Information Security and Cryptography

Series Editors

David Basin, ETH Zürich, Switzerland
Kenny Paterson, Royal Holloway, University of London, UK

Advisory Board

Michael Backes
Gilles Barthe
Ronald Cramer
Ivan Damgård
Andrew D. Gordon
Joshua D. Guttman
Christopher Kruegel
Ueli Maurer
Tatsuaki Okamoto
Adrian Perrig
Bart Preneel

More information about this series at http://www.springer.com/series/4752

Adrian Perrig · Pawel Szalachowski
Raphael M. Reischuk · Laurent Chuat

SCION: A Secure Internet Architecture

Springer

Adrian Perrig
Network Security Group
ETH Zürich
Zürich
Switzerland

Raphael M. Reischuk
Network Security Group
ETH Zürich
Zürich
Switzerland

Pawel Szalachowski
Network Security Group
ETH Zürich
Zürich
Switzerland

Laurent Chuat
Network Security Group
ETH Zürich
Zürich
Switzerland

ISSN 1619-7100 ISSN 2197-845X (electronic)
Information Security and Cryptography
ISBN 978-3-319-67079-9 ISBN 978-3-319-67080-5 (eBook)
https://doi.org/10.1007/978-3-319-67080-5

Library of Congress Control Number: 2017955641

© Springer International Publishing AG 2017
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

To Miyoung,
Thank you for your unwavering support.
Love, forever!

Adrian

To Henio,
For all these sleepless nights.

Paweł

To my family and those
who supported me along my way.

Raphael

To Manon,
For your patience and encouragement.

Laurent

Contents

Foreword

VIRGIL GLIGOR (CARNEGIE MELLON UNIVERSITY)

Despite having worked with Adrian Perrig for a few years at Carnegie Mellon University's CyLab, where he embarked on the task of developing a secure architecture for the Internet, I had had no in-depth exposure to SCION until I attended a presentation he gave at Singapore Management University in late 2010. Entitled "SCI-FI: Secure Communication Infrastructure for a Future Internet," his talk described the early project that was to become SCION. The audience reaction was predictable and all too familiar: you can't change the Internet; its foundation is immutable!

But in fact it had been clear for a long time that the Internet design had to change, as security cracks had gradually been appearing in its foundation since its early days. By the mid-1980s, it was obvious that the denial-of-service problem was not effectively addressed by Internet protocols. By the mid-90s, it was clear that BGP was prone to cascading instability, and by the mid-2000s distributed denial of service had become a predictable Internet "feature." Other security issues arose, such as prefix hijacking, IP source address spoofing, and packet-content alteration. Even when cryptographic protocols, such as SSL/TLS, were finally applied in response to e-commerce pressure, their worldwide deployment was more an exception than the rule. Besides, the public-key infrastructure (PKI) supporting SSL/TLS continues to be extremely fragile. As the Internet has expanded in size and use, security problems have become increasingly severe: both organized crime and nation states have started to launch massive attacks for economic or political gain.

Despite repeated wake-up calls for Internet redesign, the response has generally been something of a "boiling frogs" reaction: the severity of the problems has continued to increase relentlessly, but perception of the enormous effort required to solve them has blocked, frustrated and foiled any impulse for redesign from ground up. Over the past decade, it has become clear that security is a fundamental problem of Internet design, but it remains a secondary concern. So against that background, the audience reaction to Adrian Perrig's 2010 SCI-FI presentation in Singapore was only to be expected.

Since my first exposure to SCION, I have been impressed with several of its innovative ideas and new properties. For instance, the concept of isolation

domains provides control-plane protection and simplifies construction of PKI infrastructures due to the natural scoping of trust roots. (Although a concept similar to that of isolation domains was considered for the initial Internet design, the focus in that early phase was on getting the network to function at scale before introducing hierarchical decomposition mechanisms.) SCION's concepts of transparency and control, which weave through the entire architecture, result in many desirable properties, e.g., both high-performance and multipath communication for hosts. Also, cryptographically protected packet-carried forwarding state brings forwarding-path authorization without incurring any router-state cost. SCION's architecture integrates these concepts seamlessly into a coherent secure system.

This book offers a fascinating view of both the high-level concepts that drive SCION's design and its implementation, and it leads the reader to draw some surprising new conclusions.

Contrary to the common belief that security causes a loss of performance, several SCION operations are efficient despite performing cryptographic operations; e.g., SCION packet forwarding can be faster and require less energy than IP forwarding. This suggests that redesigning the Internet can be rewarding in more areas than security. I am not aware of any other project that has gone so deeply and broadly in redesigning an entire secure Internet architecture.

The SCION project contradicts another widely held opinion in demonstrating that deployment of a new Internet architecture at scale is in fact possible. This book illustrates the basic ingredients of deployment success: SCION has provided a multitude of incentives for ISPs and end domains, so that local deployment can already provide benefits to early adopters. The book also describes some of SCION's secret deployment sauce: keep the updates of the current routing infrastructure of both ISPs and end domains to a minimum, and reuse the existing intra-domain communication to the maximum extent. It should not be surprising that (e.g., Swiss) ISPs have already found it possible to deploy SCION routers in their core infrastructure and develop new services on it.

Contrary to another common belief, a single Internet architecture can enable integrated defenses against multiple types of attacks, as opposed to one which requires piecemeal solutions. In my opinion, the SCION architecture is unique in this sense, and this book illustrates the fact through the solutions it describes to long-standing problems. For example, SCION provides these unique properties:

- Global security without any global root of trust. This implies that a global "kill switch," an unavoidable feature of other secure network architectures, is not possible in SCION.
- Control-plane functions for secure path withdrawals and control messages. Although any network can always cryptographically sign messages in an

attempt to achieve secure operation, SCION secures the control plane in a very efficient way while enabling high-speed router operation.

- Global resource allocation without requiring per-flow or per-computation fairness mechanisms. This stands in contrast to the current Internet design, in which these mechanisms enable massive DDoS attacks by commercially available botnets. The book shows how SCION leverages its global resource allocation architecture to offer a range of DDoS countermeasures.
- Practical multipath architecture without having to rely on multiple communication media and heterogeneous routing interfaces; e.g., cellular or WiFi connection on cell phones. SCION is currently the only architecture I am aware of that provides general homogeneous multipath communication.
- A robust TLS PKI design with a very limited attack surface; i.e., several independent entities need to be compromised for an attack to be launched. In contrast, the current TLS PKI has a huge attack surface; e.g., if a single key is compromised of the thousand or more that are trusted to sign domain certificates, an adversary can compromise any TLS-protected channel.

So can the Internet be changed and secured from the ground up? This book provides a beacon of hope, proposing that the seemingly unsolvable problem of changing the Internet can in fact be solved. With the open-source SCION implementation and a readily available testbed, researchers can experiment on a firmer network foundation and develop solutions to today's pressing security problems. It is only through hands-on experiments on common platforms like SCION that we can build a new Internet, one that we can rely on with confidence. Let's embrace it!

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*

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.