and records), can prove how vulnerable a particular network or system is and can demonstrate the negative operational impact an attacker can create.

3) Objections and Questions From Utilities: A well-known CIO stated in the 2002 issue of CIO magazine that "most public utilities rely on a highly customized SCADA system. No two are the same, so hacking them requires specific knowledge," referring to the company's unique design and customized software [8]. He also stated that "cyber terrorism may not be nearly as worrisome as some would make it. That's because it's utterly defensible" [8].

4) Trust System Solutions: Even with technical training, regular application of the latest patches, security software and hardware, and dedicated specialists for round-the-clock monitoring, even the most heavily defended IT networks see their share of system compromises throughout the year from Internet connections.

The trust system records suspicious event details useful for IT and security personnel to prove to management the types and quantities of attacks against the network. These records should prove useful when investing in security purchases.

Unnecessary ports, obviously, should be closed. As another line of defense, the trust system protects the unprotected (i.e. systems that for some reason have open ports for which there should be no communication). In this case, the trust system blocks incoming packets destined for that port and IP address.

Institution of a national utility certification program that ranks companies and areas on their production, training, efficiency, environmental impact, rates, customer satisfaction, and security performance would increase competition for customers now able to pick and choose their energy sources.

A certification program, coupled with external vulnerability assessments and mandatory incident reporting, would reward companies with good management, policy, and security measures, encouraging network security investment. It would soon become apparent that the number of attacks on a company is irrelevant as compared to the ability to quickly and consistently detect and prevent breaches, which are the hallmarks of a security conscious organization.

The trust system makes it easy to gather and analyze attack data for reporting and proving successful mitigation by a company, allowing it to better protect its operations while gaining a higher security certification than its peers, and potentially higher profits due to consumer confidence.

VI. Experimental Scenarios

A. Overview

Two scenarios are presented. The first shows that the delays and impact of a trust system are relatively minor. This is true even when time-sensitive protocols are used such as TCP/IP. The next scenario describes a hypothetical insider-threat situation to illustrate the benefit that a trust system provides in responding to such dangers.

B. Scenario 1: Successful Root Logon by a Legitimate User

The first scenario centers on a login by a legitimate user, Sally Washington, into the management office LAN. The scenario is intended to demonstrate the low delays introduced by the trust system to TCP traffic. The certificate, key, and logon servers are located together 200 meters away through a trust system (depicted as a wall), router (R3), and switch (SW5). The background network traffic is assumed to be small when compared to the network capacity of 100 Mb/s per link. Active/router trust nodes were used in the scenario. This scenario is illustrated in Fig. 6.

Scenario 1 used on an IP-based Ethernet network. The trust system was emulated in software. The emulation ran on an Intel Pentium 3 GHz CPU with 3.5 GB of RAM and running Microsoft Windows XP Professional with Service Pack 2. In each trial, 50,000 messages ran through a complete trust system message check and the results were averaged. A total of 15 trials were run. 2,000 firewall rules were entered into the trust system. The worst-case trial results were used in the timing results given

TABLE II
SUBSET OF THE CALCULATED TRAFFIC DELAYS FOR THE SUCCESSFUL ROOT LOGON BY A LEGITIMATE USER

Pckt	Msg Type	Prot	TCP Control Flags		Source	Destination	IPSec Mode	Queue Size (B)	d_{proc} (ms)	# TS	Trust System Delay (ms)	Link Delays (ms)	Router/ Switch Delays (ms)	Per Packet Delay (ms)							
														Regular TCP				Abbreviated TCP			
														3GHz	4GHz	8GHz	12GHz	3GHz	4GHz	8GHz	12GHz
3-1	control	TCP	SYN	URG	SCADA_admin_ workstation1	logon_server	tunnel	300	0.09	1	0.2411	0.3912	0.3902	1.0589	0.9986	0.9082	0.8781	1.0589	0.9986	0.9082	0.8781
							tunnel	1500	2.00	1	0.2411	6.4303	6.4293	13.1371	13.0768	12.9864	12.9563	13.1371	13.0768	12.9864	12.9563
3-2	control	TCP	SYN-ACK	URG	logon_server	SCADA_admin_ workstation1	tunnel	300	0.09	1	0.2411	0.3912	0.3902	1.0589	0.9986	0.9082	0.8781	1.0589	0.9986	0.9082	0.8781
							tunnel	1500	2.00	1	0.2411	6.4303	6.4293	13.1371	13.0768	12.9864	12.9563	13.1371	13.0768	12.9864	12.9563
3-3	control	TCP	ACK	URG	SCADA_admin_ workstation1	logon_server	tunnel	300	0.09	1	0.2411	0.3912	0.3902	1.0589	0.9986	0.9082	0.8781				
							tunnel	1500	2.00	1	0.2411	6.4303	6.4293	13.1371	13.0768	12.9864	12.9563				
3-4	logon_ request	TCP	PSH-ACK	URG	SCADA_admin_ workstation1	logon_server	tunnel	300	0.09	1	0.1945	0.3969	0.3959	1.0250	0.9763	0.9034	0.8791	1.0250	0.9763	0.9034	0.8791
							tunnel	1500	2.00	1	0.1945	6.4507	6.4497	13.1325	13.0839	13.0110	12.9866	13.1325	13.0839	13.0110	12.9866
3-5	control	TCP	ACK	URG	logon_server	SCADA_admin_ workstation1	tunnel	300	0.09	1	0.2411	0.3912	0.3902	1.0589	0.9986	0.9082	0.8781	1.0589	0.9986	0.9082	0.8781
							tunnel	1500	2.00	1	0.2411	6.4303	6.4293	13.1371	13.0768	12.9864	12.9563	13.1371	13.0768	12.9864	12.9563
3-6	control	TCP	SYN	URG	logon_server	NTS	tunnel	300	0.09	1	0.2411	0.1308	0.1301	0.5383	0.4781	0.3877	0.3575	0.5383	0.4781	0.3877	0.3575
							tunnel	1500	2.00	1	0.2411	2.1439	2.1431	4.5644	4.5041	4.4137	4.3836	4.5644	4.5041	4.4137	4.3836
3-7	control	TCP	SYN-ACK	URG	NTS	logon_server	tunnel	300	0.09	1	0.2411	0.1308	0.1301	0.5383	0.4781	0.3877	0.3575	0.5383	0.4781	0.3877	0.3575
							tunnel	1500	2.00	1	0.2411	2.1439	2.1431	4.5644	4.5041	4.4137	4.3836	4.5644	4.5041	4.4137	4.3836
3-8	control	TCP	ACK	URG	logon_server	NTS	tunnel	300	0.09	1	0.2411	0.1308	0.1301	0.5383	0.4781	0.3877	0.3575				
							tunnel	1500	2.00	1	0.2411	2.1439	2.1431	4.5644	4.5041	4.4137	4.3836				
3-9	logon_ evaluated	TCP	PSH-ACK	URG	logon_server	NTS	tunnel	300	0.09	1	0.2646	0.1364	0.1357	0.5760	0.5098	0.4106	0.3775	0.5760	0.5098	0.4106	0.3775
							tunnel	1500	2.00	1	0.2646	2.1639	2.1631	4.6308	4.5647	4.4654	4.4323	4.6308	4.5647	4.4654	4.4323
3-10	control	TCP	ACK	URG	NTS	logon_server	tunnel	300	0.09	1	0.2411	0.1308	0.1301	0.5383	0.4781	0.3877	0.3575				
							tunnel	1500	2.00	1	0.2411	2.1439	2.1431	4.5644	4.5041	4.4137	4.3836				
3-11	logon_ denied	TCP	PSH-ACK	URG	NTS	logon_server	tunnel	300	0.09	1	0.1766	0.1323	0.1315	0.4777	0.4336	0.3674	0.3453	0.4777	0.4336	0.3674	0.3453
							tunnel	1500	2.00	1	0.1766	2.1491	2.1483	4.5113	4.4671	4.4009	4.3788	4.5113	4.4671	4.4009	4.3788
⋮																					
3-33	logon_ evaluated	TCP	PSH-ACK	URG	logon_server	NTS	tunnel	300	0.09	1	0.2646	0.1364	0.1357	0.5760	0.5098	0.4106	0.3775	0.5760	0.5098	0.4106	0.3775
							tunnel	1500	2.00	1	0.2646	2.1639	2.1631	4.6308	4.5647	4.4654	4.4323	4.6308	4.5647	4.4654	4.4323
3-34	control	TCP	ACK	URG	NTS	logon_server	tunnel	300	0.09	1	0.2411	0.1308	0.1301	0.5383	0.4781	0.3877	0.3575				
							tunnel	1500	2.00	1	0.2411	2.1439	2.1431	4.5644	4.5041	4.4137	4.3836				
3-35	logon_a pproved	TCP	PSH-ACK	URG	NTS	logon_server	tunnel	300	0.09	1	0.2565	0.1323	0.1315	0.5576	0.4935	0.3973	0.3653	0.5576	0.4935	0.3973	0.3653
							tunnel	1500	2.00	1	0.2565	2.1491	2.1483	4.5912	4.5271	4.4309	4.3988	4.5912	4.5271	4.4309	4.3988
3-36	control	TCP	ACK	URG	logon_server	NTS	tunnel	300	0.09	1	0.2411	0.1308	0.1301	0.5383	0.4781	0.3877	0.3575	0.5383	0.4781	0.3877	0.3575
							tunnel	1500	2.00	1	0.2411	2.1439	2.1431	4.5644	4.5041	4.4137	4.3836	4.5644	4.5041	4.4137	4.3836
3-37	logon_ approved	TCP	PSH-ACK	URG	logon_server	SCADA_admin_ workstation1	tunnel	300	0.09	1	0.2565	0.3956	0.3946	1.0840	1.0199	0.9237	0.8916	1.0840	1.0199	0.9237	0.8916
							tunnel	1500	2.00	1	0.2565	6.4459	6.4449	13.1846	13.1205	13.0243	12.9923	13.1846	13.1205	13.0243	12.9923
3-38	control	TCP	ACK	URG	SCADA_admin_ workstation1	logon_server	tunnel	300	0.09	1	0.2411	0.3912	0.3902	1.0589	0.9986	0.9082	0.8781	1.0589	0.9986	0.9082	0.8781
							tunnel	1500	2.00	1	0.2411	6.4303	6.4293	13.1371	13.0768	12.9864	12.9563	13.1371	13.0768	12.9864	12.9563
3-39	control	TCP	FIN-ACK	URG	SCADA_admin_ workstation1	logon_server	tunnel	300	0.09	1	0.2411	0.3912	0.3902	1.0589	0.9986	0.9082	0.8781	1.0589	0.9986	0.9082	0.8781
							tunnel	1500	2.00	1	0.2411	6.4303	6.4293	13.1371	13.0768	12.9864	12.9563	13.1371	13.0768	12.9864	12.9563
3-40	control	TCP	ACK	URG	logon_server	SCADA_admin_ workstation1	tunnel	300	0.09	1	0.2411	0.3912	0.3902	1.0589	0.9986	0.9082	0.8781				
							tunnel	1500	2.00	1	0.2411	6.4303	6.4293	13.1371	13.0768	12.9864	12.9563				
3-41	control	TCP	FIN-ACK	URG	logon_server	SCADA_admin_ workstation1	tunnel	300	0.09	1	0.2411	0.3912	0.3902	1.0589	0.9986	0.9082	0.8781	1.0589	0.9986	0.9082	0.8781
							tunnel	1500	2.00	1	0.2411	6.4303	6.4293	13.1371	13.0768	12.9864	12.9563	13.1371	13.0768	12.9864	12.9563
3-42	control	TCP	ACK	URG	SCADA_admin_ workstation1	logon_server	tunnel	300	0.09	1	0.2411	0.3912	0.3902	1.0589	0.9986	0.9082	0.8781	1.0589	0.9986	0.9082	0.8781
							tunnel	1500	2.00	1	0.2411	6.4303	6.4293	13.1371	13.0768	12.9864	12.9563	13.1371	13.0768	12.9864	12.9563
SCENARIO COMPLETE (user logged on to the network)											9.6775	184.5748	184.5378	380.3420	377.9226	374.2935	373.0839	331.2458	329.2483	326.2521	325.2534

in Table II. Trust system delay includes the time to complete a firewall rules check, a packet format check, a logon check, an access control check, and any sanitization of the message that is deemed necessary. Summing these times gives the total delay for the trust system before a packet is deemed good and is forwarded or is found to be bad and is thrown away. Processing and queuing delays were based on the emulated system. Processor speeds other than 3 GHz were calculated by scaling the processor-bound variables in the trust system. Transmission delays were calculated based on the distance and bandwidth of the links. IPsec encryption delays were calculated using results from the research of Niedermayer, Klenk, and Carl [14].

A logon_request, Packet 3-4, was sent from SCADA_admin_workstation1 by user Sally Washington, a SCADA administrator with username smwashingt. Returning after a 2-week vacation, she had forgotten and mistyped her password as depicted in Fig. 4. It is important to note that all example figures show passwords and credentials unencrypted for clarity. These fields would be encrypted in a real message.

Fig. 4 shows a representative subset of the packets used in the scenario, including requests and replies between the office LAN workstation and the login and credential servers. The active/router trust system implementation was used. In this case, there is not a compelling reason to use a passive mode or half-active mode implementation because the delay added by the active mode trust system is relatively small and tolerable in this case. A tunnel mode was also not used because all traffic is occurring inside the same utility. If a portion of the traffic were traveling over the Internet, another utility's network, or over some other shared environment then a set of gateways that tunneled encrypted traffic between them would have been appropriate. Of course, the encryption/decryption would come at the cost of a higher delay.

The password entered, !#V8k12g4X, did not match the stored password of !#V8k12g$X; therefore, the logon attempt was denied. The trust system recognized the similarity to the correct password and increased the threshold from three tries to five, to provide her more opportunities to log on.

Sally tried a second time. The second logon attempt was denied because the last character was a lowercase letter 'x' instead of the expected uppercase 'X'. The third logon attempt was denied because of a typo, an "@" sign instead of a "2".

The fourth logon attempt (Packet 3-31) supplied the proper password. Since all of the credentials supplied were correct, the logon server, sent the evaluated credentials to the trust system in a *logon_evaluated* packet, depicted in Fig. 5. The logon was

```
        MESSAGE TCP
    //begin IPv6 tunnel mode outer header
      …
    IP2_source_address
        2001:DC98:5634:2110:BD1C:BA89:7325:4051
        //nodal_TS@MPL_SCADA_workstation1
    IP2_destination_address
        2001:DC98:5634:2110:BD1C:BA89:7325:4050
        //network_TS@MPL_trust_router2
  //end IPv6 tunnel mode outer header
    //begin AH header
      …
    //end AH header
    //begin ESP header
      …
    //end ESP header
       //begin IPv6 tunnel mode inner header
      …
      IP1_source_address
       2001:DC98:5634:2110:BD1C:BA89:7325:3901
      //MPL_SCADA_admin_workstation1
       IP1_destination_address
       2001:A344:4DD1:F76F:D2CB:3B09:5629:1000
       //MPL_logon_server
    //end IPv6 tunnel mode inner header
    …
  //begin message data
    message_type     logon_request
      time_message_created 08:00:00.000-21Jun07
      username     smwashingt
      number_of_credentials  4
      credential_1_type    PASS
      credential_1     !#V8k12g4x
      credential_2_type    CARD
      credential_2
          1D43EF3409193A389BB067867D3A80C3249B8
       credential_3_type    PIN
      credential_3     10465891
      credential_4_type    FING
      credential_4
       ÿØÿàJFIFdd1i=&ÿÛ„OXÖS+x°rGŽe-Ô&9|6C‡ùw?]
       ...
       òôˆéýÿ
       Ÿ×G¶ÿÏG¤íõrartG-SË‰{wßùaõÔŽá$¿Ì{~
    //end message data
       //begin ESP trailer
    …
       //end ESP trailer
       //begin ESP ICV
              …
       //end ESP ICV
```

Fig. 4. Packet 3-4 (First Failed Logon Attempt, Wrong Password).

successful, so no security alert was generated. The trust system assigned an effective ACCN of 4 to username *smwashingt* in its *ACM*, granting Sally root-level privileges in a *logon_approved* message, as depicted in the Fig. 5 historical archive. Table II lists an excerpt of the calculated end-to-end delay measurements for this scenario as well as the cumulative total. It shows that the delay added by the trust system is consistently low, always under 0.25 ms. The cumulative totals at the bottom of Table II also shows that, if TCP is used in utility communication, that an abbreviated version of the protocol, which eliminates ACKs from three-way handshakes and graceful closes and only ACKs with data, whenever possible, can reduce response time by up to 40%.

```
        MESSAGE TCP
    //begin IPv6 header
      …
        IP1_source_address
        2001:A344:4DD1:F76F:D2CB:3B09:5629:1000
              //MPL_logon_server
      IP1_destination_address
2001:DC98:5634:2110:BD1C:BA89:7325:3901
            //MPL_SCADA_admin_workstation1
    //end IPv6 header
    //begin AH header
      …
    //end AH header
    //begin ESP header
      …
    //end ESP header
    //begin TCP header
    …
    //end TCP header
    //begin message data
      message_type     logon_evaluated
      time_message_created   …
      username       smwashingt
      number_of_credentials    4
      credential_1_type    PASS
      credential_1_pass    YES
      credential_2_type    CARD
      credential_2_pass    YES
      credential_3_type    CPIN
      credential_3_pass    YES
      credential_4_type    FING
      credential_4_pass    YES
    //end message data
       //begin ESP trailer
    …
       //end ESP trailer
       //begin ESP ICV
              …
       //end ESP ICV
```

Fig. 5. Packet 3-33 (Logon Credentials Evaluated by the Logon Server).

C. Scenario 2: Disgruntled Employees

This scenario simulates the trust system as implemented by a fictitious utility company, Middletown Power and Light (MPL). The scenarios are not intended to represent any particular power company or its employees.

Scenario 2 revolved around the same basic Middletown Power and Light layout as in Scenario 1. Scenario 2 was not simulated because timing was not a central concern. It would not be difficult to run this scenario in the emulated trust system testbed outlined in Scenario 1, which would flag unauthorized transfers and respond appropriately.

Installation of IEDs, high-speed fiber optic links, and the trust system's additional security measures had increased MPL's efficiency and security, reducing the need for as many SCADA administrators. As a result, two employees with poor performance records (who were kept around because of their knowledge of the legacy systems) were notified in advance that they would be let go. This was to be their last day. Angry, they had been plotting together, over the last week, to steal company-sensitive financial and network configuration data they could sell for profit. They also planned to sabotage the SCADA network with false data, hoping to cause a local blackout that might cost MPL hundreds of thousands of dollars in revenue this month. The individuals were aware that the company security policy required their accounts to be immediately disabled the very afternoon of

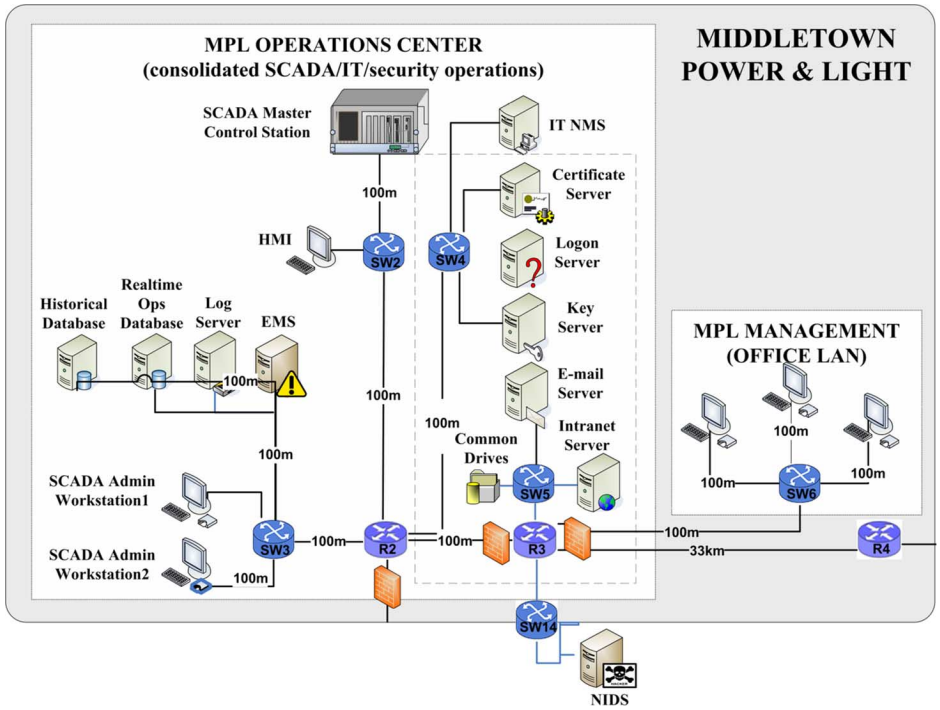

Fig. 6. Depiction of the Successful Root Logon by a Legitimate User scenario. An employee is logging on from the office LAN.

```
    MESSAGE TCP
    …
    //begin message data
     message_type   operation_request
     time_message_created …
     username   bearnold
     operation_type   copy
     file  L:\Finance\QuarterlyReports\Jul-
Sep\FinancialForecast.ppt
    //end message data
    …
```

Fig. 7. Insider's request to copy file FinancialForecast.ppt.

their last day, just after leaving the building. As administrators, still in possession of a smart card and able to provide biometric credentials in addition to a PIN, on their final day they were still authorized to logon with full root-level privileges.

One individual, an IT network administrator, attempted to steal a negative quarterly financial forecast and overdue maintenance records, which if made public, might hurt the company's reputation and potential value of company stocks. He also planned to download network diagrams, password files, and configuration settings that would be valuable to US or international hackers seeking to exploit utility networks.

He searched the common drives and found the quarterly report data which was viewable to his role. He then attempted to copy it to a thumbdrive, whereby his workstation sent the packet shown in Fig. 7, a copy request message, to the common drive server hosting the file.

The trust system, checked the administrator's role and effective ACCN against the ACM and found he was authorized to read but not copy the data. Also, as an IT network administrator, he did not have permissions to change the ACM settings, as a security administrator role could.

Next he found the folders containing network diagrams and the logon server's password cache. He had authority, by his role, to copy these and downloaded them to his thumbdrive.

```
MESSAGE TCP
…
//begin message data
message_type              e-mail
time_message_created      …
username                  bearnold
To                        hackersblog@yoohoo.com
Cc                        ihatemycompany@snotmail.com
Bcc                       jwboothe@homenetwork.net
Text                      m@dH@k3r, I got the initial
                          $5000 check, so here's the
                          LAN diagram and password
                          file for MPL as promised! I
                          expect 50% of the highest
                          bid when this gets posted.
                          -benedict
number_of_attachments     2
attachment_1              F:\Copy of
                          LAN_Diagram(current).vsd
                          //copied network diagram
attachment_1_dataType     ND
attachment_2_caveat       company-sensitive
attachment_2              F:\Copy of
                          C:\etc\passwd\MPLpw.txt
                          //copied password file
attachment_2_dataType     ND
attachment_2_caveat       restricted-release
e-mail_dataTypes          ND
e-mail_caveat             restricted-release
//end message data
…
```

Fig. 8. Disgruntled employee's first e-mail attempt.

However, all actions were logged to the historical database for which he did not have permissions to modify. Next he attempted to e-mail them to his home e-mail account, sending the Packet depicted in Fig. 8. The trust system inspected the message and found the attachments. When it checked the data type against usernames associated with the sender and receiver e-mail accounts it determined that these files contained company-sensitive data not authorized for public release, so the e-mail was blocked.

The administrator then changed the names of the files, re-attached them, and attempted to resend them. The trust system was only configured to prevent inadvertent disclosures, however, simply changing the filename of a copy of an existing file, that had already been assigned a data type, did not change the file's assigned data type. Again the e-mail was blocked. The administrator then removed his thumb drive. A workstation-level trust agent might have generated a message to the administrator's screen asking if he meant to download company-sensitive data or generating a security_alert. In such a case, even clicking 'yes' and proceeding with the theft or modifying the contents slightly and renaming, the file download would still be logged to the historical database.

In this case, the trust system updated the suspicious event, generated a security alert with the second failed attempt details, and lowered the trust level for the username. An analyst seeing the security alert event might have immediately recognized the potential harm and stopped the theft right away. Let's assume this did not happen immediately, but that all actions were recorded and viewable after-the-fact.

The second disgruntled employee, a SCADA administrator, was authorized to successfully download current SCADA configuration files. Had he been assigned any other role, he would not have had these privileges. In this case, the trust system was not configured to alert for copy actions on sensitive-data by an employee on his last day, which would have alerted security analysts of suspicious activity, however, his actions were also logged by the historical database.

The next morning, reviews of the previous day's logs indicated the activity by the administrators and they were greeted by law enforcement at their residences.

VII. Conclusion

SCADA networks are vulnerable to attack, whether from a digital source or a natural disaster. The proposed trust system will comply with the strict requirements of the SCADA network while providing a secure environment. The trust system is flexible and can be implemented in whatever way best fits SCADA networks' needs. The trust system enforces access restrictions between IP addresses that should not be allowed to communicate with one another via specific message types and interfaces. The trust system, implemented in active mode, intercepts all malicious messages. The research shows that a more secure network can be established, using a trust system, for the power grid. The trust system is a step toward security for the Utility network.

In addition, there are a number of recommendations that can be made in order to strengthen existing security. Strict access controls should be enforced and only the minimum rights should be granted to an individual to accomplish their jobs. Passwords should be robust. Transmissions from RTU's, PLC's, and IED's should be protected by digital certificates and digital signatures to prevent unauthorized users from intercepting the information or introducing false data into the SCADA system. Finally, cybersecurity needs to be a priority for system administrators. SCADA systems are of increasing interest to hackers and other unauthorized users. Increasing levels of communication and protocol standardization will only increase the seriousness of this threat. Administrators should take precautions including closing unnecessary communication ports, keeping system patches up to date, and should keep up to date on current computer security practices. The trust system in this article can serve as an aid in many of these recommendations, but administrators also need constant vigilance to protect their portions or the electric power grid.

References

[1] M. Grimes, "SCADA exposed," presented at the ToorCon 7, San Diego, CA, 2005.

[2] R. Graham and D. Maynor, "SCADA security and terrorism: We're not crying wolf," presented at the Black Hat Federal, Washington, DC, 2006.

[3] G. M. Coates, K. M. Hopkinson, S. R. Graham, and S. H. Kurkowski, "Collaborative, trust-based security mechanisms for a regional utility intranet," *IEEE Trans. Power Syst.*, vol. 23, no. 3, pp. 831–844, Aug. 2008.

[4] K. P. Birman, J. Chen, K. M. Hopkinson, R. J. Thomas, J. S. Thorp, R. Van Renesse, and W. Vogels, "Overcoming communications challenges in software for monitoring and controlling power systems," *Proc. IEEE*, vol. 93, no. 5, pp. 1028–1041, May 2005.

[5] K. Hopkinson, G. Roberts, X. Wang, and J. Thorp, "Quality of service considerations in utility communication networks," *IEEE Trans. Power Del.*, to be published.

[6] D. Bailey and E. Wright, *Practical SCADA for Industry*. Oxford, U.K.: Newnes, 2003.

[7] C. L. Bowen, T. K. Buennemeyer, and R. W. Thomas, "Next generation SCADA security: Best practices and client puzzles," in *Proc. 6th Annu. IEEE SMC Information Assurance Workshop*, West Point, NY, 2005, pp. 426–427.

[8] R. L. Krutz, *Securing SCADA Systems*. Indianapolis, IN: Wiley, 2005.

[9] J. Pollet, "Developing a solid SCADA security strategy," presented at the IEEE Sensors for Industry Conf., Houston, TX, 2002.

[10] M. Adamiak, "Intelligrid architecture . . . a system with a view," GE Multilin. [Online]. Available: http://www.iti.uiuc.edu/tcip/01_U-of-I-IntelliGrid.pdf. Urbana, IL, 2005

[11] U.S.–Canada Power System Outage Task Force, "Final report on the August 14, 2003 blackout in the United States and Canada: Causes and recommendations Apr. 5, 2004.

[12] J. D. McDonald, *Electric Power Substations Engineering*. Boca Raton, FL: CRC, 2003.

[13] G. M. Coates, "Collaborative, trust-based security mechanisms for a national utility intranet," in *Electrical and Computer Engineering*. Wright-Patterson Air Force Base, OH: Air Force Inst. Technol., 2007, vol. 262, M.Sc. WPAFB.

[14] H. Niedermayer, A. Klenk, and G. Carle, "The networking perspective on security performance—A Measurement study," presented at the 13th GI/ITG Conf. Measurement, Modeling, and Evaluation of Computer and Communication Systems, Nürnberg, Germany, 2006.

Gregory M. Coates received the M.S. degree in cyber operations from the Air Force Institute of Technology, Wright-Patterson Air Force Base, OH, in 2007.

His research interests include networking, security, and critical infrastructure protection.

Kenneth M. Hopkinson (M'04) is an Assistant Professor of Computer Science at the Air Force Institute of Technology, Wright-Patterson Air Force Base, OH. His research interests include networking and simulation.

Scott R. Graham (M'01) is an Assistant Professor of Computer Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, OH. His interests lie in networking and control systems.

Stuart H. Kurkowski (M'06) is an Assistant Professor of Computer Science at the Air Force Institute of Technology, Wright-Patterson Air Force Base, OH. His interests lie in networking and scientific visualization.