Understanding Vulnerabilities: How to Conduct Vulnerability Assessments to Know What Attackers Can, and Can't Do

Bryan Singer, CISSP, CAP*

[1]Kenexis Security, Birmingham, Alabama, USA
(*correspondence: bryan.singer@kenexis.com)

FORMAT

45 minute presentation

KEYWORDS

Security, vulnerability assessment, threat, IT, control systems

ABSTRACT

Over the course of hundreds of plant evaluations, vulnerability tests, penetration tests, and other security projects, questions often get raised about what vulnerabilities for ICS really mean. As vulnerabilities reported in ICS gain increased attention and awareness, some have been eager to try out their hand at attacking industrial processes, or have attempted to raise awareness under what ultimately proves to be false flag conditions when the "threat" is rather quickly discounted due to mitigating factors - such as hardwired controls like a tank level switch that would prevent an overflow from occurring, despite taking control of an individual controller. Moving beyond device vulnerabilities into high impact damages on control systems requires not only IT security skills, but also engineering skills and knowledge of control systems. All three together represent a critical danger to safe and efficient operations. This talk will focus on attack modes for ICS involving gaining access to the system, exploiting vulnerabilities, understanding methods of compromise and attack, but most importantly when common hacking techniques must yield to engineering skills in order to further the impact to the system beyond causing nuisance trips. Discussion of common industrial processes and how to both gain access to the system and how to effectively bypass machine protective systems will be included in this presentation.

ABOUT THE AUTHOR

Bryan Singer, CISM, CAP *is a principal investigator with Kenexis Security Corporation. He has over 23 years of experience in information technology security including 16 years specializing in industrial automation and control systems security, critical infrastructure protection, computer and ICS forensics, counter-terrorism, network design, and software development. He was the founding chairman and co-chairman of ISA/IEC 62443 (ISA-99) Industrial Automation and Control Systems Security Standards Committee from 2002 until 2012, past board member of DHS's Process Control Systems Forum (PCSF), member of the NERC CIP SAR Drafting Team, and current Director Elect of the ISA Safety and Security Division. He is co-inventor on a patent (2006015586) for firewall methods and apparatus for industrial protocols, and is a co-author on the highly rated book, "***Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS***"