Durchsetzung von End-User-Sicherheit in Smart Services mittels Kryptographie

Dipl.-Ing. Dr. Thomas Länger
Département des systèmes d'information (ISI)
Université de Lausanne thomas.laenger@unil.ch

Dipl.-Inform. M.Sc. Info.-Security Henrich C. Pöhls
Institut für IT-Sicherheit und Sicherheitsrecht (ISL)
Universität Passau hp@sec.uni-passau.de

Das „Internet der Dinge“ und seine Nutzung in allen Arten von „Smart Services“ lässt sich als weiteres Symptom der fortschreitenden Durchdringung unserer Umwelt mit Informations- und Kommunikationstechnologien begreifen. Einerseits sollen Smart Services, so meinen die Service-Anbieter, ihren Nutzerinnen und Nutzern Erleichterungen und Vorteile bieten, und zur gleichen Zeit soll die Verbreitung dieser Technologie für Wachstum und die dringend benötigten Jobs in verschiedenen Wirtschaftszweigen sorgen. Andererseits gehören Smart Services zu den neuersten alarmierenden Trends, noch viel mehr unserer persönlichsten und privatesten Daten in die schier grundlosen Speicher verschwinden zu lassen, die sich hinter opaken „Computing and Storage Clouds“ jeglicher Kontrolle durch die eigentlichen Eigentümer der Daten entziehen. Diese Daten werden dann mit Big-Data-Technologien weiter akkumuliert, verarbeitet, miteinander in Beziehung gesetzt und bewertet—um schließlich von Datenhändlern verkauft und von Geheimdiensten abgegriffen zu werden.

Smart Services dringen definitionsgemäß in Bereiche ein, die vorher als grundsätzlich privat galten, und verursachen dadurch eine potentielle massive Bedrohung der Privatsphäre von Individuen. Aber nicht nur das: Durch ihre ausdrückliche Integration von Elementen der physischen Welt können Smart Services auch unsere physikalische Integrität kompromittieren. Die mit diesen Bedrohungen verbundenen Risiken umfassen technische Risiken, Risiken, die Fähigkeit zur Kontrolle und Beherrschung (engl. „governance“) betreffend und besonders eine Anzahl von ernsten Datenschutz- und Privatsphäre-Risiken. Diesen Risiken wird heutzutage überwiegend mit organisatorischen Maßnahmen begegnet, wie zum Beispiel mit „best practices“ und „service level agreements“—aber diese Instrumente sind oft unzureichend, weil ihre Wirksamkeit vom „guten Willen“ des Datenverarbeiters abhängt, und weder die Einhaltung der Abkommen effektiv kontrolliert werden kann, noch die Verletzungen von Vereinbarungen ohne Schwierigkeit nachgewiesen werden kann.

Um diese missliche Lage zu entschärfen, und um den End-Benutzern und Benutzerinnen wieder Kontrolle über ihre Daten zu ermöglichen, schlägt das Horizon-2020-Projekt „PRISMACLOUD“ (“Privacy and Security Maintaining Services in the Cloud”; Feb. 2015-Aug. 2018) die Anwendung von neuartigen kryptographischen Technologien vor. Ziel ist es, die definierten Sicherheitsziele der End-Benutzer und Benutzerinnen in drei Bereichen mittels kryptographischer Hilfsmittel technisch sicherzustellen: (i) Datenspeicherung in der Cloud, (ii) Schutz der Privatsphäre und Reduzierung der anfallenden Meta-Daten (engl. „data minimisation“) , (iii) Speicherung und Verarbeitung von authentischen Daten. „Secret sharing“-Technologien ermöglichen die sichere Speicherung von Daten in der „public cloud“. „Anonymous credentials“ (dt. anonyme Zugangsdaten) ermöglichen die nicht-nachverfolgbare Benutzung von Smart Services, während gleichzeitig die Bekanntgabe von persönlichen Daten wirksam reduziert wird. Mittels effizienter Verfahren für die Daten-Anonymisierung wird die Zuordnung von Daten zu Individuen verunmöglicht. Spezielle „malleable signatures“ (dt. „editierbare Signaturen“) können die Authentizität von Daten bewahren, die von der Cloud nach Maßgabe der Daten-Eigentümer und –Innen verarbeitet werden. Diese Technologie ermöglicht es auch, Teile der Daten für Dritte zu „entfernen“, wobei die Authentizitäts-Eigenschaft der Daten erhalten bleibt.

Im Mittelpunkt unserer Präsentation stehen neun kürzlich neu entwickelte „cloud security patterns“, welche immer wiederkehrende Situationen in den virtuellen Welten der Clouds und Smart Services beschreiben, in denen die Sicherheit und die Privatsphäre der beteiligten Benutzerinnen und Benutzer auf dem Spiel steht. Diese „cloud security patterns“ zeigen auf, wie durch die Anwendung der erwähnten neuartigen Privatsphäre- und Sicherheitstechnologien ein effektiver Schutz von End-User-Privatsphäre und -Sicherheit gewährleistet werden kann.

Thomas Länger ist Informatiker (TU Wien) mit Schwerpunkt Informationssicherheit, Sicherheits-Zertifizierung und Standardisierung von Sicherheits-Technologien. Von 2003 bis 2012 arbeitete er als Forscher für das Austrian Institute of Techology – AIT im Bereich der Anwendung von Quantenkryptographie. In diesem Bereich schloss er 2013 seinen PhD an der Universität Lausanne ab. Seit 2015 ist er als Post-Doc-Researcher der Swiss Cybersecurity Advisory and Research Group (SCARG) der Universität Lausanne, HEC, Department of Information Systems, im Bereich „Cloud Computing Security“ tätig und erforscht die Auswirkungen der fortschreitenden Migration in Cloud-Computing-Systeme.

Henrich C. Pöhls beschäftigt sich schon seit seinem Informatikstudium (Diplom-Informatiker) an der Universität Hamburg und an der Royal Holloway University of London (M.Sc. in Information Security) mit dem Thema IT-Sicherheit. Seit 2004 forscht er im Team von Professor Posegga und seit 2008 an der Universität Passau. Sein Spezialgebiet ist die praktische und rechtssichere Anwendung von kryptographischen Methoden, insbesondere von Digitalen Signaturen, zur Erhöhung des Beweiswertes von Informationen und zur Erhöhung der Datenqualität. Des Weiteren befasst er sich ausführlich mit Privacy- und Sicherheitsaspekten des Internet-of-Things (IoT) im Forschungsprojekt RERUM (ict-rerum.eu)

Beide Autoren sind Teilnehmer des H2020 Projekts PRISMACLOUD (prismacloud.eu; 2/2015-7/2018). Der Vortrag basiert auf Resultaten des Projekts PRISMACLOUD.