

SCADA ASSESSMENT CASE STUDY

From



**NETWORK
INTELLIGENCE**
An ISO 27001 Company

NOTICE

This document contains information which is the intellectual property of Network Intelligence (India) Pvt. Ltd. (also called NII Consulting). This document is received in confidence and its contents cannot be disclosed or copied without the prior written consent of NII.

Nothing in this document constitutes a guaranty, warranty, or license, expressed or implied. NII disclaims all liability for all such guaranties, warranties, and licenses, including but not limited to: Fitness for a particular purpose; merchantability; non infringement of intellectual property or other rights of any third party or of NII; indemnity; and all others. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technologies discussed herein, and is advised to seek the advice of competent legal counsel, without obligation of NII.

NII retains the right to make changes to this document at any time without notice. NII makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein.

COPYRIGHT

Copyright. Network Intelligence (India) Pvt. Ltd. All rights reserved.

NII Consulting is a registered trademark of Network Intelligence India Pvt. Ltd.

TRADEMARKS

Other product and corporate names may be trademarks of other companies and are used only for explanation and to the owners' benefit, without intent to infringe.

NII CONTACT DETAILS

Name	K. K. Mookhey
Title	Principal Consultant
Company	Network Intelligence (India) Pvt. Ltd.
Address	204 Eco Space, Off Old Nagardas Road, Andheri (East), Mumbai 400069
E – Mail	kkmookhey@niiconsulting.com

1 Background

Recently, we were assigned to perform network assessment of the SCADA Network for one of our clients. This case study outlines a brief introduction to SCADA, the sort of assessment we carried out, and typical vulnerabilities that can be found on SCADA systems

2 SCADA (Supervisory Control And Data Acquisition):

It generally refers to an industrial control system: a computer system monitoring and controlling a process. The process can be industrial, infrastructure or facility-based as described below:

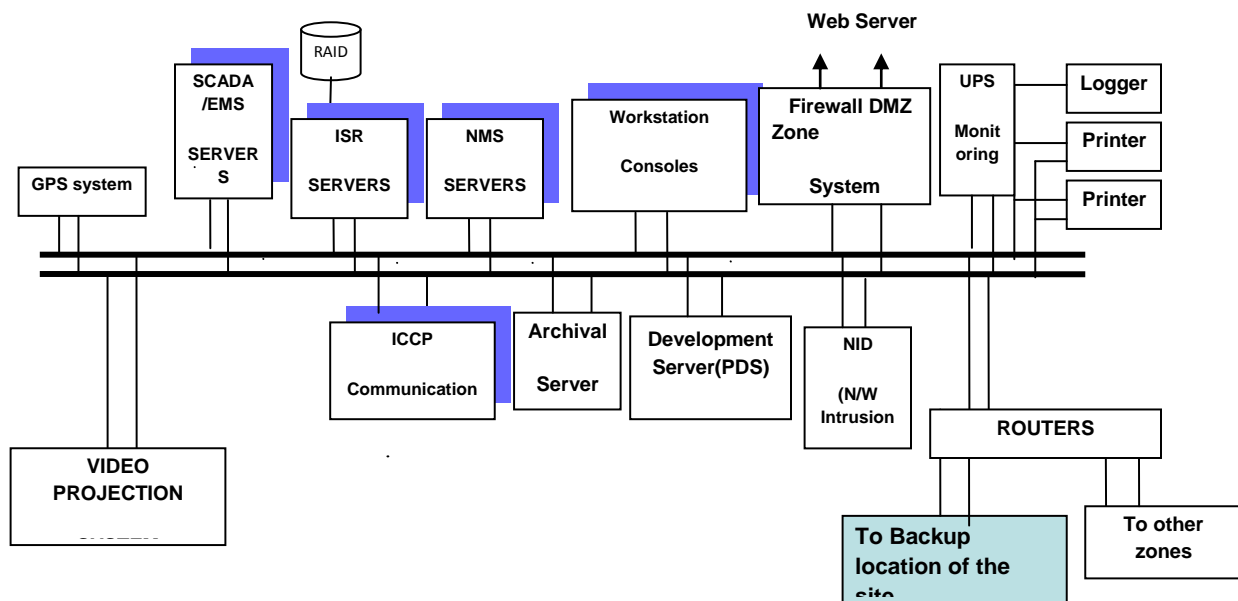
- Industrial processes include those of manufacturing, production, power generation, fabrication, and refining, and may run in continuous, batch, repetitive, or discrete modes.
- Infrastructure processes may be public or private, and include water treatment and distribution, wastewater collection and treatment, oil and gas pipelines, electrical power transmission and distribution, Wind Farms, civil defense siren systems, and large communication systems.
- Facility processes occur both in public facilities and private ones, including buildings, airports, ships, and space stations. They monitor and control HVAC, access, and energy consumption.

Common system components:-

A SCADA's System usually consists of the following subsystems:

- A Human-Machine Interface or HMI is the apparatus which presents process data to a human operator, and through this, the human operator monitors and controls the process.
- A supervisory (computer) system, gathering (acquiring) data on the process and sending commands (control) to the process.
- Remote Terminal Units (RTUs) connecting to sensors in the process, converting sensor signals to digital data and sending digital data to the supervisory system.
- Programmable Logic Controller (PLCs) used as field devices because they are more economical, versatile, flexible, and configurable than special-purpose RTUs.
- Communication infrastructure connecting the supervisory system to the Remote Terminal Units.

SCADA Server / Control Centre Architecture



The main subsystems are:

1. SCADA/EMS Subsystem
2. Inter-Site Communication ICCP Subsystem
3. Web Subsystem and the Security Infrastructure
4. ISR Subsystem (HIS)
5. Archive Subsystem
6. Network Management Subsystem
7. Video Projection System (VPS)
8. Development Subsystem
9. User Interface (UI) Subsystem
10. GPS Time & Frequency Subsystem
11. WAN Subsystem
12. LAN Subsystem
13. Peripheral Devices

SCADA/EMS Subsystem: Carries out the SCADA processing and the EMS calculations, feeds the historical information server, sends the data to the operator Consoles. The SCADA functions are Data Acquisition, Data processing, Alarm, and Tagging. EMS functions are Network Status Processor, Optimal Power Flow, Contingency Analysis, Security enhancement and Voltage VAR dispatch.

Inter-Site Communication ICCP Subsystem: The inter-site communication (or OAG -Open Access Gateway) subsystem, handles the communication with different (sites) zones of the client using the different communication protocols. The one zone (site) communicates to the other zones systems using the standard IEC870-6 (TASE.2)/ICCP protocol. It interfaces with the SCADA/EMS servers on ISD protocol.

Web Subsystem and the Security Infrastructure: The DMZ web subsystem is implemented with the SCADA/EMS server at site. Remote users can access the real-time data and displays through the DMZ web servers. Remote access is provided with appropriate permission and authorization mechanisms. The Web Access area is isolated by two Firewalls. The Web access system consists of Web server, Mail server and Data Replica Server.

ISR Subsystem (HIS): The Information Storage and Retrieval subsystem stores user-defined data and events into the ORACLE-based historic database. The ISR system will store:

- Real time database snapshot, storage and playback
- Historical Information
- SOE data
- Alarm message log
- Storage of files

Archive Subsystem: The Archive subsystem provides centralized storage for whole system's data. The Archive subsystem consists of an archive server and a tape autoloader to archive the information such as ISR data, Save cases, Source code files, System Backup (for restore) etc.

Network Management Subsystem: The Network Management system monitors the interfaces to the SCADA/EMS servers, workstations, devices, and all SCADA/EMS gateway and routers and gathers performance statistics like resource utilisation.

Video Projection System (VPS): VPS is a big display device with 8 segments of 67 inches size each. VPS is driven through a PC installed in its wall and connected on dual LAN

Development Subsystem: Development System provides complete autonomous environment for future program development, application building, testing, and system integration, etc. for the system.

User Interface (UI) Subsystem: The User Interface (UI) subsystem composed of workstation consoles with graphic cards to drive multiple monitors.

GPS Time & Frequency Subsystem: The Time & Frequency subsystem (TFS) captures the GPS time and power system frequency, and synchronizes the time of all the servers and workstations via the LAN, using the standard Network Time Protocol (NTP).

WAN Subsystem: The Wide Area Network (WAN) subsystem for connecting Main site and other sites comprises of routers and Modems and wide band communication link from ISP Network. Two Routers are installed in each zone for providing 2 Mbps (redundant) and 64 kbps Link. The main and backup sites are connected to each other through 2 Mbps channels.

LAN Subsystem: The SCADA/EMS Local Area Network (LAN) subsystem provides the inter-connection of all the servers, workstations, and peripherals. LAN is formed with redundant standard Ethernet switches.

Peripheral Devices: Loggers, Laser printers & Colour Video Copiers.

3 Network Assessment

Tools used for Assessment: Auditpro (in-house developed Auditing tool), NMAP, Nessus, Super scan,

Initial Phase:

Prior to the assessment we tried to get maximum information of SCADA from the vendor. We gathered the following information:

- 2 SCADA applications (Vendor A and Vendor B) were being used on different sites (zones) of the client's network.
- Vendor A's tech support and Vendor B's tech support were maintaining the individual site (Zone) of the client.
- Vendor A's SCADA applications were installed on Solaris OS. Oracle was being used as backend database.
- Vendor A's SCADA software was almost obsolete. There were no patches available for the SCADA software and underlying OS. Vendor A was about to withdraw the support for SCADA in the year 2011.
- AREAVA's SCADA applications were installed on the windows 2003 servers and Open VMS operating systems.
- Vendor B's SCADA applications were using its own proprietary database known as DB431.
- Also, Client were using Oracle as database for some additional applications connected to the SCADA network.
- A previously conducted Vulnerability Assessment by a different consulting firm on the SCADA Servers has resulted in the SCADA servers crashing during the port scanning stage itself.

Armed with the above information, we proceeded to perform the vulnerability assessment first on the test environment of the SCADA (Vendor A's SCADA product). This was completed successfully without any SCADA server crash. The results were emailed to Vendor A's tech support and IT representatives of the customer. We then proceeded for the actual assessment.

Vulnerabilities discovered

The following vulnerabilities were discovered

- All the operating systems were in a default configuration without any hardening having been done to the extent that:
 - Many vulnerable services i.e. echo, daytime, finger were found running on the Windows and Solaris Operating Systems.
 - Vulnerable services like telnet, BOOTP, source routing, SNMPv2 with default community string **public and private** were found on the network devices.
 - Oracle Databases were also not hardened for example we found **scott, system** user had been given full administrative privilege on database server.
 - No Patches had been applied on any of the systems

- Older IOS/Firmware were being used on the network devices i.e. router, switches, firewall.
- No password policy was defined for the SCADA Network.
- Administrator credentials of SCADA servers were commonly being shared with all users.
- Password being used for administrative accounts on Windows servers and databases, network devices were easily guessable.

Network Segregation or the Lack of it

- Some SCADA Servers were exposed to public network.
- No VLAN was segregation was found.
- The bridge connecting the SCADA network to the TCP/IP network was weakly configured – essentially in its default state

Other side-effects

During the assessment, the Nmap scan completed successfully. However, when we started with Nessus scans the SCADA applications crashed twice. Thankfully, there were redundant servers available for the crashed servers due to which no severe /major incident taken placed. But this showed that simply running a scan is enough to bring SCADA systems to their knees.

4 Root Cause Problems

1. SCADA systems are highly expensive and very mission-critical. Therefore, they are not tweaked or hardened once they're up and running
2. SCADA systems are thought to be obscure – since no one knows how they work, no one is going to mess around with them, so why bother securing them
3. SCADA systems are thought to be isolated – but this has been shown to be false multiple times. Many SCADA systems are inter-connected to the corporate TCP/IP network or other TCP/IP networks opening them up to the same issues
4. SCADA vendors don't bother with security. Once a multi-million dollars system is up and running it is just left as it is. So whether it is the Siemens network being attacked by the Stuxnet worm or others, SCADA systems are highly vulnerable due to vendor apathy

5 Conclusion

SCADA systems should be treated as highly vulnerable and can be the target of an attack. SCADA attacks are moving out of the realm of science fiction movies and are very much a reality today. Yet organizations continue to adopt a lax stance towards securing SCADA networks. The very first step should be to conduct a thorough assessment of these systems. This has to be done with care since these systems turn out to be highly susceptible to attacks.

Stuxnet is a major wake up call to all organizations who thought SCADA systems would never come under attack.