Sicherheitsforschung an der TU Wien: Authentifizierung

Das neue Jahrtausend steht gänzlich im Zeichen der Vernetzung unzähliger Bereiche des täglichen Lebens. Allein in den letzten zehn Jahren eröffneten technische Fortschritte im Bereich der mobilen Kommunikation und Miniaturisierung von Hochleistungstechnologie nie dagewesene Möglichkeiten zur Vernetzung von Privatpersonen aber auch Firmen.

Dieser Wandel wirkt sich natürlich auch auf die Forschung an der TU Wien aus. Wo früher die reine Umsetzung und technische Realisierung im Vordergrund stand, spielt heute die Sicherheit der involvierten Daten eine ebenso große Rolle. Das größte Gefahrenpotential geht dabei von mobilen Endgeräten wie Smartphones oder Tablets aus. Die extrem niedrigen Entwicklungszyklen und die enorme Geschwindigkeit, mit der neue Technologien und Endgeräte auf den Markt gebracht werden, führen nicht selten zu einem Wissensdefizit auf beiden Seiten, nämlich den Endkunden und den Anbietern von Internetdiensten. Besonders gravierend wird dieser Trend im Bereich des Cloud Computing in Verbindung mit Smartphones und Tablets sichtbar. Die meisten Benutzer haben sich bereits an den Umstand gewöhnt, dass der Zugriff auf so gut wie jede Ressource durch Benutzername und Passwort geschützt ist. Leider haben Forschungsergebnisse in diesem Bereich gezeigt, dass zwar die meisten Benutzer wissen, wie sie ihre Zugangsdaten entsprechend absichern, meistens aber aus Bequemlichkeit eine unsichere Variante vorziehen.

Selbst wenn das nicht so ist, und die Endnutzer sichere Passwörter verwenden, birgt die Unüberschaubarkeit der im Internet verstreuten Zugangsdaten enorme Risiken. Eine große Rolle spielen hier Möglichkeiten, seine Zugangsdaten im Falle eines Verlustes oder wenn sie vergessen wurden, wieder herzustellen. Zwar sind die altbekannten Sicherheitsfragen wie etwa „Wie lautet der Mädchenname ihrer Mutter“ inzwischen größtenteils verschwunden. Aus Mangel an technischen aber auch benutzerfreundlichen Alternativen, bieten die meisten Portale aber eine Möglichkeit an, Sekundäradressen oder Zweitkanäle zu nutzen, um ein Benutzerkonto zurückzusetzen. Das hat zur Folge, dass die Benutzer selbst einen Überblick haben müssen, welche Konten für welche Zugänge als Sekundäradresse dienen. Eine Information die man schnell vergisst oder erst gar nicht kennt. Das hat zur Folge, dass einem Angreifer Mittel und Wege offenstehen, einen Benutzer zu infiltrieren ohne eine einzige Zugangskennung zu besitzen. Auf der anderen Seite sind Betriebe mit Webportalen gefordert, die Daten ihrer Kunden nur dann herauszugeben, wenn auch tatsächlich der jeweilige Kunde die Anfrage stellt. Gerade diese persönliche Authentifizierung gestaltet sich für Support Hotlines oft als schwierig. Die einzig sichere Variante wäre eine Kontrolle von Retina oder anderen biometrischen Daten, eine Möglichkeit, die zwar längt technisch durchführbar, aber noch lange nicht praktikabel ist.

Aus diesem Grund wird an der TU Wien vermehrt Forschung im Bereich der sicheren Identifizierung von Personen und Möglichkeiten zum „Single-Sign-On“, also der

einmaligen Anmeldung auf verschiedenen Portalen betrieben. Dabei sind nicht nur rein technische Komponenten, wie etwa Fingerabdruckscanner, Smartphone-Sensoren oder Chipkarten zu berücksichtigen. Dieser Bereich wird auch sehr stark von sozialen und psychologischen Aspekten beeinflusst. Das ausgeklügeltste Authentifizierungssystem wird zum Scheitern verurteilt sein, wenn es zu kompliziert ist, von den Benutzern eingesetzt zu werden.

Deshalb sind vor allem die Unternehmen selbst gefordert, ihre Kundenanbindung, sei es in Form eines Webportals oder per Handy-App, entsprechend abzusichern und dafür Sorge zu tragen, dass Benutzerdaten möglichst sicher und im eigenen System bleiben.

Kontakt:
Projektass. Dipl.-Ing. Mag.rer.soc.oec.
Dr.techn. Christian Platzer
E183 - Institut für Rechnergestützte Automation
Technische Universität Wien
christian.platzer@tuwien.ac.at