

Contents

Foreword	vii
Preface	ix
I Introduction	3
1 Overview	5
1.1 Identifier-locator split	6
1.2 HIP in the Internet architecture	7
1.3 Brief history of HIP	10
1.4 Organization of the book	11
2 Introduction to network security	13
2.1 Goals of cryptographic protocols	13
2.2 Basics and terminology	14
2.3 Attack types	15
2.3.1 Eavesdropping	15
2.3.2 Impersonation	15
2.3.3 Man-In-The-Middle attacks	15
2.3.4 Delay and replay attacks	16
2.3.5 Denial of service attacks	16
2.3.6 Exhaustive key space search	17
2.3.7 Cryptoanalysis	17
2.4 Defense mechanisms	17
2.4.1 Symmetric cryptography	17
2.4.2 Public-key cryptography	21
2.4.3 One-way cryptographic hash functions	25
2.4.4 One-time signatures	28
2.4.5 Sequence numbers	28
2.4.6 Cryptographic nonces	29
2.4.7 Client puzzles	29
2.5 Security protocols	30
2.5.1 Modular exponential Diffie-Hellman groups	30
2.5.2 Keying material	31

2.5.3	Transforms	31
2.5.4	IP security architecture: IPsec	32
2.5.5	IPsec modes	33
2.5.6	IPsec security protocols	35
2.5.7	SIGMA	36
2.5.8	Internet Key Exchange: IKE	39
2.6	Weak authentication techniques	42
2.7	Secure DNS	42
 II The Host Identity Protocol		45
 3 Architectural overview		47
3.1	Internet namespaces	47
3.2	Methods of identifying a host	48
3.3	Overlay Routable Cryptographic Hash Identifiers	48
3.3.1	The purpose of an IPv6 prefix	49
3.3.2	Generating and routing an ORCHID	49
3.3.3	ORCHID properties	50
3.4	The role of IPsec	51
3.5	Related IETF activities	51
 4 Base protocol		53
4.1	Base exchange	53
4.1.1	I1 packet	53
4.1.2	R1 packet	55
4.1.3	I2 packet	57
4.1.4	R2 packet	57
4.2	Other HIP control packets	58
4.3	IPsec encapsulation	59
4.3.1	ESP transforms	59
4.3.2	ESP bound end-to-end tunnel	60
 5 Main extensions		71
5.1	Mobility and multihoming	71
5.1.1	Mobility and multihoming architecture	71
5.1.2	Multihoming as extension of mobility	73
5.1.3	Effect of ESP anti-replay window	76
5.1.4	The LOCATOR parameter	78
5.1.5	Locator states	79
5.1.6	Credit-based authentication	80
5.1.7	Interaction with transport protocols	81
5.2	Rendezvous server	82
5.2.1	Registering with a Rendezvous Server	82
5.2.2	Rendezvous parameters	83
5.3	DNS extensions	83
5.3.1	HIP requirements to DNS	84

CONTENTS	iii
5.3.2 Storing a RVS address	84
5.3.3 DNS security	86
5.4 Registration protocol	86
5.4.1 The process of registration	86
5.4.2 Packet formats	87
6 Advanced extensions	89
6.1 Opportunistic mode	89
6.1.1 Initiating opportunistic base exchange	89
6.1.2 Implementation using a TCP option	90
6.2 Piggybacking transport headers to base exchange	90
6.2.1 Piggybacking to I2	90
6.2.2 Security concerns	91
6.3 HIP service discovery	91
6.3.1 Overview of Service Discovery	91
6.3.2 On-the-path Service Discovery	94
6.3.3 Passive Service Discovery	95
6.3.4 Regional Service Discovery	95
6.4 Simultaneous multiaccess	95
6.4.1 Flow binding extension	96
6.4.2 Packet formats	97
6.5 Disseminating HITs with a presence service	99
6.5.1 HITs in the Presence Information Data Format	100
6.5.2 Disseminating protocol	100
6.6 Multicast	101
6.6.1 Challenges for IP multicast	102
6.6.2 Host Identity Specific multicast	103
6.6.3 Authenticating multicast receivers	107
7 Performance measurements	111
7.1 HIP on Nokia Internet Tablet	111
7.2 Experimental results	112
7.2.1 Test environment	112
7.2.2 Basic HIP characteristics	113
7.3 Summary	120
8 Lightweight HIP	123
8.1 Security functionality of HIP	123
8.1.1 Performance limitations of HIP	124
8.1.2 Problem statement	124
8.1.3 Scope of LHIP	125
8.1.4 Threat model	126
8.2 HIP high-level goals	127
8.2.1 LHIP high-level goals	129
8.2.2 Possible approaches	130
8.3 LHIP design	132

8.3.1	Hash chains for HIP authentication	133
8.3.2	Time-based signatures	133
8.3.3	Interactive signatures based on hash chains	135
8.3.4	LHIP authentication layer	137
8.3.5	LHIP integration	143
8.3.6	LHIP associations	146
8.3.7	Security considerations	154
8.3.8	Association upgrades: from LHIP to HIP	157
8.4	LHIP performance	160
8.4.1	LHIP base exchange	161
8.4.2	LHIP update	162
8.5	Discussion	164
8.5.1	LH1 - performance	164
8.5.2	LH2 - protocol security	165
8.5.3	LH3 - namespace security	165
8.5.4	LH4 - compatibility	165
III Infrastructure Support		167
9	Middlebox traversal	169
9.1	Requirements for traversing legacy middleboxes	169
9.1.1	NAT traversal	170
9.1.2	Firewall traversal	171
9.1.3	Strategies for legacy middlebox traversal	171
9.2	Legacy NAT traversal	172
9.2.1	NAT detection	172
9.2.2	Header format	172
9.2.3	Initiator behind a NAT	174
9.2.4	Responder behind a NAT	176
9.2.5	Initiator and Responder behind a NAT	178
9.2.6	Multihoming and mobility with NATs	180
9.2.7	Traversing firewalls	181
9.3	Requirements for HIP-aware middleboxes	181
9.4	HIP-aware firewall	182
9.4.1	Flow identification	182
9.4.2	Advanced extensions	183
9.4.3	Asymmetric routing	185
9.4.4	Security risks	185
10	Name resolution	187
10.1	Problem statement of naming	187
10.2	Distributed Hash Tables	190
10.2.1	Overview of Distributed Hash Tables	190
10.2.2	OpenDHT interface	191
10.3	HIP interface to OpenDHT	192

10.4	Overview of overlay networks	196
10.5	Host Identity Indirection Infrastructure	197
10.5.1	Separating control, data, and naming	197
10.5.2	The data plane	198
10.5.3	The control plane	204
10.5.4	Discussion of the <i>Hi3</i> design	207
11	Micromobility	211
11.1	Local rendezvous servers	211
11.1.1	Intra-domain mobility	212
11.1.2	Inter-domain mobility	213
11.2	Secure micromobility	216
11.2.1	Hash chain authentication	216
11.2.2	Secure network attachment	217
11.2.3	Micromobility handover	218
11.3	Network mobility	220
11.3.1	Delegation of signaling	220
11.3.2	Mobile router	220
11.3.3	HarMoNy	222
12	Communication privacy	227
12.1	SPINAT	227
12.2	BLIND	228
12.2.1	Location and identity privacy	228
12.2.2	Protecting host identity	229
12.2.3	Protecting location privacy	231
12.3	Anonymous identifiers	231
12.3.1	Identifiers on protocol layers	232
12.3.2	Changing identifiers	233
IV	Applications	235
13	Possible HIP applications	237
13.1	Virtual Private Networking	237
13.2	P2P Internet Sharing Architecture	239
13.3	Interoperating IPv4 and IPv6	241
13.4	Secure Mobile Architecture	242
13.4.1	Components of SMA	243
13.4.2	SMA testbed at Boeing	244
13.5	Live application migration	247
13.6	Network operator viewpoint on HIP	250
14	Application interface	253
14.1	Using legacy applications with HIP	253
14.1.1	Using IP addresses	254
14.1.2	Using DNS resolution	254

14.1.3	Directly using HIT	255
14.2	API for native HIP applications	255
14.2.1	Overview of the design	255
14.2.2	Interface specification	256
14.2.3	Socket attributes	260
15	Integrating HIP with other protocols	265
15.1	Generalized HIP	265
15.1.1	Classification of proposals	266
15.1.2	HIP implications	268
15.2	The use of Session Initiation Protocol	269
15.2.1	SIP as a rendezvous service	269
15.2.2	Complementary mobility	271
15.2.3	Securing SIP control traffic	272
15.2.4	Session Description Protocol extensions	274
15.3	Encapsulating HIP data using SRTP	275
15.4	Replacing HIP base exchange with IKEv2	280
15.5	Mobile IP and HIP	283
15.6	HIP proxy for legacy hosts	285
15.6.1	Legacy mobile hosts	285
15.6.2	Legacy correspondent hosts	287
A	Installing and using HIP	289
A.1	Overview of HIP implementations	289
A.2	HIPL tutorial	291
	Bibliography	295
	Abbreviations	301
	Index	307