University Executive

Communication and Marketing Division

Press release

From	Katrina Jordan +49 851 509 1439
Fax	+49 851 509 1433
E-mail	communication @uni-passau.de
Date	13 August 2018

Better security for sensitive data: EU project PRISMACLOUD comes to a successful conclusion

A black felt pen, good hand-eye coordination and a photocopier: while that was all you needed to black out documents before the Digital Age, it certainly doesn't pass muster these days. Scientists from the University's Chair of IT Security involved in the PRISMACLOUD research project have successfully developed innovative cryptographic methods to ensure greater security and data protection for cloud users. One such method is a form of digital redacting, or 'blacking-out', of sensitive data that have already been digitally signed.

Principal Investigator Professor Joachim Posegga (Chair of IT Security at the University of Passau) said: 'PRISMACLOUD is concerned with creating a portfolio of novel cloud services to ensure security of sensitive cloud-based data with cryptographic processes'.

Focus on securing medical data

The focus of the study at the University of Passau was on the protection of data integrity – securing people's medical data against undetected, unlawful modification. For patients, the question who has access to data on medical treatments, to which extent and how they can use it afterwards is a highly sensitive one. While health insurers need to know that a treatment took place they do not need full access to the patient's health records. In other situations, it may become important that the veracity of the data is ascertained beyond the shadow of a doubt. 'And clearly, no patient would want to risk that third-party intermediaries can in any way interfere with it', said Heinrich C. Pöhls, who co-ordinated the focus area on the development of secure cloud services within the highly international research project.

Computational errors within the cloud are instantly visible

PRISMACLOUD is therefore primarily focused on cryptographic methods to enhance security and data privacy for cloud users and the implementation of these methods in the software. Thanks to 'verifiable computing' the results of a correct statistical computation using previously-signed input values are themselves covered by a verifiable digital signature. This signature makes it possible to test the correctness of the statistical computation at any time. 'Errors in cloud computation are therefore immediately visible and the medical practitioner or the cloud user can take suitable measures to address the situation', said Pöhls.

'Blacking out' without voiding the signature

Furthermore, once again using the implementation of suitable cryptography in modern cloud services, PRISMACLOUD allows for the redaction of integrity-secured documents in such a way that specific areas of signed medical data are irretrievably deleted afterwards. Nevertheless, the digital signature retains its validity for the remaining data. This is made possible by so-called ‘redactable signatures’, whose applications, cryptographic specificities and legal relevance are being explored by Mr Pöhls at the Chair of IT Security.

Cloud security requires the collaboration of different kinds of experts

The project team in Passau simultaneously co-ordinated the interaction between experts from the three involved, highly heterogeneous disciplines: cryptography, software development and applications. Summarising the PRISMACLOUD approach to developing secure cloud services, Mr Pöhls said that to promote the swift and secure adoption of the most cutting-edge cryptographic processes in practical applications, one has to get experts from these three groups to speak the same language and work together in a co-ordinated fashion. To this end he co-ordinated the collaboration of the international experts from academia and industry, developing suitable communication strategies and tools in the process.

Interview (German) with Mr Pöhls: https://univideo.uni-passau.de/2018/07/eu-projekt-prismacloud/
English-language videos about how PRISMACLOUD makes a difference:
https://www.youtube.com/channel/UCd4rTYVtJKslZgPDNkzApjg/videos.

From 2015 to 2018 PRISMACLOUD received approximately eight million euros in funds from the European Union under the 8th research framework programme HORIZON 2020 (agreement No. 644962); furthermore, PRISMACLOUD received some 500,000 euros from SERI – Swiss State Secretariat for Education. The overall project leadership rests with the Austrian Institute of Technology.

Editors: Please address your enquiries to the Media Relations Section, phone: +49 851 509 1439.