

Contents

Foreword	xi
Preface	xv
I Overview	1
1 Introduction	3
1.1 Today's Internet	3
1.2 Goals of a Secure Internet Architecture	8
1.3 Future Internet Architectures	13
2 The SCION Architecture	17
2.1 Control Plane	21
2.2 Data Plane	25
2.3 Security Aspects	27
2.4 Use Cases	31
2.5 Incentives for Stakeholders	34
2.6 Deployment	36
2.7 Extensions	39
2.8 Main Contributions	39
3 Isolation Domains (ISDs)	43
3.1 Why Isolation?	43
3.2 The ISD Core	47
3.3 Coordination Among ISDs	48
3.4 Name Resolution	48
3.5 ISD Governance Models	51
3.6 Nested Isolation Domains	56
II SCION in Detail	59
4 Authentication Infrastructure	61
4.1 Overview	61
4.2 Control-Plane Authentication	68
4.3 Name Authentication	83
4.4 End-Entity Authentication	86

5	ISD Coordination	93
5.1	Motivation and Objectives	94
5.2	Announcing and Discovering New ISDs	97
5.3	Local Resolution of Conflicts	100
6	Name Resolution	101
6.1	Background	102
6.2	Name Resolution Architecture	104
6.3	Naming Information Model	106
6.4	The RAINS Protocol	114
6.5	The Naming Consistency Observer (NCO)	116
7	Control Plane	119
7.1	Path Exploration and Registration	119
7.2	Path Lookup	132
7.3	Secure Path Revocation	138
7.4	Failure Resilience and Service Discovery	146
7.5	AS-Level Anycast Service	153
7.6	SCION Control Message Protocol (SCMP)	155
7.7	Time Synchronization	159
8	Data Plane	161
8.1	Path Format	162
8.2	Creation of Forwarding Paths	164
8.3	Efficient Path Construction	174
9	Host Structure	179
9.1	SCION Dispatcher	179
9.2	SCION Daemon	183
9.3	Transmission Control Protocol (TCP/SCION)	185
9.4	SCION Stream Protocol (SSP)	188
10	Deployment and Operation	191
10.1	ISP Deployment	191
10.2	End-Domain Deployment	199
10.3	The SCION-IP Gateway (SIG)	201
10.4	How to Try Out SCION	211
10.5	SCION AS Management Framework	215
10.6	Deploying a New AS	218
10.7	The SCIONLab Experimentation Environment	220
10.8	Example: Life of a SCION Data Packet	223
10.9	SCION Path Policy	230

III Extensions	241
11 SIBRA	243
11.1 Motivation and Introduction	244
11.2 Goals and Adversary Model	245
11.3 Design Overview	247
11.4 SIBRA Core Paths	250
11.5 SIBRA Steady Paths	259
11.6 SIBRA Ephemeral Paths	261
11.7 Priority Traffic Monitoring and Policing	268
11.8 Use Cases	272
11.9 Discussion	273
11.10 Further Reading	276
12 OPT and DRKey	279
12.1 Introduction	280
12.2 OPT Problem Definition	281
12.3 OPT Design Overview	283
12.4 OPT Protocol Description	286
12.5 Dynamically Recreable Keys (DRKey)	291
IV Analysis and Evaluation	299
13 Security Analysis	301
13.1 Security Goals	302
13.2 Threat Model	304
13.3 Software Security	305
13.4 Control-Plane Path Manipulation	307
13.5 Data-Plane Path Manipulation	312
13.6 Censorship and Surveillance	318
13.7 Attacks Against Availability	320
13.8 Absence of Kill Switches	325
13.9 Resilience to Path Hijacking	327
13.10 Summary	330
14 Power Consumption	331
14.1 Modeling Power Consumption of an FIA Router	332
14.2 Simulation	334
V Specification	339
15 Packet and Message Formats	341
15.1 SCION Packet	341

15.2	Control Plane	355
15.3	PCB and Path Segment	356
15.4	Path Management Messages	361
15.5	PKI Interactions	362
15.6	SCMP Packet	363
16	Configuration File Formats	369
16.1	Trust Root Configuration	369
16.2	AS Certificates	370
16.3	Discovery Service Configuration	374
16.4	Router, Server, and End-Host Configuration	376
17	Cryptographic Algorithms	381
17.1	Algorithm Agility	381
17.2	Symmetric Primitives	384
17.3	Asymmetric Primitives	385
17.4	Post-Quantum Cryptography	386
	Bibliography	387
	Frequently Asked Questions	409
	Glossary	417
	Abbreviations	421
	Index	423

SCION: A Secure Internet Architecture

Perrig, A.; Szalachowski, P.; Reischuk, R.M.; Chuat, L.

2017, XX, 432 p. 120 illus., 78 illus. in color., Hardcover

ISBN: 978-3-319-67079-9