# Preface

ADRIAN PERRIG

The SCION project started in Summer 2009 at Carnegie Mellon University (CMU), when we began meeting weekly with Haowen Chan, Hsu-Chun Hsiao, and Xin Zhang to consider what a secure inter-domain Internet architecture would look like if we could start from a clean slate. The goal was to create an architecture that offered high availability and security for basic point-to-point communication — which other architectures that provide content-centric or mobility-centric properties could build upon.

The project was arduous, because for every approach we came up with, we saw at least two new problems. After several months of meetings, all we had was many pages filled with requirements that the architecture should meet, but no approach to satisfy even a major subset of the requirements. As time went on, the project seemed to be increasingly hopeless. But our perseverance paid off. In Summer of 2010 the basic ideas of beaconing and the creation of end-to-end paths through path-segment combination emerged. Although we would have been happy with any approach that satisfied half of the requirements, our basic approach appeared to meet most of our requirements. Delighted with our discovery, we accelerated the pace of the project. We were encouraged by the fact that our architecture could elegantly address every issue we came up with. We called it the Secure Communication Infrastructure for a Future Internet (SCI-FI).

In Fall 2010, Dave Andersen and Geoff Hasker joined the project and we started writing a paper. Many people took issue with the designation SCI-FI, so we went with Geoff Hasker's suggestion of SCION — despite its rather presumptuous meaning of "heir to the throne" — as an acronym for *scalability, control, and isolation on next-generation networks*. Our paper quickly took shape, and was accepted for publication at the IEEE Symposium on Security and Privacy in 2011. Oddly, the paper was placed in the "Secure Information Flow and Information Policies" session, which usually hosts papers of a different type. Unfazed, Xin Zhang gave a strong presentation and the work was well received.

Buoyed by the early promise of the project, we continued working on SCION and convinced the eXpressive Internet Architecture (XIA) team at CMU that

SCION was a worthwhile choice for host-to-host communication. So initially, SCION developed in the context of XIA, which helped support the early research.

The project developed along two major axes: research and implementation. The early research results leveraged SCION for DDoS defense [114] and anonymous communication [113]. To achieve source authentication and path validation, we designed OPT [132], and performed a formal verification of the protocol [263]. With the goal of producing a stronger public-key infrastructure (PKI) for SCION, the Accountable Key Infrastructure (AKI) was developed [133].

The initial implementation effort started with the help of several student projects. However, much of the progress was made when Soo-Bum Lee joined the project and completed a first SCION prototype in 2011, which we continuously improved throughout 2012.

In view of the opportunities offered by ETH Zurich, we built up a new research group around the SCION project in Switzerland. Pawel Szalachowski, a promising postdoctoral researcher from Poland, joined the group in March 2013 and became the core designer and developer of SCION. Under his guidance, the SCION prototype and testbed went through several generations of software and matured into the system that we currently deploy. Much progress was made when Stephen Shirley joined the group, as he improved numerous aspects of the system including design and implementation. Jason Lee deserves credit for his work on the multipath socket and the high-speed router (the latter project was in collaboration with Takayuki Sasaki who was visiting from NEC). More recently, Tobias Klausmann and Ercan Ucan joined the developer team, greatly improving SCION's infrastructure and deployment. All the hard work has paid off: in Summer 2016 we started a deployment of SCION routers in the production networks of Swisscom and SWITCH, two large ISPs in Switzerland, with several of their customers now engaging in test deployments.

On the research side, many newcomers joined the team at ETH, assisted by the postdoctoral researchers David Barrera, Raphael Reischuk, and Pawel Szalachowski. With SCION as the core focus of the research group, much progress was accomplished in many directions, such as PKIs [23, 52, 168, 169, 233–235], DDoS defense [22, 143], anonymous communication and privacy [49, 51, 153, 156], efficient forwarding [154], fault localization [21], energy analysis [50], high-speed duplicate detection [155], as well as public-policy and legal aspects [26, 194]. Besides the research contributions, Raphael Reischuk successfully contributed to outreach and promotion by designing the SCION logo and creating the SCION website, initiating a newsletter, and giving outreach presentations to help attract early adopters. Many PhD students contributed to SCION — for instance Sam Hitz has made several major contributions by suggesting Python as a base language (to speed up implementation and increase code clarity), implementing major parts of the (early) SCION core code, and

designing and implementing the secure link revocation mechanism. Also many researchers contributed to the project, for instance Virgil Gligor, Yih-Chun Hu, and members of the XIA project team, who were involved in several research projects and contributed much feedback and many insights to the project.

Over the past eight years, numerous people helped on the project through research discussions, feedback on publications, setup and operation of SCION infrastructure, research projects, and more. We estimate that around 80 people have so far played a significant role in the project (about 30 people from our group, about 30 bachelor or master students have completed a semester project or thesis, and about 20 external collaborators and industry visitors who worked closely with us). We are very grateful for everyone's help, without which the project would not have reached its current status. When adding up the amount of time researchers and engineers worked on the SCION architecture, we arrive at approximately 75 person-years of endeavor that has been spent by the end of 2016. Consequently, much thought and deliberation have gone into the design decisions presented in this book.

When we started the project in 2009, it was mostly security researchers who agreed on the importance of re-designing the Internet from a security perspective [27]. However, many events that have occurred since have brought Internet security to the forefront of awareness: several cases of Internet censorship, the Snowden revelations, NSA backdoors (e.g., in Juniper routers, standardized cryptographic algorithms), Internet kill switches, IANA's stewardship transition to a multi-stakeholder governance, increasingly large DDoS attacks, attacked certification authorities, the emergence of quantum computers, etc. Today, Internet security and privacy is a common topic of conversation. In the IETF, the main body for standardizing Internet protocols, awareness of security concerns has greatly increased — with an IETF draft stating that pervasive monitoring by governments constitutes an attack [85]. These events have given impetus to the SCION project, as it matured during this period and provides solutions to the exact problems that have moved into public awareness. Consequently, the SCION architecture goals appear aligned with the public interests and we do not seem to be swimming against the mainstream goals.

Bob Kahn mentioned that simplicity and elegance were the main reasons why TCP/IP has lasted as long as it has. When a system is simple and elegant, it is easy to understand, implement, and maintain. Thus, simplicity and elegance are important goals in SCION, besides availability, security, scalability, and efficiency. In the entire architecture, we attempt to minimize complexity to achieve the desired properties, leveraging well-understood technologies. Unless they were in line with the approach we deemed best, we avoided the urge to use "trendy" technologies of the day, such as blockchain or doubly homomorphic encryption. We hope that the readers will also appreciate the results of our endeavors to produce a clean-slate re-design of a highly available point-to-point communication architecture, and that they will join us on our journey towards a secure Internet.

## How to Read This Book

This book describes the essential components of the SCION future Internet architecture prototype (V1.0) including functional specifications of the SCION network elements (e.g., servers, routers, gateways), communication protocols among these elements, data structures, and configuration files. In particular, the book focuses on the specification of a working prototype and additional features that are not described in academic papers. We highlight contributions that we believe are particularly important and interesting with a diamond symbol.

The aim of this book is to provide an easy-to-follow introduction to SCION. To help the reader, it contains a glossary (Page 417) defining important terms and supplying background information. We indicate terms with a glossary entry as follows:

**glossary term**$^{\star}$

A gray bar in the margin indicates the presence of an example:

This is an example.

We also provide an index (Page 423), a list of abbreviations (Page 421), and answers to frequently asked questions (Page 409). A comprehensive example of SCION's operations is on Page 223 and illustrates the end-to-end communication between two hosts, including name resolution, path resolution, packet origination, and packet forwarding. The example provides references to detailed explanations of the underlying concepts and techniques, and thus serves as a good starting point for the more technically adept readers.

The book also aims to provide a comprehensive description of the main design features for achieving a secure Internet architecture. While many of the detailed design aspects are described in research papers, we have added relevant details where necessary to understand the important concepts. We have structured the book in such a way that the technical details gradually increase as it proceeds: starting with an overview and moving along to the format of configuration files at the end.

Additional SCION resources (research papers, talks, presentations, source code, and links to contributing efforts) are available on our web page:

`https://www.scion-architecture.net`

We also encourage interested readers to sign up to the SCION mailing list (through the above website). Furthermore, a discussion board for the SCION community takes questions and offers support regarding the development and deployment of SCION. As we encounter errors in the book, we will document them in an errata list on our web page.

## Acknowledgments

Many people contributed toward this book. Special thanks go to Jeffrey Barnes for his excellent copy editing, and Ronan Nugent our editor at Springer who guided us through the publication process. We also thank the following individuals for providing valuable feedback that improved the content of this book (in alphabetical order):

| | |
|---|---|
| David Basin | ETH Zurich |
| Jan Boogman | Swisscom AG |
| Srdjan Capkun | ETH Zurich |
| Alexander Gall | SWITCH |
| Virgil Gligor | Carnegie Mellon University (CMU) |
| David Hausheer | Technische Universität Darmstadt |
| Yih-Chun Hu | University of Illinois at Urbana-Champaign |
| Jill Jermyn | Columbia University |
| Burt Kaliski | Verisign, Inc. |
| Ayumu Kubota | KDDI Corporation |
| Jovan Kurbalija | Geneva Internet Platform |
| Heejo Lee | Korea University |
| Simon Leinen | SWITCH |
| René Merz | Magnetron Labs |
| Peter Müller | ETH Zurich |
| Radha Poovendran | University of Washington |
| Timothy Roscoe | ETH Zurich |
| Mark Ryan | University of Birmingham |
| Ankit Singla | ETH Zurich |
| Christoph Sprenger | ETH Zurich |
| Peter Steenkiste | Carnegie Mellon University (CMU) |
| Laurent Vanbever | ETH Zurich |
| David Watrin | Swisscom AG |

The project was made possible by the generous support of the following organizations (in alphabetical order):

- CyLab at Carnegie Mellon University;
- ETH Zurich, which provided the majority of funding for the project;
- European Research Council, under the European Union's Seventh Framework Programme (FP7/2007-2013) / ERC grant agreement 617605;
- Infosec Global, through a contract;
- Institute for Information and Communications Technology Promotion (IITP), grant funded by the Korean government (MSIP) (No. R0190-16-2011, Development of Vulnerability Discovery Technologies for IoT Software Security);

- Intel Corp., which provided equipment;
- KDDI Corporation, through a gift;
- National Science Foundation (NSF), under awards CCF-0424422 and CNS-1040801;
- Swisscom AG, through a contract;
- Zurich Information Security and Privacy Center (ZISC), through gifts from Google, NEC, Open Systems, SIX, and ZKB.

Without these sources of support, the project would not have been possible. We would like to express our sincere gratitude to all who contributed.

http://www.springer.com/978-3-319-67079-9

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