المقدمة

العنصر	الوصف
عنوان البحث / اللغة العربية	بحث رقم 1
عنوان البحث / اللغة الانجليزية	project 1
الاولوية	Computing
التخصص العام	INFORMATION SYSTEMS
التخصص الدقيق	Information security and crises management
الباحث الرئيسي / اللغة العربية	عبدالغفار محمدالهادي السيد محمد
الباحث الرئيسي / اللغة الانجليزية	
تاريخ الارسال	23-10-2015
مرحلة التقديم	30-3-2015
مدة المشروع -بالشهور	18

فريق العمل

#	اسم الباحث	التخصص العام	الوظيفة	الدرجة العلمية
1			مستشار	
2			باحث رئيسي	

الفريق المساعد

#	نوع المشاركة	الفئة	

2. xx CELLULAR AND INTERNET BASED SCADA SOLUTION

A. The water and wastewater facilities SCADA system shall be comprised of a hosted, Internet based human machine interface portal (Link2Site™ system) which communicates to remote sites utilizing a readily available commercial cellular network. The system shall be:

1. Totally integrated, fully automated control and monitoring solution suitable for stand alone local functionality and have simultaneous Internet based remote access.
2. The solution shall include the required Internet based interface software, Internet wireless terminal (Link2Site cellular modem) and dedicated pump controller unit for each of the required water and wastewater facility sites.

B. Optional redundant communication capability shall include conventional, dedicated radio or telephone and cellular connection capability operating in a fully automatic redundant mode. This communication option shall include the required controller physical connection and software as a standard product offering to support the redundancy capability.

C. The cellular connection capability shall allow any authorized user to securely connect to the system from anywhere with an Internet connection. The Link2Site system shall be accessed utilizing a standard web browser software package, which shall function as a traditional SCADA system software interface including the following functions:

1. Interface functionality such as pump start/stop setpoint adjustments, remote on/off control, and alarm setpoint adjustment shall be included as a minimum.
2. Remote site access security and controller configuration security shall be implemented via user entered passwords or with electronic key reader iAccess technology. Configuration changes and facility site access shall be recorded as time-and date-stamped events. These events shall then be reported and recorded over the wireless cellular connection.
3. Alarm acknowledgement and alarm silencing capability shall be incorporated in the Link2Site system interface package.
4. An “Update Now” function shall allow an authorized user to update the entire system automatically on demand from the Link2Site system.

D. The Link2Site system shall provide immediate notification of facility operational and security alarms utilizing the following Owner furnished communication methods:

1. E-mail account notification.
2. Standard Owner pager systems.
3. Designated phone call.
4. Text Messages
5. All four methods at once.

E. Advanced callout scheduling functionality shall ensure the appropriate person and/or persons are called in the event of a specific alarm type. Acknowledging alarms shall be handled by the authorized Owner personnel using either the telephone or Internet interface.

F. The Link2Site system shall be user-friendly, configurable, and flexible. Access to the Link2Site system shall be through a secure Login Home page. Once logged into the system, the authorized operator will be able to select from the following Menu selections and associated display pages:

1. Enterprise Status Menu shall provide a facility wide overview map with facility site statuses, site list display, site detail displays.
2. Logs Menu shall provide user access to Alarms and User/Site Event. The software shall include time- and date-stamped records for all alarms, Alarm "Acknowledgements" and Alarm "Clear" status. The software shall include time- and date-stamped records of all system Events.
3. Reports Menu shall provide both system and Site Report displays. The system Report display shall confirm site communication connection to the Link2Site system as well as Flow and Pump Summary displays. The Site report shall provide a Communication Connection History report, Site Access report, Monthly (Site) Station report, Yearly (Site) Station report, Station (Site) Rainfall Report, and Station (Site) Flow history report. The system shall include time- and date-stamped records of Site Access including who, when and how long an individual was at the site.
4. Graphic Menu shall provide Station (Site) Graphic displays, Detailed Station (Site) performance displays including pump cycle details and runtime and an Analog Values Report display. The system shall support equipment maintenance alerts for calculated unbalanced runtimes, runtimes exceeding setpoints, runtimes exceeding thirty- (30) averages and number of starts exceeding setpoint.
5. Setpoint Menu shall provide setpoint definition displays and facility detail displays.
6. Logout Menu shall allow the user to exit the Link2Site system web site.

G. Advanced pump station performance algorithms shall be provided allowing for pump station performance optimization and offering the following capabilities:

1. Optimization shall offer reduction in facility energy requirements and help prolong equipment life.
2. Configurable multiple, multi-point trend displays shall be a standard offering and shall be used to illustrate how different pieces of equipment and system components work together.
3. The trending package shall allow users to track the operation and performance of different system equipment and assets over time.
4. Users shall have the ability to determine and select variables in the system to track together and to save the custom trends for future use.
5. Advanced pump station operation and maintenance functionality shall allow the user the ability to monitor pump performance over time, which will be used to predict pump station and/or other facility asset failures before they occur.

6. The system shall provide multiple methods of volumetric flow including pump run times, wetwell drawdown, wetwell drawdown with compensation for inflow rate. The volumetric flow calculation will be available for the entire pumping station or individual pumps to assist with overall performance analysis.

H. The Link2Site system shall constantly monitor its own health and provide immediate notification of any system wide signal losses, alarms, or events while maintaining reasonable and responsible cellular long term costs.

I. An Internet wireless terminal modem shall provide the communication interface between the local site dedicated pump controller unit and the cellular network provider. This wireless terminal modem shall transmit pump controller collected data to the Link2Site system via the cellular network.

J. The provider of the Link2Site system shall be responsible for confirmation of cellular coverage for the sites to be monitored, establishment and setup of the cellular plan, procurement of the appropriate SIM modules, testing of the cellular modems, and end user billing of the cellular air time. The cellular coverage contract shall be between the end user and Siemens Water Technologies.

K. The Link2Site cellular modem shall incorporate the following general functional design requirements:

1. Power for the Link2Site modem shall originate from the local pump controller or via a separate 12 or 24 VDC power supply, as required. An integral power ON/OFF switch and operational status light shall be included
2. An RS232 serial interface 9-pin connector cable between the Link2Site modem and IntraLink LC150 pump controller shall be installed in accordance with industry standards. The required pump controller RJ45 connector to the Link2Site modem DB9F modular adapter with the correct communication protocol pin-out shall be furnished.
3. The supported standard protocols shall include as a minimum Modbus, IntraLink and DF1.
4. Include the required antenna and appropriate cable for secure and reliable operation over the cellular communication network.
5. Support an extended temperature range of -22°F (-30°C) to +158°F (+70°C) for the Link2Site cellular modem normal operation.
6. The Link2Site modem shall support Circuit Switched Data (CSD) transmission rate of up to 14.4 kbps required to support mobile cellular phone systems.
7. The Link2Site cellular modem shall support a Quad-Band Global system for mobile communication (GSM) of 850, 900, 1800 and 1900 MHz.
8. Link2Site modem support of a standard Java software development platform, which supports Information Module Profile - Next Generation (IMP-NG). The software platform shall allow the modem to update its application over the air (OTA) in a simple and reliable manner as well as transfer and receive confidential data in a secure environment using industry standard data encryption methods.

L. The IntraLink LC150 pump controller shall be furnished for local, dedicated monitoring and automatic control of the required water and wastewater facilities and shall communicate over the specified wireless cellular network to the Link2Site system.

1. It shall be a standard, catalogued product of a water and wastewater pumping automation equipment manufacturer regularly engaged in the design and manufacture of such equipment.
2. The pump controller shall be specifically designed for water and wastewater pumping automation utilizing built-in preconfigured control and telemetry strategies allowing pump up or down mode pump control of 1 to 3 pumps. "One of a kind" system hardware using custom software with a generic programmable controller will not be acceptable.
3. The pump controller operating program shall be resident in non-volatile FLASH memory and include full-scale ranging and pump-up/down determination.
4. The pump controller shall be arranged to operate up to three (3) pumps plus high and low (analog) alarms. The ON and OFF adjustments of each pump and alarm setpoint shall be full-range adjustable through use of a software configuration package or an optional operator interface keypad with appropriate security clearance. The controller operator display shall show the operation of each control stage.
5. The pump controller shall include adjustable on-delay timing logic to provide staggered pump starting following a power failure condition. Adjustable off delay timing for each pump control stage shall provide smooth transition between control stages.
6. The pump controller operating voltage shall support either a 120 Volts AC or 10–30 Volts DC power sources.
7. A power on LED shall be built on board providing local indication that power is available to the unit.
8. The unit shall be battery backed to provide continued system monitoring and alarm annunciation in the event of primary power failure. It also shall have built in battery charging circuitry to maintain and charge battery. Battery shall be sized to provide a minimum of four- (4) hours of back up power. Back up battery power will extend to necessary process sensors, local alarm lights, horns and telemetry equipment.

M. The pump controller shall be (furnished with) (available) with an optional user friendly “View-At-A-Glance™” operator interface allowing adjustment and viewing of all system parameters and status per the following. The operator interface shall be suitable for front door mounting including locations requiring wash-down and moisture protection.

1. The process variable signal, Pump 1, 2, & 3 On/Off and High & Low Setpoints, shall be displayed simultaneously via front panel mounted long lasting Ultra Bright LED bar graphs. These bar graphs shall be vertically mounted in parallel fashion to provide relational viewing of all setpoints vs. the measured process. Each display column shall have a minimum of 40 segments of resolution.

2. Each setpoint column shall have a status LED mounted on top of the associated setpoint providing indication of setpoint activation status. Units that require operator action to view the above parameters are not acceptable.
3. To assure the highest resolution and accuracy, the process display shall be configured to display the full range of the actual measured process. Range can also be offset allowing display of a pressure or level range that does not start at zero. The display ranges shall be field configurable.
4. System pumps on/off and alarm setpoint parameters shall be easily adjustable via individual up and down pushbutton arrows located next to the associated setpoint display column(s).
5. The unit shall have a built in process simulation capability allowing the operator to verify system operation by forcing the process variable up or down via pushbutton arrows located next to the process display. To prevent accidentally leaving the unit in simulation mode, the pump controller shall be configured to automatically restore monitored process display within 2 minutes after last keypad usage or immediately upon operator initiated restore.
6. The display unit shall incorporate a high contrast LCD panel allowing for viewing of higher level functions including the following:
   a. Process display to XX.X of the full scale process range.
   b. Time and Date Stamped Alarms & Events
   c. Pump Statistics (Including Run Time, Number Of Starts, Daily Average Number Of Starts)
   d. system diagnostics
   e. Controller Security
   f. Cellular communication diagnostics

   The LCD shall operate in a manual scrolling menu mode with the various displays shown in sequence as selected by the keypad's up/down arrow keys.
7. Unauthorized Station Entry Detection

N. The pump controller shall be able to monitor<u> two- (2) user selectable 4-20 mADC or 0-10 VDC or 5 VDC analog inputs</u> representing the process variable to be control The pump controller shall provide on board 24 VDC loop power output for external loop powered field mounted sensor. A built-in analog supply voltage status LED shall indicate availability of loop power. The analog input circuitry shall provide optical group isolation from the main board to the field device. The analog process signals shall be displayed locally via 40 segment vertical LED display and the LCD digital display as specified above.

O. The pump controller shall have the ability to monitor up to sixteen- (16) digital inputs, which shall provide monitoring of local facility discrete status. Each digital input shall provide optical isolation from the main board to the field device. A minimum of 1500 volts electrical isolation shall be required. An on board LED shall be provided indicating that digital input isolation is not compromised. The following inputs shall be monitored:

1. Pump 1, 2, 3 Run – This signal shall be used to provide local display of pump run status, pump total run time, pump average daily starts. For each pump.
2. Pump 1, 2, 3 In Auto – This signal shall be used by the controller to determine pump availability. A pump in this mode cannot be called into operation.
3. Pump 1, 2, 3 High Temperature/Seal Failure – This signal shall be used by the controller to disable the pump required when a High Temperature is the cause of the failure, and provide local alarm display. Controller shall be able to differentiate alarm. A Seal Failure shall not disable pump operation.
4. High & Low Float/Pressure – This signal shall be used by the controller to provide back up control of the pumps in the event of primary (analog) sensor failure.
5. Pump Inhibit – This signal shall be used by the controller to inhibit pumps from operating.
6. Power Quality – This signal shall be used by the controller to disable pumps in the event incoming station power is unsuitable for use as determined by an optional external power monitoring device.
7. Door Switch & Door Acknowledge– These signals shall be used by the controller to monitor station access as detected by an optional external door/limit switch an optional external alarm disabling switch.
8. Alarm Silence – This signal shall be used by the controller to monitor an optional external silence push button and will temporarily disable the alarm horn output.

P. The pump controller shall provide a total of seven- (7) digital outputs for interface to local pumps and alarm annunciation discrete equipment.

1. Provide five- (5) relay isolated contact outputs for activation of Pump 1, Pump 2, Pump 3, Common Alarm and Alarm Horn shall be provided. Each contact shall be rated for a minimum of 10 amps at 120 VAC or 5 Amps at 240 VAC.
2. Provide two- (2) open collector outputs for Low and High Level Alarm shall be provided for interface to off board monitoring equipment. Open collector outputs shall have a minimum operating range of 5-30 VDC @ 100 mADC.

Q. The pump controller shall provide one- (1) 4-20 mADC (1-5 VDC) analog output for interface to external equipment including VFDs, Chart Recorders or other analog monitoring devices.

R. The pump controller shall have built-in standard operator adjustable alternation functions allowing for sequencing and equalizing wear of the pumps. The following alternation sequences shall be supported:

1. Fixed
2. Rotary
3. First On First Off (FOFO)
4. Utilize One Favor Others (UOFO)
5. Emergency Mode

S. Provide built-in Pump Failure detection logic integral to the pump controller unit. In the event the pump has been called into operation and the pump run signal is not received within a pre-adjustable time period. A motor failure shall be produced. The failed motor shall be disabled, an alarm shall be displayed and the next available pump based on the selected alternation sequence shall be requested to start.

T. The pump controller shall include a volumetric lift station flow and pump performance monitoring capability allowing station flow measurement without the use of an in line flow meter. In addition to flow measurement, the pump controller shall provide pump performance related information. Pump station flow and pump performance data shall be viewable locally through built in LCD or available for telemetry transmission to master station. The following information is to be provided:

1 Average Station Influent Flow Rate
2 Maximum Station Influent Rate (K Gal) w/Date & Time
3 Current Day Total Effluent Flow (K Gal)
4 Previous Days Total Effluent Flow (K Gal)
5 Average Daily Effluent Flow (K Gal)
6 Maximum Daily Effluent Flow (K Gal) w/Date & Time
7 Total Station Effluent Flow (K Gal)
8 Average Flow Rate Pump 1, 2, 3 Over All Cycles (GPM) – Each Pump
9 Average Flow Rate Pump 1, 2, 3 Over Last Three Cycles (GPM) – Each Pump
10 Total Flow Pump 1, 2, 3 (K Gal) – Each Pump
11 Flow Rate Pumps 1, 2 (K Gal)
12 Flow Rate Pumps 1, 3 (K Gal)
13 Flow Rate Pumps 2, 3 (K Gal)
14 Flow Rate Pumps 1, 2, 3 (K Gal)
15 Pump 1, 2, 3 Low Flow Rate Alarm (Setpoint) – Each Pump
16 Pump 1, 2, 3 Run Time – Each Pump
17 Pump 1, 2, 3 Number Of Starts – Each Pump
18 Pump 1, 2, 3 Average Number Of Starts – Each Pump

U. In addition to the pump and alarm control capability, the controller shall provide alarm annunciation. The controller upon the occurrence shall initiate a local alarm audible device and flash the alpha-numeric display providing the following functionality:

1. The display shall indicate the alarm description, complete with the time and date of the alarm occurrence.
2. An acknowledge pushbutton shall be provided to allow silencing of the audible device while the digital display will continue to show the alarm function, complete with time and date information, until the condition has cleared.
3. A built-in alarm and status historian shall retain the last 100 time and date stamped events providing a historical record of recent activity.

V. The Pump Controller shall be furnished with an optional iAccess button . The iAccess button will support the ability to track manpower. iAccess technology shall be standard and integral to the pump controller and shall function as follows:

1. The iAccess button function shall include a small metal disk usually packaged in a key fob. This iAccess disk shall contain a unique serial number. The pump station controller shall contain an iAccess reader. This reader shall sense the presence of the iAccess button and transfers a unique serial number to the pump controller data base. Each person in the Owners workforce shall be in the system and given an iAccess key fob. Utilizing the key fob security pass, Owner designated person shall “login” on arrival and “logout” upon leaving each water and wastewater facility. These entry and exit events are recorded at the Internet Web-based central server, providing a history of who was at what sites, and when.
2. This iAccess security pass shall also be used to provide protection from unauthorized changes to the pump control configuration. This access protection shall support different levels of security and authority in a hierarchical structure allowing access to the pump controller providing limited to maximum capabilities.
3. Facility intrusion acknowledgment shall utilize the iAccess button providing a local time base record of securing the water and wastewater facility.

W. The pump controller shall have two- (2) RS-232C serial communications ports that shall be available for the required system wide telemetry communication.

1. These serial communication ports shall support both a traditional SCADA system telemetry link and a cellular Internet communications link.
2. Optional redundant communication capability shall be available supporting the radio or telephone communication as the main and the cellular Internet communication as the backup.
3. Each of the serial communication ports shall support open communication standards including as a minimum, MODBUS, IntraLink Open and DF1.
4. Pump controller communication ports shall support communication data rates of 1,200 to 38,800 baud rates configurable and as required by the selected communication networks.
5. On board communication diagnostic LED indicators shall be available to provide indication of communications activity for verification and troubleshooting.

X. The Cellular Internet Web-based Pump Telemetry Controller shall be the Link2Site system complete with the required hardware, equipment and software as manufactured by Siemens Water Technologies.

+ + END OF SECTION + +

Chapter 3

SCADA Security Assessment Methodology

__Greg Miles__, (Ph.D., CISSP#24431, CISM#0300338, IAM, IEM) co-author of Security Assessment: Case Studies for implementing the NSA IAM (Syngress Publishing, ISBN 1-932266-96-8), Network Security Evaluation: Using the NSA IEM (Syngress Publishing, ISBN: 1-597490-35-0), and Security Interviews Exposed: Secrets to Landing your Next Information Security Job (Wiley Publishing, ISBN-10: 0471779873) is the President, and Chief Financial Officer of Security Horizon, Inc. Security Horizon is a Global, Veteran-Owned Small Business headquartered in Colorado Springs, Colorado. Security Horizon provides global information security professional services, training, and publishes The Security Journal, a quarterly online publication. Greg is a U.S. Air Force Veteran and has been supporting the technology and security community for the last 22+ years. Greg's background includes work with NSA, NASA, and DISA. Greg has supported efforts covering security assessments, evaluations, policy, penetration testing, incident response, and computer forensics.

Greg holds a Ph.D. in Engineering Management from Kennedy Western University, a master's degree in Management Administration from Central Michigan University, and a bachelor's degree in Electrical Engineering (with a concentration in Control Systems and Power Systems) from the University of Cincinnati. Greg is a member of the Information System Security Association (ISSA) and the Information System Audit and Control Association (ISACA). He is also Adjunct Faculty for the University of Advancing Technology (www.uat.edu).

Introduction

Supervisory Control and Data Acquisition (SCADA) Systems have evolved over the years. With the growth of technology, the desire to simplify, the desire to remote manage, and the need to reduce labor costs, SCADA has moved to be more in line with traditional TCP/IP networks. With this evolution, the need for effective, comprehensive assessments of SCADA systems has never been greater. Old paradigms must change, organizations need to understand the threats they face, and appropriate protection measures must be incorporated. This chapter will discuss the need for SCADA security assessments and provide a comprehensive approach to conducting SCADA security assessments.

Why Do Assessments on SCADA Systems?

Historically, SCADA systems have been separate non-Internet-connected systems that provide the "command and control" for critical infrastructure. With the advent of technology and the desire to implement this technology to make communications and support easier and faster, SCADA systems have evolved into being very much like your typical office network. One of the challenges though is that the mentality concerning SCADA system security hasn't always been embraced. Some organizations still don't understand that the threat to SCADA systems has dramatically increased over the last several years due to these network-like connections. "Security by obscurity" is no longer an option for SCADA security.

Tools & Traps…

Security by Obscurity

"Security by obscurity" is no longer an option for SCADA security. SCADA systems are a network presence and face significant threats and vulnerabilities. This requires a paradigm change for many personnel working in the critical infrastructure business.

Assessments Are the Right Thing to Do

Protecting the confidentiality, integrity, and availability of critical process, operational, corporate, and customer information should be enough of a motivator for organizations to assure that their SCADA systems are protected. This is the concept of due diligence and is generally referenced by considering whether the security protections compare sufficiently to what would be considered normal and reasonable in the industry. Organizations must want to protect our critical infrastructure from malicious hackers, botnets, Denial-of-Service attacks, viruses, corporate espionage, and human error.

Events such as the 2003 Northeast power outage that affected parts of the United States and Canada, the 2008 Florida power outage that affected large parts of Florida, and the 2007 sponsored hack at the Idaho National Laboratories where a hacker was able to blow up a generator should be a pretty serious wake-up call for the industry. No longer is SCADA separate and not exposed. It is very much out there as a target, with enough serious threats to warrant significant attention to the protection of SCADA and the information that is processed, transmitted, and/or stored.

Assessments Are Required

Homeland Security Presidential Directive (HSPD)-7 talks about the protection of critical infrastructure. SCADA systems are generally serving a command-and-control function within this critical infrastructure and therefore have a direct mandate for protection. Other requirements come from the North American Electric Reliability Council (NERC). Believe it or not, guidance is available on how to implement and protect SCADA.

Information Protection Requirements

United States Federal Government and Department of Defense (DoD) have done a great deal of work on information protection and information assurance. The National Institute of Standards and Technology (NIST) has developed an entire series of special publications with information on things to do to protect systems. The National Security Agency (NSA) has developed and provided two methodologies that you can be certified in for assessing organizations and information systems for vulnerabilities. The NSA INFOSEC Assessment Methodology (IAM) focuses on an organizational view of vulnerabilities, while the NSA INFOSEC Evaluation Methodology (IEM) focuses on finding technical vulnerabilities within the information systems that process, transmit, and/or store critical information.

This author is a firm believer that if you study the various standards out there for any industry, greater than 80 percent of the requirements are the same. These commonsense requirements reflect a best practice approach to protecting critical information. As we discuss the standards and methodologies in this chapter, you will see some of this reflected in the comparisons.

National Institute of Standards and Technology (NIST) Guidance

NIST has defined a layered security model that has 17 control families (Table 3.1), which covers a tremendous amount of security protection mechanisms. This information can be found in NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems. SCADA systems are not necessarily Federal Information Systems; however, NIST's work lays an excellent foundation for security within organizations.

Table 3.1 NIST Control Families

Class	Control Family
Management	Risk Assessment
Management	Planning
Management	System and Services Acquisition
Management	Certification, Accreditation, and Security Assessments
Operational	Personnel Security
Operational	Physical and Environmental Protection
Operational	Contingency Planning
Operational	Configuration Management
Operational	Maintenance
Operational	System and Information Integrity
Operational	Media Protection
Operational	Incident Response
Operational	Awareness and Training
Technical	Identification and Authentication
Technical	Access Control
Technical	Audit and Accountability
Technical	System and Communications Protection

North American Electric Reliability Council (NERC) Critical Infrastructure Protection (CIP) Standards

NERC (www.nerc.com) works with the U.S. Department of Energy and the U.S. Department of Homeland Security to coordinate security needs and requirements. This collaboration allowed NERC the opportunity to create a series of Critical Infrastructure Protection Standards. These standards are:

- CIP-001 – Sabotage Reporting
- CIP-002 – Critical Cyber Asset Identification
- CIP-003 – Security Management Controls
- CIP-004 – Personnel and Training
- CIP-005 – Electronic Security Perimeter(s)
- CIP-006 – Physical Security of Critical Cyber Assets
- CIP-007 – Systems Security Management
- CIP-008 – Incident Reporting and Response Planning
- CIP-009 – Recovery Plans for Critical Cyber Assets

Water Infrastructure Security Enhancement (WISE)

The American Water Works Association, the American Society of Civil Engineers, and the Water Environment Federation have taken a grant from the United States Environmental Protection Agency to develop WISE (Water Infrastructure Security Enhancement). WISE provides security guidance for water and wastewater/storm water utilities. These voluntary (so far) standards are heavily dependent upon physical security in the water utilities, but WISE does address an entire process of risk assessment and risk management that can easily be transitioned into supporting information security needs. It is a good start and may lead to greater guidance on the technical security as well. More information on WISE can be found at www.awwa.org/science/wise/.

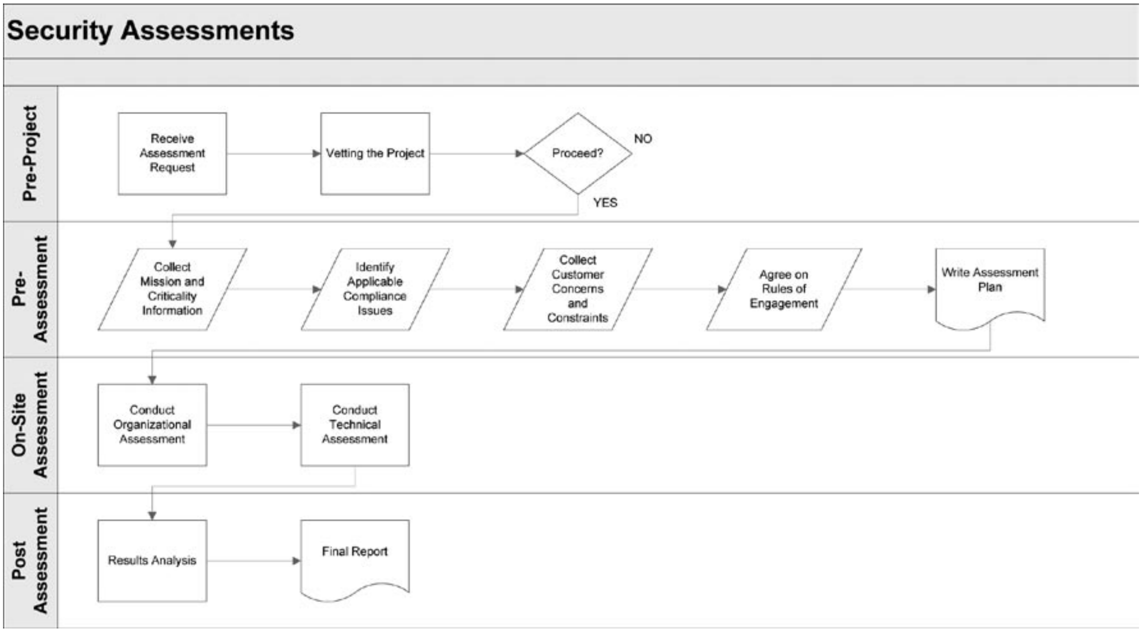
The Critical Infrastructure Information Act of 2002

The Critical Infrastructure Information Act of 2002 and subsequent procedure clarifications established how Critical Infrastructure Information (CII) is received, validated, handled, stored, marked, and used. SCADA Systems have both direct and indirect involvement with CII. The United States Department of Homeland Security defines CII as information not normally in the public domain (including system, facility, and operation security information) that is associated with the security of critical infrastructure or protected systems.

An Approach to SCADA Information Security Assessments

A methodology for conducting a security assessment is a process that utilizes a well-defined framework to identify the potential security vulnerabilities and determine what corrective measures must be implemented to protect the confidentiality, integrity, and availability of SCADA data. Figure 3.1 represents a logical flow diagram of the security assessment process. The National Security Agency (NSA) INFOSEC Assessment Methodology (IAM) and the INFOSEC Evaluation Methodology (IEM) are the cornerstone of the assessment process discussed in this chapter.

Figure 3.1 Security Assessment Flow Diagram


Security Assessments
Pre-Project
Receive Assessment Request
Vetting the Project
Proceed?
NO
YES
Pre-Assessment
Collect Mission and Criticality Information
Identify Applicable Compliance Issues
Collect Customer Concerns and Constraints
Agree on Rules of Engagement
Write Assessment Plan
On-Site Assessment
Conduct Organizational Assessment
Conduct Technical Assessment
Post Assessment
Results Analysis
Final Report

Prior to any project starting, several considerations must be taken into account to assure a complete understanding of the requirements. The pre-project activities will then lead into the three primary phases of the assessment, which are Pre-Assessment, On-Site Assessment, and Post-Assessment. Each phase will be outlined in the following sections. Table 3.2 provides a high-level breakdown of the activities that occur during the full assessment process.

Table 3.2 The Assessment Process

Pre-Project Activities	Pre-Assessment Phase	On-Site Phase	Post-Assessment Phase
Receive the Assessment request. Vet the assessment with the customer. Research the organization. Research applicable regulatory and policy requirements. Determine if it is a baseline activity or a repeat assessment. Make a go/no-go decision.	Refine customer needs. Gain an understanding of the customer mission. Gain an understanding of the criticality of the customer's information. Determine customer impact if confidentiality, integrity, and/or availability is lost. Identify systems, including system boundaries. Determine customer concerns and constraints. Coordinate logistics with the customer. Write the Assessment Plan.	Explore and confirm the information and conclusions made during the Pre-Assessment Phase. Perform data gathering and validation through interviews, documentation, and system demonstrations. Conduct technical scanning to determine technical vulnerabilities. Provide initial analysis and feedback to the customer.	Finalize analysis. Develop SVCM and OVCM information. Prepare and coordinate a final report.

Pre-Project Activities

Pre-project activities include several steps that assist the assessment providers in assuring a basic understanding of the security needs of the customer. Several primary actions in the pre-project area are important to prepare the assessors for conducting the assessment process. These include:

- Vetting the assessment request
- Gaining management and technical buy-in for the assessment
- Researching the organization
- Researching the current regulatory and policy requirements
- Determining whether the action is a baseline activity or a repeated assessment
- Making a go/no-go decision

Vetting the Assessment Request

Vetting, in this case, is simply assuring that the customer is getting both what they expect and what they need from the assessment process. Many times, organizations will catch hold of a buzzword like "penetration testing," "assessment," or "evaluation" without having an understanding of what the terms mean. A good approach to vetting is to spend quality time with the customer discussing the positive and negative aspects of each of the processes and explaining what the customer can expect at the end of the process, including deliverables.

The vetting process is accomplished by a combination of direct interaction with the customer and a small scoping questionnaire. It is then reinforced by educating the customer on the standard best practices for an assessment and any supporting regulations or policies that are applicable. Without the vetting process, you cannot understand or meet customer expectations, which can lead to project failure.

Gaining Buy-In from Management and Technical Personnel

Getting buy-in for the assessment from both the management staff and technical staff is essential to a successful project. Buy-in helps reinforce the importance of the assessment process and brings the organization's attention to the importance and benefits of conducting an assessment within the organization. Without buy-in, official and unofficial roadblocks or constraints may be put on the assessment team, which could lead to project failure. Work hard on the front-end of the project to assure this buy-in, which will assist in a good experience and a smooth-running assessment.

Management Buy-In

Management support for the assessment is absolutely required since management does several things that will drive the success or failure of the project. For instance, it sets the tone of the organization and the necessity to show how important security is to the organization. Management will also enforce the necessity of staff cooperating with, and supporting, the assessment team.

To gain management buy-in, include them in the process. Help them feel ownership of the information, the determinations, and the responsibility to assure security. The use of "Fear-Uncertainty-Doubt" (otherwise known as the FUD factor) as a tool for getting management support should only be used as a last resort. A better way is to help management understand considerations such as:

- Cost Avoidance
- Return on Investment (ROI)
- Regulatory Compliance
- Education
- Information Criticality, System Criticality, and Impact

Technical Staff Buy-In

Can you treat the technical staff the same way you treat management? The answer is, of course, NO! Technical staff will think of things from a different approach than management. Technical staff buy-in is also essential to the success of the project, however, so spend some quality time with the technical staff early in the assessment process. To gain technical staff buy-in, you must:

- Sell the assessment as an educational experience
- Show that you are there to help, not hurt, the organization
- Involve the technical staff in the process
- Demonstrate your knowledge and capabilities without being arrogant
- Develop a rapport with the technical staff

Researching the Organization

Another important step in understanding your customer is to research publicly available information about the organization. This will help display your interest in the customer, plus give you some points of discussion and clarification about the organization. Sources of information for this include:

- **The customer's Web site** Shows how the organization wants to be seen by the public.
- **The competitors of the customer Web sites** Shows the potential areas competitors see as important and may identify some deficiencies, as well as additional questions to ask the organization.
- **Whois** With a "whois" query, you can input a URL and learn what IP address is associated with that URL. In this case, it helps you understand who a customer's Internet service provider (ISP) might be and other possible interconnections within the customer environment.
- **Arin.net (American Registry for Internet Numbers)** Utilizes a special "whois" query of its database through entering an IP range; it will show ownership information of that range of IPs.
- **10Q/10K Reports** These are required quarterly (Q) and annual (K) reports that must be done by public companies to report the status of their business. It includes information like locations, employees, and so on, and may be useful in determining if there are areas of the business that may have been missed for assessment purposes.
- **Business discussion boards** These are Internet locations or blogs which discuss businesses in both a positive and/or negative way. These discussion boards can provide some useful information about the culture of the organization. However, you must be cautious since some of the information is more opinion- or emotion-driven than fact-driven.
- **Internet Search Engines** Any of the Internet search engines can help you find useful information beyond the organization's Web site. You might find articles written about the organization; press releases on products, services, or partnerships; and information about the corporation or leadership of the organization. This will help in better understanding the mission of the organization and its political and leadership structure.

TIP

Learn as much as possible about the customer before starting the project. This will assist in the assessment team's ability to effectively facilitate the assessment process.

Researching Regulatory and Policy Requirements

Most organizations are faced with the reality of falling under some kind of regulatory, legislative, or industry requirements. Especially when dealing with SCADA systems and other systems that affect critical infrastructure. Homeland Security Presidential Directive (HSPD) 7 drives the requirement for protecting critical infrastructure.

The pre-project efforts involve identifying the applicable regulations, legislation, and industry policies. This will vary between different organizations, and this research is essential to assure that you gather the appropriate requirements. You are conducting this research prior to the start of the project so you can talk coherently about the drivers and impacts within the organization. This does not mean you don't have to ask the organization about what they must follow since there may be some unique aspects of their business that must be considered. The following is just a starter list of the different regulatory or legislative requirements the organization may be affected by:

- **HIPAA** Health Information Portability and Accountability Act
- **SOX** Sarbanes-Oxley
- **PCI** Payment Card Industry
- **GLBA** Gramm-Leach-Bliley Act
- **FERPA** Family Educational Rights and Privacy Act
- **NERC** North American Electric Reliability Corporation
- **FERC** Federal Energy Regulatory Commission

Determining if this Is a Baseline Assessment or a Repeat Assessment

You are always hopeful this is not the first assessment that is being conducted on the SCADA system. However, due to the fact that SCADA security has been largely ignored over the years, this may very well be the first security assessment conducted. In that case, it is the baseline assessment. The value of it being a repeat assessment would be the existing information you can pull from to start the process. But if it is a baseline assessment, you need to expect to spend more time on the front-end of the project to document and better understand what is currently in place within the assessed organization.

Making a Go/No-Go Decision

Every project has a go/no-go decision point. In most cases, it will be a "Go"; however, if you cannot get management and technical support, or if there are severe limitations placed on the assessment team, you may have to make the difficult decision of "No-Go."

Pre-Assessment Activities

The Pre-Assessment process is an essential activity that will provide a great deal of information and important mechanisms to assure that the organization gains a level of buy-in from both management and technical staff.

The Pre-Assessment process provides the following important identification activities:

- Organizational mission
- Critical information
- Impact considerations
- Information criticality matrices
- Critical systems
- Defining of security objectives
- Logical and physical boundaries
- Rules of engagement, concerns, and constraints
- Legal authorization
- Writing the Assessment Plan

Determining the Organizational Mission

Understanding the organization mission assists in the remaining activities of the assessment. The mission will provide the final determination of what the security objectives and security requirements are for the organization. It will also drive the critical information considerations, impacts, and will lead to some of the concerns and constraints. To obtain this information, you must talk with the customer and take the information from the research completed in the pre-project activities. An example of a simplified organization mission might be: "Provide reliable electric power to the state of California while operating safely, securely, and within the federal, state, and regulatory guidelines." This will be documented in the Assessment Plan.

Identifying Critical Information

Critical information is simply the information that the organization requires to function. There is a tendency for firms to immediately jump to systems without thinking about what information is important to the organization. One aspect of critical information identification is that it must be done with the customer. In the end, it must be accepted by the organization as their information.

In order to get this critical information, a brainstorm session is typically done with various senior members of the organization in a brainstorming session. You will ask them, "What is the information you must have to make your organization function or to meet your mission?" You will then take that information and roll it up into a manageable set of critical information types. Please understand, this is not an easy process. You will need to spend a day or two with senior members of the organization to sort out this information. Some examples of possible information types might include:

- Power Consumption Information
- Generator Status Information
- Pump Station Information
- Personnel Information
- Scheduling Information
- Customer Information
- Billing Information

The lists will vary by organization and according to the industries in which the organizations function. You cannot do a "cookie cutter" listing of information types even if the organizations are in the same industry. Each organization will have different areas of concern, different customers, and different business processes, all of which will drive different critical information types.

Example: Information Criticality

The Organization for Optimal Power Supply (OOPS) example will be utilized throughout the rest of the chapter—for example, purposes under permission from National Security Agency (NSA) INFOSEC Assurance Training and Rating Program (IATRP). More information on IATRP can be found at www.iatrp.com.

Business Description

The Organization for Optimal Power Supply (OOPS) provides electricity to 1/20th of the United States' citizens. They constantly monitor power consumption and redirect power according to demands. This includes initiating or terminating operations of generator stations.

Historically, OOPS has had a difficult time starting up idle generator stations when they are needed. Therefore, they have decided to place servers in each station to control the generator's output and status. To activate a generator station, the regional office calls into the server and logs onto the machine. After a generator station has been activated, it updates its status and output to the regional server using hourly dial-up connections.

The control of all the OOPS generators is run through a main control center at the corporate headquarters. The control center decides when to activate any generators and which areas are in need of power. All of the regional offices are connected to the main server via frame relay lines, which allow for rapid updates of the current situation. All updates are done automatically by the servers, but can be initiated by authorized users if necessary.

Mission Statement

The Organization for Optimal Power Supply (OOPS) provides electricity to 1/20th of the United States' citizens. OOPS constantly monitors power consumption and redirects power according to demands. This includes initiating or terminating operations of generator stations.

Critical Information for OOPS

Through a brainstorming session and detailed conversations with the OOPS customer, the following critical information types were agreed to between the assessment team and OOPS:

- Power Consumption Information
- Power Forecast Information
- Generator Status Information
- Customer Information
- Corporate Information
- Personnel Information

Please remember, this is not system information, but information that is needed for the OOPS to continue operations. The loss of confidentiality, integrity, and/or availability (CIA) of this critical information may lead to temporary or permanent damage to overall business operations or the business mission.

Identifying Impacts

The next step in the process is to identify the impact to the organization if there is a loss of CIA of the identified critical information. It is important at this point to identify the definitions of CIA.

- **Confidentiality** The information is only viewable by those with a need and an authorization to view it. Others may not view it. Sometimes called "need-to-know."
- **Integrity** The information is unchanged from its original state.
- **Availability** The information is there when needed by those with the authorization to access or view it.

The organization may choose to add additional impact categories based on the business needs. Some of these additional categories may include (but are not limited to):

- Non-repudiation
- Accountability

- Authorization
- Accessibility

Identifying the impacts to an organization is absolutely the hardest part of the assessment methodology. An important aspect of identification of impact definition is that it must be done with the customer since it has to have the customer's stamp of approval when completed. Why is this so difficult? Getting the customer to agree with themselves on what it means to lose CIA of their critical information is very difficult. It requires them to seriously consider their overall business operations, conduct a type of business impact analysis, and actually document and agree to the impacts as a whole based on their mission. The impact definitions are generally defined as High, Medium, and Low Impact.

Example Continued: OOPS Impact

In real-world situations, definitions will typically be between half a page and one page long. For presentation purposes in this chapter, we will keep it simple. However, please understand that this is just an example and more detail is needed to get a full picture of impact. For our purposes, the identified impacts to OOPS for the loss of CIA are the following:

- **High Impact** Competitive market loss greater than 10 percent; rolling blackouts; loss of generator station control greater than one hour.
- **Medium Impact** Competitive market loss greater than 3 percent but less than 10 percent, or a regional blackout; or loss of generator station control greater than 15 minutes but less than one hour.
- **Low Impact** Competitive market loss less than 3 percent or a regional brownout; or loss of generator station control less than 15 minutes.

The Information Criticality Matrix

Taking into consideration the critical information types and the impact attributes, we can now build an information criticality matrix. The top line is simply the impact attributes (CIAs), while the rows are the critical information types identified by the organization. Table 3.3 represents the framework for the Organizational Information Criticality Matrix (OICM).

Table 3.3 OICM Framework

OICM	Confidentiality	Integrity	Availability
Critical Info 1			
Critical Info 2			
Critical Info 3			
Critical Info 4, etc...			

Using the Impact Definitions

The impact definitions previously created are used to fill out the matrix. Be sure to create the impact definitions before trying to complete the matrix. The definitions of High, Medium, and Low will be utilized to determine what the impact is for the loss of any aspect of CIA. Table 3.4 represents what the chart may look like when the values are input into the OICM.

Table 3.4 OICM Sample

OICM	Confidentiality	Integrity	Availability
Critical Info 1	H	H	M
Critical Info 2	H	M	M
Critical Info 3	L	L	M
Critical Info 4, etc...	H	M	L

Organizational Criticality

The last step with the OICM is to take the highest level in each column to summarize the table and indicate the most critical impact areas for the organization. For our sample based on Table 3.5, the Organizational Criticality (sometimes called the "high water mark") would be the following.

Table 3.5 An Organizational Criticality Sample

	Confidentiality	Integrity	Availability
Organizational Criticality	H	H	M

Example Continued: OOPS OICM

Based on the information we obtained from OOPS and through various discussions, we can now create the OICM for OOPS. Remember, we are using the definitions created earlier to fill out the matrix.

To complete this matrix, start with the first information type and ask yourself, "What can happen if I lose the confidentiality of my power consumption information?" Loss of the confidentiality of the power consumption information would result in a 3 percent or less competitive market loss, which is a Low. You then go to the next impact attribute, which is integrity. Again, ask yourself, "What can happen if I lose the integrity of my power consumption information?" In this case, inaccurate power consumption information could result in the generation of too much, or too little power, which could lead to brownouts or blackouts and loss of revenue or competitive advantage and would have a High Impact. The loss of availability of your power consumption information would have the same impact as loss of integrity.

Let us work through the Generator Status Information type. If you lose the confidentiality of the generator status information, you may end up having too much information available to the public, allowing someone with ill intent to attempt to exploit the information to their advantage. For example, if it is known that a particular generator is down for maintenance and the backup generator is in use, someone could target the backup generator as a weak point in the system with no current backup capabilities. Therefore, the loss of confidentiality of the Generator Status Information would be at least a Medium. You do the same analysis with integrity and availability and find they could lead to High Impacts because they could cause brownouts or blackouts and a loss of revenue or competitive advantage. They could also lead to serious damage to the equipment.

Use the same concepts to complete the rest of the matrix, as shown in Table 3.6. Remember, however, that the matrix must be completed with the customer, and ultimately approved by the customer.

Table 3.6 OOPS OICM

OICM	Confidentiality	Integrity	Availability
Power Consumption	L	H	H
Power Forecasts	L	M	M
Generator Status Information	M	H	H
Customer Information	M	M	M
Corporate Information	M	M	M
Personnel Information	M	M	L

Now we determine the organizational criticality based on the highest level in each column and end up with the result displayed in Table 3.7. This shows that integrity and availability have a higher importance than confidentiality in relation to OOPS. This may be a common organizational criticality you might see within the SCADA environment.

Table 3.7 OOPS Organizational Criticality

OOPS Organizational Criticality	Confidentiality	Integrity	Availability
	M	H	H

Identifying Critical Systems/Networks

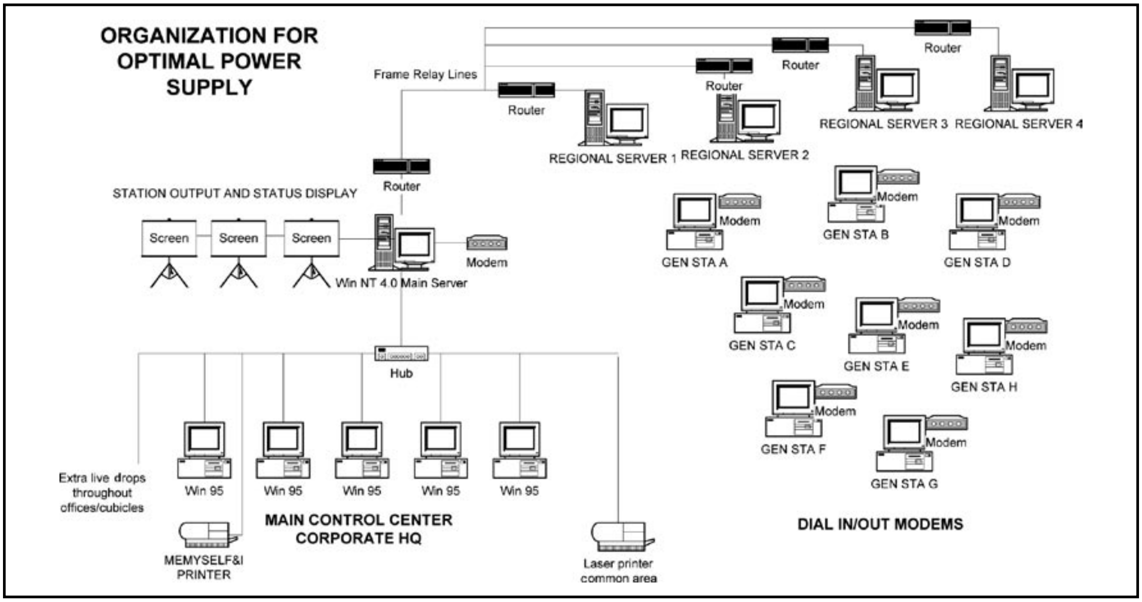
Critical systems can be defined as those systems that process, transmit, and/or store the critical information that was identified in the information criticality step. For our purposes, a system is not a single box but a group of components that work together to perform a function. You will identify the systems by communicating with the customer, looking at network and system diagrams, and asking many questions.

OOPS Example Continued

Note from Figure 3.2 that there are three (3) primary functional networks: The Main Control Center, the Corporate HQ Network, and the Regional Generator Station

Controller. After the identification of the primary systems/networks, we are going to build a system criticality matrix for each. To do this, we utilize the information from the information criticality matrix and simply identify which critical information types are processed, transmitted, and/or stored on the identified systems/networks.

Figure 3.2 The Logical Network Diagram for OOPS



You will want to confirm with the OOPS personnel, but we can make a fairly logical guess that the following information types are processed, transmitted, and/or stored on the following:

- Main Control Center
- Power Consumption
- Power Forecasts
- Generator Status
- Corporate Head Quarters Network
- Customer Information
- Corporate Information

- Personnel Information
- Regional Generator Station Controller
- Generator Status
- Power Consumption

Each system criticality matrix is created by simply cutting and pasting the applicable row from the OICM as demonstrated in the following three (3) tables. For each of the System Criticality Matrices, we can also do an overall "high water mark," which is demonstrated as well.

Table 3.8 Main Control Center System Criticality Matrix

Main Control Center	Confidentiality	Integrity	Availability
Power Consumption	L	H	H
Power Forecasts	L	M	M
Generator Status Information	M	H	H
Overall	M	H	H

Table 3.9 Corporate Network System Criticality Matrix

Corporate Network	Confidentiality	Integrity	Availability
Customer Information	M	M	M
Corporate Information	M	M	M
Personnel Information	M	M	L
Overall	M	M	M

Table 3.10 Regional Generator Station Controllers

Regional Generator Station Controllers	Confidentiality	Integrity	Availability
Power Consumption	L	H	H
Generator Status Information	M	H	H
Overall	M	H	H

Defining Security Objectives

Security Objectives are the targets the customer establishes for their security program. Without security objectives, they do not know what they are trying to accomplish for security and therefore will not reach any goals. Security Objectives are one of those areas requiring the customer's involvement, and so the assessment team cannot make up the information.

Security Objectives come from a combination of inputs, including:

- Customer Mission
- Regulatory Requirements
- Business Objectives
- Best Practices
- Industry Practices

Security Objectives need to be well-defined and made known throughout the organization. Ultimately, the security objectives should be tied to the business objectives of the organization.

TIP

Security Objectives are not where the customer's security posture is today, but where they want it to be in the future. The actual security posture will be determined by the assessment process, and the difference between the Security Objectives and the Security Posture is the Security Gap.

Determining Logical and Physical Boundaries

Understanding the logical and physical boundaries for the assessment plays an important role in managing the scope of the effort and preventing exceeding the bounds of the approved assessment and the scope. Be specific when defining the boundaries to assure a clear understanding.

Physical Boundaries

Physical boundaries are boundaries you can generally reach out and touch. These would include:

- Fences
- Doors
- Locks
- Gate Guards
- Others

Logical Boundaries

Logical boundaries are those you cannot necessarily touch, but that are logical in nature. These include such things as:

- Router ACLs
- Firewall Rule Sets
- Ownership Differences
- Loss of Network Control
- Others

Determining the Rules of Engagement, Customer Concerns, and Customer Constraints

The rules of engagement, customer concerns, and customer constraints play an important role in baselining, scoping, and in better understanding the customer and any existing limitations.

The Rules of Engagement

The rules of engagement establish an understanding between the assessment team and the customer for those actions that will be part of the assessment. By establishing these rules, it allows both the assessment team and the customer to address any special needs. Included in the rules of engagement are:

- Levels of Invasiveness
- Testing Machine Addressing
- Timeframes for Scanning and Interviews
- Notification Procedures
- Scanning Tools and Exclusions

Levels of Invasiveness

The typical technical assessment is not intended to be a penetration test or a red team. However, a customer may want additional activities above and beyond the standard evaluation to address some of their concerns. Some common additions to the standard activities for more invasive testing include:

- Denial of Service testing
- Distributed Denial of Service testing
- War dialing
- Social engineering
- Dumpster diving

Testing Machine Addressing

Arrange with the customer to obtain a static IP address for the scanning machines while conducting on-site activities. If this is not possible, ask the customer to implement an extended DHCP lease for these scanning machines to assure the IP addresses remain unchanged.You desire for the customer to know which scanning is coming from the assessment team.This is a cooperative effort and you don't want someone implementing the Incident Response Plan inadvertently.

For external scanning, assure that the customer is aware of the external IP addresses the scans will be originating from during the testing.Again, you desire the customer to know it is an approved assessment team conducting the scanning and to know when it is an unauthorized entity running scans.

Time Frames for Scanning and Interviews

Every organization varies regarding when they are comfortable having scans run on their systems and networks. Since it is a cooperative effort, the assessment team will need to understand when peak processing times are on the systems and networks, as well as the potential impact to some important clients. In some organizations it is okay to scan at anytime. Others have limitations related to batch processing, or peak access times. These will be taken into account when planning and writing the Assessment Plan.

Conducting assessment interviews will also have an impact on the organization's operations. The interview process should be documented in the Assessment Plan to assure there is an understanding of how the interviews are to be conducted and make certain that facilities are available to hold the interviews themselves.

Notification Procedures

Notification procedures are a necessity to address emergency situations where a system or server may have stopped operating during the testing. It is an objective of the NSA Methodologies to impact customers as little as possible. There also needs to be an understanding that bad things can happen and you must be prepared for any necessary recovery activities. Ask the customer to provide contacts that will be available to cover the time frames the team will be working with on the assessment effort.

Scanning Tools and Exclusions

NSA does not dictate the tools to be used for the technical scanning as part of the IEM process. However, the customer may not want certain tools used in their environment due to either a bad experience or things they may have heard from other organizations. It is important to honor these exclusions but try to understand why they have them.

Customer Concerns

Customer concerns are anything the customer has expressed as something they are particularly interested in or concerned about. This would include concerns about how the assessment might impact the customer's network. They may also express a particular interest in one of the 18 Baseline INFOSEC Classes and Categories, which is introduced later in this chapter. Be sure to document any customer concerns in the

Assessment Plan that were mentioned and be prepared to discuss them in the closing meeting and final report.

Customer Constraints

Customer constraints are simply anything that may limit the execution of the assessment or limit the recommendations that are made as a result of the assessment. Be sure to document any customer constraints in the Assessment Plan that were mentioned and be prepared to discuss these in the closing meeting and final report.

Legal Authorization

Since the assessment work includes a technical component that involves connecting to the customer's networks and systems, there is a definite need to address the legal concerns. NSA recommends the assessment team have a "Letter of Authorization (LOA)" that is signed by the customer, which shows clear approval for the work being done. A copy of the LOA should be in the possession of each assessment team member while performing this work. I am not a lawyer and my lawyer says I cannot give legal advice; therefore, any work on the LOA will need to involve legal counsel from both the assessment team and the customer.

Writing the Assessment Plan

The Assessment Plan will encompass all of the considerations to conduct both an organizational and technical assessment for the organization. This is the scoping document and agreement between the assessment team and the customer to assure the full scope is well defined. Everything we have covered in the Pre-Assessment Process is to be documented in the Assessment Plan. The Assessment Plan will then be signed off on by both sides to assure mutual acceptance.

Components of the Assessment Plan

The following outline for the Assessment Plan takes into consideration the needs for understanding both the organizational and technical information necessary to accomplish the full assessment effort. These would be minimum essential considerations and may require additional business processes built around it to meet your organizational needs. This information is a combination of the Assessment Plan and the Technical Evaluation Plan that is part of the NSA IAM and IEM frameworks.

- Important Evaluation Points-of-Contact POC name, phone number, and e-mail
- Methodology Overview Describe the methodology to be used to conduct the evaluation and identify the specific evaluation tools to be used during the evaluation process.
- Criticality Information A representation of the information criticality for each organizational system determined by discussion with the customer. Should include Organizational Criticality Matrix, System Criticality Matrices, Impact Value Definitions, and System Descriptions.
- Detailed Network Information Include physical boundaries, identified subnets and IP ranges, detailed network diagrams, and contact information for system owners and administrators.
- Customer Concerns Include organizational and technical customer concerns.
- Customer Constraints Include organizational and technical customer constraints.
- Rules of Engagement:
- Network connections and IP addresses, facilities, and so on. Scan windows, relevant IP addresses or subnets to access, and immediate administrator contact information for the customer.
- Internal and External Evaluation Team Requirements.
- Internal and External Customer Requirements.
- Evaluation team's scanning of IP addresses, immediate contact information for assessment team, notification of personnel on assessment activities, CIRT coordination for test purposes.
- Coordination Agreements:
- Level of Detail for Recommendations How detailed does the customer want the recommendations to be? Will the standard low level for the executive summary and the mid-level for technical be ok, or is more detail going to be required?
- List of Deliverables.
- Anything not addressable in the other sections.

- Letter of Authorization Include the approved Letter of Authorization.
- Time-Line of Events A sequence of important events and their associated dates. Some events include the following: the date of the receipt of the request letter, the date of the proposal or contract, customer coordination dates, planned internal and external dates, the report delivery.

On-Site Assessment Activities

The On-Site Assessment is where the majority of the actual vulnerabilities will be identified for the organization and systems. This identification will include both organizational and technical findings. The way vulnerabilities are identified for the organization and the technical areas are different and are discussed next.

Conducting the Organizational Assessment

The organizational vulnerabilities are identified using the following methods:

- Documentation Review
- Interviews
- System Demonstrations
- Observation

The organizational portion of the assessment is focused around understanding the organizational security support concerning a set of control families or classes and categories. NIST identified 17 control families that must be considered as part of the controls put into place for federal government systems. These control families were identified earlier in Table 3.1.

NSA identifies 18 baseline categories to consider as part of any security implementation and are arranged by management, technical, and operational controls. This list of 18 areas is located in Table 3.11.

Table 3.11 NSA 18 Baseline INFOSEC Classes and Categories

Management	Technical	Operational
INFOSEC Documentation	Identification and Authentication	Media Controls
		Labeling
INFOSEC Roles and Responsibilities	Account Management	Physical Environment
	Session Controls	Personnel Security
Contingency Planning	Auditing	Education Training and Awareness
Configuration Management	Malicious Code Protection	
	Maintenance	
	System Assurance	
	Networking/Connectivity	
	Communications Security	

As you can see from the table, these control families and security categories are very comprehensive lists, covering a large volume of security considerations that must be part of a security review.

Documentation Review

Documentation plays a significant role in establishing the foundation for an organization's security program. The organization should use documentation to set the organization's vision and expectations. Documentation serves several purposes, including education, enforcement, and continuity. Lack of documentation within an organization would be a potential security vulnerability; however, it is unlikely it would be your only security finding. Documentation should establish the formal way an organization should be implementing their security program.

Interviews

Interviews are a key way to discover how the organization is actually doing things. Interview techniques are out of scope for this chapter, but understand that there is a psychology to interviews or "discussions." In order to get the information you need from the individuals you are interviewing, you must first gain their trust. Remember you are not an auditor or an inspector—you are there to help the organization (and individuals) improve their security.

System Demonstrations

System demonstrations are an alternative way to get technical information from the organization without being required to run scanning tools or access their systems. It is simply a "Show-Me" activity. If you need clarification or information about something, you can simply say "Show me how you do that."

NOTE

With System Demonstrations, the assessment team does not need to touch the customer network. They are basically shoulder surfing the customer technical person to see how the action is actually conducted.

Observation

The powers of observation are an inherent capability required of the typical security professional. From the very beginning of the assessment, you are watching what the organization does, how they treat employees, how they handle visitors, and the kinds of information that are freely available within the organization. This will lead you to additional questions, system demonstrations, or interviews.

NOTE

Observation is not actually listed as an IAM activity but is an implied part of the IAM.

Conducting the Technical Assessment

The technical portion of the assessment focuses on identifying and understanding the technical vulnerabilities that may exist within the SCADA environment. The technical assessment is referred to as an evaluation by NSA. The primary basis for these activities is defined in the NSA IEM. The IEM utilizes ten baseline activities that are necessary for consideration while conducting the technical portion of the assessment. These ten activities are broken out by enumeration and vulnerability identification areas, as identified in Table 3.12.

Table 3.12 NSA Evaluation Activities

Enumeration	Vulnerability Identification
Port Scanning	Vulnerability Scanning
SNMP Scanning	Host Evaluation
Enumeration and Banner Grabbing	Network Device Analysis
Wireless Enumeration	Password Compliance Testing
	Application-Specific Scanning
	Network Sniffing

Enumeration Activities

Enumeration activities are used to determine what kinds of systems, applications, processes, and devices are on the customer systems. Enumeration activities are basically discovery activities that include:

- **Port Scanning** The act of connecting to potential services or ports on network accessible systems to determine what services and applications may be running on the network.
- **SNMP Scanning** With a known "community string," active SNMP scanning can show information on user accounts, operating systems, services, and shared printers.
- **Enumeration and Banner Grabbing** Enumeration tries to determine information such as users, servers, shared file systems, and other shared resources. Banner grabbing is a process of reaching out to an application and seeing if there is information about the application that can be pulled or "grabbed."
- **Wireless Enumeration** Looks for wireless networks that are part of the organization and how they are configured and secured. Also looks for external wireless networks that may impact the organization and searches for potential rogue wireless networks.

Vulnerability Identification Activities

Vulnerability identification activities are the activities where a majority of the technical vulnerabilities will be discovered. The activities for vulnerability identification include:

- **Vulnerability Scanning** This activity is where the majority of vulnerabilities will be found. Vulnerability scanning runs from the network presence and looks for known vulnerabilities in the tools database.
- **Host Evaluation** Look directly at individual systems to determine if they are configured with secure configurations and settings.
- **Network Device Analysis** Analyze critical network devices to determine secure configuration and to evaluate if the device itself is functioning to provide security.
- **Password Compliance Testing** Test passwords to determine if the password policies are implemented and effective.
- **Application Specific Scanning** Review the security of application functionality and secure programming techniques.
- **Network Sniffing** Analyze network traffic to determine what protocols are being used and if there is clear-text-sensitive information traversing the network.

Are You Owned?

Configuration Issues

The majority of security vulnerabilities found in the technical systems are a result of system configuration issues or lack of up-to-date patching. This is significant because with SCADA systems, integrity and availability are the highest impact attribute concerns. Configuration changes and patching can impact system availability and therefore are often ignored. As an example, a client was having an assessment conducted on their network. The moment a simple port scan started, the network went down and the technical personnel were freaking out. Turns out the organization had an older version of the Cisco IOS on their routers, which had a known flaw of crashing when port scanned. This created only denial of service (an availability issue) but if you remember, availability was rated as High Impact.

Tools

The tools used to conduct the ten IEM baseline activities are determined by the team conducting the assessment work. NSA does not specifically imply or endorse any specific technical security tool or brand of tool. You can use freeware, shareware, or licensed tools. The IEM specifically requires you to run at least one tool to cover each of the ten activities. It is highly recommended you use more than one tool to cover each activity due to the limitations of the tools themselves. The tools are only as good as their underlying databases and the configuration the security consultants give to the tool.

WARNING

One of the most DANGEROUS things you can do while conducting a security assessment is to not understand how your scanning tools work and how the configurations impact the scan results. Creating mass denial of service to a customer because of poor tool configuration is a VERY BAD IDEA and you may never regain the trust of your customer again.

Communication

Communication with the customer is required to assist in managing customer expectations. This involves assuring the proper opening meetings, closing meetings, and update meetings are conducted during the on-site effort. Good communications will reduce the number of potential issues between the customer and the assessment team.

Post Assessment Activities

The Post Assessment process involves taking all the information collected about potential vulnerabilities and determining the real risk to the organization. It is essential that the information gained in the Pre-Assessment process be taken into consideration during the analysis and reporting portion of the assessment.

Conducting Analysis

Detailed analysis not only involves looking at the scan results, it also involves using the skills and talents of the assessment team to determine the impact to the customer if a vulnerability is exploited. The assessment team cannot just "cut and paste" from the scanning tools, they must apply real analysis skills to the process. Effective analysis may involve bringing in additional expertise or conducting additional research to better determine how a particular vulnerability affects a customer.

Final Report Creation

The final report is the record of the activities conducted and the findings discovered during the assessment process. The final report needs to be a clear and concise document that provides a clear picture of the results. The minimum essential components of the final report should include:

- **Executive Summary** A short and concise description of the assessment and the major findings, written so executives can understand the results.
- **Introduction** This section will include a great deal of information from the Assessment Plan since it describes what was done during the assessment, which should be what you agreed to in the Assessment Plan.
- **Analysis** This section identifies what was found during the organization and technical assessment processes. This will include a detailed description of the finding, the analysis of how the finding affects the customer, and recommendations providing options.
- **Conclusion** Answer the question for the organization: "What is my INFOSEC posture?" Recognize good security practices. Provide a recommended priority and roadmap for improving the organization's security posture.
- **Appendices** Include the analysis documents, the Assessment Plan, and a CD or other storage device with the raw scan reports on them.

NOTE

Complete the final report within a reasonable time frame so the process and results are still fresh in the customer's minds. Taking too long to complete the report will make it more difficult for the organization to get started on your recommendations.

Resources

It is always helpful to have recommended resources for your client to get additional information on SCADA security or security assessments. I mention only a few here, but remember that your Web browser is a tremendous research tool. Some Assessment- and SCADA-related sites include:

- **NSA INFOSEC Assurance Training and Rating Program** www.iatrp.com
- **NIST Special Publication 800-82: Guide to Industrial Control System Security** www.nist.gov
- **Digital Bond** www.digitalbond.com

Summary

The evolution of SCADA systems toward standard TCP/IP networking and common applications is driving the need to implement and monitor effective security. Historically, SCADA systems have been considered separate systems that were not interconnected with the corporate network. Now the movement has been toward connecting to the internal intranets and even the Internet. This opens the possibility for the exploitation of holes in the security of these connected components. Implementing effective security and evaluating this security is critical to the continued successful operation of the SCADA environment.

An effective security assessment involves utilizing a solid defined framework that is repeatable. The NSA IAM and IEM provide a framework to work within for purposes of conducting the security assessment process. Four primary activities are discussed as part of the IAM and IEM, which support the security assessment process. These are:

- Pre-Project Activities
- Pre-Assessment
- On-Site Assessment
- Post Assessment

The Pre-Project activities focus on gaining an understanding of what the customer is looking for in their security assessment engagement. Helping the customer get the service that will best benefit them will assist in establishing and managing the customer's expectations. You will also want to address business processes, such as contracting and initiating legal aspects.

The Pre-Assessment process is an essential process for better understanding the customer's needs. A great deal of the Pre-Assessment process involves understanding the customer mission and understanding the business information needed to make the organization run. This is a business focus, not just a security focus. Business risk and security risk are closely associated. An understanding of the impact to the organization if confidentiality, integrity, and/or availability are lost helps the assessment team better recommend improvements to the organization's environment. Following the assessment team's understanding of the mission, critical information, and impact, we go through the process of understanding which systems process, transmit, and/or store this critical information. The remaining portion of the Pre-Assessment process involves finalizing the scope of the assessment, establishing rules of engagement, defining customer concerns and constraints, and establishing timelines to meet and manage customer expectations.

The On-Site Assessment is broken down into two (2) areas: organizational and technical. The organizational assessment focuses on understanding what policies and procedures are in place in the organization and how the organization actually implements the security program. The information for the organizational assessment is collected based on interviews, documentation review, system demonstrations, and observation. The organizational assessment is also conducted based on the NSA IAM 18 Baseline INFOSEC Classes and Categories, or the NIST 17 Control Families. The organizational assessment is flexible enough to pull in the security requirements of any organizational need, including SCADA.

The second part of the On-Site Assessment is the technical assessment (or evaluation). The basis for the technical assessment is the NSA IEM 10 Baseline Activities, which encompass the majority of the technical scanning and analysis needs for a security assessment. The key consideration of using the NSA IEM is that it is not a "cut and paste" from the scanning tools, but a true analysis of the data collected to determine the technical vulnerabilities.

The Post Assessment process involves conducting the final analysis and putting together the final report. This process is important because it outlines the findings from the assessment process and gives the recommendations for improvement of the organization's security posture. A critical aspect of the Post Assessment is to give a well-defined logical roadmap for security posture improvement.

SCADA systems control the majority of our critical infrastructure to include power, water, and sewage. Without the right security implementations and the continuous monitoring and assessment of SCADA system security, there could be a significant loss of confidentiality, integrity, and availability of the critical infrastructure.

Solutions Fast Track

The Evolution of SCADA

☑ SCADA systems have historically been treated as isolated entities that are relatively safe from security issues.

☑ SCADA has evolved to utilize the same protocols as traditional networks; therefore, additional exposure now exists.

- ☑ SCADA is now being connected to the business network, exposing it to potential security issues.
- ☑ SCADA configurations and security must be tightly controlled.

SCADA Assessment Methodologies

- ☑ Choose a viable repeatable methodology for doing SCADA security assessments.
- ☑ The NSA IAM and IEM are recognized methodologies to consider.
- ☑ NIST has created guidance for securing SCADA systems with their NIST SP 800-82.

Pre-Project Activities

- ☑ Vet the assessment request to assure the customer is getting what they need/want.
- ☑ Collect and analyze as much publicly available information as possible.
- ☑ Implement business processes to gain an agreement to proceed.

Pre-Assessment Activities

- ☑ Collect mission and business critical information, and impact if confidentiality, integrity, and/or availability are lost.
- ☑ Determine the systems that process, transmit, and/or store the critical information.
- ☑ Fully scope out the effort with the customer to include concerns, constraints, and rules of engagement.
- ☑ Write the Assessment Plan based on the Pre-Assessment activities and get a signature from the customer.

On-Site Assessment: Organizational Security

- ☑ Conduct interviews utilizing the NSA IAM 18 Baseline INFOSEC Classes and Categories as a guide or something similar, such as the NIST 17 Control Families.

☑ Review organizational security and business documentation.

☑ Utilize system demonstrations to verify information or reduce conflict concerning the same.

☑ Use observation to continuously determine how the organization actually implements security.

On-Site Assessment: Technical Security

☑ Conducted based on the NSA IEM 10 Evaluation Activities.

☑ Start by enumerating the network and systems.

☑ Conduct activities to collect actual vulnerability information (for example, scanning).

Post Assessment Activities

☑ Analyze the data to determine the vulnerabilities.

☑ Complete the final report in a timely manner.

☑ Provide the organization with a roadmap to an improved security posture.

Resources

☑ www.iatrp.com

☑ www.nist.gov

☑ www.digitalbond.com

Frequently Asked Questions

Q: I have never needed to worry about SCADA security in the past. Why should I now?

A: SCADA systems have migrated toward common protocols such as TCP/IP instead of previously proprietary protocols. SCADA systems are now being interconnected on the same network as the business network, allowing for greater avenues of attack.

Q: Why are the NSA IAM and IEM recommended as the methodology to use for SCADA assessments?

A: These are extremely flexible methodologies that provide a clear and comprehensive framework for doing any kind of security assessment. The NSA IAM and IEM are not the only methodologies out there and the assessment team can choose which methodology to use. Be sure that, no matter which methodology you use, it covers a similar or better cross-section of information security topics.

Q: Why not just give the potential customer exactly what they ask for?

A: Because what they ask for may not be what they are really looking for. Be sure to conduct the Vetting process to give the customer what they need.

Q: Is understanding critical information and impact important? Don't we just need to know the systems?

A: Understanding critical information and impact is essential to defining appropriate recommendations to improve the security posture. This process answers the question of "Why" security needs to be implemented and how much security is required.

Q: Why is the On-Site Assessment work broken out between organizational and technical?

A: The quick answer is because of the skill set. The skill set required for an individual to conduct the technical assessment is significantly different than those individuals who are conducting the assessment.

Q: Can't I just "cut and paste" the results out of the scanning tools?

A: No. You must conduct an analysis to make it specifically relevant to that particular organization.

Q: Can I get more help when I am conducting an analysis?

A: Absolutely. Don't be afraid to seek assistance either by doing additional research or bringing in additional expertise.

Q: Are the NSA IAM and IEM rigid methodologies?

A: No. The NSA IAM and IEM are very flexible methodologies that are usable across a broad section of organizational types.

تأكيد

رقم الحجز: **4QFFPT - 042615152529**

تفاصيل الإسترداد

السعر الحالي للمسافر

ثمن التذكرة	**SD 129.00**
الضرائب	**SD 56.26**

مجموع المبالغ المدفوعة

USD 185.26

الرسوم

رسوم الإسترداد	**SD 67.00**

رسوم الإسترداد

USD 67.00

إجمالي مبلغ الإسترداد	**USD 118.26**

استرداد المبلغ المدفوع

تم إعادة المبلغ بنجاح:

استرداد المبلغ عبر بطاقة الإئتمان: السيدة Bahia Elissawi, البطاقة فيزا 4204************
إجمالي مبلغ الإسترداد: **(USD)118.26**

حجز جديد

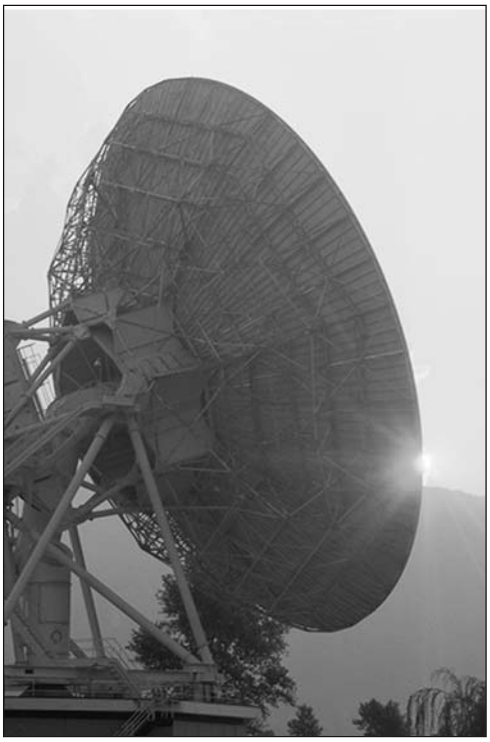
إتصل بنا | الأمن والخصوصية | لوائح الإستخدام | الأسئلة المتكررة | تحالف سكاى تيم | الصفحة الرئيسية

Practical

SCADA SYSTEMS

for Industry

AHMEDABAD - 30th SEPTEMBER & 1st OCTOBER, 2009



IDC TECHNOLOGIES

Technology Training that Works

FOCUSSING ON:

- Fundamentals of SCADA Systems
- Communication Protocols & Standards
- Essentials of OPC applied to SCADA
- Wireless for SCADA
- SCADA System Security

WHAT YOU WILL GAIN:

At the end of this workshop participants will have an understanding of:

- The fundamentals of SCADA systems
- The essentials of SCADA software configuration
- Tricks and tips in installation of SCADA systems
- The essentials of SCADA telecommunications links
- The use of Industrial Ethernet in SCADA systems
- OPC and SCADA systems
- SCADA network security issues
- How to troubleshoot SCADA systems

WHO SHOULD ATTEND:

- Instrumentation and Control Engineers
- Process Control Engineers
- Electrical Engineers
- Consulting Engineers
- Design Engineers
- Control Systems Sales Engineer
- Maintenance Supervisors
- Control System Application Engineers
- Project Engineers
- Technicians
- Plant Engineers
- IT Personnel

FOR REGISTRATION CONTACT (044)-42089353 or E-mail to india@idc-online.com

THE WORKSHOP

SCADA has traditionally meant a window into the process of a plant or gathering of data from devices in the field, but now the focus is on integrating this process data into the actual business and using it in real time. The emphasis today, is on using Open Standards such as communication protocols (eg IEC 60870, DNP3 and TCP/IP) and 'off-the-shelf' hardware and software to keep the costs down. This comprehensive two day workshop covers the essentials of SCADA systems.

A selection of case studies is used to illustrate the key concepts with examples of real world working SCADA systems in the water, electrical and processing industries. This workshop will be an excellent opportunity to network with your peers as well as gain significant new information and techniques for your next SCADA project.

Although the emphasis of the workshop will be on practical industry topics highlighting recent developments using case studies. The latest application of SCADA technologies and the fundamentals of SCADA systems will be covered. The workshop is aimed at those who want to be updated on the latest developments in SCADA systems and want to get a solid appreciation of the fundamentals of SCADA design, installation and troubleshooting.

Your Instructor

Mr. Ashish Ranjan Nath
B. Tech. (Hons.) –
Instrumentation & Electronics Engineering
M. E.–Electronics in Computer Engineering

An Engineer and a Professor with 32 years years of experience, he has been involved large capacity projects for many industries including the power, petrochemicals, paper, cement and fertiliser industries. To add to his extensive industry experience he has also worked with utilities such as HVAC, electric furnaces, water and waste water.

Through this he has gained valuable experience in project engineering, project management, erection and commissioning and facility engineering.

He has supervised the development of a large number of products and systems for industrial application and as a technical educator has taught engineering subjects at a university level.

He was also involved in developing a custom built PC based automation system using virtual instrumentation.

THE PROGRAM

DAY ONE

BACKGROUND TO SCADA

- Fundamentals
- Comparison of SCADA, DCS, PLC and Smart Instruments
- Typical SCADA installations
- Definition of terms

SCADA SYSTEMS HARDWARE

- Fundamentals
- Comparison of SCADA, DCS, PLC and Smart Instruments
- Typical SCADA installations
- Definition of terms
- Remote Terminal Unit (RTU) structure
- Analog and Digital input/output modules
- Application programs
- PLC's used as RTU's
- Master site structure
- Communications architectures
- Point-to-point and point-to-multipoint systems
- System reliability and availability
- Configuration of a master station

SCADA SYSTEMS SOFTWARE

- Fundamentals
- Components of a SCADA system
- Software - Design of SCADA packages
- Configuration of SCADA systems
- Building the user interface
- Connecting to PLC's and other hardware
- SCADA system design
- The Twelve Golden Rules

HUMAN MACHINE INTERFACES (HMI'S)

- Human and ergonomic factors
- HMI configuration
- Design and layout
- Alarming and reporting philosophies
- Alarm system design

GOOD INSTALLATION PRACTICE

- Recommended installation practice
- Ergonomic considerations

LANDLINE MEDIA

- Background to cables
- Noise and interference on cables
- Twisted pair cables
- Fibre optic cables
- Public network provided services

ON-SITE TRAINING

✔ **SAVE** over 50% by having an IDC workshop presented at your premises.

✔ Customise the training to **YOUR** workplace.

✔ Have the training delivered when and where you need it.

Contact us for a **FREE** proposal.

DAY TWO

WIDE AREA NETWORK (WAN) TECHNOLOGIES

- Digital hierarchies, T1 and E1
- Packet switching
- Frame relay
- ATM
- SDH/sonet

LOCAL AREA NETWORKS (LAN'S)

- Ethernet networks
- Industrial Ethernet
- TCP/IP
- LAN connectivity: Bridges, Routers and Switches
- Redundancy options
- Web based Industrial SCADA
- Wireless
- OPC

INDUSTRIAL COMMUNICATIONS PROTOCOLS

- RS-232 interface standard
- RS-485 interface standard
- Fieldbus
- Modbus
- DNP3.0

MODEMS

- Introduction
- Modem principles
- Asynchronous/synchronous
- Modulation techniques
- Error detection and correction
- Modem troubleshooting

SCADA NETWORK SECURITY

- Introduction
- Authentication
- Encryption
- SCADA firewalls
- Firewall architectures
- Firewall guidelines

TROUBLESHOOTING AND MAINTENANCE

- Troubleshooting SCADA systems
- Maintenance tasks

SPECIFICATION OF SYSTEMS

- Common pitfalls
- Standards
- Performance criteria
- Testing
- Documentation
- Future trends

PROJECT MANAGEMENT OF SCADA SYSTEMS

- Phases of a SCADA project
- Specification of systems
- Implementation and commissioning

SUMMARY, OPEN FORUM AND CLOSING

مراحل المشروع

مسلسل	المرحلة	وصف المرحلة
1	مرحلة 1	
2	مرحلة 2	

أهداف المشروع

مسلسل	الهدف
1	هدف 11

طريقة تحقيق أهداف المشروع

مسلسل	الهدف	طريقة تحقيق الهدف
1	هدف 11	هدف 1هدف 1هدف 1هدف 1هدف 1هدف 1هدف 1هدف 1هدف 1هدف 1هدف 1

خريطة أهداف - مراحل- مهام المشروع

الهدف	المرحلة	المهمة
هدف 11	مرحلة 1	مهمة 1
هدف 11	مرحلة 2	مهمة 2

أدوار الفريق البحثي ومدة التنفيذ لكل عضو

أعضاء الفريق - الدور	مدة التنفيذ
عبدالغفار محمدالهادي السيد محمد --- باحث رئيسي	12 شهر
عبدالله عمر محمد باز --- مستشار	25 يوم

خطة العمل - الجدول الزمني

المراحل والمهام	الفريق البحثى	مدة المشروع																	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
مرحلة 1	عضو الفريق / الدور																		
مهمة 1	عبدالغفار محمدالهادي السيد محمد --- باحث رئيسي	■	■																
مهمة 1	عبدالله عمر محمد باز --- مستشار					■													
مرحلة 2	عضو الفريق / الدور																		
مهمة 2	عبدالغفار محمدالهادي السيد محمد --- باحث رئيسى						■	■	■	■	■	■	■	■	■	■			
مهمة 2	عبدالله عمر محمد باز --- مستشار					■													

خريطة مخرجات وأهداف المشروع البحثى والأهداف الاستراتيجية للبرنامج

مخرجات المشروع المتوقعة	أهداف المشروع المطلوب تحقيقها	الأهداف الإستراتيجية للبرنامج					
		1	2	3	4	5	6
11مخرج	هدف 11	Y					

الأهداف الإستراتيجية للبرنامج

مسلسل	الهدف الإستراتيجي
1	إدماج أعضاء هيئة التدريس الجدد فى العملية البحثية، وتوفير احتياجاتهم البحثية
2	إتاحة الفرصة للباحثين الجدد للتعرف على أوعية البحث العلمي المتاحة، وتشجيع ثقافة المبادرة
3	تحقيق الاستدامة العلمية، والبحثية، وكسر الفجوة بين الأجيال، ونقل الخبرات بين أعضاء هيئة التدريس القدامى، والجدد
4	تشجيع أعضاء هيئة التدريس الجدد على الوصول إلى مبدأ الريادة
5	تدريب أعضاء هيئة التدريس الجدد على إدارة المشروعات البحثية، وكتابة، ونشر البحوث، والتقارير العلمية
6	إيجاد الاليات، والحوافز اللازمة لاستقطاب المبدعين، والمبتكرين المتميزين من الوطنيين للعمل فى المراكز البحثية

البند	القيمة بالريال السعودي
الموارد البشرية	
الموارد البشرية	6,000.00
الاجمالي	8,500.00
المواد	
الأدوات	0.00
التجهيزات الأساسية	0.00
الأعمال المهنية	0.00
المواد	0.00
الاجمالي	0.00
السفريات	
المؤتمرات	0.00
التدريب	1.00
الزيارات الميدانية	0.00
الاجمالي	1.00
مصروفات أخري	
تكاليف النشر	0.00
مساعدات الكتابة	2.00
الكتابة العلمية	0.00
الاجمالي	2.00
الاجمالي	8,503.00

Trusted Information Sharing Network
for Critical Infrastructure Protection

Managing Denial of Service (DoS) Attacks

Summary Report for CIOs and CSOs

December 2009

DISCLAIMER: To the extent permitted by law, this paper is provided without any liability or warranty. Accordingly it is to be used only for the purposes specified and the reliability of any assessment or evaluation arising from it are matters for the independent judgment of users. This paper is intended as a general guide only and users should seek professional advice as to their specific risks and needs.

Executive Summary

As organisations continue to incorporate the Internet as a key component of their operations, the global cyber-threat level is increasing. As part of its *Cyber Security Strategy*, the Australian Government has recognised the need for Australian businesses to operate secure and resilient information and communications technology environments[1].

One of the most common types of cyber-threats to these environments is known as a Denial of Service (DoS) attack – an attack preventing users from accessing a system for a period of time. Recent DoS attacks have left large corporate and government web sites inaccessible to customers, partners and users for hours or days, resulting in significant financial, reputational, and other losses. The growing use of cloud computing services and shared infrastructure is further increasing the importance of having a considered plan for managing such DoS attacks.

Developing an effective mitigation strategy is an important measure to minimise the risk posed to an organisation by the threat of DoS attacks. The threat of a DoS attack is most effectively addressed as a risk-management issue, and considered as an overall business risk, as opposed to a technical or operational risk.

A comprehensive DoS management framework structured around the Protect, Detect and React triad is required to address the complete lifecycle of a DoS attack:

- Strengthening systems and networks against attacks.
- Detecting attacks when they occur.
- Reacting appropriately to counter current and future attack trends.

Developing an effective DoS threat-management strategy is a significant task and one that requires extensive communications with partners and suppliers – particularly Internet and telecommunications service providers – prior to an incident occurring.

Prudent planning and preparation can mean the difference between a total shut down of the organisation and a slight inconvenience. Following the recommendations contained in this paper will provide the organisation with a solid base for minimising the impact of these potentially damaging attacks.

Introduction

The ultimate aim of a DoS attack is to prevent users from accessing a system or resource, and the potential cost to critical infrastructure can be considerable. The impact of downtime to critical infrastructure organisations may not be limited to lost revenue and goodwill, but can extend to social and human costs. Internet-dependent and networked infrastructure components are generally most at risk of a DoS attack.

[1] Australian Government, *Cyber Security Strategy,* 2009, http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(4CA02151F94FFB778ADAEC2E6EA8653D)~AG+Cyber+Security+Strategy+-+for+website.pdf/$file/AG+Cyber+Security+Strategy+-+for+website.pdf

A sufficiently motivated and skilled attacker may be able to commandeer adequate resources to overwhelm an organisation's infrastructure regardless of its level of preparedness. However, implementing an appropriate framework to manage the DoS threat can maximise the robustness of systems and minimise their downtime in the event of an attack.

There are three papers in this series:

- The full report which provides an introduction to the DoS threat to critical infrastructure and establishes a framework which details a governing strategy and recommendations at both operational and technical levels to protect, detect and respond to DoS attacks.
- The CEO paper, which provides an outline designed to provide senior executives and Directors of Critical Infrastructure organisations with guidance on the processes associated with managing DoS attacks.
- This CIO paper, which summarises the full report and contains a deeper analysis than the CEO paper of operational issues associated with managing DoS attacks

Threat Assessment

A Threat Assessment is the most effective way to identify the DoS risks to your organisation. Following the AS 4360 Standard for Risk Management is considered best practice. Firstly, the context of DoS as relevant to your organisation is established, then attack vectors are identified, followed by an analysis of risk, and finally the evaluation of those risks, as illustrated in Figure 1, below.

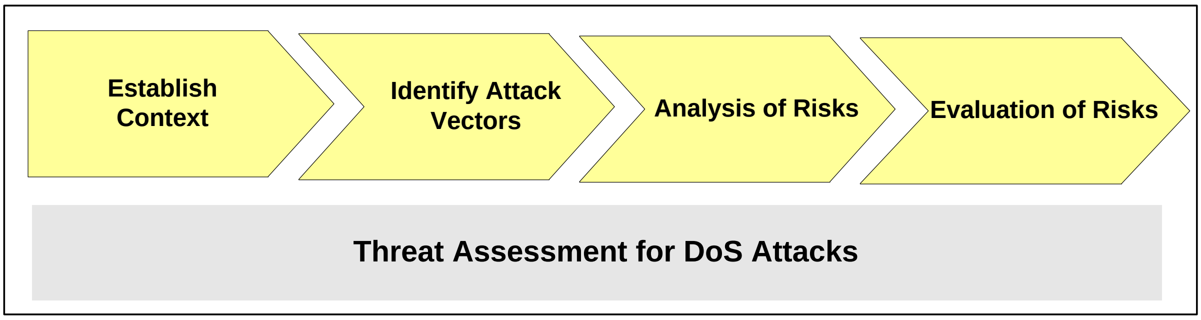


Figure 1 – High Level AS 4360 Risk Assessment Model

This section provides information to help organisations identify potential DoS targets in their business operations and IT environments, qualify the level of risk these targets are subject to, and consider the evolution of technology and threats and how this will change the risk assessment over time.

At first glance DoS attacks appear simple to define and distinguish; however, they can be categorised and sorted in numerous overlapping ways, and have a variety of very important factors to consider when assessing likelihood and impact. Important distinctions are:

- **Attack vectors** – Services subject to DoS attacks are not restricted to the electronic medium; people can be 'socially engineered' and procedural loopholes can be abused. In addition, pre-existing relationships between organisations can be exploited by attackers and leveraged in DoS attacks. For example, domain names can potentially be hijacked if an attacker is able to convince a domain name registrar to point a URL belonging to an organisation to an IP address controlled by the attacker. This prevents the web site of that organisation from being accessible to legitimate Internet users.

- **Attack mechanics** – For any DoS attack, it is important to ask "how was the attack executed?" and the most widely accepted categories are:
  - Consumption of scarce resources, such as network connectivity and bandwidth consumption.
  - Destruction or alteration of configuration information.
  - Physical destruction or alteration of network components.
  - Abuse of business logic.
- **Single point vs. distributed** – The aim of a DoS attack is to abuse specific weaknesses in business logic or system components. A Distributed DoS (DDoS) typically involves using a number of previously compromised computers to attack a target. A DDoS attack can be more difficult to defend against and detect. Reaction to a DDoS attack usually requires the help of the organisation's external service providers.
- **Client vs. server** – Compromising a networked service or functionality can be achieved either by impeding the ability of the server to provide the service or by impeding the client's ability to access the service. DoS attacks against the server are by far the most common, with the intention of affecting all clients of a resource rather than a particular subset.
- **External vs. internal** – DoS incidents can originate both from sources external to an organisation, or from within the organisation itself. Internal incidents can include the deliberate acts of disgruntled employees, inadvertent acts such as mis-configuration of systems or through internal security incidents that affect the availability of systems.
- **Internally managed vs outsourced** – Your business operations may rely on systems and networks over which you have little or no control, especially with the increasingly common use of cloud computing services and Software as a Service (SAAS). In such an environment, protective measures implemented by external service providers are also important for an organisation to consider.
- **Communication layers** – It is possible to target any of the seven OSI communications layers. Attacks directed at the higher layers (particularly the application layer) are generally more prevalent, sophisticated and harder to detect and prevent.
- **Weaknesses Exploited** – Most DoS attacks, especially distributed attacks, rely on fundamental weaknesses in computing infrastructure:
  - Unpatched systems
  - Lack of authentication
  - Poorly configured systems (including virtual systems)
  - Existence of reflectors/amplifiers
  - Difficulties in identifying an attack
  - Shared, vulnerable infrastructure
- **Motivation for Attack** – DoS attacks began to occur when a critical mass of organisations and individuals became Internet connected, giving attackers real incentive to strike. Their motivations include:
  - Credibility with other hackers for compromising a high-profile site
  - Retaliation for real or perceived slights or injustices
  - Monetary gain (criminal extortion or competitive tactics)
  - Political activism and cyber terrorism
  - Simple boredom, a desire for entertainment, or 'experimenting' with new attack techniques

Some organisations may also be unintended targets for a DoS attack, either through a misdirected attack or sharing infrastructure with the intended target. Even in these cases, an appropriate strategy will still need to be in place to respond to such an attack.

- **Scope of attack** – While a DoS attack may be targeted against a specific component of an organisation's infrastructure (for example, its public website), the attack may also affect other systems as well (for example, the ability to send and receive email).

Attack Trends

The following summarises current and future trends in DoS attacks for use in identifying current DoS threats, and how these are likely to evolve over time:

Current:

- Reflection and amplification (including DNS recursion)
- Larger botnets & autonomous propagation
- Botnet markets which are increasingly sophisticated in nature
- Peer-to-peer botnets
- Botnets using encrypted communications
- Attacks against government infrastructure for political purposes
- Use of DoS by organised crime
- Attacks against virtual servers
- Increasing sophistication of malware and malware packaging

Future:

- Attacks on emerging technologies
- Application layer DoS
- Realistic behaviour of DoS traffic (further difficulty in detection)
- Attacks against anti-DoS infrastructure
- Attacks against SCADA systems
- Attacks against shared infrastructure and the 'cloud'
- Attacks against web services

Case Study: Major Australian ISPs subjected to DDoS Attacks

What happened?
In late 2009, two prominent Australian ISPs, aaNet and EFTel, were reportedly subjected to sustained DDoS attacks for a number of weeks. This severely inhibited their ability to provide quality service to customers due to a significant increase in packet loss and network latency.

The source of the attacks was initially unable to be pinpointed. Despite the longevity of the attacks, it is not clear whether the ISPs chose to contact law enforcement authorities for assistance.

Nevertheless, the attacks confirmed that Australian organisations with a reliance on the Internet are a legitimate target for DoS attacks and need to take appropriate precautions to deal with the threat posed by such attacks.

What was the impact?
It was reported that for several weeks the customers of both ISPs experienced significant deterioration in the quality of their service. The attacks received significant publicity in the media and resulted in several complaints from customers.

How was the situation handled?
The ISPs embarked upon a series of core network upgrades, including installing additional equipment to alleviate the attacks and provide additional capacity to their customer base.

In addition, the ISPs contacted their upstream providers and worked with them to implement filtering mechanisms to block the hosts identified as playing a key role in the attacks.

The initial effectiveness of the attacks, however, highlights the importance of Australian organisations proactively implementing a management framework to address the threat of DoS attacks.

Sources & Further information:
http://www.infosecurity-magazine.com/view/3371/australian-isps-tackling-ongoing-ddos-attack/
http://www.itnews.com.au/News/153241,eftel-aanet-suffer-denial-of-service-attack.aspx
http://forums.whirlpool.net.au/forum-replies.cfm?t=1263410#r1

Threat management

Developing an effective DoS threat-management strategy is a significant task. Therefore, focusing on key operational infrastructure rather than attempting to protect all systems from all DoS threats is the most productive approach.

Actions that can be taken by organisations in their policies and strategic approach to managing the DoS threat are:

- Incorporating DoS into organisational risk management
- Implementing a security management framework
- Undertaking staff training
- Negotiating Service Level Agreements with external service providers
- Participating in joint exercises
- Improving information sharing
- Obtaining insurance
- Encouraging industry / government collaboration (examples include the Cyberstorm and Cyberstorm II security exercises)

At operational and technical levels, a range of actions can be taken to protect against attacks, detect attacks, and provide a structured and effective response.

Protect

Protection from DoS attacks poses a challenge because no single technology or operational process will provide adequate protection.

The following **operational** processes may be used to help protect an organisation from DoS attacks:

- Conducting technology risk assessments considering the key variables discussed in this paper in the Risk Identification section
- Capacity planning
- Ensuring secure network design
- Ensuring physical security
- Utilising secure application design
- Including DoS in business continuity management
- Including DoS in security testing scope

The following **technical** measures can be used to provide a degree of protection against DoS attacks to network and system resources:

- Deploying anti-DoS devices and services
- Traffic filtering
- Utilising timely patch management
- Deploying anti-virus software
- Performing system hardening
- System & network segregation

Detect

Given the range of attacks covered by the broad titles DoS/DDoS, it is often not easy to know when an organisation is under attack. In the DoS case, the effects are likely to be immediate and result in a system or subsystem becoming unavailable. The symptoms of a DDoS attack may take longer to appear and are usually apparent in slow access times or service unavailability.

One **operational** measure is to develop relationships with key sources of current IT security intelligence. Groups such as CERT Australia are in a good position to predict, trace, and even work to shut down immediate threats to Australian critical infrastructure. Security vendors, including anti-virus firms and consulting firms, can also provide valuable advice on industry trends and response approaches. For this reason, it is recommended strong relationships are established with key security resources to keep abreast of the latest techniques and impending threats.

The following **technical** mechanisms do not always accurately detect and identify DoS/DDoS attacks. However, when used in combination a correlation of information can prove very effective. The following technical approaches can aid in attack detection:

- Deploying intrusion detection systems
- Developing and deploying monitoring and logging mechanisms
- Deploying honeypot systems to lure attackers away from the real systems

React

Reaction to attack is likely to be of greatest importance to many organisations but may be hampered by outsourcing and other technical hurdles. Organisations must be well prepared to act in the event of a significant and/or sustained DoS attack.

'Reactive' **operational** processes generally involve incident response and analysis. As such, items recommended for consideration to improve operational response capability are:

- Implementing incident response planning to define people's roles and responsibilities, and the processes to be followed in an incident situation. Having clear incident escalation thresholds and clear internal communication paths between business areas in an organisation were identified in the Cyber Storm II exercise as key methods for improving incident response.
- Establishing relationships with telecommunications and internet service providers as these organisations can provide practical protection, detection, filtering and tracing in the event of a DoS attack. As identified in the Cyber Storm II exercise, established relationships with key organisations facilitates rapid information sharing during a DoS attack, helping to maintain situational awareness and ensuring more effective incident response and recovery. Establishing these relationships proactively is crucial because it is difficult to create trusted relationships during the middle of a DoS attack.
- Performing attack analysis to react to a current attack and to prevent future attacks.

Technical measures which can be deployed by organisations to respond to DoS or DDoS attacks include:

- Using upstream filtering to relieve pressure on subsequent infrastructure. This is the most common method used to mitigate active DoS attacks.
- Deploying Intrusion Prevention Systems (IPS) to automatically stop intrusion attempts when they are detected.
- Applying rate limiting to ensure that legitimate messages are not mistakenly discarded.
- Black holing malicious traffic to ignore network communications based on criteria that were identified in the attack analysis.
- Increasing capacity to maintain availability of systems in response to a resource consumption attack.
- Redirecting domain names as a short term mitigation approach to alleviating attack impacts by modifying or removing the IP address the domain name resolves to.

Available Resources

A considerable amount of work has been done in establishing strategies to cope with DoS and other malicious attacks. Following these established frameworks for DoS management will not only help to protect against DoS attacks but the flow-on effects to organisational security will be noticeable. These frameworks include:

- CERT/CC, *Managing the Threat of DoS Attacks* (2001) is the foremost best-practice framework for managing DoS risks. It is structured around the Protect, Detect and React triad, providing practical advice for all stages of the DoS lifecycles.
- *Consensus Roadmap for Defeating DDoS Attacks* (2000), developed by the Project of the Partnership for Critical Infrastructure Security in the United States, describes the problems and suggests remediation measures.
- ISO 27002 *Code of Practice for Information Security Management* (2005) outlines best practices for organisational protection of information resources. Aligning practices with these requirements will aid in the overall management of DoS threats.
- ISM *Australian Government Information Security Manual* (2009) provides policies and guidance to Australian Government agencies on how to protect their ICT systems.
- *ISP Voluntary Code of Practice for Industry Self-Regulation in the Area of e-Security* (2009) provides a code of conduct for Australian ISPs regarding the management of situations where subscribers have malware-infected computers that form part of botnets.

Key questions to consider

These questions are designed to encourage discussion on the organisation's preparedness for a DoS attack. Answers to these questions should underpin the development of a comprehensive DoS risk-mitigation strategy.

Questions to expect from your CEO

How prepared are we and our trading partners to resist a DoS attack?

The preparedness of an organisation for a DoS attack is dependent on the technical and operational measures it has in place. Ensuring trading partners are also prepared for the threat of DoS attacks is important as interruptions to their business can affect your organisation.

What systems, connections and applications are most at risk?

Identifying the infrastructure and applications considered most vulnerable to DoS attacks is an important part of the Threat Assessment process and will assist in deploying appropriate controls to protect, detect and respond to attacks against these components.

Do external services we utilise (such as cloud computing solutions) have appropriate strategies to reduce the threat of DoS attacks?

It is important to ensure prior to engaging service providers that they have strategies and controls in place to address the threat of DoS attacks.

Would our organisation benefit from participating in an industry-wide preparedness test?

Participation in industry-wide tests allows for identification of common issues and vulnerabilities across organisation and allows for information-sharing to occur regarding the management of DoS attacks.

What are our contingency plans in the event that service has been denied to us?

Having Business Continuity Plans in place to deal with situations where a DoS attack affects your organisation or an organisation with whom your business is closely linked will assist in minimising the impact(s) of such an attack

Questions you should ask

Which resources would be potential targets for attackers and where are they vulnerable to attack?

Identifying resources vulnerable to DoS attacks is an important step in determining where the deployment of technical and operational measures to manage the DoS threat should be focussed.

Do we have any virtualised systems that require additional strategies to be in place to protect against DoS attacks?

The increasing use of virtual systems means that the potential effect of a DoS attack can be increased, since a successful attack on the underlying server can affect many systems located on the same physical infrastructure.

How can we recognise a DoS attack and how effective would our response be?

An organisation's ability to effectively recognise and respond to DoS attacks will be significantly enhanced through implementing the technical and operational measures identified in this paper as part of the Protect, Detect and React triad.

Are our service providers well placed to manage the threat of a DoS attack?

Ensuring service providers have protective measures in place should they be subjected to a DoS attack (for example, having sufficient bandwidth capacity and being able to maintain continuity of critical services such as web and email) is an important component of ensuring an organisation can continue to function in the event of an attack.

Do our contracts with providers allow us to expand our resource usage if required?

The ability to increase the resources available to an organisation during a DoS attack can provide an important means of minimising the impact of the attack on the business.

Conclusion

Denial of service attacks are a real threat to the operation of any networked computer system. While they can be difficult to detect and react to, prudent planning and preparation can mean the difference between a total shut down of the organisation and a slight inconvenience. The DoS management framework presented provides coverage of security before an incident, during an incident and after an incident. This is achieved by detailing a governing strategy and specific recommendations at both operational and technical levels for:

- Protecting against DoS attacks.
- Detecting attacks when they occur.
- Responding appropriately to counter current and future attacks.

Following the recommendations contained in this paper will provide your organisation with a solid base for minimising the impact of these potentially damaging attacks.

Summary of recommended actions

Strategic	• Incorporate DoS into risk-management program • Negotiate service-level agreements with suppliers for DoS protection and response levels • Consider running DoS scenarios to identify weaknesses (individually and also with business partners) • Participate in DoS information-sharing networks such as TISN, ITSEAG and CERT Australia

	Operational	**Technical**
Protect	• Include DoS security in testing scope (IT Security Manager) • Complete bottleneck analysis on finite network resources (Network Architect/System Administrator) • Include security in application and network design (Application/Network Architect) • Plan for capacity to endure DDoS attacks (Network Architect) • Implement appropriate physical security measures (IT Security Manager/Operation Manager) • Include DoS in business continuity management (Operations Manager)	• Utilise anti-DoS devices and services (Network Architect) • Apply ingress and egress filtering at network gateways (Network Architect) • Ensure rigorous patch management (System Administrator) • Ensure anti-virus controls are updated and effective (IT Security Manager/System Administrator) • Perform system hardening (System Administrator) • Configure routers and network edge devices according to best practice (Network engineer / System administrator)
Detect	• Create strong relationships with anti-virus vendors to keep abreast of the latest techniques and potential attacks (IT Security Manager)	• Deploy intrusion detection systems (IT Security Manager/Incident Response Team) • Develop monitoring & logging mechanisms (IT Security Manager/System Administrator)
React	• Form co-operative relationships with service providers (Operations Manager) • Establish DoS incident response plan (IT Security Manager) • Perform attack analysis (IT Security Manager/Operations Manager)	• Deploy intrusion prevention systems (IT Security Manager/Incident Response Team) • Implement rate limiting (System Administrator) • Apply black holing to drop malicious packets (Network Administrator) • Increase network/system capacity (System Administrator) • Redirect redundant domain names (System Administrator)

The Trusted Information Sharing Network

Since 2005, the IT Security Expert Advisory Group (ITSEAG)[i] of the Trusted Information Sharing Network (TISN)[ii] has released a series of papers designed to help CEOs, Boards of Directors and CIOs understand the threats to the information and IT infrastructure of their organisations and provide recommendations for mitigating those threats.

The papers cover many topical issues including information security governance, the strategy of defence in depth, managing denial of service attacks, effectively implementing user access management, and the security implications of technologies such as global positioning systems, Voice over IP, mobile devices and wireless networking.

Further information, reports and resources are available at the TISN website (www.tisn.gov.au).

The Australian Government provides support to critical infrastructure organisations in maintaining a secure IT environment. Services and support available include:

- Trusted Information Sharing Network (TISN)
  http://www.tisn.gov.au/
- SCADA Community of Interest
  Secretariat - scada@dbcde.gov.au

CERT Australia

To enhance Australia's cyber security capability, the Australian Government announced in May 2009 that it would create CERT Australia, the new national computer emergency response team. CERT Australia will be managed by the Australian Government

CERT Australia will be a source of cyber security information for the Australian community and point of contact for Australia's international cyber security counterparts. It will also provide a trusted environment for information exchange between the Government and business on cyber security related issues.

CERT Australia will coordinate government and non-government cyber security efforts and have a coordination role in the event of a serious cyber event.

By facilitating the sharing of information between Australian Internet service providers (ISP), major corporations, anti-virus researchers and information technology security vendors, CERT Australia will provide the Australian community with relevant and timely information on cyber security issues.

CERT Australia will incorporate a number of cyber security activities currently undertaken by Australian Government agencies, including the Australian Government Computer Emergency Readiness Team (GovCERT.au). It will also complement the work undertaken by the Cyber Security Operations Centre (CSOC), recently established in the Defence Signals Directorate, and help inform the Australian Government about the national cyber threat picture.

Contact details:

Website: www.cert.gov.au

Email: info@cert.gov.au

[i] The ITSEAG is one of three Expert Advisory Groups established within the Trusted Sharing Information Network for Critical Infrastructure Protection. The ITSEAG provides advice to the Critical Infrastructure Advisory Council (CIAC) and the sector based Information Assurance Advisory Groups on IT security issues as they relate to critical infrastructure protection. The ITSEAG membership consists of academic specialists, vendors, consultants and some industry association representatives who are leaders in the information technology/e-security fields.

[ii] TISN enables the owners and operators of critical infrastructure to share information on important issues. It is made up of a number of sector-specific Infrastructure Assurance Advisory Groups, three Expert Advisory Groups, and the Critical Infrastructure Advisory Council (CIAC—the peak body of TISN that oversees the IAAGs and EAGs). More on TISN can be sought from www.tisn.gov.au or by contacting cip@ag.gov.au

End of Document