PRACTICE - Privacy-Preserving Computation in the Cloud

Newsletter

February 2016 - Issue 4

Main Project Information

The PRACTICE project aims to:

- Provide **modern and novel technologies** for secure computation on **encrypted data**, allowing the data owners to fully utilize the economies of scale provided by cloud computing while **protecting their data** from cloud provider insider attacks.
- Create a **secure cloud framework** allowing for the realization of advanced but practical **cryptographic technologies** that are integrated in virtualized environments to provide **efficient and sophisticated security and privacy guarantees for users and providers** of cloud-based services while reducing trust in the cloud provider to the utmost extent.
- Develop models and techniques to quantify the return on investment for **security investment** for the deployment of secure computation algorithms. The model will allow for computing the **risk landscape associated with outsourcing data and computation**, and **simulate different scenarios** where both the investment in security and the required security level associated with the data can be changed.
- **Evaluate the legal aspects** related to the outsourcing of data and of computation to the cloud beyond national and European boundaries, and **establish guidelines**.

Message from the coordinator

The second project year of the PRACTICE project has already passed and was very successful. All in all, fourteen deliverables have been submitted and two milestones have been reached so far. Within a very successful 3rd PRACTICE Review Meeting the project was rated as excellent. The project has fully achieved its objectives and technical goals for the period and has even exceeded expectations. The objectives are still relevant and achievable. The potential impact of the project remains high. According to the reviewers, the approach and methodology of PRACTICE continue to be extremely relevant. In September 2015 all partners met for a technical meeting in Tallinn/Estonia where the upcoming partner contributions and dissemination activities for PRACTICE were discussed among other issues. Furthermore, the partners participated at several events and in addition to that they published numerous scientific publications in the most important conferences and journals, such as CRYPTO, CCS, IEEE S&P, etc. 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

During the second project year the PRACTICE team worked carefully on the following deliverables:

D11.2 - An evaluation of current protocols based on identified model describes a set of applications for secure multi-party computation and a performance comparison of secure multi-party computation systems.

D12.2 - Adversary, trust, communication and system models is the outcome of Task 1.2.2 and summarizes the assumptions on the adversaries, trust, communication and system models for the applications scenarios identified in D12.1.

D12.3 - Formal verification requirements documents the formal verification requirements that have been identified for the high-assurance secure computation framework.

D13.1 - A set of new protocols were published in multiple scientific papers at top-tier academic conferences in the field of computer security.

D14.1 - Architecture describes the architecture for integrating the secure computation technique implementations into DAGGER systems.

D21.2 - Unified architecture for programmable secure computations describes the general architecture for building and using programmable secure computation systems on the cloud.

D24.2 - Business modelling describes new business models for MRO segments of the aeronautic industry and for the consumer goods industry. Mathematical models and algorithms representing collaborative forecasting and planning in the aeronautic MRO process and vendor managed inventory business model in the consumer goods industry were developed.

D24.3 - Industrial settings introduces the architecture and design strategy of the prototype cloud SCM system. Further an assessment framework to evaluate the pilot cases was prepared.

D31.2 - Risk-aware deployment and intermediate report on status of legislative developments in data protection reports an overview of the current legal framework regulating storage and processing the data on the cloud and develops a methodology to analyse the business risks associated with outsourcing data, supported by a web-based tool.

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

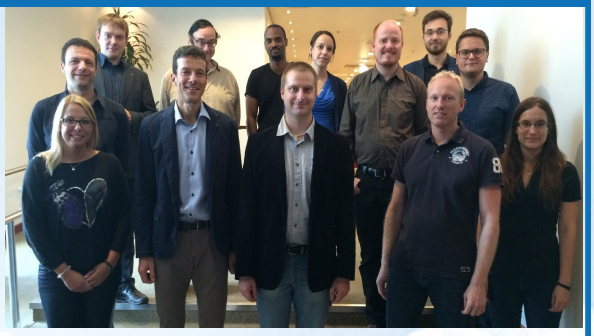
PRACTICE - Privacy-Preserving Computation in the Cloud

Newsletter

February 2016 - Issue 4

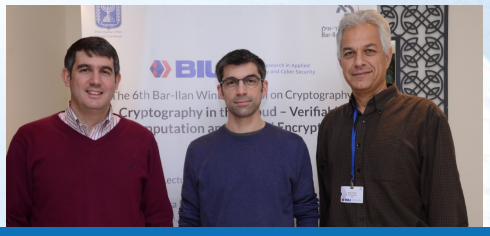
Meetings and events

From 16th-18th September 2015 PRACTICE partners met for a technical, General Assembly and Advisory Board meeting in Tallinn / Estonia hosted by partner Cybernetica. Main topics of this face-to-face meeting were the discussion of the technical status of each WP, preparation work for the second review meeting as well as management related issues. Project results were shown to the Advisory Board members Moti Yung (Google), Seny Kamara (Microsoft) and Christian Cachin (IBM Research Zürich). The feedback from the AB members was uniformly positive and we received valuable comments and advices for the last project period.



The 6th BIU Winter School on cryptography in the cloud - verifiable computation and special encryption was held from 4th-7th January 2016 in Ramat Gan / Israel. The topics were verifiable computation and different types of encryption methods that enable clients to encrypt data and carry out limited processing (e.g., search) while keeping it encrypted. The school program included approximately 21 hours of lectures and a half-day excursion.

The first EU FP7 PRACTICE Summer School on Secure and Trustworthy Computing in collaboration with the Polytechnic Institute Bucharest was a great success. The event occurred from 23rd-28th September 2015 in Bucharest / Romania. Eighteen speakers provided a wide range of topics from advanced cryptography to system security and cloud computing.



Upcoming meetings and events

- **20th-28th February 2016, Financial Cryptography, Barbados / Caribbean**
  A paper on the developed prototype in WP23 will be presented as well as computations on encrypted data.
- **13th-14th April 2016, Technical Meeting, Tel Aviv / Israel**
  The PRACTICE consortium will meet to discuss the technical status and further technical process for the last project period.
- **30th May - 2nd June 2016, Workshop on Theory and Practice of MPC, Aarhus / Denmark**
  Workshop on the theory and practice of Secure Multiparty Computation, bringing together experts in all aspects of the subject.

Outlook for the third PRACTICE project year

During the second year of PRACTICE, good progress was made and thus a solid basis for the last period could be created. In the 3rd project year, the focus lies on efficient verifiability and precise specifications of secure computation functionalities. A full set of new protocols will be provided, prototypes of the key protocols will be implemented and validated. Further an online portal providing secure computation capabilities will be finalized and the legal aspects of data protection will be evaluated and integrated. According to the reviewers recommendations the consortium will focus on delivering the identified innovations to the market by specifying usage patterns for the PRACTICE framework application, thus facilitating easier adoption of the framework by potential users. Further the exploitation plans will be strengthened, aiming to exploit as soon as possible the window of opportunity that PRACTICE has managed to create for itself in various areas. The following deliverable and milestone are considered to be created in the next two months:

- **D13.2** "Efficient verifiability and precise specification of secure computation functionalities"
- **MS6** "A) Domain specific prototypes. B) Efficient verifiability of secure computation functionalities."

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

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