MedWiss.Online

Langfristig sicherer Speicher für sensible Gesundheitsdaten

Forscher der Technischen Universität Darmstadt, die im Sonderforschungsbereich CROSSING der Deutschen Forschungsgemeinschaft zusammenarbeiten, haben gemeinsam mit japanischen und kanadischen Partnern einen technologischen Prototypen entwickelt, der eine jahrzehntelange sichere Speicherung sensibler Gesundheitsdaten gewährleisten soll. Das Ergebnis der Kooperation präsentierten sie soeben während einer Fachkonferenz in Peking, China. Das System geht in den nächsten Wochen in Japan in den Testbetrieb.

Die elektronische Patientenakte wird nicht nur in Deutschland seit längerer Zeit diskutiert. Doch immer wieder bremst die Frage nach der Datensicherheit die Entwicklung aus. Denn insbesondere Gesundheitsdaten – die mit dem Fortschritt der modernen Medizin auch immer öfter Genomdaten der Patienten enthalten – müssen ein Leben lang und teilweise sogar darüber hinaus sicher gespeichert werden können.

Eine große Herausforderung dabei sind die technologischen Entwicklungen, die in dieser langen Zeitspanne zu erwarten sind, denn diese haben einen großen Einfluss auf die Sicherheit der bestehenden Verfahren. „Alle heute genutzten Verschlüsselungsverfahren werden in den nächsten Jahren und Jahrzehnten unsicher“, erläutert TU-Professor Johannes Buchmann, Sprecher des Sonderforschungsbereichs CROSSING. „Die Rechenkapazitäten von Angreifern werden immer größer und ihre Angriffe besser. Wir können darum davon ausgehen, dass nach spätestens 20 Jahren alle verschlüsselten Daten offenliegen.“

Um das zu verhindern, starteten Buchmann und sein Team schon 2015 die Zusammenarbeit mit dem japanischen Forschungsinstitut NICT (National Institute of Information and Communications Technology) am Projekt „LINCOS – Long-Term Integrity and Confidentiality Protection System“. Seit 2017 sind auch der japanische Krankenhausbetreiber Kochi Health Science Center und das kanadische Unternehmen ISARA mit an Bord. Das entwickelte System kombiniert erstmals informationstheoretisch sicheren Vertraulichkeitsschutz mit erneuerbarem Integritätsschutz. Das bedeutet: Unabhängig von zukünftig verfügbaren Rechenkapazitäten und Algorithmen kann niemand Zugang zu den geschützten Daten bekommen oder sie verändern.

Erreicht wird die langfristige Vertraulichkeit durch eine Technologie namens „Secret Sharing“ (Geheimnisteilung). Dabei wird der Original-Datensatz so auf verschiedene Server aufgeteilt, dass einzelne Teile für sich genommen keinen Sinn ergeben. Erst wenn man genügend Teile – sogenannte Shares – übereinanderlegt, ergibt sich wieder der Original-Datensatz der Patientenakte. Sollte einer der beteiligten Server kompromittiert werden, kann der Angreifer mit seinem erbeuteten Share also nichts anfangen. Zusätzlich wird die Aufteilung regelmäßig erneuert. Die Integrität, also die Unveränderheit, der Daten wird durch quantencomputer-resistente Signaturen erreicht. Doch auch für den Fall, dass sie im Laufe der Zeit als unsicher eingestuft werden, haben die Forscher vorgesorgt: Die Signaturen werden regelmäßig ausgetauscht. Der Integritätsschutz wird dadurch lückenlos sichergestellt.

Als dritte Komponente des LINCOS-Systems schützt das kanadische Unternehmen ISARA als Industriepartner des Projekts die Daten, die zwischen dem Krankenhaus und den Server-Betreibern hin und her geschickt werden, mit quantencomputer-resistenter Verschlüsselung. In Zukunft wollen die Forscher noch eine weitere Sicherheitsstufe hinzufügen, die sie prototypisch schon mit den

japanischen Kollegen realisiert haben: Quanten-Schlüsselaustausch. Dieses Verfahren garantiert langfristig sichere Schlüssel, da hundertprozentig ausgeschlossen werden kann, dass ein Angreifer beim Schlüsselaustausch zuhört. Daran arbeiten die Wissenschaftler im Sonderforschungsbereich CROSSING sogar in einem eigenen Quanten-Labor an der TU Darmstadt.

„Der nachhaltige Schutz von elektronischen Patientenakten ist nur ein Beispiel, wo nachhaltige Sicherheit dringend benötigt wird. In unserer digitalisierten Welt produzieren wir täglich eine unvorstellbare Anzahl sensibler Daten, die über lange Zeit vertraulich und unverändert bleiben müssen, etwa bei Industrie-4.0-Anwendungen am Industriestandort Deutschland. Hier ist die Politik gefragt, den garantierten langfristigen Schutz unserer Daten sicherzustellen“, appelliert Buchmann.

www.crossing.tu-darmstadt.de

Mehr als 65 Wissenschaftlerinnen und Wissenschaftler aus Kryptographie, Quantenphysik, Systemsicherheit und Softwaretechnik arbeiten im Sonderforschungsbereich CROSSING zusammen und betreiben sowohl Grundlagen- als auch anwendungsorientierte Forschung. Ziel ist es, Sicherheitslösungen zu entwickeln, die auch in der Zukunft sichere und vertrauenswürdige IT-Systeme ermöglichen. CROSSING wird seit 2014 von der Deutschen Forschungsgemeinschaft gefördert.

Die TU Darmstadt zählt zu den führenden Technischen Universitäten in Deutschland. Sie verbindet vielfältige Wissenschaftskulturen zu einem charakteristischen Profil. Ingenieur- und Naturwissenschaften bilden den Schwerpunkt und kooperieren eng mit prägnanten Geistes- und Sozialwissenschaften. Weltweit stehen wir für herausragende Forschung in unseren hoch relevanten und fokussierten Profilbereichen: Cybersecurity, Internet und Digitalisierung, Kernphysik, Energiesysteme, Strömungsdynamik und Wärme- und Stofftransport, Neue Materialien für Produktinnovationen. Wir entwickeln unser Portfolio in Forschung und Lehre, Innovation und Transfer dynamisch, um der Gesellschaft kontinuierlich wichtige Zukunftschancen zu eröffnen. Daran arbeiten unsere 312 Professorinnen und Professoren, 4.450 wissenschaftlichen und administrativ-technischen Mitarbeiterinnen und Mitarbeiter sowie knapp 26.000 Studierenden. Mit der Goethe-Universität Frankfurt und der Johannes Gutenberg-Universität Mainz bildet die TU Darmstadt die strategische Allianz der Rhein-Main-Universitäten.