CCSW'17 — 2017 ACM Cloud Computing Security

Ghassan O. Karame
NEC Laboratories Europe
Heidelberg, Germany 69115
ghassan@karame.org

Angelos Stavrou
George Mason University
Fairdax, VA, USA 22030
astavrou@gmu.edu

ABSTRACT

The use and prevalence of cloud and large-scale computing infrastructures is increasing. They are projected to be a dominant trend in computing for the foreseeable future: major cloud operators are now estimated to house millions of machines each and to host substantial (and growing) fractions of corporate and government IT and web infrastructure. CCSW is a forum for bringing together researchers and practitioners to discuss the challenges and implications of current and future trends to the security of cloud operators, tenants, and the larger Internet community. Of special interest are the security challenges from the integration of cloud infrastructures with IoT and mobile application deployments. CCSW welcomes submissions on new threats, countermeasures, and opportunities brought about by the move to cloud computing, with a preference for unconventional approaches, as well as measurement studies and case studies that shed light on the security implications of cloud infrastructure and use cases.

KEYWORDS

Cloud Computing; Security.

1 MOTIVATION

No matter what the latest buzzword (grid, cloud, utility computing, SaaS, etc.), large-scale computing and cloud-like infrastructures are here to stay. How exactly they will look like tomorrow is still for the markets to decide, yet one thing is certain: clouds bring with them new untested deployment and associated adversarial models and vulnerabilities. Thus, it is essential that our community becomes involved. CCS is the ideal target for this workshop due to its often avant-garde position in the broader security landscape. According to Google Scholar (as of a year ago): 4 of the top 20 cited ACM CCS papers of the past five years come from CCSW.

2 TOPICAL COVERAGE

ACM CCSW is a forum for presenting novel research or empirical studies from academia, industry, and government on all theoretical and practical aspects of security, privacy, and data protection in cloud scenarios. Topics of interest include, but are not limited to: including:

- Secure cloud resource virtualization
- Secure data management outsourcing
- Practical privacy and integrity mechanisms for outsourcing
- Cloud-centric threat models
- Secure outsourced computation
- Remote attestation mechanisms in clouds
- Sand-boxing and VM-based enforcements
- Trust and policy management in clouds
- Secure identity management mechanisms
- Cloud-aware web service security paradigms and mechanisms
- Cloud-centric regulatory compliance issues and mechanisms
- Business and security risk models for clouds
- Cost and usability models and their interaction with cloud security
- Scalability of secure clouds
- Trusted computing technology and clouds
- Analysis of software for remote attestation and cloud protection
- Network security (DoS, IDS etc.) mechanisms for clouds
- Security for cloud programming models
- Privacy-enhancing machine-learning in clouds
- Secure and privacy protecting IoT clouds
- Accountable Data Analytics for clouds

We would like to especially encourage novel paradigms and controversial ideas that are not on the above list. The workshop is to act as a fertile ground for creative debate and interaction in security-sensitive areas of computing impacted by clouds.

3 PROGRAM COMMITTEE

We are grateful to the members of our technical program committee:

- Frederik Armknecht, University of Mannheim
- Erik-Oliver Blass, Airbus Research
- Sherman Chow, Chinese University of Hong Kong
- Mihai Christodorescu, Qualcomm
- Mauro Conti, University of Padua
- Cas Cremers, Oxford University
- Reza Curtmola, NJIT
- Roberto Di Pietro, Roma Tre University of Rome
- Dario Fiore, IMDEA Software
- Sara Foresti, University of Milano
- Sotiris Ioannides, FORTH
- Vasileios P. Kemerlis, Brown University
- Florian Kerschbaum, SAP Research
- George Kesidis, Penn State University
- Ivan Martinovic, Oxford University
- Soumendra Nanda, BAE Systems
- Nick Nikiforakis, Stony Brook University
- Melek Onen, Eurecom

CCS'17, October 30–November 3, 2017, Dallas, TX, USA
© 2017 Copyright held by the owner/author(s). ISBN 978-1-4503-4946-8/17/10.
DOI: http://dx.doi.org/10.1145/3133956.3137050

- Jason Polakis, University of Illinois
- Kasper Rasmussen, Oxford University
- Rei Safavi-Naini, University of Calgary
- Matthias Schunter, Intel Research
- Thomas Schneider, Technical University Darmstadt
- Elaine Shi, Cornell University
- Claudio Soriente, NEC
- Abhinav Srivastava, AT&T
- Nikos Triandopoulos, Stevens Institute of Technology
- Haining Wang, University of Delaware
- Yinqian Zhang, Ohio State University
- Fengwei Zhang, Wayne State University

4 PROGRAM CHAIRS

Ghassan Karame. is the Manager and Chief researcher of the Security Group of NEC Labs in Germany. Ghassan joined NEC Labs in April 2012. Prior to that, Ghassan was working as a postdoctoral researcher in the Institute of Information Security of ETH Zurich, Switzerland. He holds a Master of Science degree in Information Networking from Carnegie Mellon University (CMU), and a PhD degree in Computer Science from ETH Zurich.

Ghassan is interested in all aspects of security and privacy with a focus on cloud security, IoT security, network security, and Blockchain security.

Angelos Stavrou. is a full professor at George Mason University and the Director of the Center for Assurance Research and Engineering (CARE) at GMU. Stavrou has served as principal investigator on research awards from NSF, DARPA, IARPA, DHS, AFOSR, ARO, ONR, he is an active member of NIST's Mobile Security team and has written more than 90 peer-reviewed conference and journal articles.Stavrou received his M.Sc. in Electrical Engineering, M.Phil. andPh.D. (with distinction) in Computer Science all from Columbia University. He also holds an M.Sc. in theoretical Computer Science from University of Athens, and a B.Sc. in Physics with distinction from University of Patras, Greece.

Over the past few years, Dr. Stavrou's research has focused on two aspects of security: Systems' Security and Reliability with focus on large distributed systems and IoT.