



Technology Training that Works

Industrial Network Security for SCADA, Automation, Process Control and PLC Systems

Contents

1	An Introduction to Industrial Network Security	1
1.1	Course overview	1
1.2	The evolution of networking	1
1.3	What is network security?	2
1.4	Why has security assumed more importance in recent times?	2
1.5	Security in the context of industrial automation systems	3
1.6	Information networks vs industrial networks - the similarities and differences	4
1.7	Organizational issues	4
1.8	Network security solutions	4
1.9	Wireless networks	5
1.10	Security testing	5
2	Networking Basics	7
2.1	Introduction	7
2.2	Network topologies	7
2.3	Medium Access Control	8
2.4	Ethernet	10
2.5	Networking components	14
2.6	Network architectures and protocols	15
2.7	The architecture of real time industrial networks	16



Technology Training that Works

3	Network Threats, Vulnerabilities and Risks	19
3.1	Introduction	19
3.2	Security goal	20
3.3	Threats and underlying causes	21
3.4	Motivation for threats	22
3.5	Knowledge	22
3.6	Vulnerabilities	22
3.7	Network attacks	23
3.8	Security measures	26
3.9	Risks resulting from attacks	26
3.10	Attack scenarios in public utility systems	26
3.11	Common criteria based approach for analysis of threats and vulnerabilities	29
4	An Overview of IP network Security	31
4.1	Introduction	31
4.2	Why do networks become vulnerable?	32
4.3	Weaknesses in the TCP/IP protocol suite	33
4.4	Attack mechanisms	33
4.5	Preparing for an attack	34
4.6	Attack through unauthorized access	34
4.7	Attack the data (data diddling)	35
4.8	Attack the service through Denial of Service (DoS)	36
4.9	Vulnerabilities of OSI layers	38
4.10	Network security at the Transport layer	40
4.11	Network layer security	41
4.12	Data Link layer security	42



Technology Training that Works

5	A Comprehensive Approach to Network Security Planning	45
5.1	Network security	45
5.2	A comprehensive approach to network security planning	46
5.3	Risk evaluation	46
5.4	Plan for preventive measures	47
5.5	Detection of an attack and response	49
5.6	Recovery plan	49
5.7	Prepare a security policy document	49
5.8	Dissemination and implementation	51
5.9	Auditing and monitoring of the policy	51
5.10	Special guidelines in respect of Industrial Automation networks	51
5.11	Negative aspects of Internet access	52
6	Securing a Network by Access Control	53
6.1	Introduction	53
6.2	What is ACL?	54
6.3	What is a firewall?	55
6.4	Type of firewalls	56
6.5	Packet filter firewalls	56
6.6	Stateful inspection firewalls	58
6.7	Application-proxy gateway firewalls	59
6.8	Dedicated proxy server	60
6.9	Hybrid firewalls	60
6.10	Security through NAT	60



Technology Training that Works

6.11	Port Address Translation (PAT)	61
6.12	Host based firewalls	61
6.13	Personal firewall and firewall appliances	61
6.14	Guidelines for establishing firewalls	62

7	Authentication, Authorization, Accounting (AAA) and Encryption	65
----------	---	-----------

7.1	Introduction	65
7.2	What is AAA?	65
7.3	Authentication	66
7.4	Authentication protocols	69
7.5	Authorization	72
7.6	Accounting	73
7.7	AAA Implementation using TACACS+ and RADIUS protocols	74
7.8	Use of the remote security database	76
7.9	Encryption	77
7.10	Encryption implementation	78

8	Intrusion Detection Systems	81
----------	------------------------------------	-----------

8.1	Who is an Intruder and what can he do?	81
8.2	Why do Intrusions happen?	81
8.3	What are Intrusion Detection Systems?	82
8.4	Network-based IDSs	82
8.5	Host based systems	85
8.6	Comparison of the two types of IDS	86
8.7	Choice of IDS system	86
8.8	Responding to an attack	86



Technology Training that Works

9	VLANs	89
9.1	Introduction	89
9.2	The need for VLANs	89
9.3	Benefits of a VLAN	92
9.4	VLAN constraints	93
9.5	Operating principle of a VLAN	93
9.6	VLAN implementation methods	94
9.7	Method of connections	97
9.8	Filtering table	98
9.9	Tagging	98
10	VPNs and their Security	101
10.1	Introduction	101
10.2	The Internet and the new communication paradigm	102
10.3	What is a VPN?	103
10.4	Types of VPN	103
10.5	Requirements for designing a VPN system	103
10.6	Defining of policy	104
10.7	Functional requirements	105
10.8	Scalability	105
10.9	Manageability	107
10.10	Simplicity	108
10.11	Network infrastructure	109
10.12	Security	110
10.13	VPN protocols	112



Technology Training that Works

11	Wireless networks and their security issues	119
11.1	Basics of wireless technologies	119
11.2	WLANs as per IEEE 802.11	119
11.3	Security risks	121
11.4	Implementation of security measures for industrial networks	122
12	Security Testing	127
12.1	Introduction	127
12.2	The need for security testing	127
12.3	Security testing over the life cycle of the system	128
12.4	Who will be responsible for security testing?	129
12.5	Testing techniques	129
12.6	Documentation	135
12.7	Prioritizing	135
	Exercises	137
	Appendix 1: 21 steps to improve cyber security of SCADA networks	153
	Appendix 2: NISCC Good practice guide on firewall deployment for SCADA and process control networks	165
	Appendix 3: Guidelines for deploying WPA and WPA2	207