COMPLIANCECROSSING™
THE LARGEST COLLECTION OF COMPLIANCE JOBS ON EARTH

www.marketingcrossing.com

FEATURE

THE SATURN PARTNERS, INC.
Network and Environmental Security Auditing

SCADA Testing Steps: Using This Assessment to Protect Your Critical Infrastructure

[By Carole Crawford]

Our recent assessment work has brought us in contact with transportation clients as well as those protecting other critical infrastructures, such as electric and water utilities. What the transportation and utilities fields both have in common is that their operations have little to no room for downtime in case of a disaster or emergency.

SCADA testing focuses on using certain protocols to test infrastructure, and we have been called upon recently to merge our vulnerability assessment and penetration skill on the IT side with helping to prepare clients for any emergency which could take down power stations, grids, and other pieces of vital infrastructure besides a network.

This type of testing is not a comfortable subject to broach with our transportation clients. There are still many top operations officers in the industry who balk at the notion of forming a close partnership with IT to protect critical infrastructure. The simple truth, however, is that with recent advances in networking and wireless technology, combined with the faster pace of communications and increasing sophistication of terrorist attacks, the transportation industry has more to lose than other industries from an attack or failure in their systems. This is because we are very dependent on transportation to move people, food, supplies, and other important things which keep businesses and individuals up and running in the day-to-day world.

The elements of the SCADA test are very straightforward, and all steps must be included for every test to provide the best read-out on how prepared the client organization is for various emergencies.

External testing. This testing is done in two ways: without any information provided by the client and with information provided. The goal is to determine what an attacker can find out about the client's systems using only information available publicly over the internet. Accordingly, this part of the assessment also looks for any references to the client SCADA network or infrastructure on the internet.

Testing from a war dialing dial-up access provided by the client. The objective here is to determine what an attacker can discover and connect to involving client systems using dial-up access modem banks or modems. The use of Citrix, with its huge presence in this area, makes this a high-risk area to look at.

Accessibility of the SCADA system from the corporate IT department. Here the attempt is made to gain access to the SCADA environment from the corporate IT environment. Internal SCADA testing comes first: during this stage, SCADA traffic is captured. Also at this stage the firewall, router, and switch configuration are analyzed. Then, workstation and server hardening takes place by manually logging into VMS workstations. Finally, interviews are conducted with SCADA administrators, and security policies are analyzed. These interviews are used to determine how data information is linked back up to the enterprise systems. Key personnel will also be asked how SCADA information is shared with the enterprise IT and other third party networks, and personnel will be asked about remote access to the SCADA system. Questions may then dig deeper into VPN concentrators-RAS or modem banks that may be in use for remote access to the SCADA system from the enterprise IT environment or from home.

Host operating security. Information is collected from each type of operating system in use within the SCADA environment in order to get a sample set that can indicate how the rest of the workstations and server might be configured. Once the testers are offsite, this configuration information is compared to determine missing patches, default insecure operating systems settings, and any potential opportunities to further harden the workstations and servers.

Tools are used to discover potential vulnerabilities via scanning at the network, host, or application layer. Once these weaknesses are identified, the testers will perform exploits on the test or development systems in an attempt to gain full control of the system. Screen shots of each part of this process will be provided to show the staff how these exploits were performed. If possible, the tester will attempt to gain full control of the system. Physical locations are also assessed during this test, including an assessment of the entire perimeter of the client network.

Running multiple tests. Tests will be done on any other end devices available in the

continued on back

development environment to determine failure points at which a given device ceases to function. Multiple denial-of-service (D.O.S) attacks and session hijacking attempts will be made to discover if the communications protocol between the control room and these end devices is vulnerable to D.O.S, session injection, or hijacking.

In the final report stage, we summarize our assessments in accordance with industry best practices definitions and guidelines. The objective of the assessment process is to assess all systems in accordance with the developed methodology and current standards, and to discover and document all security-related vulnerabilities of the SCADA system in question. Finally, the overall intent is to document security-related mitigation strategies that are feasible and sound.

In summary, we have seen increasing concern within the transportation industry about attacks on these systems, and a lack of information on how to prepare. Speaking with our federal government clients, we find a great deal of interest in cybersecurity to prevent terrorism, but an unwillingness to commit to these tests, even though attention is being paid to overall protection of the network environment. But whether you are a transportation or utilities organization, you cannot afford to gloss over the importance of running regular SCADA testing to see how sound your infrastructure is at all levels and departments. Getting top officers on board to back this initiative is crucial, as they have a great deal to lose if the infrastructure fails. There is nothing like being on the front lines to see the real risks if these tests find those dangerous vulnerabilities.

About the Author

Carole Crawford is the CEO and president of The Saturn Partners, Inc., a company specializing in all forms of network and environmental security testing, policy development, and compliance assistance for clients in the public and private arenas. The company site can be found at www.saturnpartners.com; Carole's email is cacrawf@saturnpartners.com.