Arbeitswelt Der Mensch als schwächstes Glied der Wertschöpfungskette

Knacknüsse sind zum Knacken da

Die Forschung präsentiert zunehmend ausgeklügelte mobile Geräte wie beispielsweise Smartphones oder Garagenöffner, die den Anwendernutzen über das «Normale» hinaus zu steigern vermögen. So hat ein Team vom Lehrstuhl für Kryptografie der Universität Bochum neue Verfahren für Authentifizierungen und Verschlüsselungen entwickelt, die auf besonders schwierigen mathematischen Problemen basieren. Wie verlautet, sind die auch auf mobilen Endgeräten implementierbaren Verfahren praktisch nicht zu knacken und deshalb besonders sicher. Ihr Geheimnis: Sie basieren auf dem mathematischen Gitterproblem.

Uraltes Mathematikproblem

Was aber muss sich ein Laie darunter vorstellen? «Wenn es jemand schaffen würde, die Verfahren zu brechen, könnte er auch ein mathematisches Problem lösen, an dem die schlauesten Köpfe seit 100 oder 200 Jahren arbeiten», meint Eike Kiltz, der an den Verschlüsselungen tüftelt. Um sich das Gitterproblem zu vergegenwärtigen, muss man sich ein Gitter mit einem Nullpunkt an einer bestimmten Stelle vorstellen. Nun gilt es, jenen Punkt herauszufinden, an dem sich zwei Gitterlinien kreuzen und der am nächsten zum Nullpunkt liegt. Bei einem Gitter mit rund 500 Dimensionen eine kaum lösbare Aufgabe. Momentan sind die Forscher am Ausprobieren verschiedener Parameter, mit deren Einsatz das Gitterproblem wahlweise etwas leichter oder schwerer gestaltet werden kann. Darauf basierend wird sodann ein kryptografischer Algorithmus erarbeitet, der die Fähigkeit zur Implementierung auch auf kleinen Geräten besitzt.

Zum System gehört ein sogenanntes Authentifizierungsprotokoll. Damit kann ein Objekt seine Identität beweisen, beispielsweise der elektronische Garagenöffner beim zugehörigen Tor. Das Protokoll funktioniert so, dass sich der Öffner beim Garagentor durch die Kenntnis eines internen Geheimnisses ausweist, beispielsweise den erwähnten Kreuzungspunkt nahe dem Gitter-Nullpunkt. Das Testen verschiedener Parameter wird dabei helfen, das Fine-Tuning objekt- und aufgabengerecht zu gestalten. Anhand dieses «Feinschliffs» dürfte sich wohl entscheiden, ob das Verfahren tatsächlich den Durchbruch schafft und ob es durch seine erst zu beweisende Praxistauglichkeit gelingt, die begründete Skepsis gegenüber dem gewöhnungsbedürftigen «Geheimnis-Design» zu zerstreuen.

Allerdings profitieren nicht nur Garagenöffner von überraschenden Innovationsschüben; auch Lageristen – neben vielen andern – können auf Fortschritte hoffen, indem in Zukunft taktile Griffe ihre bisweilen harte Arbeit erleichtern. So haben Forscher am Fraunhofer-Institut für Fabrikbetrieb und Automatisierung (IFF) zahlreiche experimentalpsychologische Tests mit taktiler Interaktion durchgeführt und basierend darauf entsprechende Griffe für Kommissionierungswagen in Lagern entwickelt, die Kollisionen vermeiden und eine optimierte Steuerung ermöglichen. Die Spezialgriffe erkennen via Drucksensoren, in welche Richtung der Nutzer den Wagen schiebt oder zieht; bei drohender Kollisionsgefahr stoppt das Gerät umgehend.

So lenkt der Anwender das Gefährt lediglich durch den Druck seiner Hände. War dies früher sehr kraftraubend, verfügt der Griff nun über eine Art Servolenkung. Dabei vergleicht die Software den Druck der linken mit demjenigen der rechten Hand und erkennt so die gewählte Fahrtrichtung. Die entsprechenden Anweisungen des Mitarbeiters an den Kommissionierungswagen werden dabei an einen Motor weitergeleitet, wobei dieser die Befehle innert Millisekunden umsetzt.

Da der Mensch langsamer reagiert und durch das ungewohnte Tempo verunsichert werden könnte, baut man nun künstliche Verzögerungen ein, um die Reaktionszeit auf das menschliche Mass zurückzuschrauben. Mittels psychologischer Untersuchungen mit Testpersonen wird gegenwärtig die Dauer dieser Verzögerungen ermittelt, damit sich der Nutzer sicher und nicht überrumpelt fühlt.

Im Verlaufe der Testphase werden alle Anweisungen und Erfahrungen der Mitarbeitenden in eine Cloud übergeführt, gesammelt und koordiniert. Biegt etwa ein Bediener mit dem Gefährt um eine unübersichtliche Kurve und droht ein Zusammenstoss mit einem andern Fahrzeug, stoppen beide Wagen automatisch – analog zur Vision der Car-to-Car-Kommunikation. Erfreulicherweise ist es gelungen, die kritische Latenzzeit auf zehn Millisekunden zu reduzieren. Mit andern Worten braucht das Signal lediglich zehn Millisekunden, um vom taktilen Griff über die Cloud zurück zur Motorsteuerung zu gelangen. Auch diese Knacknuss der zu langen Latenzzeit ist also beseitigt worden.

Passwortschutz ist relativ

Je länger, desto ausgeprägter entpuppt sich hingegen der Mensch als schwächstes Glied innerhalb der technologiebasierten Wertschöpfungskette. Psychologen der Universität Luxemburg haben im Rahmen einer breit angelegten Untersuchung mit 1208 Teilnehmenden erkannt, dass die Menschen bereits mit kleinen Gefälligkeiten dazu gebracht werden können, ihre Passwörter zu verraten, im Digitalisierungszeitalter ihr grösstes – und gleichzeitig am meisten gefährdetes – Gut. Zufällig ausgewählten Passanten wurden Fragen zu deren Umgang mit Computersicherheit gestellt, wobei man sie «beiläufig» auch nach ihrem Passwort fragte – die Interviewer trugen Taschen der Universität Luxemburg, waren den Teilnehmenden aber unbekannt.

Wenn die Probanden unmittelbar vor der Frage nach dem Passwort Schokolade als Geschenk erhielten, gab fast die Hälfte ihr Passwort preis. Das Fazit der Wissenschafter dazu ist eindeutig: «Dabei war diese simulierte Attacke keineswegs eine ausgefeilte kriminelle Strategie. Aber während die Folgen solcher Angriffe für Individuen oder Firmen schwerwiegend sein können, fehlt vielen Nutzern das Bewusstsein für derartige Gefahren», betonte einer der Mitautoren dieser ernüchternden Studie.

Werner Knecht