



A S4 Bonus Training Opportunity Tuesday, 20 January 2009

Advanced Security Testing of Control System Components

Digital Bond's Offensive Security Team is offering a special 6-hour, hands-on advanced security class to S4 attendees the day prior to S4. Class size is limited to 24 students and there will be 4 instructors in the class. Spend an extra day in beautiful Miami Beach and learn about security tools and techniques well beyond nmap and Nessus.

1. Attacking Historians and other web interfaces on the control system DMZ

Even properly architected and configured control system networks often expose a web server interface on a DMZ to the enterprise network to provide information to corporate users. Vulnerabilities in this web server, such as the vulnerability in Udassin's 2008 S4 paper, can lead to a DMZ compromise and attack path to the control system network.

In this module students will be taught how to test for, find and exploit a variety of web session vulnerabilities using WebScarab and other tools. Students will be able to assess their DMZ servers upon returning back to their control system.

2. Finding and exploiting overflows on control system application workstations and servers

In this module students will learn how to customize a fuzzing framework to run against a control system application. While the application is being fuzzed, students will learn to run a debugger program to identify the root cause of overflows that cause system crashes and other errors as well as provide information to further modify the fuzzer.

The instructors will show how to turn an overflow to a proof of concept exploit.

Extra Credit

Digital Bond will open up its lab to students during the class. The lab contains many different brands of controllers, HMI and control system applications. Try some of the skills learned in the class on a variety of control system devices and applications.

Prerequisites and Cost

- Understanding of networking and some programming experience is recommended. Digital Bond will provide preparatory materials in advance of the course for students who are less experienced. Multiple instructors will be available to help with varying skill levels.
- A laptop with CD drive and a wireless LAN card.
- Cost: \$600

