SECODIC 2016
Workshop on Secure
and Efficient Outsourcing of Storage
and Computation of Data in the Cloud
August 31, 2016 – Salzburg, Austria
Co-organized by EU - H2020
tredisec
witdom
ARES Conference
International Conference on Availability, Reliability and Security

International workshop on Secure and Efficient Outsourcing of Storage and Computation of Data in the Cloud

The H2020 projects WITDOM (www.witdom.eu), and TREDISEC (www.tredisec.eu) organize the International Workshop SECODIC 2016 on “Secure and Efficient Outsourcing of Storage and Computation of Data in the Cloud” to be held during the ARES 2016 Conference at the Salzburg University of Applied Sciences, Salzburg, Austria.

This workshop aims at discussing the recent advances in managing security and performance in the cloud as well as protection of data at rest and in transit.
This research is not only motivated by users’ satisfaction, but also by the enforcement of **European Data Protection Regulations** as well as **institution’s internal regulations**. Since the majority of institutions lack resources and computing power to deal with large amount of data, and therefore outsourcing data to the cloud is strictly necessary, not complying with those regulations means not advancing in research.
These challenges drive a number of EU projects to devise effective solutions that meet the growing need for data protection in a number of security-critical scenarios (e.g. Financial Services and ehealth). Two of these projects are TREDISEC and WITDOM.

The workshop has the honour to include in its agenda a keynote given by professor N.Asokan, distinguished scientific who has focused his research on the application of cryptographic techniques to design secure protocols for distributed systems.
Besides, a selected group of recognized researchers in privacy and security in the cloud will present different topics which are being investigated in the framework of on-going EU projects related to this issue.
Eduarda Freire from IBM, will chair the slot named “Private and Secure Data Storage in the Cloud”. Within this slot, Florian Thiemer (Franhoufer), and Jose Ruíz (Atos) will give respectives talks about data sharing in the cloud.
Next, Mattias Neugschwandtner (IBM) will chair “Private and Secure Processing in the cloud”, with the participation of Sujoy Sinha Roy (Ku Leuven) and Daniel Slamanig (Graz University) who will talk about state-of-the-art cryptographic and homomorphic encryption techniques
Finally, there is a third slot chaired by Melek Önen (EURECOM) called “Integrity and Verifiability of Outsourced Data/ Computation”. Melek also talk about “Efficient Techniques for Publicly Verifiable Delegation of Computation”, and James Alderman (Royal Holloway University of London) will talk about “Verifiable Searchable Encryption”.

For more information visit:
https://www.ares-conference.eu/conference/ares-eu-symposium/secodic-2016/**.**

Or contact: Elena González, elena.gonzalez@atos.net

SECODIC 2016 Agenda

10:30 Introduction

1st talk: “Empowering privacy and security in non-trusted environments”: a WITDOM overview

- **Speaker:** Elsa Prieto, Atos
- **Abstract:** The WITDOM project focuses on developing innovative solutions for truly efficient and practical privacy enhancing techniques and efficient signal and data processing in the encrypted domain for the increasingly demanded outsourced environments, while easing the compliance with the European data protection regulation. The main strength of WITDOM resides in that the innovations in these areas are not applied independently or autonomously, but adequately and effectively composed and in an end-to-end secure and private architecture that defines a platform able to deploy privacy-preserving services on outsourced data with quantifiable and assessable technological guarantees.

2nd talk: Trust-aware, reliable and distributed information security in the Cloud”: a TREDISEC Overview

- **Speaker:** Ghassan Karame, NEC
- **Abstract:** The current trend for data placement shows a steady shift towards "the cloud". The advent of cloud storage and computation services however comes at the expense of data security and user privacy.
  To remedy this, customers nowadays call for end-to-end security whereby only end-users and authorized parties have access to their data and no-one else. This is especially true after the outbreak of data breaches and global surveillance programs in 2014.
  In the TREDISEC project, this problem is addressed by developing systems and techniques which make the cloud a secure and efficient heaven to store data. We plan to step away from a myriad of disconnected security protocols or cryptographic algorithms, and to converge on a single framework where all objectives are met.

11:00 Keynote: “Securing cloud-assisted services”

Speaker: N.Asokan, professor of Computer Science at Aalto University, Finland

Abstract: All kinds of previously local services are being moved to a cloud setting. While this is justified by the scalability and efficiency benefits of cloud-based services, it also raises new security and privacy challenges. Solving them by naive application of standard security/privacy techniques can conflict with other functional requirements. In this talk, I will outline some cloud-assisted services and the apparent conflicts that arise while trying to secure these services. I will then discuss a specific instance: the case of cloud-assisted detection of malicious mobile application packages and the privacy concerns involved. I will discuss how techniques for private membership test, assisted by hardware security mechanisms, can be used to address these concerns.

11:30 1st slot: “Private and Secure Data Storage in the Cloud”

Moderated by: Eduarda Freire, IBM

1st Talk: “Key-evolving dynamic data masking”

- **Speaker:** Eduarda Freire, IBM

Abstract: Data masking is the process of de-sensitizing data in a way that they remain useful for their original purpose. It is often applied for preventing that personal data such as social-security numbers, passport data, or patient identifiers leak to untrusted parties. Furthermore, masking also eliminates legal risks when data move across borders. Although many practical solutions have been introduced and are in commercial operation today, no formal security models exist.

This talk aims at discussing about models for dynamic data masking with key evolution, where sensitive data classified as direct identifiers are masked into epoch-and-identifier specific values, and large outsourced masked data sets can be dynamically updated by adding new values during operation. In terms of usability, the models discussed guarantee that masked data sets preserve a so-called referential integrity, i.e., correlated data can be linked together by authorized users in a non-production environment the same way as in the production system. Security in those models guarantee irreversibility of the masking process, and unlinkability of masked data across different epochs by unauthorized users.

2nd Talk: "Data Sharing in the cloud with Proxy-Re-Encryption and Malleable Signature“

- **Speaker:** Florian Thiemer, Fraunhofer
- **Abstract:** Data sharing plays a vital role in many online systems. There exists multiple cloud service provider on the market that offer data storing and sharing solutions for end user and business applications.

  This presentation gives an overview of the common privacy and security problems that data sharing platforms are facing and how sophisticated cryptographic mechanisms like proxy-re-encryption and malleable signature can improve the privacy and security level.

3rd talk: “Data-centric security is the right approach for Digital Single Market”

- **Speaker:** Jose Ruiz, Atos
- **Abstract:** One of the main goals of EU is the creation of a single market that fits for this digital age, tearing down regulatory walls and moving from 28 national markets to a single one. Data-centric security is a new approach that emphasizes the security of the data itself rather than the security of networks, servers or applications. In this model the data is self-describing and self-defending, provides elements for checking policies and controls and allows data to be protected as it is in transit, stored or changing business context. Therefore, data-centric security is evolving rapidly as enterprises increasingly rely on digital information to run their business.

15:15 “2nd slot: Private and Secure Processing in the Cloud”

Moderated by Matthias Neugschwandtner, IBM

1st talk: “Challenges for Isolating Computational Resources in Cloud Software Stacks"

- **Speaker:** Matthias Neugschwandtner, IBM
- **Abstract:** Isolation of computational resources in the software stacks that run today's cloud services is a key factor in both their resilience to withstand attacks as well as limiting the consequences of successful exploitation. At the same time isolation potentially hinders efficient use of computational resources - efficient isolation depends on how and where it is employed. This talk discusses state-of-the-art resource isolation techniques as well as the different levels they apply to.

2nd talk: “Hardware Assisted Fully Homomorphic Function Evaluation”

- **Speaker:** Sujoy Sinha Roy, KU Leuven
- **Abstract:** In this work we propose a scheme to perform homomorphic evaluations of arbitrary depth with the assistance of a special hardware module that we call the recryption box. All existing lattice based somewhat homomorphic encryption schemes can only perform homomorphic operations until the noise in the ciphertexts reaches a critical bound depending on the parameters of the homomorphic encryption scheme.

The classical approach of bootstrapping also allows for arbitrary depth evaluations, but has a detrimental impact on the size of the parameters, making the whole setup inefficient. We describe two different instantiations of our recryption box for assisting homomorphic evaluations of arbitrary depth.

3rd talk: "Malleable Cryptography for Security and Privacy in the Cloud"

- **Speaker:** Daniel Slamanig, Graz University
- **Abstract:** Cloud computing is highly dynamic as data is moved around and processed by different services running on third party infrastructure shared by numerous tenants. Such a setting clearly demands (previously unconsidered) security related challenges to be solved. While strong security guarantees can be achieved by means of cryptography, the traditional paradigm for use of cryptography is static. But when data is processed by different parties and one simultaneously requires cryptographic guarantees such as end-to-end confidentiality and authenticity the picture changes. Cryptographic primitives such as encryption and digital signature schemes now need to support such dynamicity. In this talk we will look at different types of cryptographic primitives that support such so called malleability and discuss how such cryptographic schemes can be employed to increase the security of cloud services.

15:15 3rd slot: “Integrity and Verifiability of Outsourced Data/ Computation”

Moderated by Melek Önen, EURECOM

1st talk: "Efficient Techniques for Publicly Verifiable Delegation of Computation"

- **Speaker:** Melek Önen, EURECOM
- **Abstract:** In this talk, we introduce two cryptographic protocols for publicly verifiable computation that allow a lightweight client to securely outsource to a cloud server the evaluation of high degree univariate polynomials and the multiplication of large matrices.

  Similarly to existing work, our protocols follow the amortized verifiable computation approach.

  Furthermore, by exploiting the mathematical properties of polynomials and matrices, they are more efficient and give way to public delegatability.

2nd talk: "Verifiable Searchable Encryption"

- **Speaker:** James Alderman, Royal Holloway University of London
- **Abstract:** When outsourcing the storage of sensitive data to an (untrusted) remote server, a data owner may choose to encrypt the data beforehand to preserve confidentiality. However, it is then difficult to efficiently retrieve specific portions of the data as the server is unable to identify the relevant information. Searchable encryption has been well studied as a solution to this problem, allowing data owners and other authorised users to generate search queries which the server may execute over the encrypted data to identify relevant data portions.

  However, many current schemes lack two important properties: verifiability of search results, and expressive queries. In this talk, we will introduce Extended Verifiable Searchable Encryption (eVSE) that permits a user to verify that search results are correct and complete. eVSE also permits verifiable computational queries over keywords and specific data values, that go beyond the standard keyword matching queries to allow functions such as averaging or counting operations.

Workshop Chairs

Melek Önen. EURECOM, France

Ghassan Karame. NEC, Germany

Matthias Neugschwandtner. IBM Research, Switzerland

Elsa Prieto. Atos, Spain

Eduarda Freire. IBM Research, Switzerland

Acknowledgements

WITDOM and TREDISEC want to thank the projects Coco Cloud, PRISMACLOUD, CREDENTIAL, and CLARUS for their contribution to the SECODIC 2016. We also would like to thank the ARES conference for their support in the organization of this workshop.

WITDOM and TREDISEC have received funding from the European Union’s Horizon 2020 (H2020) research and innovation programme under the Grant Agreements no. 64437 and 644412. This work was supported in part by the Swiss State Secretariat for Education, Research and Innovation (SERI). The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission or the Swiss Government.