ABSTRACT for the 2017 ISA WWAC Symposium

Lessons from the Field, a Pen Tester's Adventures in Water Sectors and ICS

Bryan L Singer[1]*

[1]IOActive, Inc.

(*Email: bryan.singer@ioactive.com and Phone: 206-455-9300)

SUBMISSION TYPE

30 minute presentation

KEYWORDS

Cloud Computing, Virtualization, Remote Access, ICS, Cyber Penetration Testing

ABSTRACT

As technologies such as cloud computing, virtualization, and remote access continue to drive more connectivity to our water environments, the threats of cyber security mount a growing challenge. But what are the real targets of attackers? Red teaming and penetration testing can be a great service to help understand the attack surface for a given ICS environment. To date, however, a prevalent issue is that people still don't recognize cyber security threats when they happen, or don't know what to do and ignore clear evidence of breach. Effective penetration testing exercises all aspects of your incident detection and response plan, and when well conducted can help increase visibility and awareness of cyber threats and how to train personnel to respond to them. This talk will present the results of a (sanitized) penetration test at an actual water treatment facility to highlight what can be found, how the service can help in not only cyber security but also all aspects of reliable operation, and what to look for in selecting a partner to conduct cyber penetration testing.

ABOUT THE AUTHORS

Bryan L Singer *has over 20 years' experience in information technology security including 15 years specializing in industrial automation and control systems security, critical infrastructure protection, and counter-terrorism. As an industry catalyst, Mr. Singer has focused on all source threat intelligence and attack techniques again industrial automation including enterprise systems, manufacturing, and process intelligence systems (DCS, SCADA, etc), and research and attach methodologies at the process control and safety intersection. He has successfully completed red team and penetration testing against liquid natural gas pipelines, gas pipelines, fossil power generation, nuclear, automotive, food and beverage, hydroelectric generation, and a myriad of other facilities. Mr. Singer's key area of interest is in discovering and exploiting out of band non-traditional attack techniques. These attacks include such events as successfully compromising a pipeline from a phone and while on a major international airline, discovering VHF and TNC radio communications against substation automation at a major power supplier, successful compromise of a smart meter tower communication system that spanned multiple power suppliers in the US, and a*

successful takeover of an entire nuclear plant's emergency communications system. All completed under authorized contract to do so. He holds the CISSP and CAP certifications, and is actively pursuing GPEN and OCSP. Contact: bryan.singer@ioactive.com