

PRESSEINFORMATION

Wie Biometrie gegen das Passwort gewinnt

PRESSEINFORMATION17. Juni 2014 || Seite 1 | 4

Biometrische Systeme haben gegenüber dem Passwort Vor- und Nachteile. Ein Fraunhofer-Forscher meint, dass die Nachteile eine Frage der Technologie sind.

(Darmstadt/Rostock/Graz) Vor kurzem wurde der Diebstahl von Millionen von Zugangsdaten bekannt [<http://s.fhg.de/bsiPI0704>]. Hiermit hätten sich Kriminelle leicht Zugang zu E-Mail-Konten verschaffen können. Millionen von Menschen mussten ihre Passwörter ändern. „Mit dem richtigen biometrischen Verfahren wäre das nicht notwendig gewesen“, sagt Alexander Nouak, Leiter „Identifikation und Biometrie“ am Fraunhofer IGD und Vorsitzender der „European Association for Biometrics“.

Nouaks Team arbeitet schon seit mehreren Jahren an Verfahren, die in biometrischen Systemen gespeicherte Referenzdaten schützen. Die Fraunhofer-Forscher verzichten dabei gänzlich darauf, biometrische Daten als solche zu speichern. Stattdessen generiert ihr Ansatz mit Hilfe verschiedener Techniken und dem biometrischen Merkmal einen digitalen Schlüssel, der nichts mehr mit dem Körpermerkmal gemein hat. Ist der neu erzeugte Schlüssel bei einem Vergleich, zum Beispiel bei der Anmeldung für einen Internetdienst, mit dem gespeicherten identisch, wird der Nutzer erkannt. Sollten Kriminelle jedoch diesen Schlüssel erbeuten, könnten sie damit nichts anfangen, denn zur Anmeldung bei einem Dienst bräuchten sie ja das ursprüngliche Merkmal. Mit unterschiedlichen Einstellungen lassen sich aus ein und demselben Körpermerkmal beliebig viele Schlüssel generieren. „Ein Gesicht, ein Finger oder ein Auge ergibt so eine unendliche Vielzahl an digitalen Schlüsseln“, sagt Nouak. „So lässt sich dasselbe Körpermerkmal für die Anmeldung in verschiedenen Systemen verwenden, als ob man für jeden Dienst ein eigenes Passwort hätte.“

Was ist nun aber, wenn eine hoch aufgelöste Aufnahme eines Körpermerkmals wie Fingerabdruck, Handvenenstruktur oder Irismuster Unbefugten in die Hände fällt? Vor zwei Wochen argumentierte der Facebook-Ingenieur Gregg Stefancik, dass Passwörter gegenüber der

PRESSEINFORMATION

Biometrie den Vorteil hätten, leicht ersetzbar zu sein. Die körpereigenen Merkmale seien nun einmal sehr individuell und gleichzeitig begrenzt [<http://s.fhg.de/ta610>]. Diesen Nachteil muss Biometrie durch hohe Fälschungssicherheit ausgleichen. Auch hier haben Nouak und seine Forscherkollegen Technologien zum Schutz der Daten vor Augen. „Moderne Verfahren zur Fälschungserkennung können es sehr schwer bis faktisch unbezahlbar machen, eine geeignete Attrappe zu erstellen“, erklärt Nouak. „Eine Lösung wäre, mehrere biometrische Merkmale gleichzeitig zu erfassen und so die Sicherheit zu erhöhen.“ Wenn neben dem Fingerabdruck gleichzeitig noch das Venenmuster des Fingers überprüft wird, dann reichte selbst das bei einigen Grenzkontrollen digital aufgenommene Fingerabdruckbild nicht mehr aus, um eine geeignete Attrappe zu erstellen.

PRESSEINFORMATION17. Juni 2014 || Seite 2 | 4

Häufig werde auch der Aufwand unterschätzt, dessen es bedarf, um an die originalen biometrischen Merkmale zu kommen. Die Anstrengungen zur Überwindung eines modernen biometrischen Systems stehen häufig in keinem Verhältnis zum dadurch erhaltenen Gewinn. Zudem lässt eine gewöhnliche Wohnungstür, deren Schloss über einen Fingerabdruckscanner gesteuert wird, sich mit einem Stemmeisen häufig wesentlich einfacher öffnen. „Selbst der an vielen Gegenständen unfreiwillig hinterlassene Fingerabdruck reicht für gewöhnlich nicht aus, um ein hochwertiges biometrisches System zu bedienen, geschweige denn zu überlisten“, erklärt Nouak. „Wenn ich demgegenüber bedenke, wie viele Smartphone-PINs und PC-Passwörter ich kenne, ohne es zu wollen, einfach, weil die Nutzer diese viel zu offen vor mir eingegeben haben, dann bin ich sehr froh, dass ich mein Smartphone jetzt komfortabel mit meinem Finger entsperren kann.“

Nouaks Forscher-Gruppe lädt Interessierte aus Industrie und Politik ein, sich einmal direkt über die Möglichkeiten der Biometrie zu informieren.

Kontakt: identification@igd.fraunhofer.de

PRESSEINFORMATION



PRESSEINFORMATION17. Juni 2014 || Seite 3 | 4

Bild: Biometrische Systeme haben gegenüber dem Passwort Vor- und Nachteile. Fraunhofer-Forscher Alexander Nouak, Leiter „Identifikation und Biometrie“ am Fraunhofer IGD und Vorsitzender der „European Association for Biometrics“ meint, dass die Nachteile eine Frage der Technologie sind.
(Nutzungsrechte: Fraunhofer IGD)

PRESSEINFORMATION

Institutsprofil

PRESSEINFORMATION17. Juni 2014 || Seite 4 | 4

Das Fraunhofer IGD ist die weltweit führende Einrichtung für angewandte Forschung im Visual Computing. Visual Computing ist bild- und modellbasierte Informatik und umfasst unter anderem Graphische Datenverarbeitung, Computer Vision sowie Virtuelle und Erweiterte Realität.

Vereinfacht ausgedrückt, machen die Fraunhofer-Forscher in Darmstadt, Rostock, Graz und Singapur aus Informationen Bilder und holen aus Bildern Informationen. In Zusammenarbeit mit seinen Partnern entstehen technische Lösungen und marktrelevante Produkte.

Prototypen und Komplettlösungen werden nach kundenspezifischen Anforderungen entwickelt. Das Fraunhofer IGD stellt dabei den Menschen als Benutzer in den Mittelpunkt und hilft ihm mit technischen Lösungen, das Arbeiten mit dem Computer zu erleichtern und effizienter zu gestalten.

Durch seine zahlreichen Innovationen hebt das Fraunhofer IGD die Interaktion zwischen Mensch und Maschine auf eine neue Ebene. Der Mensch kann so mithilfe des Computers und der Entwicklungen des Visual Computing ergebnisorientierter und effektiver arbeiten. Das Fraunhofer IGD beschäftigt über 200 Mitarbeiter. Der Etat beträgt über 17 Millionen Euro.