

Contents

Preface	xi
Chapter 1: Overview: A Kerberos FAQ	1
1.1 What Is Kerberos?	2
1.2 What Is Kerberos Good For?	3
1.3 What Versions Are Available?	4
1.4 Where Can I Get Kerberos?	4
1.5 What On-Line Information Is There?	5
1.6 How Is Kerberos Used for Security?	6
Chapter 2: Kerberos for Users	9
2.1 Using Kerberos	9
2.2 Manipulating Credentials	11
2.3 Changing Your Kerberos Password	13
2.4 Performing Basic Kerberos Operations	14
2.5 Using MIT-Kerberized Applications	17
2.6 Encrypting Your Session	18
2.7 Forwarding Tickets	20
2.8 Specifying the User	24
2.9 Knowing When Something Isn't Right	26
2.10 Using the Windows 95/NT Interface	29
2.11 Using Eudora	31
Chapter 3: Kerberos for Administrators	35
3.1 Knowing What You're Trying to Protect	35
3.2 Building the Kerberos Distribution	37
3.3 Installing the KDC	41
3.3.1 The <code>krb5.conf</code> Configuration File	42
3.3.2 The <code>kdc.conf</code> Configuration File	44
3.4 Creating the Kerberos Database	45
3.5 Setting Up the Administrative Principals	47

3.6	Starting the KDC and the Admin Server	49
3.7	Accessing the Database	50
3.7.1	Adding a New Principal	52
3.7.2	Deleting a Principal	55
3.7.3	Modifying a Principal	56
3.7.4	Changing a Password	56
3.7.5	Retrieving a Principal's Database Entry	57
3.7.6	Listing the Database Entries	57
3.7.7	Compiling a Keytab File	58
3.7.8	Removing Principals from a Keytab File	59
3.7.9	Finding Out What Commands Are Available	60
3.7.10	Quitting	60
3.8	Setting Up Cross-Realm Authentication	60
3.9	Administering an Application Server	63
Chapter 4: Kerberos for Developers		65
4.1	Contents of a Kerberized Application	65
4.2	Example of a Kerberized Application	66
4.2.1	The Client	69
4.2.2	The Server	73
4.2.3	Extensible Function Calls	76
4.2.4	Error Handling	78
4.3	Replay Caches	80
4.4	A Password-Changing Program	82
4.5	Other Kerberos API Calls	84
4.6	GSS-API	85
4.6.1	Understanding How the GSS-API Calls Work	86
4.6.2	Taking Advantage of GSS-API	90
Chapter 5: The Basics of Kerberos		93
5.1	The Origins of Kerberos	93
5.2	Principals	94
5.3	A Primer on Cryptography	95
5.3.1	Ciphers	95
5.3.2	One-Way Hashes	98
5.4	Authentication with Kerberos	99

5.4.1	The (High-Level) Details	100
5.4.2	Mutual Authentication	105
5.4.3	KDC = AS + TGS	105
5.4.4	Cross-Realm Authentication	106
5.5	The Kerberos Environment	108
5.5.1	A Note about Passwords	108
5.5.2	Local Security	109
Chapter 6: Other Versions of Kerberos		113
6.1	Pre-V5 and Commercial Versions	113
6.1.1	Kerberos V1, V2, V3	113
6.1.2	Kerberos V4	113
6.1.3	Bones, E-Bones, and Heimdal	114
6.1.4	TrustBroker	114
6.2	V4 and V5 Operational Differences	115
6.2.1	kinit	116
6.2.2	klist	117
6.2.3	kdestroy	118
6.3	V4 and V5 Anatomical Differences	119
6.3.1	Byte Ordering	119
6.3.2	Ticket Lifetimes	121
6.3.3	Delegation	121
6.3.4	Password Hashing	122
6.3.5	Preauthentication	123
6.3.6	Cryptographic Algorithms	124
Chapter 7: New Directions for Kerberos		127
7.1	Public Key Cryptography	127
7.1.1	The Basics of Public Key Cryptography	128
7.1.2	The Strength of Public Key Cryptography	129
7.1.3	Public Key Certification	130
7.1.4	Effect on the Kerberos Protocol	132
7.1.5	Use in Cross-Realm Authentication	135
7.1.6	Public Key Kerberos Today	136
7.2	Kerberos and Windows 2000	137
7.3	Smart Cards and Other Portable Devices	140
7.3.1	Smart Cards and PC Cards	141
7.3.2	PC Cards and the Kerberos Protocol	142

Appendix A: Glossary	145
Appendix B: Annotated Bibliography	155
B.1 Books	155
B.2 Papers	156
B.3 Internet Specifications	156
B.4 On-Line References	158
Index	161