CCSW 2015: The 7th ACM Cloud Computing Security Workshop

Florian Kerschbaum
SAP
Karlsruhe, Germany
florian.kerschbaum@sap.com

Cristina Nita-Rotaru
Purdue University
West Lafayette, IN, USA
cnitarot@purdue.edu

Indrajit Ray
Colorado State University
Fort Collins, CO, USA
indrajit.ray@colostate.edu

ABSTRACT

Notwithstanding the latest buzzwords (grid, cloud, utility computing, SaaS, etc.), large-scale computing and cloud-like deployment are the fastest growing computing infrastructures today. How exactly they will look like tomorrow is still for the markets to decide, yet one thing has already been identified: clouds have new, untested deployment, associated adversarial models and vulnerabilities and hence a very different threat landscape. It is essential that our community becomes involved in shaping the future security of cloud computing. The CCSW workshop aims to bring together researchers and practitioners in all security and privacy aspects of cloud-centric and outsourced computing.

Categories and Subject Descriptors

C.0 [**Computer Systems Organization**]: General—*System architectures*; D.4.6 [**Operating Systems**]: Security and Protection

Keywords

Cloud Computing; Security; Privacy

1. INTRODUCTION

Cloud computing is the fastest growing, large-scale industry trend. However, cloud computing also entails a new threat landscape than traditional computing paradigms. The CCSW workshop has had significant impact in the research community and tries to aim at a catalyst for new ideas in cloud computing security and privacy.

Cloud computing security and privacy has brought along a number of new threats and protection measures. Among those are secure virtualization, integrity verification and computing on encrypted data.

Secure Virtualization: Cloud computing infrastructures heavily rely on virtualization and co-location as a means to increase utilization. Multi-tenancy – the common use of resources such as processor, operating system or database among multiple clients – is a core concept in cloud computing. However, in order to achieve levels of security similar to traditional computing separation controls need to be in place. If one tenant can access the data from another tenant, this entails very new security risks. However, completely separating processes that share resources is hard, if not impossible. From multi-user computer systems security research is well acquainted with the topic of side and covert channels. We have seen this topic arise again in the era of cloud computing where one OS tenant could snoop the key of another OS tenant on the same physical machine. Common controls in security research include information flow policies, such as mandatory access control.

Integrity Verification: When computing is outsourced how does the client know that the result is trustworthy? Integrity verification techniques can help ensure trustworthiness. Recently, verifiable computation has seen a spike in interest, since it was possible to significantly reduce the time to verify the result. Most importantly, result verification can be performed in constant time, such that the effect of outsourcing the computation is not annihilated. Next to verification of computation verification of storage (and retrieval results) is an important topic. Often, it is not possible to retrieve the entire stored data for verification. For this purpose, proofs of retrievability and provable data possession have been introduced. These allow to check whether the cloud service provider stores the entire data with low local storage.

Computing on Encrypted Data: Besides integrity confidentiality is another important issue in cloud computing. The holy grail is to entirely compute on encrypted data in the cloud, such that no decryption operation needs to be performed. While fully homomorphic encryption promises this, its performance hinders practical adoption. The much faster multi-party secure computation requires to split the computation among multiple, mutually distrustful parties, which is a security concept that is not widely deployed. Industrial solutions based on tokenization or deterministic encryption fill the void. They come with the significant advantage that existing applications only require minimal changes. Nonetheless, their security remains debatable and lacking of academic standards. A step further goes symmetric searchable encryption with a much stronger security model, yet very acceptable performance.

These topics are only to provide a glimpse of security and privacy issues in cloud computing. They are here to serve as examples of the techniques and problems are discussed at the CCSW workshop.

CCS'15, October 12–16, 2015, Denver, Colorado, USA.
ACM 978-1-4503-3832-5/15/10.
DOI: http://dx.doi.org/10.1145/2810103.2812620.

2. SCOPE AND OBJECTIVES

The CCSW workshop brings together researchers and practitioners in all security and privacy aspects of cloud-centric and outsourced computing. The organizers especially encourage novel paradigms and controversial ideas that are not on the list of topics. The workshop is to act as a fertile ground for creative debate and interaction in security-sensitive areas of computing impacted by clouds.
em List of topics:

- practical cryptographic protocols for cloud security
- outsourced privacy-preserving computation
- secure cloud resource virtualization mechanisms
- secure data management outsourcing (e.g., database as a service)
- practical privacy and integrity mechanisms for outsourcing
- privacy-enhancing technologies for the cloud
- foundations of cloud-centric threat models
- secure computation outsourcing
- remote attestation mechanisms in clouds
- sandboxing and VM-based enforcements
- trust and policy management in clouds
- secure identity management mechanisms
- new cloud-aware web service security paradigms and mechanisms
- cloud-centric regulatory compliance issues and mechanisms
- business and security risk models and clouds
- cost and usability models and their interaction with security in clouds
- scalability of security in global-size clouds
- trusted computing technology and clouds
- binary analysis of software for remote attestation and cloud protection
- network security (DOS, IDS etc.) mechanisms for cloud contexts
- security for emerging cloud programming models
- energy/cost/efficiency of security in clouds
- security for software defined networking

3. PROGRAM

The 2015 ACM Cloud Computing Security Workshop (CCSW 2015) was held on October 16, 2015 in Denver, Colorado, USA in conjunction with the 22nd ACM CCS Conference. We received a total of twenty-one high quality submissions, out of which six were selected by the program committee through a rigorous reviewing process. We are delighted to have three keynote talks that bring new perspectives and practical problems from industry to the research community related to issues like security and privacy of data stored in the cloud, economic impact of security, and risk management in cloud settings. The three invited speakers are:

- Mike Reiter (University of North Carolina, USA)
- Chenxi Wang (Ciphercloud, USA)
- Bruce Grenfell (Concur / SAP, USA)

4. ORGANIZERS

Florian Kerschbaum is chief research expert at SAP in Karlsruhe, Germany. In the academic year 2011/12 he was on leave as the deputy professor (Lehrstuhlvertreter) for the chair of privacy and data security at Dresden University of Technology. Before his ten years at SAP he has worked for the San Francisco-based startup Arxan as a software architect. He holds a Ph.D. in computer science from the Karlsruhe Institute of Technology, a master's degree from Purdue University, and a bachelor's degree from Berufsakademie Mannheim.

Cristina Nita-Rotaru is an Associate Professor in the Department of Computer Science at Purdue University where she established the Dependable and Secure Distributed Systems Laboratory (DS^2) and is a member of the Center for Education and Research in Information Assurance and Security (CERIAS). Cristina Nita-Rotaru is a recipient of the NSF Career Award in 2006. She is also a recipient of the Purdue Teaching for Tomorrow Award in 2007, Purdue Excellence in Research Award, Seeds for Success in 2012, Purdue College of Science Research Award in 2013. Cristina Nita-Rotaru holds a Ph.D in Computer Science from Johns Hopkins University and a MS from Politehnica University of Bucharest, Romania.

Indrajit Ray is a Professor at Colorado State University. He joined the faculty of the Computer Science Department at Colorado State University in fall of 2001. Prior to that (Fall 1997 to Winter 2001) he was an Assistant Professor in the Computer and Information Science at University of Michigan-Dearborn. He received the PhD. degree in Information Technology from George Mason University in Fairfax, VA in 1997.
Steering committee:

- *Chair:* Gene Tsudik (University of California, Irvine, USA)
- Srdjan Capkun (ETH Zurich, Switzerland)
- Kristen Lauter (Microsoft, USA)
- Ahmad-Reza Sadeghi (Technical University Darmstadt, Germany)
- Rei Safavi-Naini (University of Calgary, Canada)
- Moti Yung (Google and Columbia University, USA)

5. ACKNOWLEDGEMENTS

We would like to thank Luca Ferretti for serving as web and publicity chair. We would like to thank the authors for submitting high-quality papers and the program committee for their time to review those and a considerate discussion in selecting the very best ones. A particularly thanks goes to our industry sponsors Microsoft Research and SAP.