PRACTICE - Privacy-Preserving Computation in the Cloud

Newsletter

July 2014 - Issue 2

PRACTICE

Main Project Information

The PRACTICE project aims to build a **secure cloud framework** that allows for the realization of advanced and practical cryptographic technologies providing sophisticated **security and privacy** guarantees for all parties in cloud-computing scenarios. The fundamental technologies that will be investigated are:

- **Secure Multiparty Computation** (MPC)
- **Fully Homomorphic Encryption** (FHE)
- **Domain-Specific Development Tools**
- **Application of Formal Methods** to verify relevant properties of resulting systems

In this Issue

Message from the Coordinator

PRACTICE at TDW Conference in Vienna

The first couple of months of the PRACTICE project have already passed successfully. Four deliverables and one report have been submitted and two milestones have been reached. At the end of March and beginning of April a couple of partners met in Berlin/Germany for a technical meeting. The main objective was to discuss relevant partner contributions and further progress of the project as well as planned dissemination activities in order to better promote PRACTICE. Moreover, several partners participated in various conferences and workshops where they represented the project. Such dissemination activities will also continue throughout the summer months and beyond. For the end of September/ beginning of October a technical meeting in Istanbul has been scheduled. For a more detailed overview of upcoming meetings and conferences, as well as PRACTICE related scientific publications and other dissemination material, please visit our project website: www.practice-project.eu.

PRACTICE present at past events:

- **DIMACS Workshop on Secure Cloud Computing**
  27th March 2014, New Jersey/USA
- **PRACTICE Technical Meeting**
  31st March - 2nd April 2014, Berlin/Germany
- **The Trust in the Digital World Conference**
  7th-8th April 2014, Vienna/Austria
- **Workshop: Theory and Practice of Secure Multiparty Computation**
  5th-9th May 2014, Aarhus/Denmark
- **Annual Privacy Forum 2014**
  20th-21st May 2014, Athens/Greece
- **2nd ACM Workshop on Information Hiding and Multimedia Security**
  11th-13th June 2014, Salzburg/Austria
- **Cryptography Summer School**
  21st-24th July 2014, Bucharest/Romania

Upcoming Meetings & Events:

- **23rd USENIX Security Symposium**
  20th - 22nd August, San Diego (CA)/USA
- **Technical, General Assembly & Advisory Board Meeting**
  29th September - 1st October, Istanbul/Turkey
- **ACM Cloud Computing Security Workshop**
  7th November, Arizona/USA
- **2nd Meeting of the Network and Information Security Platform Plenary**
  11th December, Brussels/Belgium
- **WG3 of the EU Platform on Network and Information Security**
  12th December, Brussels/Belgium

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

July 2014 - Issue 2

PRACTICE

Scientific Publications

Notes on non-interactive secure comparison in "Image feature extraction in the encrypted domain with privacy-preserving SIFT"
Matthias Schneider, Thomas Schneider (TUDA), in 2nd ACM Workshop on Information Hiding and Multimedia Security, 2014

GSHADE: Faster privacy-preserving distance computation and biometric identification
Julien Bringer, Hervé Chabanne, Mélanie Favre, Alain Patey, Thomas Schneider (TUDA), Michael Zohner (TUDA), in 2nd ACM Workshop on Information Hiding and Multimedia Security, 2014

Ad-hoc secure two-party computation on mobile devices using hardware tokens
Daniel Demmler (TUDA), Thomas Schneider (TUDA), Michael Zohner (TUDA), in 23rd USENIX Security Symposium, 2014

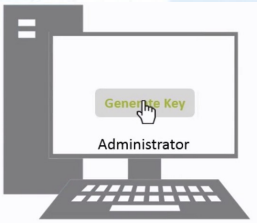
Faster private set intersection based on OT extension
Benny Pinkas (BIU), Thomas Schneider (TUDA), Michael Zohner (TUDA), in 23rd USENIX Security Symposium, 2014

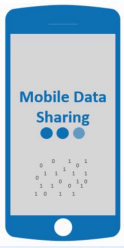
Automatic protocol selection in secure two-party computations
Florian Kerschbaum (SAP), Thomas Schneider (TUDA), Axel Schröpfer (SAP), in 12th International Conference on Applied Cryptography and Networks Security, 2014

Cut-and-Choose Yao-Based Secure Computation in the Online/Offline and Batch Settings
Yehuda Lindell (BIU), Ben Riva (BIU), in CRYPTO 2014

Results and ongoing activities

In the last months, the PRACTICE partners worked diligently on different Deliverables:
D12.1 - Application scenarios and their requirements identifies application scenarios that can greatly benefit from secure computation technology. Moreover it describes their requirements, the participating parties and attacker models. Short videos visualize the basic idea behind the application scenarios and how they operate in an abstract way. The scenario animations are published on our PRACTICE website: http://practice-project.eu/publications-deliverables?id=22





D22.1 - State-of-the-art analysis provides a capability analysis of existing secure application frameworks and secure programming languages.
D24.1 - Business and Security Requirements focuses on supply chain processes optimization.
R31.1 - Intermediate report on risk assessment and current legal status on data protection works on descriptions of the current state of law with a focus on the relevant norms and legal problems for cloud computing solutions.

Upcoming Deliverables & Milestones:

- **D11.1** "A theoretical evaluation of the existing secure computation solutions"
- **D31.1** "Risk assessment and current legal status on data protection"
- **D32.1** "Updated plan and initial report on dissemination, standardisation, exploitation and training
- **MS3** "A) Tools design and deployment methodologies. B) Risk metrics and report on legislative development

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.