Solving the Puzzle: Providing Appropriate Cyber Security While Providing Operations Effectiveness and Efficiency

Bill Phillips, Bao Le, Linnon Parker,
Ron Booth, Richard Emanuel, and Reggie Peagler

Utilities today are faced with conflicting needs to operate more efficiently (do more with less) and to protect the public water supply from attack. Many of the automation and information systems installed in the 1990s to improve efficiency are now being revisited to patch security shortcomings uncovered during security vulnerability assessments. System designers are now being asked to build cyber security into new automation and information systems. The question confronting utilities is, "What is the best strategy to balance efficiency and security, and how much is 'enough' to budget for cyber security improvements?"

Before 1990, most utility computer systems were stand-alone systems composed of hardware and software from a single source, typically a value-added-reseller of computer hardware from one of the predominant manufacturers. Remote users were connected using dedicated leased phone lines. This model was used throughout the utility industry for most applications, including financial management, customer information, billing, and Supervisory Control And Data Acquisition (SCADA).

In the early 1990s, utilities began to take advantage of rapidly evolving network, communications, platform, and connectivity standards to automate many of the data-management tasks that previously had been done manually. It became practical to share information among applications, improving both customer service and operations efficiency.

Internet access and wireless networks further improved connectivity, but increased connectivity is virtually synonymous with increased vulnerability. Many of the computers, network appliances, operating systems, and applications being used by utilities are the same commercial applications broadly used by other businesses and at home, exposing vulnerabilities and providing a rich environment for their exploitation.

The result was rapid escalation in the number and type of computer attacks, with many being widely publicized and some doing significant financial damage, requiring companies to spend money restoring applications and data, patching holes exploited by the attack, and mitigating the impact of data theft.

Exhibits 1 and 2 show that Internet attacks are a daily occurrence and originate from all over the world. **Exhibit 1** is a snapshot of Internet attack activity from February 15, 2003. The exhibit is based on attack activity over the previous 30 days and shows that Internet attacks originate from all over the world, but that most attacks are coming from the USA. A total of about 3.5 million attacks were reported for this 30-day period. **Exhibit 2** shows that the number of attacks (incidents) is escalating rapidly. Each of the incidents reported in Exhibit 2 could impact hundreds or thousands of sites and could continue for long periods.

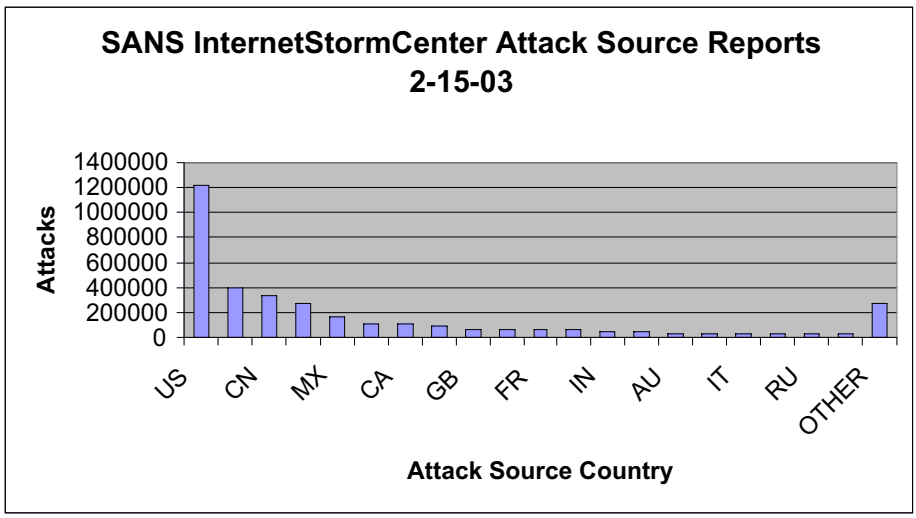


Exhibit 1 - Attack Source Reports. Source: SANS InternetStormCenter - Feb. 15, 2003

The authors are all employed by CH2M Hill Inc., an engineering and project delivery company specializing in water, environment, transportation, industrial processing, and related infrastructure. Bill Phillips is the firm's Facility Automation Global Technology leader; Bao Le is chief technical officer for the firm's Communications Group; Linnon Parker is a member of the Global Utility Management Services Team; Ron Booth is the Southest Region Security Services director; Richard Emanuel is the Southeast Region Utility Management Service Team leader; Reggie Peagler is director of Southeast Region Information Services.

Computer Systems Critical to Utility Operation

Networks of computers are now woven into the fabric of utility operations and are virtually indispensable. Computers are used to monitor and control the water-production, treatment, and delivery processes; to assist in managing infrastructure assets; to collect and manage customer information; to manage documents, including facility drawings; and to handle billing and payroll, among other tasks. Returning to the days when computers were optional isn't really a choice in today's complex world.

Exhibit 3 demonstrates the projected revenue impact the loss of a utility's computerized billing system could have on the business. As losses escalate rapidly, the financial impact on the utility becomes onerous after less than two weeks. **Exhibit 4** identifies typical applications deployed in water utilities and **Exhibit 5** graphically depicts the interaction and data sharing among the applications.

Loss of any one of these applications for more than a few days is likely to dramatically impact operations costs, customer service, or both. For even medium-size utilities, loss of the SCADA system or automatic meter reading (AMR) could also be devastating as staff attempts to maintain operations or billing data collection. Without billing, revenue is immediately impacted as well.

Cyber Security Action Plan

To mitigate the risk of cyber attack on these critical assets, every utility should have detailed, written computer information system security procedures that address, among other things, access control, authentication, backup, and disaster recovery. These security procedures should focus on accountability, privacy, and access control. An action plan for developing and deploying security procedures should include:

• **Conduct a Risk Assessment –** Conduct a thorough risk assessment of the entire computer network, not just SCADA. The Risk Assessment Methodology for Water (RAM-W^{SM}) process developed specifically for the water industry by the American Waterworks Association Research Foundation (AwwaRF) and Sandia addresses the SCADA system. One important product of this process is SCADA fault trees, which are graphical representations that show how each point of vulnerability can be used by an attacker to either destroy or disable critical SCADA assets or interfere with normal utility operation. The fault trees are then used in conjunction with risk calculations to rank and select security improvements.

A separate information technology (IT) security vulnerability assessment is usually required for the overall computer system network, including the business network, that is not addressed by RAM-W^{SM}. Because physical security will be a key component in the plan, it's a good idea to coordinate the computer information-system assessment and planning work with all facilities risk assessment and countermeasures planning work.

• **Identify Critical Information –** What would an adversary need to know about your facilities and operations to penetrate or damage facilities; harm personnel; endanger the water supply, public health or the public; or gain unauthorized access to information systems?

• **Do Not Rely on Arcane or Proprietary Protocols –** Don't rely on the fact that many SCADA protocols are arcane and/or proprietary for protection against attack. These obscure protocols provide very little, if any, protection.

• **Disconnect Unnecessary Connections –** Disconnect network, Internet and modem connections that are unnecessary, are too difficult to protect, or cost more to protect than they are worth to the business. This step includes eliminating vendor "back door" connections. Back doors are entry points into systems that facilitate easy access, usually by system vendors or system administrators.

• **Conduct Penetration Tests –** Conduct penetration tests on any remaining connections to the SCADA network to evaluate their degree of vulnerability and develop a protection and prevention strategy.

• **Develop, Keep Current and Enforce Security Policies and Procedures –** Develop polices and procedures. Address personnel and use policies, business processes, and system and device setup. Define cyber security roles, responsibilities, and authorities for managers, system administrators, and users. Fully exploit the security features of SCADA applications and devices. Establish and maintain effective device and system configuration management processes.

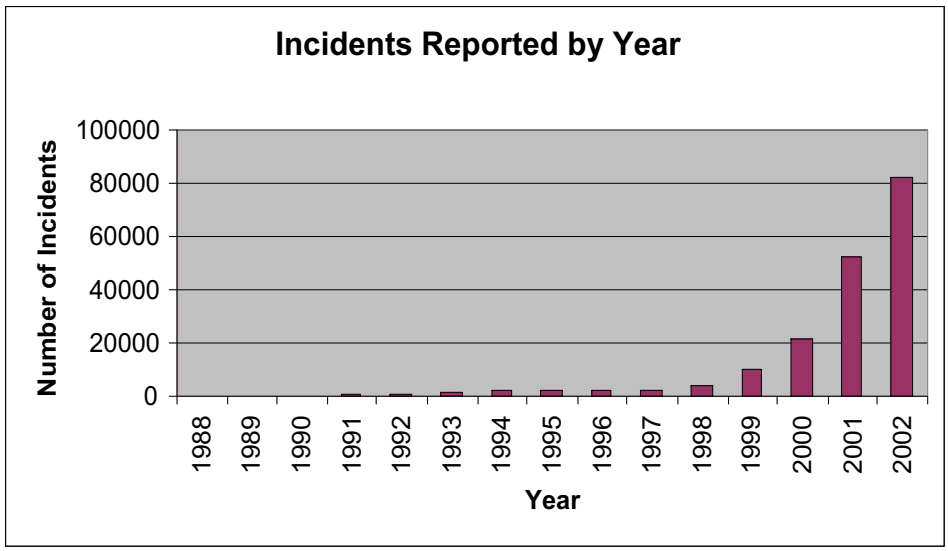
• **Develop, Keep Current and Practice Disaster Recovery Planning –** Develop a business continuation and disaster recovery plan. Include a crisis (incident) management plan. Conduct routine practice exercises and use "lessons learned" to fine tune the plan and keep it current.

• **Practice Vigilance –** Routinely perform audits and compliance monitoring, re-assess the utilities security posture, review audit logs, and evaluate technological advances that may improve security.

• **Outsource –** Rely on outside network security experts to periodically review networks, procedures and logs, and to recommend improvements.

• **Backup –** Save backup copies of all data on all servers daily. Also, routinely save backup images of server system drives. Keep the backups in secure, climate-controlled, offsite facilities.

Exhibit 2 - Incident Reports by Year from CERT Coordination Center



Security Procedures

Security procedures are essential and should satisfy the following criteria:

• Define user access and responsibilities. Focus on accountability, privacy, and access control. Integrate user responsibilities into personnel polices that define consequences.

• Define physical security requirements and procedures for network devices, servers, communications equipment, and other computer-network system components.

• Define system, device, and operating system and applications setup and configuration. Fully exploit the security features of network devices, computers, and applications, including SCADA. Establish and maintain effective

Continued on page 17

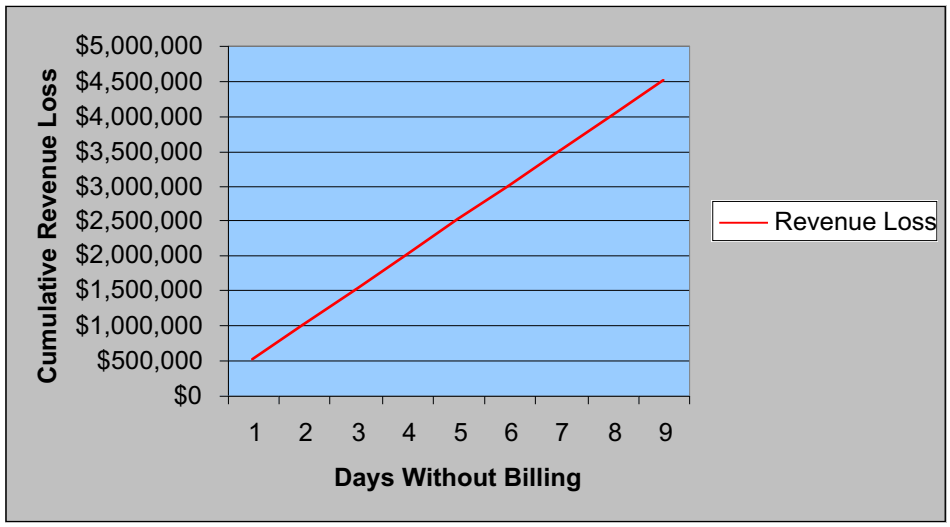


Exhibit 3 - Cumulative Revenue Loss Based on Interest Cost of $500,000 per Day

Exhibit 4
Typical Utility Computer Applications

- **Billing/CIS**
- **Financial System**
- **Human Resources System**
- **Telephone System**
- **Document Management**
- **Time Keeping**
- **SCADA**
- **AMR**
- **GIS**
- **CMMS**
- **LIMS**

Continued from page 15

device and system configuration management processes. Separately address the network perimeter or edge.

• Define cyber security roles, responsibilities, and authorities for managers, system administrators, and users.

• Include a business continuation and disaster recovery plan. Include crisis and incident management.

• Include schedules and procedures for conducting periodic internal and external audits.

Typical Network

Utility computer network architectures vary a lot. **Exhibit 6** is a simplified logical block diagram of a hypothetical network and includes most of the vulnerabilities commonly found in utility networks.

Vulnerabilities

Computer systems are generally vulnerable to the following categories of attack:

• ***Access*** – Access by outsiders [access without authentication].

• ***Authentication*** – Masquerading as someone else [unauthorized access].

• ***Data Interception or Theft*** – Data is diverted or read in transit.

• ***Data Modification or Destruction*** – Data is wrongfully modified and invalid or it is destroyed.

• ***System Availability*** – The computer information system fails or is not responsive or less responsive.

Points of vulnerability can be divided into two categories: internal and external. The same is true for attackers: insiders or outsiders. Insiders misuse their access and outsiders gain access.

Internal points of vulnerability include any keyboard, removable media drive, or communications port. Sources of internal attacks include physical break-ins, unauthorized use of an unattended computer, errors or malicious acts of privileged users, and disgruntled employees.

"Eighty percent of all attacks originate from inside the firewall," according to David M. Hager, vice president of network security and disaster recovery at OppenheimerFunds Distribution Inc. During a security audit of his corporation, Hager managed to crack 800 user passwords in three minutes using a standard password-cracking tool. Within 36 hours, he was able to crack all of the 27,000 passwords being used throughout the enterprise.

External points of vulnerability include interfaces to external networks, Internet connections, wireless links, remote user ports, and wide area network (WAN) connections. Internal points of vulnerability are generally well understood, but external points are not always as easy to identify. Starting from the top, external points of vulnerability for the hypothetical utility network shown in Exhibit 6 include:

• The connection to the Internet. This is usually a permanent connection to an Internet service provider (ISP). Many cities host Web sites and some provide interactive services such as trouble reports and utility bill payment. All of the incident reporting and statistics presented in Exhibit 1 are for Internet attacks.

• The three public switched telephone network (PSTN) connections. The connections to the two servers [remote access service (RAS) and SCADA] allow dial-up access to the business network and one of the SCADA servers. Dial-up access can be plain old telephone service (POTS) or integrated service digital network (ISDN). These connections allow outsiders or insiders stealth access to attack the network. Insiders would use insider information to gain access; outsiders could use war dialers and password cracking tools to gain access. The workstation connection is used for Internet access and does not support dial-in, but does expose the network to virus and other Internet attacks.

• WAN connections. Frame relay, gigabit Ethernet, and asynchronous transfer mode (ATM) are common WAN technologies. Though much less vulnerable than the ISP or PSTN connections, all external connections are vulnerable to attack. The actual service used and the WAN configuration strongly influence the degree of vulnerability.

• The wireless bridge and wireless access point connections. These use standard protocols such as the Institute of Electrical and Electronic Engineers (IEEE) 802.11b and are easily attacked. Encryption protocols like wired equivalent privacy (WEP) offer little protection. Improved protection is under development (802.1x) and some bridge and access-point equipment is available with proprietary solutions that offer much-improved protection.

• The licensed and unlicensed telemetry links. Note that these links connect a programmable logic controller (PLC) master to remote ter-

Continued on page 18

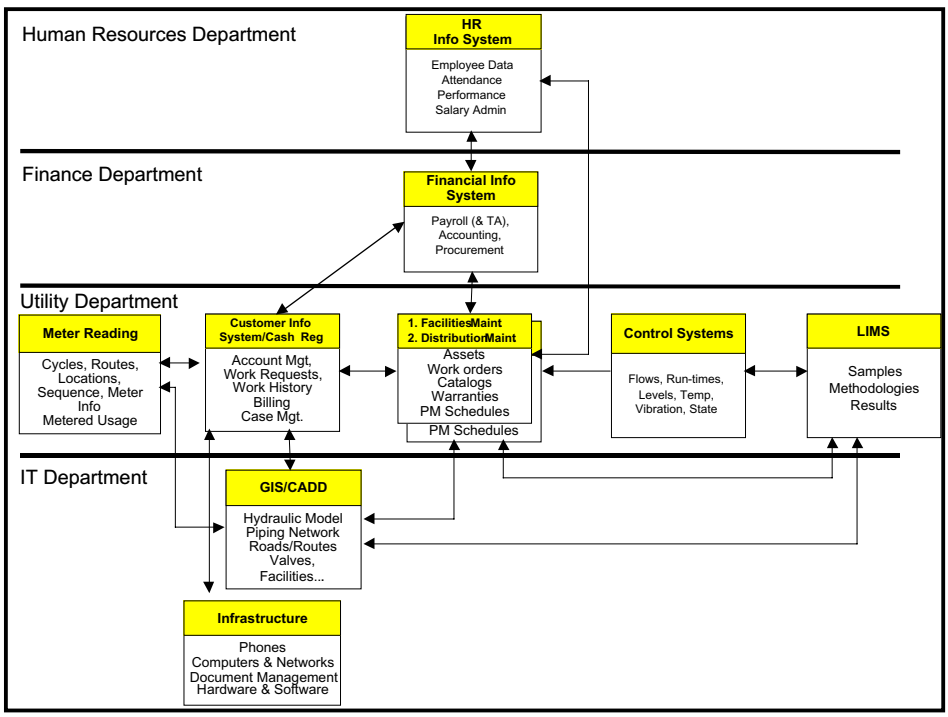
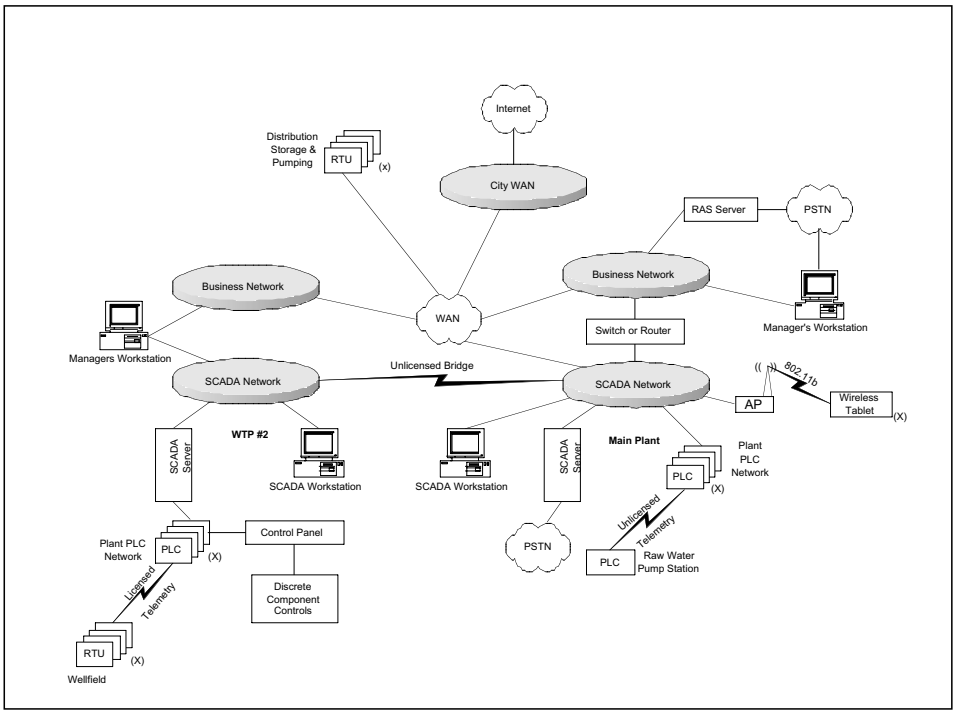


Exhibit 5 - Computer Application Data Exchange Diagram

Exhibit 6 - Hypothetical Utility Computer Network Logical Block Diagram



Continued from page 17

minal units (RTUs) or a PLC. These links are vulnerable and have been attacked; however, the damage that can be done is generally limited to process disruption, data theft, or data manipulation because the master PLC usually will not provide direct access to the SCADA Ethernet network. A growing trend that does expose the entire SCADA Ethernet network to attack is to use wireless bridge or wireless access point technology for telemetry.

• Backdoor access to the business and SCADA networks. Business network users are outsiders to the SCADA network, as are SCADA network users to the business network; therefore, either network can be attacked from the other. Backdoor access at the main plant is provided by the router or switch. At WTP #2, access is provide by the workstation using dual network interface cards (NICs) to connect to both networks.

Computer Network Improvements

• ***Use Strong Authentication*** – Strong authentication verifies (authenticates) the identities of users, clients, and servers over networks without relying solely on name and password. Strong authentication uses two elements: something you know and something you possess. It does not require that the network be protected. Both parties in a connection must demonstrate knowledge of some "secret" to establish their identities. Strong authentication can include the use of biometrics and tokens. Examples of biometrics authentication include retinal scanners and fingerprint readers. Tokens may generate a personal identification number (PIN), which changes frequently and must be entered by the holder to complete authentication.

• ***Limit Access*** – Disable workstation floppy and CD drives and Internet access where they are not needed–for example, on SCADA system workstations. Also disable Internet connections that are often included with the prepackaged monitoring and control applications furnished as part of packaged process and mechanical systems. If these Internet connections are important, they can be installed on selected SCADA client workstations that reside on non-SCADA local area networks (LANs).

Use operating-system user profiles and policies, and file access settings to restrict access to that required to support each user's role. Also, disable guest accounts. For SCADA and other servers and workstations using Microsoft operating systems and used for a single or a limited number of mission-critical applications, disable Microsoft Explorer and use scripting to launch applications to further restrict configuration access. Applications are also available which do not allow the user to install any additional applications or change the configuration of the machine.

• ***Unauthorized Device Discovery*** – Use available tools to routinely discover unauthorized devices such as wireless access points and modems installed by authorized users.

• ***Patch Holes*** – Install application and operating-system patches and bug fixes promptly. Subscribe to application support services for mission-critical applications like SCADA.

• ***Provide Physical Security*** – Locate servers, network equipment, and other sensitive equipment in confined areas. Limit access and monitor activity in those areas. Use fiber-optic cable in accessible areas to prevent passive eavesdropping.

• ***Install Virus Protection Software*** – Install automatically-updating virus-protection software on all Internet, proxy, FTP (file transfer protocol) and e-mail servers. Also, where practical, install automatically-updating virus-protection software on all workstations. Network access limitations and application restrictions may make it impractical to deploy this software on some workstations.

• ***Install Stateful Inspection Firewalls*** – Install stateful inspection firewalls at all connections to the Internet. As shown in **Exhibit 7,** traditional routers and multi-layer switches provide packet filtering that uses access control lists (ACLs) and base access and routing decisions on protocol type, Internet protocol (IP) addresses, and application transmission control protocol (TCP) port numbers.

In contrast, stateful packet inspection maintains a table of active TCP sessions and user datagram protocol (UDP) "pseudo" sessions. Active sessions are those that satisfy defined security policies. Sessions that fail to satisfy security policies are denied access, as are any packets that aren't part of an active session. Stateful inspection firewalls can also authenticate users when the session is established, perform uniform resource locator (URL) filtering to deny access to blacklisted sites, and determine if packet contents are acceptable (HTTP for TCP port 80, for example).

Stateful inspection firewalls are also faster than application proxy firewalls because application proxies require two TCP connections for each session. Hybrid firewalls using stateful inspection and selective proxies provide additional protection against denial-of-

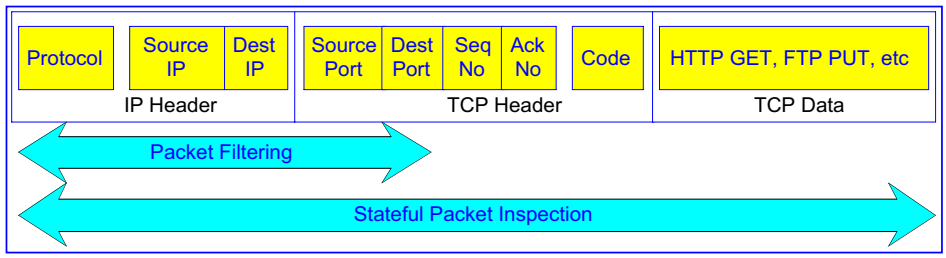
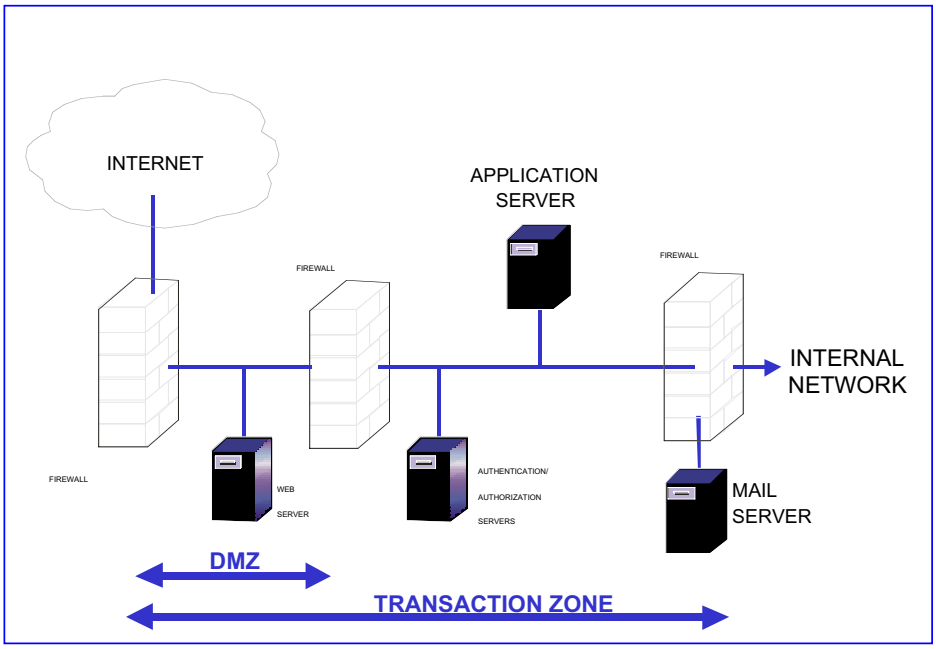


Exhibit 7 - Packet Filtering and Stateful Inspection Compared

Exhibit 8 - Transaction Zone Firewall Architecture



service attacks. Firewalls will soon appear that will allow inspection of the packet payload (to check for malicious code) at wire speed.

• ***Consider Intrusion Detection*** – Consider selected host-based or network-based intrusion detection systems (IDS) for detection and mitigation of unauthorized network activity. A number of techniques are in use, but most generate significant numbers of false alarms and require excessive maintenance; however, Gartner Group believes that advances in the areas of data collection, analysis, alerting, and reporting will soon be available, making IDS a more effective enterprise security tool.

• ***Use Transaction Zone Firewall Architecture*** – The demilitarized zone (DMZ) concept doesn't provide adequate protection. Gartner has proposed a "transaction zone" architecture depicted in **Exhibit 8**, including redundant (load balanced, high availability) firewalls at the gateway to the Internet, IDS within the transaction zone on each host and network segment, redundant Internet connectivity, and firewall access from the transaction zone into the corporate network. This architecture is intended for enterprises with mission-critical Internet applications. Water utilities may be able to achieve adequate reliability and security with a subset of this architecture.

• ***Use Virtual Private Networks*** – Use virtual private networks (VPN) and a security protocol like IP security (IPsec), Layer 2 tunneling protocol (L2TP) or point-to-point tunneling protocol (PPTP) to provide secure connections for remote users over the Internet. IPsec provides two choices of security service: authentication header (AH), which essentially allows authentication of the sender of data, and encapsulating security payload (ESP), which supports both authentication of the sender and encryption of data as well. IPsec isn't always the best choice, however, and may not work at all in some situations.

• ***Use Firewalls and VPNs for Wireless Local Area Networks*** – Use firewalls at every wireless access point and VPNs for network communications using wireless technology.

• ***Uninterruptible Power Supplies*** – Provide uninterruptible power supplies (UPS) for all servers, communications equipment, intrusion detection devices, mission-critical workstations, and PLC. Without these devices, any loss of power brings the network and any connected devices down.

SCADA Remote Monitoring and Control Networks

SCADA systems, though common in the water and other process industries, are not as common and well understood by the general public as business and general-purpose computing systems. SCADA networks also tend to be more isolated than other computer networks, so they haven't been subjected to the number of well-publicized attacks experienced by other computer systems.

For that reason, the information available on vulnerabilities and mitigation is limited, but IEEE 1402-2000, the in-progress Electric Power Research Institute (EPRI) Enterprise Infrastructure Security Initiative, and the in-progress EPA/awwaRF initiative, as well as the large volume of vulnerability-assessment activity triggered by recent terrorist attacks, are producing considerably more information.

The impact of an attack on SCADA systems depends on where the attack occurs. An electronic intruder who gains access to communications with a SCADA workstation or server can do much more (and more widespread) damage than an intruder gaining access to a pump station or well PLC. Consequences of electronic intrusion into SCADA systems can be as severe as physical sabotage and include the following:

- Shut down the SCADA system, either immediately or in a delayed manner.
- Steal or alter data gathered or produced by the SCADA system.
- Shut down plant or remote facilities, either immediately or in a delayed manner.
- Change process settings or degrade reliability and subsequently endanger water quality, personnel safety, or the public health.
- Gather information to be used in a subsequent attack.
- Plant malicious code that could later trigger a delayed or coordinated attack.
- Obtain public or protected customer, supplier, personal, and utility information by using SCADA as a backdoor into the utility computer information system.

SCADA remote monitoring and control networks historically are used in master/slave type protocols (MODBUS®) and machine-specific application protocols (for example, RSLogix™ for Allen-Bradley PLCs). Today, TCP/IP is routinely used and other types of protocols such as producer/consumer (ControlNet™) are becoming more common.

• ***General Attributes*** - SCADA networks usually interconnect a network of PLCs, SCADA servers and SCADA workstations. Where ethernet and TCP/IP are used, SCADA LANs should be independent segments protected from other computing traffic. The messaging between PLCs and SCADA servers is machine (PLC) specific. Discussion of vulnerabilities and mitigation is divided into applications-specific, protocol-specific and media-specific topics.

• ***Applications-Specific Vulnerabilities*** - These networks and the machine-specific messaging used usually support monitoring and control activities that require the SCADA server to read and write from memory registers in the PLC to make process changes and collect information about process performance. PLC programming activities which allow PLC monitoring and control functions to be modified are also supported. These vulnerabilities can be mitigated as follows:

• ***Physical Access Limitations*** - Physical access restrictions are probably the strongest deterrent. These networks–or at least their end points–are usually located in facilities (treatment plants, pump stations) with restricted access. Providing physical-access restrictions is important because these networks are usually designed so anyone with a

Continued on page 20

properly configured laptop can plug into the network and gain access.

• ***Machine-Specific Knowledge Required*** – Machine-specific knowledge is also needed to modify the controller functions, make process changes, or provide invalid information.

• ***Protocol-Specific Vulnerabilities*** - Protocol-specific vulnerabilities vary with protocol type as follows:

• ***TCP/IP*** - TCP/IP protocol is very commonly used over Ethernet LANs and WANs for SCADA communications. The machine-specific messaging used requires machine-specific knowledge as noted above to make process or configuration changes; however, SCADA networks usually lack strong authentication and require only a valid user name, selection of an unused IP address within the valid range, and a password for access. Once accepted on the network, an attackeer could gain remote access to SCADA servers and workstations, as well as backdoor access to any other servers and workstations on other networks accessible from the SCADA network. Adding strong authentication would mitigate this vulnerability; however, the strong authentication methodology used must be selected and configured to prevent interference with the SCADA application software.

• ***Machine-Specific*** – Machine-specific protocols such as the longstanding *de facto* standard MODBUS, as well as newer protocols, usually lack security features; however, they require machine-specific knowledge and are limited to monitoring and control and PLC configuration modification capabilities.

• ***Media-Specific Vulnerabilities*** – Media-specific vulnerabilities vary with media type as follows:

• ***Network Devices*** - Most networks are not protected against unauthenticated users connecting to the network. Once connected, these unauthenticated users have access to discover the network and interfere with network operation.

• ***Fiber Optic*** – Fiber-optic media provide excellent intrusion protection because passive eaves-dropping isn't possible and attaching to the network will probably draw attention to the intrusion before any damage can be done.

• ***Copper*** – Passive eaves-dropping on copper networks is possible, though for SCADA networks machine-specific and process-specific knowledge would be required to interpret and use the information. The level of effort of attaching to the network would depend on the network type but is likely to be relatively easy; therefore, physical-access limitations are needed to provide a deterrent to unauthorized access.

• ***Dedicated Telephone Circuits*** - Dedicated telephone circuits include frame relay, digital subscriber line (DSL) if mapped to a frame-relay connection, and leased lines. These services are dedicated and not accessible to unauthorized access, except that some portions of the circuits use copper media, providing the intrusion opportunities described for copper media.

• ***Integrated Service Digital Network*** - Integrated service digital network (ISDN) is a switched service allowing access to anyone with the ISDN service; however, ISDN interfaces can be configured to accept calls only from specific locations, providing protection from unauthorized access.

• ***Plain Old Telephone Service*** – Plain old telephone service (POTS), or dial-up service, is accessible to anyone with a modem or phone. Most SCADA communications applications have no features to prevent unauthorized access. Generally the SCADA server calls remote PLCs, so the SCADA server modem can be configured not to receive calls. A PLC can be called and accessed with the proper machine-specific applications and knowledge, allowing intrusion into that PLC's monitoring and control domain.

• ***Radio*** – SCADA radio links are usually master/slave links. As such, the SCADA server will usually reject unwanted messages, providing some protection against unauthorized access to the server. Digital radios also use manufacturer-specific encoding, providing some additional protection. Any radio signal is subject to being blocked by an obstruction or interrupted if the intended receiver is overpowered by a strong nearby signal. Most analog licensed SCADA radios are being replaced by digital radios because of the Federal Communications Commissions (FCC) refarming regulations. Unlicensed radios also use manufacturer-specific encoding plus spread spectrum technology, which adds additional protection.

• ***Cellular Digital Packet Data*** – Cellular digital packet data (CDPD) is a cellular service that sends data over unused or dedicated cellular voice channels where it's supported. CDPD uses IP addressing and protocol and can connect to utility WANs, as well as the Internet. Encryption technology is available but may not be suitable for SCADA applications. Without encryption, the vulnerabilities described above for TCP/IP protocol would apply.

Getting Started

Utilities serving more than 100,000 customers were required by law (Public Health Security and Bioterrorism Response Act of 2001) to complete a RAM-W[SM] security vulnerability assessment by March 31st, 2003. Emergency operations plans (EOPs) have to be completed within six months of completing the security vulnerability assessment. If your utility hasn't done so, conducting a RAM-W[SM] vulnerability assessment including SCADA is a good first step. The personnel conducting the security vulnerability assessment have to be certified to use the RAM-W[SM] process.

In many cases, the primary computer-system improvements recommended have been to conduct an IT vulnerability assessment and to develop and implement computer-system security procedures. The cost of completing the assessments will vary a lot, depending on the size of the network and number of devices. Typical costs will vary between $30,000 and $150,000.

The costs of implementing security procedures will also vary. Outside assistance is recommended. Deployment of the procedures can often be completed by utility IT staff, except where upgrading mission-critical applications such as CIS and SCADA are required. Costs for these upgrades will depend on existing support agreements and the current state of the application.

Cyber security should be viewed as part of the overall internal control system of an organization. While there are many technical considerations to implementing good security, ultimately the policies, communications, and culture of the organization must be designed to support the organization's overall security and business objectives. Again, the first step is to understand your organization's strengths and challenges related to security in order to establish a path that ensures your organization has taken all reasonable measures to mitigate risk.

Resources

The President's Critical Infrastructure Protection Board and the U.S. Department of Energy have developed "21 Steps to Improve Cyber Security of SCADA Networks" to help organizations improve SCADA network security. Also, the following organizations and Web sites provide valuable background material and cyber security guidance:

- *U.S. Dept. of Energy, Computer Incident Advisory Capability (CIAC) http://ciac.llnl.gov/ciac/*
- *CERT® Coordination Center (CERT®/CC) http://www.cert.org/*
- *Federal Computer Incident Response Center (FedCIRC) http://www.fedcirc.gov/*
- *Computer Security Resource Center (CSRC) http://csrc.ncsl.nist.gov/*
- *Common Vulnerabilities and Exposures http://www.cve.mitre.org/cve/index.html*
- *World Wide Web Consortium (W3C) http://www.w3.org/*
- *Microsoft Security Patches http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/secpatch.asp*
- *U.S. Critical Infrastructure Assurance Office http://www.ciao.gov/*