

Contents

1 Introduction

1.1 Purpose and Scope	1-1
1.2 Objectives and Goals of Security Requirements	1-2
1.3 Security Infrastructure	1-3
1.4 Network Elements (NEs) and Network Systems (NSs)	1-3
1.5 Intent and Target Audience	1-4
1.6 Perspective	1-6
1.7 Structure and Use of This Document	1-7
1.8 New – Requirements Terminology	1-7
1.9 Requirement Labeling Conventions	1-8
1.9.1 Numbering of Requirement and Related Objects	1-8
1.9.2 Requirement, Conditional Requirement, and Objective Identification	1-9
1.10 Summary	1-9

2 Data Communications Networks

2.1 What Is a Network?	2-1
2.1.1 Physical Boundaries	2-1
2.1.2 Protocol Boundaries	2-2
2.1.3 Functional Boundaries	2-3
2.1.4 Ownership Boundaries	2-3
2.1.5 Administrative Boundaries	2-3
2.1.6 Distributed Computing Boundaries	2-3
2.2 Interdependence of Networks and Network Security	2-4
2.3 Network Components	2-5
2.3.1 The Role of the Workstation in Network Security	2-5
2.3.2 Network Integrity	2-6
2.3.3 Intermediate Data Handling Nodes	2-6
2.4 Network Management	2-7
2.4.1 SNMP Basics	2-7
2.4.2 SNMP Security	2-8
2.4.3 SNMPv1 Community Function	2-8
2.4.3.1 Using Community for SNMP MIB View and Access Control	2-9
2.5 Basic Communication Process	2-9
2.6 Need for Security Requirements	2-10
2.7 Concerns of Piecewise Approach to Security Requirements	2-11

3 Rationale for Network Security Measures

3.1 Major Security Concerns	3-1
3.2 Network Security Threats	3-2
3.3 Vulnerabilities and Exposure	3-3
3.3.1 Critical Threat Models	3-4
3.3.2 Today's Increasing Vulnerabilities	3-5

3.3.3 Security Policy 3-6
3.4 Fitting Security into the Overall Business 3-8

4 Security Administration Requirements

5 Network Security Services and Requirements

5.1 Trusted Computing Base 5-1
5.2 TCB and System Integrity 5-2
5.3 Basic Security Services 5-3
5.4 Identification 5-4
 5.4.1 User Identification 5-4
 5.4.2 Network Address Identification 5-6
5.5 Authentication 5-6
 5.5.1 Reusable Passwords 5-8
 5.5.2 Third-Party Authentication Servers 5-9
 5.5.2.1 Shared Secret Key Authentication Service 5-9
 5.5.2.2 Public Key Authentication Service 5-11
5.6 Access Control 5-12
 5.6.1 Subjects 5-14
 5.6.1.1 Group Membership 5-14
 5.6.1.2 Roles 5-14
 5.6.1.3 Proxies 5-14
 5.6.2 Access to the Network 5-15
 5.6.2.1 Network Login Procedure 5-17
 5.6.2.2 Dial-Back Modems 5-18
 5.6.3 Access to Network Services 5-18
 5.6.4 Resource Access Control 5-19
5.7 Data Integrity Services 5-20
 5.7.1 Confidentiality 5-21
5.8 Auditing 5-21
 5.8.1 Security Log Generation 5-21
 5.8.2 Report Generation/Audit Trail 5-24
5.9 Continuity of Operations 5-24

6 LAN Security Requirements

6.1 Security Problems and Threats in the LAN Environment 6-1
6.2 Requirements Applicability 6-2
6.3 Workstation Security 6-3
 6.3.1 User Identification and Authentication at the Workstation 6-3
 6.3.2 Workstation Viruses 6-3
 6.3.2.1 Virus Detection in the Workstation 6-3
 6.3.2.2 Virus Prevention for the Workstation 6-4
6.4 LAN Security Fundamentals 6-5
 6.4.1 LAN Topologies 6-5
 6.4.2 LAN Wiring Hub Security 6-6
 6.4.3 LAN Media Access Control (MAC) 6-6

6.4.3.1 Broadcast LANs	6-7
6.4.3.2 Switched LANs	6-8
6.5 LAN Security Administration	6-8
6.6 LAN Server Security	6-9
6.6.1 Server Physical Security	6-10
6.6.2 Virus Prevention in the LAN Server Environment	6-10
6.6.3 Dedicated vs. Non-Dedicated Servers	6-11
6.7 LAN NOS Authentication	6-11
6.7.1 User Identification and Authentication for the LAN Server	6-12
6.7.1.1 Identification	6-12
6.7.1.2 Authentication	6-12
6.7.2 Workstation Authentication	6-14
6.7.3 Login Restrictions	6-14
6.8 File and Directory Access Control	6-15
6.8.1 Access Control	6-15
6.8.2 Dial-Up Access	6-17
6.9 Auditing Mechanisms	6-18
6.9.1 Day-to-Day Audit Functions	6-18
6.9.2 Periodic Security Reviews	6-19
6.10 LAN Integrity	6-19
6.11 Internetworking Issues	6-20
6.11.1 Interconnection with Public Networks	6-20
6.11.2 Packet Filtering	6-21
6.11.3 Security Interoperability	6-21

Appendix A: References

Appendix B: Glossary

Index

List of Figures

Figure 1-1	Security Requirements Triad	1-4
Figure 2-1	Network Topology	2-2
Figure 2-2	Basic Communication Process	2-10