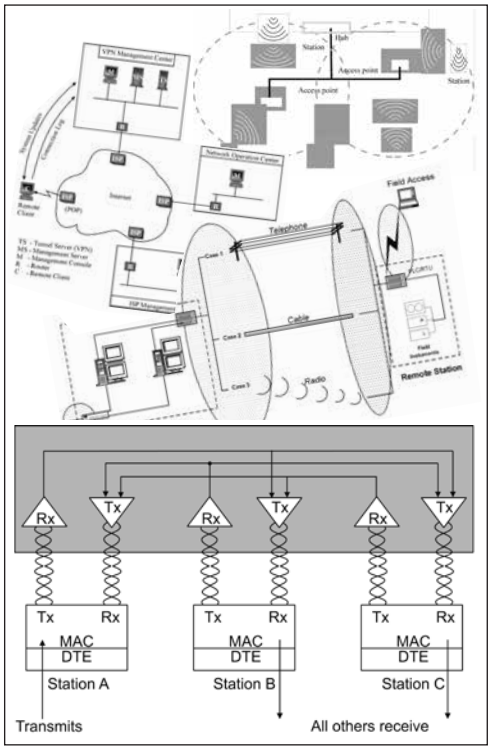
INDUSTRIAL NETWORK SECURITY
FOR SCADA, AUTOMATION, PROCESS CONTROL AND PLC SYSTEMS



YOU WILL LEARN HOW TO:

- 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

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

IDC TECHNOLOGIES

Technology Training that Works

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.

Pre-requisites

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

Practical Sessions

This is a practical, hands on workshop enabling you to work through practical exercises which reinforce the concepts discussed.

To gain full value from this workshop, please bring your laptop/notebook computer.

On-Site Training

- ✓ SAVE over 50% by having an IDC workshop presented at your premises.
- ✓ Customise the training to YOUR workplace.
- ✓ Have the training delivered when and where you need it.

Contact us for a FREE proposal.

The Program

INTRODUCTION
- Background to workshop
- Overview of basic concepts

DANGERS
- Hackers
- Viruses
- Denial-of-service
- Information leakage
- File manipulation
- Database access
- Elevation of privileges
- Spoofing
- SYN flooding
- Router attacks
- Sniffing

SECURITY POLICIES AND ADVISORY SERVICES
- Corporate policies
- CERT
- Audits
- Threats
- Vulnerabilities
- Countermeasures
- Disaster recovery

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)

INTRUSION DETECTION SYSTEMS (IDSS)
- Types
- 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

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

SUMMARY, OPEN FORUM AND CLOSING