ADVANCED 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:

- Explain the concept of cyber security
- Identify different types of Cyber Security threats
- 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
- Identify steps to improve Cyber Security of SCADA Systems

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:

- Design engineers
- Electrical engineers
- Engineering managers
- Instrumentation engineers
- Network engineers
- Network system administrators
- Technicians

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

INTRODUCTION TO INDUSTRIAL NETWORK SECURITY

- Course outline
- The evolution of networking
- What is network security, Cyber Space and Cyber security?
- Security Myths
- 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 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

DEVELOP CYBER SECURITY MANAGEMENT SYSTEM (CSMS)

- Initiate development of CSMS
- High level risk assessment
- Detailed risk assessment
- Establish policy and procedures
- Define and implement countermeasures
- Maintain CSMS

PHYSICAL SECURITY

Physical and logical access to networked equipment
Network segmentation

AUTHENTICATION

Authentication basics
Client-side certificates
Passwords
Smart cards
Tokens
Biometrics
PAP
CHAP
RADIUS
TACACS/TACACS+

ENCRYPTION

Symmetrical encryption schemes (DES, RC4)
Public-key encryption schemes (RSA)
Certificate Authorities (CAs)

PROXIES/FIREWALLS

Basic firewall operation
Natural Address Translation (NAT)
Firewall types (IP filtering, stateful inspection, proxy, DMZ)
Implementing firewalls for industrial protocols

INTRUSION DETECTION SYSTEMS (IDSS)

Network-based Intrusion detection systems
Host based systems
Comparison of the two types of IDS
Choice of IDS system
Responding to an attack
Deployment

ROUTER SECURITY

Administrator access
Firmware upgrades
Logging
Access Control Lists (ACLs)

SWITCH SECURITY

Administrator access
Port based MAC address management
ACL filtering
Virtual LAN (VLAN) implementation
Industrial switch security

VPNS

Virtual Private Network (VPN) concept
Tunnelling
L2TP
IPSec
SOCKS 5

WIRELESS LANS

Encryption and authentication - current problems and developments
IEEE 802.1x
WEP
WZC
WPA
AES
LEAP
EAP-TLS
EAP-TTLS
Implementing security for industrial wireless networks

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

APPENDICES
STEPS TO IMPROVE CYBER SECURITY OF SCADA NETWORKS

NISCC Good Practice Guide on firewall deployment for SCADA and process control networks

Guidelines for securing Wireless Networks

SUMMARY & OPEN FORUM

COMPLETE FEEDBACK SHEETS

CLOSING