SCADA Security and Terrorism: The X-Force Experience

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In this second of two reports, we continue with a summary of the January 2006 BlackHat Federal Conference presentation by David Maynor, who was at that time an R&D Research Engineer for Internet Systems Security (ISS) X-Force[2] and colleague Robert Graham from ISS (both are now founders and top executives at Errata Security <http://www.erratasec.com/about.html>). Having summarized their conclusions that supervisory control and data acquisition (SCADA) system security is in a parlous state, they continued their presentation with case studies that were simultaneously appalling and hilarious. The following sections are paraphrases of several slides from their brilliant presentation.

At a power plant where they were trying to negotiate a contract for penetration testing, they met resistance from executives who were confident that their systems were so secure that no break-ins were possible. Indeed, said the executives, there weren’t even any wireless networks at their site; Maynor and Graham turned their notebook around to demonstrate an unsecured wireless access point (WAP). Ah, but there was no way to get useful information from that WAP; the experts immediately connected and received a Dynamic Host Configuration Protocol (DHCP) address. Well, but it was just in the lab; but a scan showed at once that on the contrary, the wireless network was linked to the main office local area network (LAN). OK, but that LAN wasn’t connected to the SCADA systems controlling the power plant; so the pen-testers immediately got into the Solaris UNIX SCADA system with a decade-old exploit. At this point, write Maynor and Graham, the executives said, “Please stop.” They continue, “We had broken into a system that was on both networks and, indeed, was in direct control of something extremely sensitive and we were in danger of breaking it…. The skills of “average” hackers are adequate to gain access to the systems.[1]

At a component of US power grid, the customer claimed that “Backend networks are not interconnected with the Internet.” Maynor and Graham asked, “But don’t you have power-trading Websites on the Internet? Don’t those have some interconnection with the backend networks?” The customer admitted that and the pen-test proved it. The slide notes

- Got in via SQL injection on website/portal
- Established VPN-like tunnel through SQL server
- Followed the data from system to system to the backend network, which of course was weak on authentication and patches
- Confirmation
- Indeed, there was no air-gap between the backend network and the Internet
- A hacker on the Internet could press a button and shut off the system.[2]

In a pen-test at another nation’s power grid, the experts noted that unlike the US, most nations have a single power grid and a single target. Their pen-test used different attack vectors: via Internet, via dialup and via wireless. They found that despite claims that “Office networks not interconnected to production networks” in fact there were connections. For example, “the time on the production network that gets the 50/60 Hz sine wave is synchronized primarily with NTP across the Internet.” Analysis showed that the SCADA systems were insecure; canonical
passwords supplied at the time of installation had never been changed and were universally shared, precluding proper logging and assignment of responsibility for actions on the network. The experts demonstrated that “Access from the Internet to the backend network existed.” For example, they showed, “…accessing a specially crafted (long) URL with a web-enabled phone was all that was needed to shutdown the entire grid.”[3].

In subsequent slides in their presentation, Maynor and Graham present convincing evidence that, contrary to the naïve belief in security through obscurity (“We think the threat is low because outsiders know nothing about our systems”[4] and “SCADA too obscure for hackers”[5]) of their industrial-control clients, the pen-testers were able to obtain detailed information about specific companies and sites using

- Search engines such as GOOGLE
- Detailed case studies used as marketing documents by vendors and placed on public Web sites
- Internal documents available on unprotected FTP sites, dual-homed workstations, and unprotected intranets.

Another security failure of concern was poor physical security. They were driving through a rural area with a customer employee and walked into a power substation through an unlocked door to find a Windows PC “running in [the] shed connected to all the equipment and connected to the Internet SCADA backbone through wireless connection and TCP/IP protocols….”[6]

The X-Force team also reported that audit trails on most SCADA systems were mostly absent or unusable, since users logged in using canonical usernames and passwords such as “console” or “administrator.” The investigators found that most of their penetration-testing activity was never logged.[7]

Finally, the X-Force team analyzed production programs in several SCADA systems and immediately found serious security flaws which they summarized as follows:[8]

- Insecure coding practices
- Trusting input from the network (e.g. buffer-overflows[9])
- Widespread use of known villains: strcpy(), sprintf(),[10]etc.
- Little or no ability for authentication or encryption
- Clear-text data storage
- Difficulty in firewalling, patching, hardening, and other security techniques.

I think that Maynor and Graham have provided strong real-world evidence that SCADA systems need serious attention from security practitioners. However, we may need experts in yoga or chiropraxis who can show non-technical executives how to move their heads out of their current anatomically-improbable locations.

NOTES (all URLs checked 4 Nov 2010)


Copyright © 2010 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.