PRACTICE - Privacy-Preserving Computation in the Cloud

Newsletter

March 2015 - Issue 3

PRACTICE

In this Issue

Main Project Information

Information processed by businesses, government organizations and individuals often comes with confidentiality and integrity requirements that the processing party must adhere to. As a result, data processors must deploy security controls for their ICT infrastructure, protecting it against external as well as internal attackers. This is relatively easy when this infrastructure is local and is controlled by the processing party, but much harder when the infrastructure is provided by an external service provider. Due to financial savings, an easy and convenient access to data and services, and business agility, organizations as well as individuals choose to outsouce their data to a cloud, where an untrusted party is in charge of storage and computation. However, user trust cannot be built since common computing techniques cannot be applied on encrypted data meaning that the data and the programs that compute on the data must be decrypted before being run on the cloud infrastructure. A comprehensive solution for securing the cloud computing infrastructure can be based on cryptographic mechanisms of secure computation. These mechanisms support computation on encrypted data. In this context, PRACTICE addresses all of the following settings:

- **Hiding user data from other users of the same cloud service**
- **Hiding user data from the cloud provider**
- **Securing computation between several servers**
- **Securing computation between untrusting parties**

Message from the Coordinator

The first project year of the PRACTICE project has already passed and was very successfully. All in all, ten deliverables have been submitted and three milestones have been reached so far. In September and October 2014 all partners met for a technical meeting in Istanbul/Turkey where the upcoming partner contributions and dissemination activities for PRACTICE were discussed among other issues. In January 2015 the 1st PRACTICE Review Meeting took place. Furthermore, the partners participated at several events and in addition to that they published numerous scientific publications. These publications as well as further relevant information about the project can be found on the project website: www.practice-project.eu

Results and ongoing activities

Over the past months the PRACTICE team worked carefully on the following deliverables:

D11.1 - A theoretical evaluation of the existing secure computation solutions summarizes an evaluation of existing state-of-the-art protocols for secure multi-party computation, and highlights the protocols that seem most relevant for actual deployment in the near term. The area of secure multi-party computation has experienced considerable progress in recent years, but research results were described in many separate and independent publications.

D22.1 - State-of-the-art Analysis gives a survey of techniques and tools which might be contributing to realize privacy preserving computations in the cloud.

The first part of **D31.1 - Risk assessment and current legal status on data protection** includes an overview on the legal issues concerning cloud computing under the current European data protection law, while second part contains a report on the state of the art on techniques for assessing and managing risks targeted to cloud-based business processes.

Among other issues, a survey about the website's visitors has been conducted in **D32.1 - Updated plan and initial report on dissemination, standardisation, exploitation and training** which pointed out that during the first project period the PRACTICE website has been visited by 2,548 unique visitors which shows the interest in this topic. Furthermore, this deliverable reports on the progress and further plans for dissemination activities, standardisation and exploitation of project results, and education and training.

Key Data:

Start Date:	1 November 2013
End Date:	31 October 2016
Duration:	36 months
Project Reference:	609611
Project Costs:	€ 10.465.059
Project Funding:	€ 7.550.000

Consortium:	18 partners (11 countries)
Project Coordinator:	Dr. Klaus-Michael Koch coordination@practice-project.eu
Technical Leader:	Dr. Florian Kerschbaum florian.kerschbaum@sap.com
Scientific Leader:	Prof. Dr. Ahmad-Reza Sadeghi ahmad.sadeghi@trust.cased.de
Project Website:	www.practice-project.eu

FOLLOW US ON twitter

https://twitter.com/FP7_PRACTICE

LinkedIn

PRACTICE - Privacy-Preserving Computation in the Cloud

Newsletter

March 2015 - Issue 3

PRACTICE

Scientific Publications

Searchable Encryption with Secure Efficient Updates
Florian Hahn, Florian Kerschbaum, in ACM Conference on Computer and Communications Security, 2014

Tutorial: Client-Controlled Cloud Encryption
Florian Kerschbaum, in ACM Conference on Computer and Communications Security

ABY - A framework for efficient mixed-protocol secure two-party computation
Daniel Demmler, Michael Zohner, Thomas Schneider, in NDSS'15, 2015

Publicity Auditable Secure Multi-Party Computation
Ivan Damgard, Claudio Orlandi, Carsten Baum, in 9th Conference on Security and Cryptography for Networks

Compact Ring-LWE Cryptoprocessor
Sujoy Sinha Roy, Frederik Vercauteren, Nele Mentens, Donald Songlong Chen, Ingrid Verbauwhede, in Workshop on Cryptographic Hardware and Embedded Systems, 2014

Optimal Average-Complexity Ideal-Security Order-Preserving Encryption
Florian Kerschbaum, Axel Schröpfer, in ACM Conference on computer and communications Security, 2014

Zur Problematik des Personenbezuges beim Cloud Computing
Matthis Grenzer, Niklas Heitmueller, in PinG –Privacy in Germany, 2014

Outlook for the second PRACTICE project year

During the first year of PRACTICE, good progress was made and thus a solid basis for the upcoming period could be created. In the 2nd project year, the focus lies on the subsequent list of public deliverables and milestones which are considered to be created and reached:

- **D12.2** "Adversary, trust, communication and system models"
- **D23.1** "Platform for secure surveys"
- **D24.2** "Business Modelling"
- **MS4** "A) Business specification. B) Adversary, trust, communication, system models. C) Platform secure surveys"

Upcoming and past events

Technical, General Assembly and Advisory Board Meeting in Istanbul

Upcoming Meetings & Events

- **PRACTICE Technical Meeting**
  8th-10th April 2015, Vienna/Austria
- **10th ACM Symposium (ASIACCS 2015)**
  14th-17th April 2015, Singapore/Asia
- **EUROCRYPT 2015**
  26th-30th April 2015, Sofia/Bulgaria

PRACTICE present at past events

- **5th Bar-Ilan Winter School in Cryptography on Advances in Practical Multiparty Computation**
  15th-19th February 2015, Rama-Gan/Israel
- **AAAS Annual Meeting and NDSS Symposium 2015**
  8th-16th February 2015, San Jose, San Diego/USA
- **Financial Cryptography and Data Security 2015**
  24th January-1st February 2015, San Juan/Puerto Rico
- **2nd Meeting and WG3 Meeting of the Network and Information Security Platform Plenary**
  11th-12th December 2014, Brussels/Belgium
- **ACM Cloud Computing Security Workshop**
  7th November 2014, Arizona/USA
- **9th Conference on Security and Cryptography Networks**
  3rd-5th September 2014, Amalfi/Italy
- **23rd USENIX Security Symposium**
  20th-22nd August 2014, San Diego/USA
- **CRYPTO 2014**
  17th-21st August 2014, Santa Barbara/USA

Contact:

PRACTICE Project Coordination Team
Dr. Klaus-Michael Koch
Technikon Forschungs – und Planungsgesellschaft mbH
Burgplatz 3a, A-9500 Villach
Tel.: +43 4242 23355 - 71
Fax.: +43 4242 23355 - 77
E-Mail: coordination@practice-project.eu
Website: www.practice-project.eu

TECHNIKON

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 609611.