Lecture Notes in Computer Science 10453

More information about this series at http://www.springer.com/series/7410

Marc Dacier · Michael Bailey
Michalis Polychronakis · Manos Antonakakis (Eds.)

Research in Attacks, Intrusions, and Defenses

20th International Symposium, RAID 2017
Atlanta, GA, USA, September 18–20, 2017
Proceedings

Springer

Editors

Marc Dacier
Qatar Computing Research Institute
Doha
Qatar

Michalis Polychronakis
Stony Brook University
Stony Brook, NY
USA

Michael Bailey
University of Illinois at Urbana Champaign
Champaign, IL
USA

Manos Antonakakis
Georgia Institute of Technology
Georgia
USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-66331-9 ISBN 978-3-319-66332-6 (eBook)
DOI 10.1007/978-3-319-66332-6

Library of Congress Control Number: 2017952320

LNCS Sublibrary: SL4 – Security and Cryptology

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

Preface

The International Symposium on Research in Attacks, Intrusion, and Defenses (RAID) is celebrating its 20th anniversary this year! You have the proceedings of this event in your hands and we hope you will enjoy it.

RAID was created to offer a venue for researchers looking at the emerging field of intrusion detection. It was the follow up to the CMAD workshop (future directions in Computer Misuse and Anomaly Detection), which was held for the fourth and last time in 1996. CMAD was initiated by Becky Bace, who sadly passed away in 2017, and had approached intrusion detection from both an operational as well as from an "intelligence" point of view. RAID has grown in much the same spirit, expanding its scope beyond the sole intrusion detection area, encouraging research on real-world problems, fostering sound, thorough, and reproducible experiments, and building bridges to other communities (e.g., measurement, networking, systems) that share these same values. Twenty years later, RAID is a well-established international conference that enjoys truly worldwide recognition. Hosted every year in a different location, it has alternated between Europe and the USA with a few notable exceptions, including Australia (2007), Saint Lucia (2013), and Japan (2015).

This year, RAID 2017 received 105 admissible submissions of which 21 were accepted (20% acceptance rate). Each paper received at least 3 reviews and 43 papers (41%) received two additional reviews to settle disagreements between the first three reviewers, to answer questions raised during the online discussion phase, or to address issues brought forth by the authors' rebuttal. As in previous years, a double blind reviewing process was used to ensure that the reviewers remained unaware of the authors' names and affiliations during the discussion. The final decision for each paper was made during a face-to-face PC meeting following the IEEE Symposium on Security and Privacy in San Jose (CA), in May 2017. More than two thirds of the PC members attended that meeting.

The quality, diversity, and commitment of the Program Committee is paramount to the success of any conference and, with RAID, we have striven to broaden the pool of reviewers. Over the last ten years, an average of 50% of the members of the PC were changed from year to year. Furthermore, this year, nearly a third of the new PC members had never served on the RAID PC before, ensuring the healthy development of the community by reaching out to external experienced reviewers. It is also worth noting that RAID always tries to maintain a balance between industry and academia within its PC members, as well as between the various geographies. This year, around 75% of the PC members came from academia and 25% from industry. Approximately half of the members work in the USA, a bit less than a third in Europe, and the rest, 15%, were from the rest of the world, mostly Asia.

We endeavor to provide quality reviews to those who submit a paper to RAID and we try to provide constructive feedback when a paper is unfortunately rejected. In order to improve transparency, accepted papers are accompanied by a public summary, which is available within the online proceedings as supplementary material. It briefly explains the reasons why a given paper has been accepted but also, sometimes, acknowledges some reservations expressed by members of the PC. We hope that these open summaries will encourage future researchers to address the limitations identified by the PC members and consider new directions for research.

In 2012, for the 15th anniversary of RAID, we began the process of awarding, every five years, an "influential paper" award to a previously published paper at RAID that has had a major influence on the community. This year's award was given to the 2004 RAID paper by K. Wang and S.J. Stolfo, entitled "Anomalous Payload-Based network intrusion detection." That paper has been cited 869 times since its publication, which is an average of 67 times per year, every year, since its publication, the highest yearly average for every paper published at RAID since its creation.

RAID wouldn't exist without the dedication of the reviewers, who play a special role and spend a great deal of time reviewing papers, discussing them online, attending the PC meeting, shepherding papers, etc. To express our gratitude to them, every year RAID awards an "Outstanding Reviewer" prize. The winner is selected based on a number of factors: the quality of the reviews as judged by the other reviewers (usefulness, technical depth, etc.), timeliness of the reviews, participation in the online discussion and the face-to-face meeting, and the willingness to defend papers as opposed to quickly discard them. While we had a difficult time identifying a winner amongst so many excellent reviewers, it is with great pleasure that we announce that this year the award goes to Jon Giffin, from Hewlett Packard Enterprise.

RAID only exists because of the community that supports it. Indeed, RAID is completely self-funded. Every organizer independently shoulders the financial risks associated with its organization. The sponsors, therefore, play a very important role and ensure that the registration fees remain very reasonable. Therefore, we want to take this opportunity to thank Spamhaus and Comcast for their generous sponsorships of RAID 2017. We, of course, are very grateful to the general chair, Manos Antonakakis, from Georgia Tech, and his assembled team for ensuring that the conference ran smoothly. Special thanks go to the local arrangement chair, Roberto Perdisci, University of Georgia; to the publication chair, Michalis Polychronakis, from Stony Brook University; to the publicity chair, Nick Nikiforakis, from Stony Brook University; to the sponsor chair, Yacin Nadji, from Georgia Tech; to the local infrastructure chair, William R. Garrison, from Georgia Tech; and to the poster chair and webmaster, Chaz Lever, from Georgia Tech.

Happy Birthday, RAID. We all look forward for many more years to come.

September 2017

Marc Dacier
Michael Bailey

Organization

Organizing Committee

General Chair

Manos Antonakakis	Georgia Tech, USA

Program Committee Chair

Marc Dacier	QCRI/HBKU, Qatar

Program Committee Co-chair

Michael Bailey	University of Illinois at Urbana Champaign, USA

Publication Chair

Michalis Polychronakis	Stony Brook University, USA

Publicity Chair

Nick Nikiforakis	Stony Brook University, USA

Sponsor Chair

Yacin Nadji	Georgia Tech, USA

Local Arrangement Chair

Roberto Perdisci	University of Georgia, USA

Local Infrastructure Chair

William R. Garrison	Georgia Tech, USA

Poster Chair and Webmaster

Chaz Lever	Georgia Tech, USA

Program Committee

Magnus Almgren	Chalmers University of Technology, Sweden
Johanna Amann	ICSI, USA
Leyla Bilge	Symantec Research Labs, France
Lorenzo Cavallaro	Royal Holloway, University of London, UK
Mihai Christodorescu	Qualcomm Research, USA
Hervé Debar	Télécom SudParis, France
Manuel Egele	Boston University, USA

Sandro Ettale	Technical University Eindhoven, The Netherlands
Aurélien Francillon	Eurecom, France
Jon Giffin	HPE Fortify, USA
Virgil Gligor	Carnegie Mellon University, USA
Guofei Gu	Texas A&M University, USA
Sotiris Ioannidis	FORTH, Greece
Yongdae Kim	Korea Advanced Institute of Science and Technology, South Korea
Andrea Lanzi	University of Milan, Italy
Wenke Lee	Georgia Tech, USA
Corrado Leita	Lastline, UK
David Naccache	ENS Paris, France
Roberto Perdisci	University of Georgia, USA
Jason Polakis	University of Illinois at Chicago, USA
Bill Sanders	University of Illinois at Urbana-Champaign, USA
Kevin Snow	Zeropoint, USA
Angelos Stavrou	George Mason University, USA
Sal Stolfo	Columbia University, USA
Purui Su	Institute of Software/CAS, China
Mark Tehranipoor	University of Florida, USA
Al Valdes	University of Illinois at Urbana Champaign, USA
X. Sean Wang	Fudan University, China
Xiaogang (Cliff) Wang	US Army Research Office and adjunct with NC State University, USA
Ting Fang Yen	DataVisor, Inc., USA
Kehuan Zhang	Chinese University of Hong Kong, China

External Reviewers

Ali Abbasi	University of Twente, The Netherlands
Mahdi Alizadeh	University of Eindhoven, The Netherlands
Luca Allodi	University of Eindhoven, The Netherlands
Wissam Aoudi	Chalmers University of Technology, Sweden
Grégory Blanc	Télécom SudParis, France
Nicole Borrelli	Google, USA
Bram Cappers	University of Eindhoven, The Netherlands
Jiongyi Chen	Chinese University of Hong Kong, China
Phakpoom Chinprutthiwong	Texas A&M University, USA
Aisling Connolly	ENS, France
Nassim Corteggiani	Maxim Integrated, France
Andrei Costin	Jyväskylä University, Finland
Wenrui Diao	Chinese University of Hong Kong, China
Shuaike Dong	Chinese University of Hong Kong, China
Mohamed Elsabagh	George Mason University, USA
Houda Ferradi	NTT, France

Remi Geraud	ENS, France
Thomas Hayes	Eurecom, France
Weili Han	Fudan University, China
Kevin Hong	Texas A&M University, USA
Panagiotis Ilia	FORTH, Greece
Mikel Iturbe	Mondragon University, Spain
Ryan Johnson	George Mason University, USA
Yuan Kang	Columbia University, USA
Aljoscha Lautenbach	Chalmers University of Technology, Sweden
Florian Lugou	Télécom ParisTech, France
Clémentine Maurice	TU Graz, Austria
Abner Mendoza	Texas A&M University, USA
Soo-Jin Moon	Carnegie Mellon University, USA
Marus Muench	Eurecom, France
Boel Nelson	Chalmers University of Technology, Sweden
Dario Nisi	Eurecom, France
Nasser Nowdehi	Volvo Car Corporation and Chalmers University of Technology, Sweden
Melek Önen	Eurecom, France
Thomas Rosenstatter	Chalmers University of Technology, Sweden
Vyas Sekar	Carnegie Mellon University, USA
Boris Skoric	University of Eindhoven, The Netherlands
Saumya Solanki	University of Illinois at Chicago, USA
Charalampos Stylianopoulos	Chalmers University of Technology, Sweden
Adrian Tang	Columbia University, USA
Di Tang	Chinese University of Hong Kong, China
Stefan Thaler	University of Eindhoven, The Netherlands
Haopei Wang	Texas A&M University, USA
Yunfeng Xi	DataVisor, Inc., USA
Fenghao Xu	Chinese University of Hong Kong, China
Lei Xu	Texas A&M University, USA
Min Yang	Fudan University, China
Zhemin Yang	Fudan University, China
Emmanuele Zambon	SecurityMatters, The Netherlands
Yuan Zhang	Fudan University, China
Yunlei Zhao	Fudan University, China
Zhe Zhou	Chinese University of Hong Kong, China

Steering Committee

Davide Balzarotti	Eurecom, France
Herbert Bos	Vrije Universiteit Amsterdam, The Netherlands
Herve Debar	Télécom SudParis, France
Deborah Frincke	NSA Research, USA
Ming-Yuh Huang	Northwest Security Institute, USA

Somesh Jha	University of Wisconsin, USA
Erland Jonsson	Chalmers University of Technology, Sweden
Engin Kirda	Northeastern University, USA
Christopher Kruegel	UC Santa Barbara, USA
Wenke Lee	Georgia Tech, USA
Richard Lippmann	MIT Lincoln Laboratory, USA
Ludovic Me	CentraleSupélec, France
Robin Sommer	ICSI/LBNL, USA
Angelos Stavrou	George Mason University, USA
Sal Stolfo	Columbia University, USA
Alfonso Valdes	University of Illinois at Urbana Champaign, USA
Giovanni Vigna	UC Santa Barbara, USA
Andreas Wespi	IBM Research, Switzerland
S. Felix Wu	UC Davis, USA
Diego Zamboni	Swisscom, Switzerland

Sponsors

Spamhaus
Comcast

Contents

Software Security

Intrusion Detection

Android Security

Systems Security

Cybercrime

Cloud Security

Network Security