Dieter Bartmann

Internet-Payment und Online-Banking mit der BioTAN

Die Umsetzung der PSD2 wird schwierig, denn statische Passwörter und Besitzmerkmale halten aktuellen Hackerangriffen nicht stand. Fingerprint- und Gesichtserkennung mangelt es an Vertraulichkeit. Dynamische Besitzmerkmale wie SmartTAN und DeviceTAN sind für Internet-Payment wenig geeignet. Google bringt erstmals die Tippbiometrie ins Spiel. An der Universität Regensburg wurde sie so sicher gemacht wie die Fingerprint-Biometrie. Die Anwendungsvariante BioTAN ist der erfolgversprechendste PSD2-konforme dynamische zweite Authentifizierungsfaktor. Er ist immun gegen Ausspähen und garantiert die Integrität des Überweisungsauftrags. Damit vereint er die Vorteile der SmartTAN mit der Stärke einer sensorlosen Software-Biometrie.

1 Das Dilemma der Regulierer: Die Sicherheit hinkt den Anforderungen im digitalen Markt hinterher

Das Schutzbedürfnis steigt kontinuierlich.

In der digitalen Ökonomie möchte man online bezahlen. Man kann dies auf zweierlei Weise erreichen. Die erste ist digitales fälschungssicheres Geld. Dies ist ein entwicklungstechnischer Quantensprung. Damit lässt sich im Internet genauso sicher bezahlen wie mit Sorten. Deshalb kann digitales Geld auch anonym sein wie Bargeld. Gerade das wollen aber Regierungen und Notenbanken nicht. Die zweite Weise ist eine inkrementelle Weiterentwicklung. Man benutzt die riesige bestehende Infrastruktur von Zahlungsmaschinen der Kreditinstitute. Um sie an der Anwenderschnittstelle onlinegerecht zu machen, hat sich im Markt zu diesem Zweck eine Dienstleistungs-Zwischenschicht zwischen Kunde/Händler einerseits und Zahlungsabwicklung andererseits etabliert, die eine Quasi-Onlinefähigkeit der Zahlungssysteme erzeugt. Derzeit entbrennt ein harter Wettbewerb, wer die großen Player in dieser Dienstleistungs-Zwischenschicht sein werden. Das digitale Bezahlen selbst zerfällt in die beiden Schritte „bezahlen auslösen" und „bezahlen abwickeln". Online-fähig heißt: dem Händler als Zahlungsempfänger reicht es aus, wenn ihm der digitale Zahlungsauslösedienst meldet, dass die Zahlung auf den Weg gebracht wurde. Dieser Weg ist altbekannt und umfassend regulatorisch abgesichert. Aber es kommt in der Zahlungsvorgangskette ein neues Glied hinzu. Beim Auslösen einer Internet-Bezahlung in digitalen Netzen entstehen neue Risiken. Die Regulierungsbehörden sind deshalb einem Handlungsdruck ausgesetzt. Sie müssen das Finanzsystem in Hinblick auf Online-Bezahlsysteme ausweiten. Es ist auch hier ein geeignetes Maßnahmenbündel zur Betrugsabwehr vorzusehen.

Der Regulierer muss mit dem auskommen, was flächendeckend vorhanden ist

Das bringt die Regulierer in eine schwierige Situation, denn die gesamte digitale Ökonomie leidet bislang immer noch an einem ungelösten Problem:

Flächendeckend gibt es weder eine starke Authentifizierung noch digitale Pendants zur rechtsverbindlichen Unterschrift sowie zum Einschreiben mit Rückschein. So kann z. B. eine Steuerbehörde dem Bürger noch immer nicht nachweisen, dass der per E-Mail versandte Bescheid auch angekommen ist [Bohsem 2016]. Man hoffte viele Jahre lang auf die Private-Public-Key-Kryptografie als Enabling Technology für diese essentiellen Dienste, jedoch bisher vergebens – auch in Deutschland (dort soll sie sich über das Vehikel Personalausweis verbreiten, jedoch bisher ohne nennenswerten Erfolg).

Die Regulierungsbehörde muss deshalb ohne Public-Key-Infrastruktur (PKI) auskommen und das verwenden, was flächendeckend vorhanden ist: Passwort und Karte (Debitkarte oder Kreditkarte). Derzeit verbreitet sind bei der Kreditkartenzahlung das Wissensmerkmal Passwort (z. B. bei 3D-Secure mit TAN/PIN) und die Besitzmerkmale Kartennummer und Prüfnummer (CVV-Code). Letztere sind keine Wissensmerkmale, jeder Kellner kann sie ablesen.

Ihrem Wesen nach wären biometrische Merkmale am besten geeignet, denn sie besitzen laut Definition eine direkte Personalisierungskraft. Leider war bisher ihre flächendeckende Nutzung nicht möglich. Deshalb bleibt es bei Passwort und Besitzmerkmal. Dort ist die Personalisierungskraft nur indirekt gegeben (der Benutzer kennt das Passwort bzw. besitzt ein vereinbartes technisches Merkmal, deshalb muss er wohl der Richtige sein). Beide Merkmale sind so schwach geworden, dass der Regulierer in Brüssel tätig werden musste. Beim Passwort variiert die Sicherheit je nach Betrachtungsweise sehr stark. Die Wahrscheinlichkeit, dass der Angreifer das Passwort zufällig errät, liegt im millionstel Prozentbereich. Dass er es aber ausspioniert (z. B. Zettel mit Passwort unter die Tastatur geklebt), schätzen manche auf bis zu 20 %. Diese Zahl ist sehr unsicher, denn man kann diesen Vorgang nur schlecht in einer wissenschaftlichen Feldstudie beobachten, aber sie ist dennoch ein Alarmsignal. Ähnlich schlecht ist es um Kreditkartennummer und CVV bestellt. Wer die Karte auch nur kurzfristig in Händen hält, besitzt das Merkmal.

Deshalb verlangt der Regulierer in der EU-Richtlinie 2015/2366, der sog. PSD2 [PSD2 2015], einen zusätzlichen zweiten Authentifizierungsfaktor und spricht dann von einer starken Authentifizierung:

„30. ‚starke Kundenauthentifizierung' eine Authentifizierung unter Heranziehung von mindestens zwei Elementen der Kategorien Wissen (etwas, das nur der Nutzer weiß), Besitz (etwas, das nur der Nutzer besitzt) oder Inhärenz (etwas, das der Nutzer ist), die insofern voneinander unabhängig sind, als die Nichterfüllung eines Kriteriums die Zuverlässigkeit der anderen nicht in Frage stellt, und die so konzipiert ist, dass die Vertraulichkeit der Authentifizierungsdaten geschützt ist."

Bis November 2017 muss die PSD2 in der nationalen Gesetzgebung umgesetzt sein. Technisch saubere Umsetzungen sind deshalb dringend geboten.

2 Aktuelle Angreiferszenarien und Konsequenzen für PDS2-Compliance

Die Logik dieser Richtlinie ist ganz einfach. Muss sich ein Angreifer zwei Merkmale aneignen, dann bedarf es zweier Angriffe auf zwei unterschiedliche Objekte, welche ihrerseits jeweils eigens gesichert sind (Geheimnis, Wegsperren des Besitzmerkmals). Mittlerweile arbeiten aber die Angreifer mit Spähangriffen, welche diese Logik aushebeln. Passwörter und statische Besitzmerkmale sind für sie eine unverschlossene Tür. Sie bedrohen das weltweite SWIFT-Zahlungssystem auf Ebene der Notenbanken. Sie verschaffen sich permanenten Zugang zu Online-Konten und untergraben so das Vertrauen in ein sicheres Online-Banking. Damit gefährden sie ein strategisch sehr bedeutsames Geschäftsmodell für Retail-Kunden. Gerade in Zeiten negativer Zinsen kann dies existenzbedrohend für Kreditinstitute werden. Die gehackten Kunden-Accounts bei Webshops und Payment-Providern bringen das digitale Bezahlen in Misskredit. Dabei gehen sie nach folgendem Schema vor.

Angriff auf SWIFT-Nachrichten bei der Zentralbank von Bangladesh

Dort wurde auf einem Rechner der SWIFT-Alliance eine Malware als Service installiert. Einmal dort gelandet, stahlen die Angreifer mit ihrer Hilfe SWIFT-Nachrichten, kopierten die Credentials, löschten dann die Nachrichten und initiierten mit den gestohlenen Credentials betrügerische Überweisungen von Nostro-Konten in Höhe von 81 Millionen USD [Finkl/Quadir 2016; Sevchenko 2016]. Die Manipulationen wurden via https vom Angreifer-Rechner außerhalb der Zentralbank aus vorgenommen.

Angriff auf die PIN

Nach einem ähnlichen Muster erfolgen derzeit Angriffe auf Online-Banking-Konten. Der Angreifer startet einen Spähangriff. Wenn es ihm gelingt, Schadsoftware auf dem Kundenrechner zu installieren, kann er alle Daten absaugen, die der Kunde eingibt, so auch Direct-Banking-Nummer und PIN. Von diesem Zeitpunkt an späht er das Kundenkonto systematisch aus. Er sieht alle Kontobewegungen. Er findet heraus, ob der Kunde für ihn interessant ist und sich das Risiko eines Angriffes lohnt.

Angriff auf die iTAN

Bei hohem Kontostand erfolgt der Transaktionsangriff. Dazu muss sich der Angreifer die iTAN aneignen. Entweder er stiehlt aus dem Rechner die iTAN-Liste, die der Benutzer eingetippt hat, oder er geht folgendermaßen vor. Sobald der Kunde eine Online-Transaktion durchführen will und dazu die Überweisungsmaske ausgefüllt sowie die iTAN eingetippt hat, wird er unter dem Vorwand einer Fehlermeldung aus der Sitzung gedrängt. Der Angreifer besitzt nun alle Daten, die er braucht. Er wählt einen günstigen Zeitpunkt für die Überweisung und schlägt dann mit dem höchst möglichen Betrag zu. Anschließend späht er aus, ob seine Überweisung erfolgreich war.

Abwehr

Den derzeit einzigen wirksamen Schutz gegen solche Angriffe liefern Anti-Malware-Pakete, integriert in Antivirensoftware. Dies ist aber stets ein Wettlauf zwischen Hase und Igel. Man darf keinesfalls davon ausgehen, dass die Kunden-Endgeräte immer mit aktueller Schutzsoftware ausgestattet sind. Das Gegenteil wird häufiger der Fall sein, zumindest in den nächsten paar Jahren. Der einzig zuverlässige Weg wäre, dass die Bank die Hoheit über das Kunden-Endgerät besitzt. Das ist illusorisch.

Konsequenz für die PSD2-Compliance

Was für Online-Banking gilt, trifft gleichermaßen auf Internet-Payment-Applikationen zu. Solange Passwort und Besitzmerkmal statische Größen sind, werden sie vom Hacker ausgespäht. Er kann sie dann nach Belieben verwenden. Unter diesem sehr realistischen Angriffsszenario ist es vollkommen unerheblich, ob es sich um ein personalisiertes Sicherheitsmerkmal handelt oder um zwei. Mit zweien wird man nicht sicherer als mit einem alleine. Statische Merkmale erfüllen nicht hinreichend die PSD2-Forderung „…, dass die Vertraulichkeit der Authentifizierungsdaten geschützt ist." Da es sinnlos ist, in einer EU-Richtlinie zu fordern, dass das Kunden-Endgerät gegen Spähangriffe geschützt werden muss, bleibt nur ein Ausweg: Man muss das Sicherheitsmerkmal dagegen immunisieren. Dies ist theoretisch ganz simpel. Man macht das Merkmal dynamisch. Bei jedem Login, bei jeder Transaktion wird ein anderes eingegeben. Die Umsetzung ist jedoch schwierig.

3 Referenzmodell dynamische TAN im Online-Banking

Wie kann man von den Besten lernen? Was machen die Banken? Sie bieten seit langem FinTS auf der Basis der Private-Public-Key-Kryptografie an. Diese Lösung ist aber proprietär und, wie oben bereits erwähnt, wenig verbreitet. Man hoffte, dass im Zuge einer sich im breitesten Umfang durchsetzenden PKI diese Lösung sich quasi von selbst als der Standard durchsetzt. Diese Hoffnung trog. Man muss im Mengenkunden-Geschäft ohne PKI auskommen.

Die Kreditinstitute haben sich damit abgefunden, dass sie derzeit den Zugang zu Online-Konten nicht zuverlässig schützen können. Sie haben sich des-

halb darauf konzentriert, wenigstens die Transaktionen zu schützen. Dazu verwenden sie als Vehikel die TAN. Früher war die TAN eine Willenserklärung. Jetzt wird sie zu einem Sicherheitsmerkmal.

Die dynamische TAN

Die Banken haben als Schutzmechanismus eine dynamische TAN entwickelt, welche die Integrität der Überweisungsdaten sichert. Dies geschieht mit Hilfe kryptografischer Funktionen. Sie binden die TAN untrennbar an die jeweils vorliegende Transaktion. Auf diese Weise entsteht aus der ehemaligen TAN eine fälschungssichere dynamische TAN. Jeder Manipulationsversuch an den Überweisungsdaten zerstört ihre Gültigkeit, weil sie dann nicht mehr zum Überweisungstext passt.

Variante 1: die SmartTAN

Möglichkeit eins: Die dynamische TAN wird bei jedem Überweisungsvorgang in der Hochsicherheitsdomäne des Bankrechenzentrums als SmartTAN erzeugt und dem Kunden online auf einem zweiten Kanal zur Verfügung gestellt, der vor einem Hacker-Angriff sicher ist. Wichtig ist, dass nicht beide Kanäle ihren Kunden-Endpunkt in ein und demselben Endgerät haben, sondern dass ein „Luftspalt" dazwischen liegt (sog. Luftspaltsicherheit). Ansonsten würde der Hacker, da er die Hoheit über das Endgerät besitzt, sich eine zu seiner manipulierten Überweisung passende SmartTAN holen und dem Kunden auf dem Display vorspiegeln, dass diese SmartTAN zu den von ihm eingetragenen originalen Überweisungsdaten passen würde.

Variante 2: die DeviceTAN

Möglichkeit zwei: Die Kryptofunktion zur Berechnung der dynamischen TAN läuft kundenseitig ab. Auf dem Endgerät des Kunden macht dies jedoch keinen Sinn, denn dort regiert der Hacker. Deshalb gibt man dem Kunden ein speziell dafür geeignetes Device an die Hand. Es liest die codierte Überweisung ein und errechnet daraus auf der lokalen Hardware die DeviceTAN.

Die dynamische TAN ist ein Besitzmerkmal

Als Authentifizierungsfaktor ist die dynamische TAN ein Besitzmerkmal. Als SmartTAN wurde sie dem Besitzer über einen zweiten Kanal auf einem zweiten Endgerät ausgehändigt, auf dem er sich per Passwort ausgewiesen hat. Als DeviceTAN wurde sie auf dem Device berechnet, welches sich im Besitz des Kunden befindet und welches er per Passwort aktiviert hat.

Eine Zwischenstellung nimmt die PushTAN ein. Sie landet über einen zweiten Kanal beim gleichen Endgerät, auf dem der Kunde gerade Online-Banking (oder später vielleicht auch Online-Shopping) betreibt. Der Zugang zu diesem zweiten Kanal ist per Passwort gesichert. Die Luftspaltsicherheit ist aber nicht gegeben.

Kurze Technologiebewertung für Online-Banking

Sicherheitstechnisch gesehen sind sowohl die SmartTAN als auch die DeviceTAN Besitzmerkmale. Deshalb sind sie nur dann sicher, wenn nachgewiesen wird, dass sich das Smartphone bzw. das Device in Händen des Berechtigten befinden. Dies geschieht derzeit mittels Passwort. Hat der Hacker Zugriff auf das Gerät, dann kann er nach erfolgreichem Spähangriff auf das Online-Passwort risikolos jede Überweisung tätigen. Mit etwas Bauchgrimmen könnte man mit diesen Lösungen zufrieden sein. Auf der Strecke bleiben jedoch Kundengruppen, die von Hause aus technik-avers und gerade noch fähig oder willens zum Online-Banking sind. Als beharrliche Anhänger der iTAN werden sie über niedrige Überweisungslimiten reglementiert. Als Online-Banking-Verweigerer tragen sie hohe Gebühren einer beleghaften Transaktion (die dennoch nicht kostendeckend ist). Aber auch die Benutzer der DeviceTAN verursachen Probleme. Immer wenn Hardware im Spiel ist, verursacht dies auf Seiten der Kreditinstitute hohe Handling-Kosten. Außerdem belasten Kundenfragen die Service-Hotline. Die Devices sind nicht weltweit standardisiert. Sogar im Inland hat jedes Kreditinstitut sein eigenes Device. So kommt es, dass Kunden mit Mehrfach-

bankverbindungen auch mehrere Devices in der Schublade haben. Für Mobile Banking ist das äußerst hinderlich.

Kann man die dynamische TAN für Internet-Payment verwenden?
Die DeviceTAN nicht. Folgende Überlegungen sprechen dagegen:

- Wer soll das Device bezahlen? Im Online-Banking macht das teilweise der Kunde und teilweise das Kreditinstitut, welches die Möglichkeit für eine Mischkalkulation im Rahmen der Kundenbeziehung besitzt. Aber im Internet-Payment? Vielleicht der Payment-Service-Provider? Oder der Webshop-Betreiber? Oder der Online-Händler?

- Nur die Banken besitzen die Logistikstruktur zur sicheren Aushändigung des Devices.

- Das Device ist nicht standardisiert. Wie viele Devices hat der Kunde in seiner Schublade? Eines von jeder der drei Banken, bei denen er eine Kontobeziehung pflegt, dann noch eines für PayPal, eines für …?

Die SmartTAN eigentlich auch nicht. Sie ist nur dann wirklich gegen obige Hacker-Angriffe gefeit, wenn die TAN auf einem zweiten Endgerät zur Verfügung gestellt wird. Das engt die Anwendung ein. Der Kunde müsste online zwei Geräte zur Verfügung haben. Unterwegs ist das kaum gegeben.

Gegen beide, SmartTAN und DeviceTAN, sprechen außerdem die Erfahrungen des Online-Banking mit den Kunden. Vielen ist das zu kompliziert.

Kann das Smartphone die DeviceTAN für Internet-Payment retten?
Das Smartphone stellt im Prinzip ein ideales Hardware-Device für Sicherheitsmaßnahmen dar. Es ist weltweit verbreitet und bietet genügend Rechenleistung. Im Gegensatz zu TAN-Generator etc. trägt der Kunde die Kosten bzw. das Gerät ist sowieso schon bezahlt. Das Smartphone kann biometrische Merkmale wie Fingerabdruck, Gesicht oder Stimme erfassen und zur Authentifizierung heranziehen. Aus Expertensicht ist jedoch der Sicherheitslevel für Online Banking derzeit nicht ausreichend, weil sich sowohl die Erfassungslogik des biometrischen Merkmals als auch die Auswertungslogik auf ein und demselben Gerät befinden. Hält der Angreifer das Smartphone in Händen, kann er es ungestört manipulieren.

Dieses Manko lässt sich aber beseitigen. Es ist möglich, die biometrische Authentifizierung als Software-as-a-Service zu installieren. Dann geschieht alleinig die Merkmalserfassung auf dem Endgerät. Die biometrischen Profile und die Auswertungslogik liegen an zentraler Stelle auf einem Authentifizierungsserver, zumeist im Ausland. Es ist aber derzeit kaum vorstellbar, dass sich Banken hierauf einlassen (dürfen), wenn nicht das Sicherheitsmerkmal zentral bei ihnen gespeichert ist.

Der Google-Vault könnte das Smartphone geeignet für die DeviceTAN machen
Einen innovativen Weg beschreitet Google mit dem Projekt Vault [Reily 2016]. Eine spezielle microSD-Karte mit eigenem Betriebssystem verschlüsselt Daten, Sprache und Videos in Echtzeit auf dem Chip, sodass der Computer selbst die Originalinhalte nicht erfährt. Die Karte kann man in PCs und Smartphones einstecken. Damit ist den oben beschriebenen Hackerangriffen der Boden entzogen. Diese Technologie ist zunächst für den Zielmarkt der Firmenkunden vorgesehen und sicher kostenpflichtig. Ob sie dem Privatkunden kostenlos zur Verfügung gestellt wird, ist fraglich. Deshalb kann man nicht davon ausgehen, dass sich der Google Vault als weltweiter Standard etabliert.

Ist die dynamische TAN PSD2-konform?
Nach strengem Wortlaut nicht, denn sie ist zwar ein Besitzmerkmal, aber nicht vertraulich. Trotzdem erfüllt sie dem Geiste nach die PSD2. Die Formulierung müsste geeignet nachgeschärft werden. Das ist ein sehr mühsamer Weg. Deshalb wird im Folgenden ein anderer Weg aufgezeigt, der PSD2-

kompliant ist und keine technischen Barrieren für einen weltweiten Einsatz besitzt. Die geeignete Technologie hierfür ist die Tippbiometrie. Google will auf seinem Vault das Passwort durch die Tippbiometrie ersetzen. Dies ist ein wichtiger Türöffner für diese neuartige Technologie.

4 Noch mehr Sicherheit mit der Tippbiometrie

Die ersten Anfänge gehen zurück in das 19. Jahrhundert, als sich Funker einen Spaß daraus machten, sich anhand ihrer „Morse-Handschrift" gegenseitig zu erkennen. In den beiden Weltkriegen nutzte man dies zur Beobachtung feindlicher Truppenbewegungen zu Lande und zu Wasser. Was auf einer Taste geht, müsste umso treffsicherer auf einem ganzen Keyboard funktionieren. Erstmals wird in den 1970er Jahren darüber berichtet. In kommerziellen Produkten wird die Tippbiometrie seit ca. 20 Jahren auf dem Qualitätsniveau von Plausibilitätsprüfungen der Benutzeridentität angeboten und zwar in Verbindung mit anderen Authentifizierungsmerkmalen. Für eine eigenständige starke Authentifizierung hat sie sich bisher als zu schwach erwiesen. Auch Google setzt im Projekt Vault auf die Verstärkung der Tippbiometrie mit weiteren, sensorbasierten Verfahren.

Bisher mangelte es an der für eine echte Biometrie notwendigen Trennschärfe, weil drei Kernprobleme nur unzureichend gelöst waren:

- Das Tippverhalten ist je nach Situation Schwankungen unterworfen (Stress, verletzter Finger, Tastaturwechsel etc.).
- Zuviel Eingabetext erforderlich.
- Auch das Tippverhalten lässt sich ausspähen, z. B. mit Hilfe eines intelligenten Keyloggers.

An der Universität Regensburg wurde die Tippbiometrie praxistauglich für die Authentifizierung gemacht

In dem langjährigen Cloud-Biometrics-Projekt an der Universität Regensburg ist es dem Forscherteam unter der Leitung des Verfassers gelungen, die genannten Probleme zu lösen:

- Es konnten Merkmale identifiziert werden, die gegen Schwankungen robust sind. Damit erreichte das Tippverhalten die Qualität einer Fingerprint-Biometrie.
- Die Algorithmen wurden soweit verbessert, dass der Eingabetext wesentlich kürzer geworden ist.
- Die Tippbiometrie ist mit einem integrierten Schutz gegen Keylogger und andere Arten von Merkmalsdiebstahl ausgerüstet.

Dazu waren insgesamt sieben Innovationsschritte notwendig. Sie wurden zum Teil patentiert bzw. zum Patent angemeldet. Das Resultat ist die sogenannte Cloud Biometrics Technology (CBT). Sie schneidet im wissenschaftlichen Vergleich zu den bisher publizierten Verfahren in allen Kennzahlen mit großem Abstand am besten ab [Bartmann 2016; Beer 2012; Erdenreich 2012; Schenkl 2012]. Im Jahr 2008 wurde die Lösung mit dem Deutschen IT-Sicherheitspreis wissenschaftlich ausgezeichnet [BSI 2008]. Bei der Global Security Challenge 2007 wurde sie als europäischer Finalist nominiert (World Top Five Innovation). Zusätzlich errang sie weitere nationale Innovationspreise. Der Proof-of-Concept wurde im jahrelangen praktischen Einsatz mit zigtausenden von Benutzern erbracht [Bartmann/Wimmer 2007; Viola 2010].

Abbildung 1: Dialogmaske BioTAN

Ihre BioTAN:	324	← aus der IBAN erzeugt
Bitte in Worten tippen:	*Dreihundertvierundzwanzig*	← dies ist die BioTAN

5 Die dynamische BioTAN

Online-Überweisungen ohne TAN

Auf die TAN könnte man mit der Tippbiometrie eigentlich ganz verzichten. Man bräuchte sie nicht, weder als Willenserklärung noch als Sicherheitsmerkmal. Der Benutzer füllt die Online-Überweisungsmaske aus und erzeugt dabei einen tippbiometrischen Abdruck. Anhand dessen lässt sich nachweisen, dass er persönlich die Überweisung veranlasst hat (Willenserklärung). Will der Angreifer ein vom Benutzer ausgefülltes Formular nachträglich manipulieren, dann zerstört er das originale Tippverhalten des Benutzers und die Überweisung wird nicht akzeptiert.

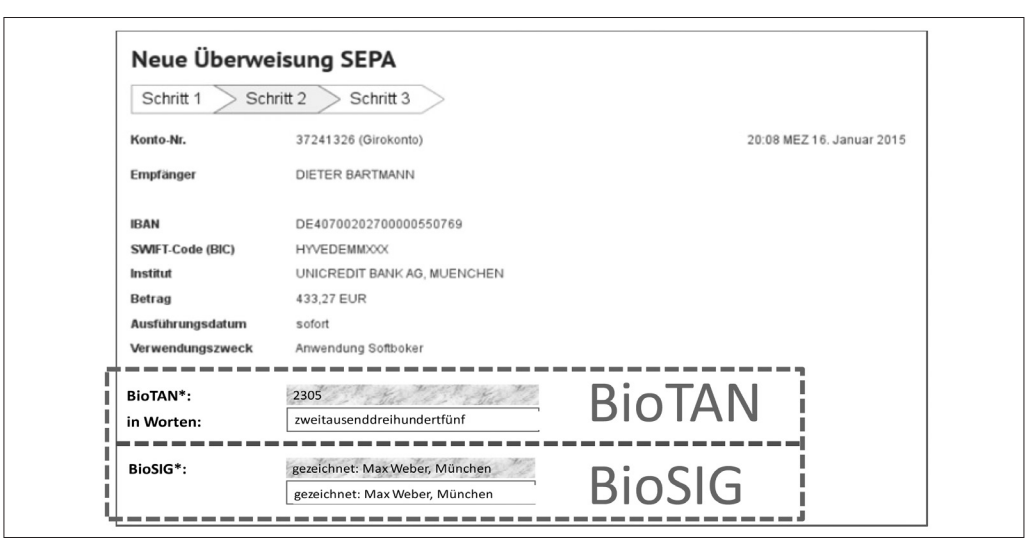
Die dynamische BioTAN

Vielleicht ist es zu radikal, ganz auf die TAN zu verzichten, wo sie doch fest eingeführt ist, die Infrastruktur einschließlich der Regularien bereits vorhanden und beim Benutzer eine „gefühlte zusätzliche Sicherheit" entstanden sind. Aber wenn schon eine TAN, dann sollte es eine biometrische sein, die sog. BioTAN, mit dem einher gehenden Zusatznutzen der Biometrie versehen. Das erreicht man, wenn der Benutzer die TAN in Worten eintippt. Dabei wird das biometrische Tippmerkmal erfasst und die TAN dadurch eine biometrische TAN. Es reichen hierfür drei Stellen. Da es nur auf das Tippverhalten ankommt, darf die TAN zum Abtippen auf dem Bildschirm erscheinen. Dies ist die einfachste Art der Anwendung. Das macht sie so einfach, siehe hierzu die Abbildung 1.

Nun gibt es noch den Angriff, bei dem der Hacker die Überweisung nur an ganz wenigen Stellen manipuliert und evtl. die Gefahr besteht, dass dies tippbiometrisch unentdeckt bleibt. Um auch dies zu verhindern, wählt man letztendlich als TAN einen „manipulationsgefährdeten" Ausschnitt aus der IBAN des Empfängers. Falls die Überweisungsmaske automatisch befüllt wird, dann sollte der Benutzer entweder eine zweite BioTAN verwenden, z. B. einige Ziffern aus dem Überweisungsbetrag, oder die erste BioTAN, die sich auf die IBAN bezieht, vierstellig wählen. Der Benutzer darf sich bei der Texteingabe ein oder zweimal vertippen. Sein Tippverhalten wird dadurch nicht beeinträchtigt.

Zur Erhöhung der Sicherheit im Online-Banking kann man bei größeren Überweisungsbeträgen den Kunden auch noch tippbiometrisch unterschreiben lassen (BioSIG), siehe Abbildung 2.

Abbildung 2: Beispielhafte Dialogmaske für eine SEPA-Überweisung mit BioTAN und BioSIG



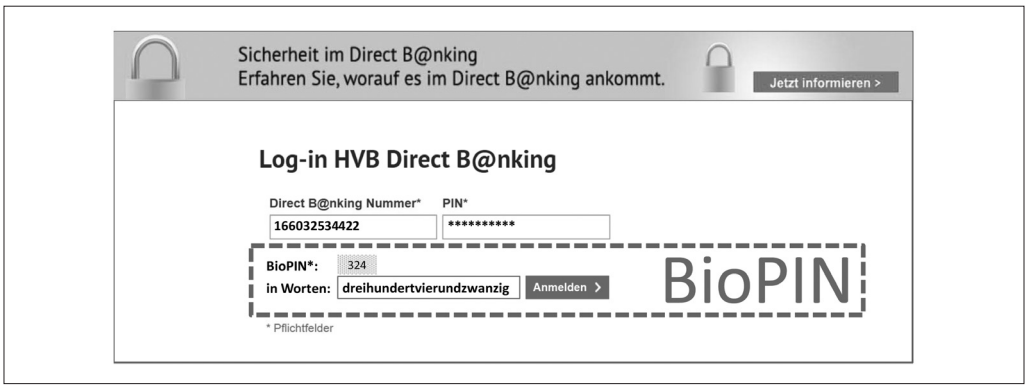


Abbildung 3: Beispielhafte Dialogmaske BioLogin mit Wissensmerkmal PIN und biometrischer BioPIN

Die biometrisch gehärtete TAN

Will die Bank auf ihrem bisherigen TAN-Verfahren beharren, gewinnt sie zusätzliche Sicherheit, wenn der Kunde die TAN als BioTAN in die Überweisungsmaske einträgt. Dann wird ihr nämlich das zusätzliche Sicherheitsmerkmal Biometrie aufgeprägt. Dies ist beim Smartphone wichtig, denn dieses multifunktionale Gerät ist eher Angriffen ausgesetzt als ein TAN-Device. Noch wichtiger ist es bei der PushTAN, weil dort der „Luftspalt" als Sicherheit fehlt. Die BioTAN wertet also SmartTAN und PushTAN sicherheitstechnisch wesentlich auf. Die SmartTAN erhält eine 3-Faktor-Sicherheit (Biometrie, Besitz des Smartphones, Passwort als Zugriffsschutz auf die SmartTAN), die PushTAN eine 2-Faktor-Sicherheit (Biometrie, passwortgeschützte PushTAN-App). Auch die alte iTAN könnte man auf diese Weise härten und sie so sicher machen, dass man sie nicht abschaffen müsste.

Internet-Payment mit der BioTAN

Die BioTAN und auch die gehärtete dynamische TAN sindein biometrisches Merkmal. Als Verhaltensbiometrie erfüllt sie die PSD2-Forderung nach Vertraulichkeit, denn das Tippmerkmal ist verborgen. Das Personentypische beim Tippen spielt sich im Millisekundenbereich ab. Deshalb ist das Tippverhalten auch nicht vom Menschen imitierbar.

6 Dynamisches BioLogin mit der BioPIN

Challenge-Response macht die Tippbiometrie immun gegen Spähangriffe

Die Tippbiometrie besitzt ideale Voraussetzungen für dynamische Sicherheitsmerkmale. Mit ihr lässt sich die Merkmalsdynamik sehr gut als Challenge-Response-Muster abbilden, denn es kommt bei ihr nicht darauf an, was man tippt, sondern wie man tippt. Das System gibt dem Benutzer jedes Mal einen anderen Text vor (Challenge), den er abzutippen hat (Response). Damit wird der Text immun gegen Spähangriffe. Der Nachteil war bisher, dass die Challenge mindestens eine ganze Zeile lang sein musste. Den Regensburger Forschern gelang es, diesen Aufwand mit einem Trick beträchtlich zu reduzieren. Dazu muss der Eingabetext bestimmte Charakteristika aufweisen (Näheres hierzu siehe [Bartmann 2016]). Dies ist z. B. der Fall, wenn man Zahlen in Worten schreibt.

Die Bank möchte auf die PIN als Wissensmerkmal nicht verzichten. Sie verwendet neben dem Wissensmerkmal PIN die biometrische BioPIN als zweiten, dynamischen Authentifizierungsfaktor. Die Challenge wird zufällig erzeugt und nicht aus Überweisungsdaten berechnet (deshalb jetzt BioPIN genannt). Im Ergebnis ist dieser BioLogin eine 2-Faktor-Authentifizierung. Die tippbiometrische Analyse umfasst auch die PIN. Diese wird damit noch zusätzlich biometrisch gehärtet. Ein Beispiel einer BioLogin-Maske ist in Abbildung 3 gezeigt.

Abbildung 4: BioLogin mit BioPIN und Wissensfrage statt Passwort

BioLogin

Benutzername:	bad23600
BioPIN 324 in Worten:	Dreihundertvierundzwanzig
Geheimnis:	Mein Favorit: ******
Geheimnis vergessen?	Statt dessen SMS-PIN

Man kann es dem Benutzer einfacher machen und statt der PIN ein Geheimnis wählen, das er nicht so leicht vergisst, z. B. den Namen seines Favoriten (Lieblingslehrer, Hund etc.), siehe Abbildung 4.

Erstmalig 3-Faktor-Login ohne zusätzliche Hardware

Das Höchstmaß an Sicherheit erhält man mit der Hinzunahme eines dritten Faktors. Dazu verwendet das System einen Transformationsschlüssel, in der Fachsprache einen Salt. Mit ihm werden alle Tippproben noch auf Client-Ebene transformiert. Auf dem Zentralrechner liegen weder Originaltippproben des Benutzers noch Original-Tippprofile. Bei einer ähnlichkeitserhaltenden Transformation lassen sich Samplecluster verschiedener Benutzer im hochdimensionalen Merkmalsraum so weit separieren, dass eine Falschakzeptanz mit astronomisch hoher Gewissheit unmöglich wird, falls der Angriff von einem anderen Endgerät aus erfolgt.

Diese Maßnahme macht das System sogar gegen einen langfristig angelegten Diebstahl des Tippverhaltens immun. Auch wenn die Tippprobe von einem künstlich intelligenten Tippgenerator erzeugt würde, der mit Daten aus einem langfristigen Spähangriff gefüttert wird, so bliebe doch der Transformationsschlüssel unentdeckt und damit die Tippprobe wertlos, wenn sie nicht auf dem Endgerät des Kunden eingegeben würde.

Touchscreen

Labortests haben gezeigt, dass dort die Tippbiometrie ebenfalls funktioniert, und sogar besser als auf der Tastatur. Man erhält nämlich neben der eigentlichen Tastenbetätigung noch zusätzliche Information über Fingergröße, Form der Fingerkuppen, ob Daumen oder anderer Finger, gestreckter oder angewinkelter Finger etc. Damit werden Smartphone und Tablet-PC auch für Online-Banking hinreichend sicher.

Internet-Payment mit BioLogin

Die Authentifizierung mittels BioLogin erfüllt die Forderungen der PSD2 bestens. Die dynamische BioPIN macht sie immun gegen Spähangriffe, was bei einem Besitzmerkmal als zweitem Faktor nicht

Abbildung 5: Ähnlichkeitserhaltende Transformation von Tippproben, auf dem Kunden-Endgerät durchgeführt

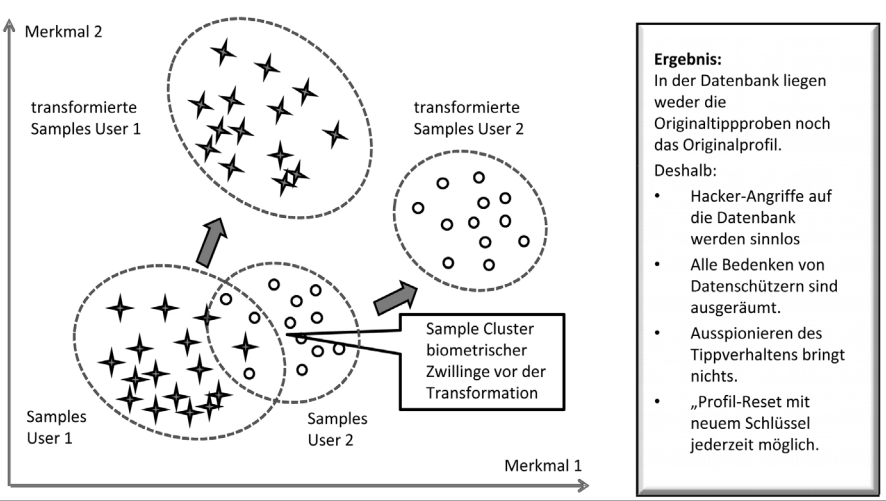


Abbildung 6: Fingerabdruck von Wolfgang Schäuble

der Fall ist. Unter Einbeziehung des Transformationsschlüssels wird sie sogar zu einer 3-Faktor-Authentifizierung mit dem Alleinstellungsmerkmal einer reinen Softwarelösung.

7 Technologiebewertung

Technologieverbreitung

Die Tippbiometrie bietet beste technische Voraussetzungen für den Masseneinsatz. Sie ist eine reine Softwarelösung, als solche Web-fähig und nicht von proprietären Standards eingeschränkt. Sie ist auf allen handelsüblichen Endgeräten PC, Smartphone, Tablet-PC ohne Zusatzausrüstung weltweit sofort einsetzbar.

Dauerhaftigkeit der Innovation

Das Merkmal Tippverhalten werden auch künftig alle Kunden, die zum Online-Banking befähigt sind, aufweisen. Auch Endgeräte mit Keyboard oder Touchscreen werden langfristig dominieren. Substitutionstechnologien für die Tippbiometrie sind nicht in Sicht. Bildhafte Biometrien wie Fingerprint, Face Recognition, Iris Scan sowie die Stimmerkennung können bei Applikationen mit hohem Schutzbedürfnis höchstens ergänzend benutzt werden, denn sie liegen offen zutage. Deshalb sind sie relativ leicht zu stehlen. Von diesem Zeitpunkt an werden sie für Authentifizierungszwecke unbrauchbar. So ist ein Fingerabdruck von Wolfgang Schäuble im Netz veröffentlicht [Chaos Computer Club 2008] (vgl. Abbildung 6) und als fertige Fingerabdruck-Attrappe käuflich erhältlich.

Hardware-Devices sind keine Substitutionsprodukte, weil man zu deren Aktivierung nicht ohne Authentifizierungsverfahren auskommt. Dass Google hier vom Passwort weggeht hin zur Tippbiometrie, bestätigt den dauerhaften Charakter der Tippbiometrie.

Sicherheitskonzept

- Das Tippverhalten besitzt den typischen Vorteil einer Biometrie: die strenge unmittelbare Bindung des Erkennungsmerkmals an die Person.

- BioPIN und BioTAN sind immun gegen Replay-Attacken und im Modus der Drei-Faktor-Authentifizierung sogar gegen langfristig angelegten Merkmalsdiebstahl.

- Die Authentifizierung geschieht nicht auf dem Endgerät, sondern in der hochsicheren Domäne des Bankrechners. Der Profile-Owner ist die Bank bzw. die (verbands-)eigene Servicegesellschaft.

Organisatorische Gesichtspunkte seitens des Kreditinstituts

- Die Bezahlsoftware ist sehr leicht um Cloud Biometrics Technology erweiterbar: Die Lösung wird als Software-as-a-Service eingebunden. Die Eingabefelder der Dialogmaske werden lediglich um Code-Schnipsel erweitert, mit denen zusätzlich zu den Key Codes auch noch die tippbiometrischen Parameter aufgezeichnet werden.

- Der Kunde enrollt sich en passant. Er gibt seine BioTAN/BioPIN wie in der Dialogmaske in Abbildung 3 gezeigt ein. Nach ein paarmal sind genügend viele Tippdaten vorhanden. Das Tippprofil wird berechnet und das System schaltet sich automatisch scharf. Bei Änderungen des Tippverhaltens lernt die Software mit, ebenso bei kleinen Tipp-Handicaps, z. B. wenn man sich in den Finger geschnitten hat.

- Kein Aufwand für das Handling von Sensoren, TAN-Generatoren etc.

Kundenaspekte

- Die Anwendung ist selbsterklärend. Das Sich-Vertippen ist in Grenzen erlaubt.

- Eine BioTAN einzutippen geht schneller als wenn man die TAN von einem externen Gerät ablesen und dann fehlerfrei eintippen oder wenn man mit einem Device hantieren muss.

- Das Tippverhalten ist harmlos. Beim Fingerprint besteht die Angst, dass Kriminelle einen gewaltsam „um den Finger bringen". Das Tippprofil verrät auch nichts über das persönliche Befinden des Benutzers wie z. B. das Gesicht, schon gar nicht, wenn es in transformierter Form abgespeichert ist.

Fallback-Lösung

Jedes Authentifizierungssystem benötigt eine Fallback-Lösung, z. B. wenn das Passwort vergessen wurde, der Finger stark verschmutzt oder verwundet ist oder ein gravierendes Tipphandicap vorliegt. Als Ersatz für die BioTAN kann der Benutzer z. B. eine SMS-TAN eingeben. Falls ein Ersatz für die Bio-PIN gewünscht wird, kann er per E-Mail eine One-Time-PIN zugesandt bekommen.

Fazit

Die BioTAN bringt nicht nur im Online-Banking Vereinfachungen. Sie ist auch für Internet-Payment ein PSD2-konformer Authentisierungsfaktor. Sie bringt ideale Voraussetzungen mit:

- Sie ist eine reine Software-Lösung auf der Basis internationaler Standards und kann sich deshalb ohne technische Barrieren ungehindert weltweit verbreiten.

- Die Tippbiometrie lässt sich sehr gut mit dem Wissensmerkmal Password oder Passphrase ohne Medienbruch verbinden. Damit hat man eine integrierte 2-Faktor-Authentifizierung als reiner BioLogin, voll PSD2-konform, mit einem vertraulichen biometrischen Merkmal.

- Mit ihr ist es möglich, als logische Applikation eine dynamische TAN darzustellen.

Die Tippbiometrie allgemein ist eine Enabling Technology. Sie schafft in diversen Anwendungsvarianten wichtige neue Mehrwertdienste in der digitalen Ökonomie. Sie wird den Wettbewerb von Kreditinstituten, Non- und Nearbanks, FinTechs und Internet-Services-Providern befeuern [von Poser/Wittmann 2015], gemäß der Maxime: Wer das Tippprofil besitzt, dem gehört der Kunde.

Literatur

Bartmann, D. (2016). Typing Behavior as a Biometrics for Strong Authentication – Selected Results of the Regensburg Cloud Biometrics Project. ibi research, submittet to BioSIG 2016.

Bartmann, D./Wimmer, M. (2007). No more problems with forgotten passwords – Web-based Password Reset with the psychometric feature typing behavior. DuD Datenschutz und Datensicherheit 31/3, 1-4.

Beer, A. (2012). Optimierung tippverhaltensbasierter, biometrischer Verfahren im Umfeld kurzer Eingabetexte. Aachen.

Bohsem, G (2016). Kontrolle unmöglich – Das Digitalgesetz überfordert die Finanzverwaltung. Süddeutsche Zeitung Nr. 139, S. 28, 18./19. Juni 2016.

BSI (Bundesamt für Sicherheit in der Informationstechnik) (2008). Verleihung des Deutschen Preises für IT-Sicherheit. https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2008/dtitsi-preis241008_htm.html.

Chaos Computer Club (2008). Das biometrische Sammelalbum. In: Die Datenschleuder 92.

Erdenreich, S. (2012). Negative Identifizierung anhand des Tippverhaltens bei Verwendung fester und freier Textbestandteile. Wiesbaden.

Finkl, J./Quadir, S. (2016). Exclusive: SWIFT to advise banks on security as Bangladesh hack details emerge. https://www.yahoo.com/tech/exclusive-swift-advise-banks-security-bangladesh-hack-details-204318565--finance.html, abgerufen am 03.06.2016.

PSD2 (2105). RICHTLINIE (EU) 2015/2366 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG.

Reily, M. (2016). Google Has a Plan to Kill Off Passwords. MIT Technology Review. https://www.technologyreview.com/s/601575/google-has-a-plan-to-kill-off-passwords/, abgerufen am 03.06.2016.

Sevchenko, S. (2016). Two-bytes-to-951m. http://baesystemsai.blogspot.de/2016/04/two-bytes-to-951m.html, abgerufen am 03.06.2016.

Schenkl, J. (2012). Tippverhaltenserkennung auf Basis benutzerindividueller, fester Eingabetexte. Shaker.

Von Poser, H. /Wittmann, G. (2015). Banken sollten nicht die Chance des Zahlungsverkehrs verschlafen. In: Banking and Information Technology (BIT) 16/1, 66-70.

Viola, G. (2010). Hochschule Landshut schützt Account per Tipp-Biometrie. http://www.egovernment-computing.de/hochschule-landshut-schuetzt-accounts-per-tipp-biometrie-a-251103/, abgerufen am 03.06.2016.

Autor

Prof. Dr. Dieter Bartmann war Inhaber des Lehrstuhls für Wirtschaftsinformatik, insbesondere Bankinformatik, an der Universität Regensburg. Er gründete das Forschungsinstitut ibi research an der Universität Regensburg GmbH (gemeinsam mit Prof. Dr. Penzel). Derzeit ist er Aufsichtsrat bei der ibi research an der Universität Regensburg GmbH.