

Contents

1 Introduction

1.1 Terminology	1-1
1.1.1 Communications Service Provider (CSP)	1-1
1.1.2 Security Policy	1-1
1.1.3 Security Services and Mechanisms	1-2
1.1.4 Network Elements	1-2
1.1.4.1 Operating Systems	1-4
1.1.4.2 Network System Component (NSC)	1-4
1.1.5 Functional Systems (FSs)	1-5
1.1.6 Network Systems (NSs)	1-6
1.1.7 NE Classes	1-7
1.2 Objectives	1-8
1.3 Intended Audience	1-8
1.4 Scope	1-8
1.5 Assumptions	1-10
1.6 Organization of Document	1-10
1.7 Requirements Terminology	1-11
1.8 Requirement Labeling Conventions	1-12
1.8.1 Numbering of Requirement and Related Objects	1-12
1.8.2 Requirement, Conditional Requirement, and Objective Identification	1-12

2 Threats and Vulnerabilities

2.1 External Intrusion	2-1
2.2 Internal Intrusion	2-2
2.2.1 Violation of Privilege	2-2
2.2.2 Ease of Access	2-2
2.3 Software Intrusion and Harmful Code	2-3
2.4 Common NE/FS/NS Attack Points	2-4
2.4.1 Management System Access	2-4
2.4.2 Main Console Access	2-5
2.4.3 Craft Access	2-5
2.4.4 Packet-based Communications Protocols	2-5
2.5 Common Attack Techniques	2-6
2.5.1 Time Falsification	2-6
2.5.2 IP Eavesdropping	2-6
2.5.3 Masquerade	2-6
2.5.4 Message Sequence Alterations	2-6

3 Security Feature Requirements

3.1 Overview	3-1
3.1.1 General Security Services Requirements	3-3
3.2 Identification and Authentication (I&A)	3-4

- 3.2.1 Identification 3-4
 - 3.2.1.1 Identification Requirements for Login Services 3-5
- 3.2.2 Authentication Service 3-6
 - 3.2.2.1 Strong Authentication 3-7
 - 3.2.2.2 Authentication Requirements for Login Services 3-8
- 3.3 Confidentiality Requirements 3-13
 - 3.3.1 Data Confidentiality 3-13
- 3.4 System Access Control 3-14
 - 3.4.1 Connection-Oriented Communications Security Requirements 3-16
 - 3.4.1.1 Connection Authentication 3-16
 - 3.4.2 Connectionless Communications Security Requirements 3-17
 - 3.4.3 Message Protection 3-18
 - 3.4.3.1 Gateway Screening 3-19
 - 3.4.3.2 Message Integrity 3-19
 - 3.4.3.3 Message Origin Authentication 3-20
 - 3.4.3.4 Message Content Confidentiality Requirements 3-21
 - 3.4.3.5 Message Timeliness and Replay Protection 3-21
 - 3.4.4 Craft and Emergency Entry Port (EEP) Requirements 3-21
 - 3.4.5 System Access Requirements for Login Services 3-22
- 3.5 Resource Access Control 3-25
- 3.6 Security Audit 3-29
 - 3.6.1 Security Log Generation 3-29
 - 3.6.2 Report Generation/Audit Trail 3-32
- 3.7 Data Integrity 3-32
- 3.8 System Integrity 3-33
- 3.9 Continuity of Service 3-34
- 3.10 Security Administration 3-35
- 3.11 Non-Repudiation 3-39
 - 3.11.1 Non-repudiation of Message Origin 3-40
 - 3.11.1.1 Whole Message Hashing 3-40
 - 3.11.2 Non-repudiation of Message Delivery 3-41

4 Development Life Cycle Requirements

- 4.1 Threats Associated With Software Development 4-1
- 4.2 Generic Requirements 4-3
- 4.3 Security Policy 4-3
- 4.4 Requirement Analysis 4-3
- 4.5 System Design 4-4
- 4.6 Detailed System Design 4-5
- 4.7 Implementation 4-5
- 4.8 Development Environment 4-6
- 4.9 System Test 4-7
- 4.10 Packaging and Delivery 4-8
- 4.11 Documentation 4-9
- 4.12 Support 4-11

Appendix A: References

Appendix B: Acronyms

Appendix C: Glossary

Requirement-Object Index

List of Figures

Figure 1-1	Network System Components (NSCs) Residing in NEs within an NS	1-5
Figure 1-2	Functional Systems within an NS	1-6
Figure 1-3	VOP NS With CCA FS and NSCs Located in NEs	1-7