

Handvenenerkennung zur Authentifizierung

Das auf der Security 2008 mit dem „Security Innovation Award“ in Bronze ausgezeichnete System der Handvenenerkennung „Intus-Palmsecure“ von PCS Systemtechnik basiert auf der von Fujitsu entwickelten Palmsecure-Technologie. Da das Verfahren in Deutschland bisher noch wenig Anwendung findet, werden folgend Funktionsgrundlagen und Sicherheitsaspekte näher erläutert.

Die Funktionsweise

Der Palmsecure-Sensor ist eine biometrische Authentifizierungslösung mit hohem Sicherheitsniveau und erkennt mit Präzision die Strukturierung des Venenmusters innerhalb der menschlichen Handfläche. Dabei bietet die Technologie einige Vorteile gegenüber anderen Lösungen, denn sie ist zugleich einfach und schnell in der Bedienung, hygienisch (da **berührungslos**) sowie hochsicher. Daher wird ihr eine zunehmende Verbreitung prognostiziert.

Der Sensor sendet dafür einen **Nahinfrarotstrahl** in Richtung der Handfläche aus. Das in den Venen zum Herzen zurückfließende sauerstoffreduzierte Blut absorbiert diese Strahlung und lässt die Venen als schwarzes Muster erscheinen (Bild 1). Dieses Muster wird vom Sensor erfasst und verschlüsselt in eine Datenbank, auf einem Token oder auf

einer Smartcard abgelegt (Bild 2). Zur Verifizierung oder Identifizierung einer bereits registrierten Person wird das aktuell erfasste Venenmuster dann mit dem Venenmuster verglichen, das z. B. in der Datenbank für diese Person gespeichert wurde. Der Scanprozeß läuft dabei in sehr kurzer Zeit und berührungslos ab. Damit erfüllt der Sensor auch die hygienischen Voraussetzungen, die für den Einsatz im öffentlichen Umfeld meistens erforderlich sind.

Sicherheitsaspekte

Die Struktur und Position der Handflächenvenen ist bei jeder Person unterschiedlich und ändert sich zeitlebens nicht. Selbst eineiige Zwillinge weisen unterschiedliche Handflächenvenenmuster auf.

Da sich die zu erfassenden biometrischen Informationen inner-

halb des menschlichen Körpers befinden und das Venenmuster zudem äußerst komplex ist, ist eine Manipulation oder Fälschung praktisch unmöglich. Die Erkennung wird auch nicht durch Hautverunreinigungen, Haare oder Verletzungen der Hautoberfläche beeinflusst.

Die Abweisungsrate Berechtigter (False Rejection Rate/FRR) beträgt weniger als 0,01 % (bei einem möglichen Re-Scan) und die Zulassungsrate Unberechtigter (False Acceptance Rate/FAR) beträgt weniger als 0,00008 %.

Aktuelle Sicherheits-zertifizierung

Die biometrische Handvenen-Authentifizierungstechnologie von Fujitsu ist darüber hinaus seit Dezember 2008 nach den Evaluierungsrichtlinien für IT-Sicherheit des internationalen ISO15408 Sicherheitsstandards *Common Criteria* der *Evaluation Assurance Stufe 2* vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert.

Damit wurde erstmals ein handflächenvenenbasierendes Authentifizierungssystem und die weltweit dritte biometrische Authentifizierungstechnologie mit diesem internationalen Sicherheitsstandard amtlich bestätigt.

Common Criteria ist eine Sammlung etablierter Kriterien zur Bewertung und Zertifizierung der Datensicherheit von IT-Produkten

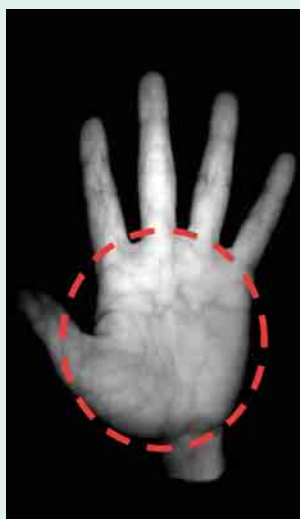
und Informationssystemen und wird derzeit in 25 Ländern anerkannt. Die Sicherheitsevaluierung von *Common Criteria* richtet sich nach Leistungsprinzipien und Erfüllung von Sicherheitsgrundlagen sowie der Zuverlässigkeit (Qualitätssicherung) des zielgerichteten Systems. Umfang und Tiefe der Prüfung werden in dem *Evaluation Assurance Level* beschrieben.

Die *Evaluation Assurance Level* Richtlinien sind je nach Strenge in sieben aufsteigenden Stufen ausgerichtet. Je höher die *Evaluation Assurance Level* Stufe ist, desto höher sind Prüfungsumfang und -tiefe des Evaluierungsgegenstandes (Target Of Evaluation, TOE). Ein hohes *Evaluation Assurance Level* bedeutet jedoch nicht unbedingt eine höhere Sicherheitseinstufung.¹⁾ Das *Evaluation Assurance Level 2* der Palmsecure Zertifizierung weist auf einen strukturellen Testvorgang hin.

Bewährte Technologie

Fujitsu bietet die Palmsecure Authentifizierungstechnologie weltweit für Kunden mit erhöhten Sicherheitsansprüchen wie Regierungsbehörden und Geldinstitutionen an. Zunehmend wurden in den vergangenen Jahren die biometrischen Authentifizierungs-

¹⁾ Siehe dazu folgende Erläuterung: www.bsi.de/cc/eal_stufe.htm



1 Die Infrarotaufnahme einer Hand zeigt das Venenmuster als schwarze Linien



2 Funktionsweise der Handvenenerkennung und Umwandlung in eine Vorlage (Template)



④ Mobiler Sensor zur Handvenenerkennung

Quelle: Siemens

③ Authentifizierungssystem Intus PS

Quelle: PCS

Kreditkarte mit Chip



Das gescannte Venenmuster des Kartenhalters ist im Chip

Übereinstimmung von PINs und Venenmuster **nein** → Abweisung



ATM mit integriertem Venensensor



Auszahlung

⑤ Einsatz der Handvenenerkennung bei Geldausgabeautomaten

Quelle: Fujitsu

technologien wie Venen- und Iriserkennung sowie Fingerscanning in verschiedensten Bereichen eingesetzt. So etwa bei PC- oder Business-Login-Anwendungen sowie bei Identitätsüberprüfungen an Geldautomaten oder in Zugangskontrollsystemen von Gebäudekomplexen.

Anwendungsbeispiele

Im **ep**-Messebericht von der Security 2008 [1] wurde bereits kurz über das System der Handvenenerkennung „Intus Palmsecure“ berichtet, welches in die Intus Zutritts- und Zeiterfassungslösungen voll integrierbar ist (Bild ③).

Bereits im Jahr 2007 kooperierte Siemens (IT Solutions and Services) mit Fujitsu zur Einführung der Technologie auf dem europäischen Markt, wobei eine Kombination der Softwarelösung ID-Center von Siemens mit dem Palmsecure-Sensor erfolgte.

Der Sensor lässt sich beispielsweise auch für mobile Authentifizierungs-Anwendungen in Geräte

ähnlich einer Computermaus integrieren (Bild ④).

Auf der Handvenenerkennung basierende Sicherheitslösungen sind in größerem Maßstab bisher hauptsächlich in Japan im Einsatz. Dort wird die Technologie z. B. bereits seit 2004 bei der Tokio Mitsubishi Bank ohne Probleme eingesetzt. Dabei haben die Kunden auf ihrer Bankkarte bzw. Kreditkarte ihr eingescanntes Handvenenmuster und die Geldautomaten verfügen über die Palmsecure-Sensoren (Bild ⑤). Die Verifizierung erfolgt nach der Match-on-Card-Methode im Chip der Karte.

In Deutschland ist die Technologie dagegen bisher kaum im Einsatz. Ein Pilotprojekt im Finanzbereich gab es u. a. bei Geldausgabeautomaten der Deutschen Bank in Berlin.

Literatur

[1] *Peterseins, H.*: Security 2008 vom 7. – 10. Oktober in Essen: Systeme und Lösungen werden immer komplexer. *Elektropraktiker*, Berlin 62 (2008) 12, S. 1052–1054.

IP in EDELSTAHL

Telecom Behnke

IP zur Türtelefonie

Einfach via Voice- / Video-over-IP mit jedem vernetzten PC-Arbeitsplatz im Gebäude telefonieren ... ohne großen Verkabelungsaufwand!

Edelstahl-Stelen und -Pylone

Individuell zugeschnittenes und edles Design, das sowohl die Gebäudearchitektur als auch das ansässige Unternehmen widerspiegelt!



Telecom Behnke GmbH • Gewerbepark „An der Autobahn“ • Robert-Jungk-Straße 3 • 66459 Kirkel
Info-Hotline: +49 (0) 68 41 / 81 77-700 www.behnke-online.de

MOBIL-STROM



Dieselstromerzeuger
Produktion/Service/Verkauf/Vermietung

Mietaggregate von MOBIL-STROM

- Bei Wartung/ Reparatur von Starkstromanlagen (z. B. Transformatoren) halten unsere MOBIL-STROM-Aggregate die Stromversorgung der Verbraucher aufrecht!
- Wir stellen Mietaggregate bis zu 1400 kVA kurzfristig zur Verfügung!

Fragen Sie an unter ☎ 034294 714 0 oder besuchen Sie uns unter www.mobil-strom.com

Effizienter als ein EVG?!

ÖKOSTART®



- „End of Life“ - Schutz
- flackerfreier Warmstart, dadurch Verlängerung der Röhren-Lebenszeit
- ersetzt einfach den Glimmlampenstarter
- 10 Jahre Garantie

M+R Multitronik GmbH
Kaninchenbergweg 78 • 23564 Lübeck
Tel. 0451-609950 • Fax 0451-604695
info@multitronik.com • www.multitronik.com



KALKULATIONSPROGRAMM

elvira V 7.0 compact 99.– €

mehr Info's und kostenlose Software unter

www.softwarekosten-sparen.de

Photovoltaik

ist unsere Sache!

Das Elektrohandwerk.