Semester 2

Paper 203: Supervisory Control and Data Acquisition (SCADA) System and Information Hiding Techniques

Marks: 100 **Lectures 60**

Objective: What Internet of things would be to consumers, SCADA and Industrial control systems would be to enterprises, the heavy machinery that we have been thinking of its intelligent management is going to be completely taken over by the technology. Although it looks like a great boon however if take over, we have seen in the past some of the national critical infrastructures of some very developed countries being compromised and the damages happening which are irreversible hence it becomes most important to understand the cyber risks that such technologies posses and to give the education of the best practices followed for securing such technologies.

Unit I: Introduction

Network Segmentation and Segregation , Boundary Protection, Firewalls , Logically Separated Control Network , Network Segregation, Recommended Defence-in-Depth Architecture, General Firewall Policies for ICS , Recommended Firewall Rules for Specific Services , Network Address Translation (NAT), Specific ICS Firewall Issues , Unidirectional Gateways , Single Points of Failure , Redundancy and Fault Tolerance , Preventing Man-in-the-Middle Attacks , Authentication and Authorization , Monitoring, Logging, and Auditing, Monitoring, Logging, and Auditing , Response, and System Recovery

Unit II: Network Segregation

Dual-Homed Computer/Dual Network Interface Cards (NIC) , Firewall between Corporate Network and Control Network , Firewall and Router between Corporate Network and Control Network , Firewall with DMZ between Corporate Network and Control Network , Paired Firewalls between Corporate Network and Control Network , Network Segregation Summary

Unit III: Recommended Firewall Rules for Specific Services

Domain Name System (DNS) , Hypertext Transfer Protocol (HTTP) ,FTP and Trivial File Transfer Protocol (TFTP) ,Telnet ,Dynamic Host Configuration Protocol (DHCP) , Secure Shell (SSH) ,Simple Object Access Protocol (SOAP) , Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol (SNMP) ,Distributed Component Object Model (DCOM),SCADA and Industrial Protocols: DNP3 Protocol. Smart Grid Security.

Unit IV Information Hiding Techniques

Introduction to Steganography, Watermarking. Differences between Watermarking and Steganography, A Brief History. Digital Steganography, Applications of Steganography, Covert Communication, Techniques of steganography(for Text and Image) . Steganographic Software: S-Tools, StegoDos, EzStego, Jsteg-Jpeg.

Unit V : Digital Water Marking

Classification in Digital Watermarking, Classification Based on Characteristics: Blind versus Nonblind, Perceptible versus Imperceptible, Private versus Public, Robust versus Fragile, Spatial Domain-Based versus Frequency Domain-Based. Classification Based on Applications: Copyright Protection Watermarks, Data Authentication Watermarks, Fingerprint Watermarks, Copy Control Watermarks, Device Control Watermarks. Watermarking Techniques for Visible and Invisible Watermarks. Watermarking tools: uMark, TSR Watermark. Steganalysis

Suggested Readings

1. Macaulay, T. & Singer, B. (2016). *Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS*. Boca Raton, FL: CRC Press.

2. Langner, R. (2011). *Robust control system networks: How to achieve reliable control after Stuxnet*. New York: Momentum Press.

3. Knapp, E.D. & Langill, J.T. (2011). Industrial network security: Securing critical infrastructure networks for smart grid, SCADA , and other industrial control systems. Waltham, MA: Syngress Media, U.S.

4. Katzenbeisser, S. & Fabien A P. (2000). *Information Hiding Techniques for Steganography and Digital Watermarking*. Petitcolas, Artech House.

5. Cox, I., Miller, M., Bloom, J., Fridrich, J. & Kalker, T. (2007). *Digital Watermarking and Steganography* (2nd Ed.). Elsevier.

Latest research papers from refereed journals discussed by the faculty may also be referred.