

Contents

Special Report Notice of Disclaimer	iii
List of Figures	xi
List of Tables	xii
Foreword	xiii
Executive Summary	xv
1 Introduction	
1.1 Purpose	1-2
1.2 Background	1-2
1.2.1 The Bearer Network	1-4
1.2.1.1 Subscriber Loops	1-4
1.2.1.2 Switching Systems	1-4
1.2.2 Signaling Networks	1-4
1.2.3 Operations Support Network	1-5
1.3 Conclusions	1-5
2 PSN Security Basics	
2.1 The Security Concerns	2-1
2.1.1 Scope and Magnitude of the Threats	2-3
2.1.2 The Effect a Single Service Provider Can Have	2-5
2.1.3 Business Incentives	2-5
2.1.4 Legal Ramifications	2-5
2.1.5 The Problem, and Steps to Address it	2-6
2.2 Recommendations and Guidelines	2-7
2.2.1 Security Architecture	2-7
2.2.2 Security Policy	2-9
2.2.3 Security Measures	2-11
2.2.4 Generic Security Requirements	2-13
2.2.5 Legal Concerns	2-14
2.2.6 Fraud and Fraud Management	2-15
2.2.7 General Recommendations	2-17
2.2.7.1 UNIX	2-19
2.2.7.2 Windows NT	2-21
2.3 Closing Comments	2-22
3 Security Policy Overview for Carriers	
3.1 Value of Network Security Policy	3-1
3.2 Characteristics of a Security Policy	3-1
3.3 Steps in Developing Security Policy	3-2
3.3.1 Establish Objectives	3-2

- 3.3.2 Define Scope 3-3
- 3.3.3 Assess Risks 3-3
- 3.3.4 Determine Components of Policy 3-4
- 3.4 Components of a Network Security Policy 3-5
 - 3.4.1 Physical Security Policy 3-5
 - 3.4.2 Network Element Policy 3-6
 - 3.4.3 Operations Support System Policy 3-7
 - 3.4.4 Access Network Policy 3-7
 - 3.4.4.1 Connectivity 3-8
 - 3.4.4.2 Software 3-8
 - 3.4.4.3 Access Control 3-8
 - 3.4.4.4 Security Administration 3-9
 - 3.4.5 Network Management Policy 3-9
 - 3.4.6 Transport Policy 3-9
 - 3.4.7 Intrusion Response Policy 3-10
- 3.5 Security Awareness 3-11
 - 3.5.1 Audience 3-11
 - 3.5.2 Methods of Promoting Awareness 3-13
- 3.6 Further Information 3-13

4 Assessing Public Switched Network (PSN) Security

- 4.1 Asset Analysis 4-2
 - 4.1.1 Physical Assets 4-3
 - 4.1.2 Service Assets 4-4
 - 4.1.3 Information Assets 4-4
- 4.2 Threat Analysis 4-5
- 4.3 Vulnerability Analysis 4-6
- 4.4 Deciding Which Assets Must Be Reviewed – Risk Assessment 4-6
- 4.5 Functional Isolation of Assets 4-7
- 4.6 Physical Security 4-7
 - 4.6.1 Physical Premises Security 4-8
 - 4.6.1.1 General Building Security 4-8
 - 4.6.1.2 Guards, Locks, and Identification Badges 4-9
 - 4.6.1.3 Physical and Logical Key Administration 4-10
 - 4.6.1.4 Functional Separation of Facilities and Multilevel Access Control 4-11
 - 4.6.2 Building Services 4-11
 - 4.6.2.1 Utilities (Power, Water, Telecommunications, Waste Disposal) 4-12
 - 4.6.2.2 Emergency Facilities 4-13
 - 4.6.2.3 Transport Redundancy and Physical Protection of Critical Facilities 4-13
 - 4.6.3 Environmental and Geographical Threats 4-13
 - 4.6.4 Collocation Procedures 4-14
- 4.7 Logical Security 4-15
 - 4.7.1 Logical Security Features 4-15
 - 4.7.1.1 Identification and Nonrepudiation 4-15
 - 4.7.1.2 Authentication 4-16

4.7.1.3	System Access Control	4-16
4.7.1.4	Authorization	4-17
4.7.1.5	Audit	4-17
4.7.1.6	Integrity	4-18
4.7.1.7	Confidentiality	4-18
4.7.1.8	Security Administration	4-18
4.7.2	Network Elements	4-19
4.7.2.1	Analysis of the Operations Interface	4-19
4.7.2.2	Ascertaining the NE's Security Features	4-20
4.7.2.2.1	Comparing Against Policy	4-20
4.7.2.2.2	Assessing the Security Configuration	4-21
4.7.2.2.3	Installation	4-21
4.7.2.3	Analysis of the Call-Processing Interface	4-22
4.7.3	Operations Support Systems	4-22
4.7.3.1	Security for OSS Ingress	4-22
4.7.3.2	Security Issues for the OSS/NE Interface	4-23
4.7.4	Network Management	4-24
4.7.5	Access Networks	4-27
4.7.5.1	Access Network Architecture Review	4-28
4.7.5.2	Access Mechanism Review	4-29
4.7.5.3	Other Considerations	4-29
4.7.5.3.1	Business Partner, Reseller, and Vendor Access	4-30
4.7.5.3.2	Law Enforcement Access	4-30
4.7.5.3.3	Customer Access	4-31
4.7.6	Transport Networks	4-31
4.7.7	Operating Systems	4-32
4.7.8	Security Administration	4-32
4.7.8.1	Responsibilities of Security Administration	4-32
4.7.8.2	Assessment of Security Administration	4-33
4.8	Documenting and Presenting the Findings	4-35
4.8.1	Categorizing Findings	4-35
4.8.2	Addressing the Findings	4-36
4.8.3	Informing Management	4-36
4.9	Summary	4-36

5 Transmission Control Protocol (TCP)/Internet Protocol (IP) Security Issues

5.1	IP Vulnerabilities	5-1
5.1.1	Eavesdropping	5-2
5.1.2	IP Spoofing	5-2
5.1.3	Source Routing	5-3
5.1.4	Denial of Service	5-3
5.2	TCP Vulnerabilities	5-3
5.2.1	Session Hijacking	5-3
5.2.2	Denial of Service	5-4

6 Asynchronous Transfer Mode (ATM) Security

6.1 Introduction to ATM	6-1
6.1.1 Definition and Motivation	6-1
6.1.2 How ATM Works	6-3
6.1.3 General ATM Security Issues	6-4
6.2 ATM Architectures and Security	6-5
6.3 Security Measures	6-7
6.3.1 Protection of Users' Data	6-7
6.3.1.1 The ATM Forum's Security Working Group	6-7
6.3.1.2 The ATM Forum's Security Specification, Version 1.1	6-7
6.3.2 Protection of ATM Services and Applications	6-11
6.3.3 Protection of ATM Control Protocols	6-12
6.3.4 Protection of NEs	6-12
6.3.4.1 NE Security	6-13
6.3.4.2 Network Management Security	6-15
6.3.4.3 Firewalls, Activity Logging, and Intrusion Detection	6-16
6.4 Conclusions	6-17
6.4.1 Summary	6-17
6.4.2 Serious Exposures	6-18

7 Digital Subscriber Line (DSL) Security

7.1 Introduction to DSL	7-1
7.1.1 Definition and Motivation	7-1
7.1.2 How DSL Works	7-2
7.1.3 Types of DSL	7-4
7.1.4 General DSL Security Issues	7-6
7.1.4.1 New NEs	7-6
7.1.4.2 Intelligent Peripheral Management	7-7
7.1.4.3 General DSL-Specific Issues	7-7
7.1.5 DSL Architectures and Security	7-9
7.1.5.1 Bridged DSL Connections	7-9
7.1.5.2 Routed DSL Connections	7-10
7.1.5.3 PPP Connections	7-11
7.2 Security Measures	7-13
7.2.1 Dual-Homed Gateways	7-13
7.2.2 Virtual Private Networks (VPNs)	7-14
7.2.3 SOHO VPNs	7-17
7.2.4 Protecting the Corporate LAN	7-18
7.3 Conclusions	7-20
7.3.1 Summary	7-20
7.3.2 Serious Exposures	7-21

8 Local Number Portability (LNP) Security

8.1 Introduction to LNP	8-1
8.1.1 Definition and Motivation	8-1

8.1.2	How LNP Works	8-2
8.1.2.1	Local Service Provider Portability	8-3
8.1.2.2	Management of Ported Number Information	8-6
8.2	Security Issues	8-8
8.2.1	Network	8-8
8.2.2	LNP Database Platform	8-9
8.2.3	SMS and Operations Support Issues	8-10
8.2.4	Fraud Issues	8-10
8.2.4.1	Customer Failure to Pay	8-10
8.2.4.2	Questionable Business Practices	8-11
8.2.5	Other Concerns	8-11
8.3	Security Measures	8-12
8.3.1	LNP Database	8-12
8.3.2	SMS and Support Systems	8-13
8.4	Conclusions	8-13
8.4.1	Summary	8-13
8.4.2	Serious Exposures	8-14

9 Next Generation Network (NGN) Security

9.1	Introduction to NGN	9-1
9.1.1	Definition and Motivation	9-1
9.1.2	How NGN Works	9-1
9.1.2.1	Agents	9-3
9.1.2.2	Gateways	9-4
9.1.2.3	Support Systems	9-4
9.1.3	General Security Issues	9-4
9.2	NGN Architecture and Security	9-5
9.2.1	Platforms	9-5
9.2.2	Network Elements and Operations Support Systems	9-7
9.2.2.1	Service Agent	9-7
9.2.2.2	Call Connection Agent	9-7
9.2.2.3	Billing Agent	9-8
9.2.2.4	Access Gateway	9-8
9.2.2.5	Signaling Gateway	9-9
9.2.2.6	Trunk Gateway	9-9
9.2.2.7	Wireless Gateway	9-9
9.2.2.8	Support Systems	9-9
9.2.3	Network Management	9-10
9.2.4	Protocols	9-10
9.2.5	Ingress Points	9-12
9.3	Security Measures	9-13
9.3.1	Operating Platforms	9-13
9.3.2	Network Elements (NEs) and Operations support Systems (OSSs)	9-14
9.3.3	Facilities Housing Network Components	9-15
9.3.4	Network Management	9-15
9.3.5	Protocols Associated with Signaling and Trunking	9-15

9.3.6 Ingress Points to the Network 9-16
9.4 Conclusions 9-16
9.4.1 Summary 9-16
9.4.2 Serious Exposures 9-17

Appendix A: References and Resources

A.1 Section 1: Introduction (General References) A-1
A.2 Section 2: PSN Security Basics A-2
A.3 Section 3: Security Policy Overview for Carriers A-3
A.4 Section 4: Assessing PSN Security A-4
A.5 Section 5: TCP/IP Security Issues A-5
A.6 Section 6: Asynchronous Transfer Mode (ATM) Security A-5
A.7 Section 7: Digital Subscriber Line (DSL) Security A-7
A.8 Section 8: Local Number Portability (LNP) Security A-7
A.9 Section 9: Next Generation Network (NGN) Security A-8
Note A-9
 To Contact Telcordia Customer Service or to Order Documents A-9
 To Order Documents From Within Telcordia (Employees Only) A-9

Appendix B: Glossary

B.1 Definitions B-1
B.2 Acronyms B-6

List of Figures

Figure 1-1	Simplified PSN Architecture	1-3
Figure 6-1	ATM Protocol Layer Mapping	6-2
Figure 6-2	ATM Reference Model	6-2
Figure 6-3	ATM Cell Format	6-3
Figure 6-4	ATM Forum Security Agents	6-10
Figure 7-1	Theoretical Bit Rate Capacity of Twisted Pair	7-2
Figure 7-2	Use of Twisted-Pair Spectrum for ADSL	7-3
Figure 7-3	DSL Architecture Showing Line Sharing	7-4
Figure 7-4	Types of DSL	7-5
Figure 7-5	Bridged DSL Connection	7-10
Figure 7-6	Routed DSL Connection	7-11
Figure 7-7	PPP DSL Connection	7-12
Figure 7-8	Dual-Homed Gateway Connection	7-14
Figure 7-9	Small Office, Home Office Connectivity	7-16
Figure 7-10	VPN Between SOHO and Corporate LAN	7-17
Figure 7-11	Multiple Connections Over DSL	7-18
Figure 7-12	Extending the Corporate Firewall	7-19
Figure 8-1	Schematic of LSPP	8-4
Figure 8-2	Sample Ported Call Flow	8-6
Figure 8-3	Process Flow for Porting a Number	8-7
Figure 8-4	CCS Network Schematic	8-9
Figure 9-1	Simplified NGN architecture	9-2

List of Tables

Table 7-1	xDSL Characteristics	7-5
-----------	--------------------------------	-----