BASICS OF INDUSTRIAL NETWORK SECURITY FOR SCADA, AUTOMATION, PROCESS CONTROL AND PLC SYSTEMS

A 3-day Workshop Summary

OBJECTIVES:
At the end of this workshop participants will be able to:

- Identify with various terminology when speaking about cyberspace
- Explain the concept of cyber security
- Apply the fundamental concepts of industrial network security to your SCADA and automation systems
- Conduct a preliminary analysis of your industrial networks and prepare to withstand and anticipate attacks and apply defences
- Discuss the issues of Industrial Network security competently with your associates in IT and vendors
- understand and be able to construct a secure robust Local Area Network
- learn how to plan and design your networks better
- analyse and construct a typical firewall

THE WORKSHOP:
This workshop will give you a fundamental understanding of security in effective industrial networking and data communications technology. It will also present you with the key issues associated with security in industrial communications networks and will assist managers, system operators and industrial data communications specialists in setting up secure systems.

One completion of the workshop you will have developed a practical insight into how to achieve optimum industrial network security for your organisation.

Topics covered include: Introduction and terminology; firewalls; authentication, authorisation and anonymity; remote access to corporate networks; cryptography; VPN's; data security; desktop and network security; security precautions in a connected world; and internet security.

WHO SHOULD ATTEND?
If you are using any form of communication system this workshop will give you the essential tools in securing and protecting your industrial networks whether they be automation, process control, PLC or SCADA based. It is not an advanced workshop – but a hands-on one.

Anyone who will be designing, installing and commissioning, maintaining, securing and troubleshooting TCP/IP and Intra/Internet sites will benefit including:

Instrumentation Engineers, Technicians, Design Engineers, Network Engineers, Electrical Engineers, Engineering Managers, Network System Administrators

PRE-REQUISITES
A basic working knowledge of industrial communications and applications is useful.

TIMING:
Workshop timing is generally 8am registration and a prompt start at 8.30am with lunch at 12.30 and a finish no later than 5pm. There will be 15minute morning and afternoon breaks. These can easily be varied for on-site presentations.

WORKSHOP CONTENT SUMMARY

REGISTRATION

AN INTRODUCTION TO INDUSTRIAL NETWORK SECURITY
- Course outline
- The evolution of networking
- What is network security, Cyber Space and Cyber security?
- Why has security assumed more importance in recent times?
- Security in the context of Industrial automation systems
- Information networks and industrial networks - the similarities and differences
- Organizational issues
- Network security solutions
- Wireless networks
- Security testing
- Summary

NETWORK BASICS
- Introduction
- Network topologies
- Networking approaches
- Commonly used networking technologies
- Internet work connections
- Network architectures and protocols
- Architecture of real time industrial networks
- Summary

NETWORK THREATS, VULNERABILITIES AND RISKS

- Introduction
- Security goal
- Threats and underlying causes
- Motivation for threats
- Knowledge
- Vulnerabilities
- Network attacks
- Security measures
- Risks resulting from attacks
- Attack scenarios in public utility systems
- Common criteria based approach for analysis of threats and vulnerabilities
- Summary

AN OVERVIEW OF IP NETWORK SECURITY

- Introduction
- Why do networks become vulnerable?
- Weaknesses in TCP/IP Protocol
- Attack mechanisms
- Preparing for an attack
- Attack through unauthorized access
- Attack the data (Data diddling)
- Attack the service through Denial of Service (DoS)
- Vulnerabilities of OSI model layers
- Network security at transport layer
- Network layer security
- Data link layer security
- Summary

SECURING A NETWORK BY ACCESS CONTROL

- Introduction
- What is an Access Control List (ACL)?
- What is a firewall?
- Type of firewalls
- Packet filter firewalls
- Stateful inspection firewalls
- Application-proxy gateway firewalls
- Dedicated proxy server
- Hybrid firewalls
- Security through NAT
- Port Address Translation (PAT)
- Host based firewalls
- Personal firewall and firewall appliances
- Guidelines for establishing firewalls
- Summary

NETWORK SECURITY THROUGH AUTHENTICATION, AUTHORIZATION, ACCOUNTING (AAA) AND ENCRYPTION

- Introduction
- What is AAA?
- Authentication
- Authentication protocols
- Authorization
- Accounting
- AAA Implementation using TACACS+ and RADIUS protocols
- Use of remote security database
- Encryption
- Encryption implementation
- Summary

INTRUSION DETECTION SYSTEMS

- Who is an Intruder and what can he do?
- Why do Intrusions happen?
- What are Intrusion detection systems?
- Network-based Intrusion detection systems
- Host based systems
- Comparison of the two types of IDS
- Choice of IDS system
- Responding to an attack
- Summary

VIRTUAL LAN

- Introduction
- Need for VLAN
- Benefits of a VLAN
- VLAN constraints
- Operating principle of a VLAN
- VLAN-Implementation methods
- Method of connections
- Filtering table
- Tagging
- Summary

VIRTUAL PRIVATE NETWORKS (VPN) AND THEIR SECURITY

- Introduction
- The Internet and the new communication paradigm
- What is a VPN?
- Types of VPN
- Requirements for designing a VPN system
- Defining of policy
- Functional requirements
- Scalability
- Manageability
- Simplicity
- Network infrastructure
- Security
- VPN protocols

WIRELESS NETWORKS AND THEIR SECURITY ISSUES

- Basics of wireless technologies
- Wireless standards
- WLANS as per IEEE 802.11
- Wireless security threats
- Security requirements of WLANs
- Security risks
- WLAN security services
- Authentication
- Confidentiality
- Integrity
- Wireless network security attacks
- Operational countermeasures
- Technical countermeasures
- Secure wireless communication in Industrial networks
- Summary

SECURITY TESTING

- Introduction
- The need for security testing
- Security testing over the life cycle of the system
- Who will be responsible for security testing?
- Testing techniques
- Documentation
- Prioritizing
- Summary

STEPS TO IMPROVE CYBER SECURITY OF SCADA NETWORKS

INTRUSION DETECTION SYSTEMS

SUMMARY & OPEN FORUM

COMPLETE FEEDBACK SHEETS

CLOSING