Universitätsleitung

Abteilung Kommunikation und Marketing

Pressemitteilung

Auskunft erteilt	Katrina Jordan 0851 509-1439
Telefax	0851 509-1433
E-Mail	katrina.jordan @uni-passau.de
Datum	23. Juli 2018

Mehr Sicherheit für sensible Daten:
EU-Projekt PRISMACLOUD zieht erfolgreiche Schlussbilanz

Zweimal mit dem schwarzen Filzstift drüber und dann durch den Kopierer lassen: So stellte man früher sicher, dass ein Dokument nur noch an den gewünschten Stellen lesbar war. Wissenschaftler des Lehrstuhls für IT-Sicherheit an der Universität Passau haben im EU-Forschungsprojekt PRISMACLOUD erfolgreich neuartige kryptographische Methoden eingesetzt, um für mehr Sicherheit und Datenschutz für Nutzerinnen und Nutzer der Cloud zu sorgen – u. a. durch eine Form der digitalen Schwärzung bereits digital signierter Daten, die sensible Daten nachträglich entfernbar macht.

„PRISMACLOUD erarbeitet ein Portfolio neuartiger Cloud Services, um die nötige Sicherheit sensibler Daten in der Cloud mit kryptographischen Verfahren zu erhöhen“, so Projektleiter Prof. Dr. Joachim Posegga, Inhaber des Lehrstuhls für IT-Sicherheit an der Universität Passau.

Im Fokus: Sicherung von Gesundheitsdaten

An der Universität Passau lag der wissenschaftliche Fokus auf der Sicherung von Gesundheitsdaten gegen unerkannte unerlaubte Änderung (Schutz der Integrität). Für Patientinnen und Patienten ist alleine schon die Frage, wer Daten über medizinische Behandlungen in welchem Maße einsehen und verwenden können soll, sehr sensibel: „Der Krankenkasse möchte man die Behandlung belegen, aber nicht unbedingt deren Ergebnisse. In anderen Situationen kann es wichtig sein, dass die Echtheit der Daten zweifelsfrei beweisbar ist. Und ganz sicher wollen Patienten nicht riskieren, dass Drittanbieter, welche die Daten verwalten, in irgendeiner Weise Eingriffe vornehmen können“, erklärt Henrich C. Pöhls, der den Schwerpunktbereich zur Entwicklung sicherer Cloud-Services innerhalb des international besetzten Forschungsprojektes koordiniert hat.

Rechenfehler der Cloud werden sofort erkennbar

Der Fokus von PRISMACLOUD liegt daher auf kryptographischen Methoden zur Erhöhung der Sicherheit und der Privatsphäre für Cloud-Nutzerinnen und -Nutzer, sowie auf der Umsetzung dieser Methoden in der Software. Dabei wurde durch das sogenannte „verifiable computing“ erreicht, dass das Ergebnis einer korrekten statistischen Berechnung aus zuvor signierten Eingangswerten auch eine prüfbare digitale Signatur trägt. Diese

Signatur erlaubt, dass die Korrektheit der statistischen Berechnung stets geprüft werden kann. „Rechenfehler der Cloud fallen damit sofort auf und der Arzt oder Cloud-Kunde kann sich umgehend beschweren“, so Pöhls.

Schwärzen ja – aber die Signatur bleibt erhalten

Des Weiteren ermöglicht PRISMACLOUD, abermals über die praktische Implementierung geeigneter Kryptographie in modernen Cloud-Services, integritäts-gesicherte Dokumente nachträglich so zu „schwärzen“, das gewisse Bereiche von signierten Gesundheitsdaten hinterher unwiederbringlich gelöscht sind. Dennoch behält die digitale Signatur für die restlichen Daten ihre Gültigkeit. Dies wird durch sogenannte „editierbare Signaturen“ („redactable signatures“) bewerkstelligt, deren Einsatzmöglichkeiten, kryptographische Feinheiten und rechtliche Relevanz am Lehrstuhl für IT-Sicherheit von Henrich C. Pöhls erforscht werden.

Sichere Cloud benötigt Zusammenarbeit unterschiedlicher Expertinnen und Experten

Der Projektbeitrag der Universität koordinierte zugleich auch die Interaktion zwischen Expertinnen und Experten aus den drei beteiligten – zum Teil recht unterschiedlichen – Disziplinen: Kryptographie, Software-Entwicklung und Anwendungs-Experten. „Erst wenn diese drei Gruppen eine gemeinsame Sprache sprechen und koordiniert zusammenarbeiten, fördert dies den schnellen und sicheren Einsatz auch modernster kryptographischer Verfahren in der Praxis“, fasst Henrich C. Pöhls den Lösungsansatz von PRISMACLOUD zur Entwicklung sicherer Cloud-Services zusammen. Er koordinierte hierzu die Zusammenarbeit der internationalen Experten aus Industrie und akademischer Forschung und entwickelte hierfür geeignete Kommunikationsstrategien und -hilfsmittel.

Ein **Videointerview mit Henrich C. Pöhls** sehen Sie unter https://univideo.uni-passau.de/2018/07/eu-projekt-prismacloud/

Mehr alltagsnahe Anwendungsszenarien, in denen die Ergebnisse von PRISMACLOUD einen Unterschied machen, sehen Sie unter https://www.youtube.com/channel/UCd4rTYVtJKslZgPDNkzApjg/videos

Die EU förderte PRISMACLOUD von 2015-2018 mit rund acht Millionen Euro aus dem 8. Forschungsrahmenprogramm HORIZON 2020 (Vereinbarung Nr. 644962), zudem erhielt PRISMACLOUD rund 500.000 Euro Fördermittel von SERI-Swiss State Secretariat for Education. Die Gesamtprojektleitung hat das Austrian Institute of Technology inne.

Bildhinweis: Die Forscher der Universität Passau legen in PRISMACLOUD den Fokus auf kryptographische Methoden zur Erhöhung der Sicherheit und der Privatsphäre für Cloud-Nutzerinnen und –Nutzer. (Symbolbild: Colourbox)

Rückfragen zu dieser Pressemitteilung richten Sie bitte an das Referat Medienarbeit der Universität Passau, Tel. 0851/509-1439.