Magdeburger Journal zur Sicherheitsforschung

Gegründet 2011 | ISSN: 2192-4260
Herausgegeben von Stefan Schumacher und Jan W. Meine
Meine Verlag – Wissenschafts-, Sach- und Fachbuchverlag, Magdeburg

Dieser Artikel erscheint in der Serie „Informationstechnologie und Sicherheitspolitik. Wird der dritte Weltkrieg im Internet ausgetragen?“ Herausgegeben von Jörg Sambleben und Stefan Schumacher

Sichere Benutzer-Authentifikation an sensiblen IT-Systemen

Frank Hofmann

Verschiedenste technische Geräte und Dienste benötigen zur Authentifikation eines berechtigten Benutzers Zugangsdaten. In der Regel bestehen diese Zugangsdaten aus einem Benutzernamen und einem Passwort. Dieser Artikel stellt alternative Möglichkeiten vor, wie eToken, Smartcards und mTAN.

Zitationsvorschlag: Hofmann, F. (2012). Sichere Benutzer-Authentifikation an sensiblen IT-Systemen. *Magdeburger Journal zur Sicherheitsforschung*, 2, 270–284. Zugriff am 20. November 2012, unter http://www.wissens-werk.de/index.php/mjs

Personalisierter Zugang zu Informationen

In unserem Alltag sind viele technische Lösungen, Geräte und Dienste über einen persönlichen Zugang individuell von uns nutzbar. Grundlage sind sogenannte Benutzerkonten (»Accounts«) mit den entsprechenden Zugangsdaten. Diese Zugangsdaten bestehen aus zwei Komponenten – einer Benutzerkennung (»Login«) und einem Geheimnis (»secret«) oder Schlüssel, beispielsweise in Form einer Ziffern- und Buchstabenkombination (PIN[1] oder Passwort).

Über dieses Benutzerkonto wird der Bezug zwischen dem Anbieter, dem Benutzer und dem vereinbarten Leistungs- oder Nutzungsumfang (»Services«) hergestellt. Wir vertrauen darauf, dass derjenige, der die korrekten Zugangsdaten vorweist, diese berechtigterweise besitzt und gestatten ihm daher die damit verbundenen Leistungen oder den Zugang zu einem Datenbestand.

Das betrifft nicht mehr nur ausgewählte Personen in besonderen Branchen, sondern uns alle. Jeder Mensch verfügt über eine mehr oder weniger große Menge von Benutzerkonten mit Zugangsdaten. Von Person zu Person unterscheidet sich lediglich die Anzahl und Art der verwendeten Dienste sowie die Intensität, mit der diese genutzt werden.

Beispielsweise zählen dazu Haus-, Wohnungs- und Büroschlüssel, Magnetkarten für Schließeinrichtungen, Parkkarten für die Tiefgarage, der Personalausweis mit Chip, die elektronische Gesundheitskarte, Bank- und Kreditkarte und der Studentenausweis. Letztere vereinen neben der Zugangsberechtigung für Labore häufig noch Semesterticket, Bibliotheksausweis und Geldkarte in sich. Computer-affine Menschen sind inzwischen darin trainiert, sich verschiedene Rechner- und Gerätezugänge zu merken und darüberhinaus sowohl die eigenen, als auch fremde WLAN-Router, Drucker, tragbare Telefone und Messenger im Zaum zu halten.

Bereits heute muß jeder Mensch über eine zuverlässige Strategie verfügen, wie er Zugangsdaten auswählt, speichert und zu einem späteren Zeitpunkt wieder auf diese zugreift. Das wird immer wichtiger, um den Überblick bei den verschiedenen Zugängen zu (Informations)Diensten zu behalten, bei denen man sich angemeldet hat. Für viele jüngere Menschen ist ein Leben ohne Google, Facebook, Twitter und YouTube nicht mehr denkbar. Ohne Onlinebanking verliert auch virtuelles Einkaufen seinen Reiz. Gerät dann noch die PIN für das Mobiltelefon, Smartphone oder iPad in Vergessenheit, bricht Panik aus. Dann hilft nur noch die PUK[2] und ein Gang zur Filiale des Telefonanbieters. Offline und nur innerhalb der Öffnungszeiten, sofern es diese Filiale noch gibt und man sich die Fähigkeit bewahrt hat, diese auch ohne Hilfe eines mobilen Routenplaners wiederzufinden.

Übertragung und Validierung

Die Zugangsdaten werden zunächst über einen möglichst gesicherten Kanal zwischen dem Benutzer und dem angefragten Dienst übertragen. Auf der Dienst-Seite werden die übermittelten Daten geprüft. Falls diese gül-

1 Abkürzung für Persönliche Identifikationsnummer

2 Abkürzung für Personal Unblocking Key, ein Schlüssel zum Entsperren einer SIM-Karte

tig sind, wird dem Benutzer die Verwendung des Dienstes gestattet und der Zugang freigeschaltet.

Verschlüsselungsverfahren

Bei der Authentifizierung kommen verschiedene Verfahren zum Einsatz. Es wird zwischen symmetrischer und asymmetrischer Verschlüsselung der übermittelten Daten unterschieden. Bei symmetrischen Verfahren werden Ver- und Entschlüsselung mit dem gleichen Schlüssel durchgeführt (siehe Abb. 1). Das hinterlegte Geheimnis ist auf beiden Seiten der Kommunikation identisch.

Bei asymmetrischen Verfahren sind die Schlüssel hingegen unterschiedlich, es wird zwischen einem öffentlichen (public key) und einem privaten Schlüssel (private key) unterschieden. Der private Schlüssel bleibt stets geheim, der öffentliche Schlüssel kann auf einem Key Server bereitgestellt werden (siehe Abb. 2).

Die Verschlüsselung erfolgt vom Absender mit seinem privaten Schlüssel, die Entschlüsselung vom Empfänger mit dem öffentlichen Schlüssel des Absenders. Nachrichten können von jedermann mit dem öffentlichen Schlüssel des Empfängers codiert werden, aber nur der Empfänger kann die an ihn adressierten, verschlüsselten Daten wieder mit seinem privaten Schlüssel für sich lesbar machen.

Bedingungen für Zugangslösungen

Die Qualität eines Verfahrens hängt nicht nur von der Schlüssellänge und der genutzten Codierung ab, sondern im wesentlichen auch von der Art und Weise, wie verantwortungsvoll die Beteiligten mit ihren Zugangsdaten umgehen. Die stärkste Sicherheit geht verloren, wenn alle Geheimnisse öffentlich sind.

Eine Reihe weiterer Kriterien beeinflussen die Sicherheit einer Zugangslösung. Bei der Auswahl einer passenden Variante sind diese Kriterien je nach Situation angemessen zu berücksichtigen. Für den Anwender stehen neben Einfachheit und Handhabbarkeit der Lösung die Stabilität und Zuverlässigkeit ganz oben auf der Wunschliste. Bestimmte Branchen, beispielsweise Bauwirtschaft, Bergbau und Land- und Forstwirtschaft legen zudem stärkeren Wert auf Robustheit und Wetterunabhängigkeit. Aus Sicht des Systemadministrators sollte die Lösung an veränderte Rahmenbedingungen (beispielsweise zeitlich begrenzte Gültigkeit) anpassbar sein und möglichst unkompliziert in die bereits bestehende Infrastruktur integrierbar sein. Alle Beteiligten wünschen sich eine bezahlbare und sichere Lösung.

Login und Passwort

Die heute am meisten genutzte Lösung ist eine Kombination aus Login und Passwort (siehe Abb. 3). Das Login ist ein Benutzername, eine Kombination aus Buchstaben und Ziffern (beispielsweise eine Matrikelnummer) oder eine Emailadresse. Das Passwort ist eine Zeichenfolge und besteht aus Buchstaben, Ziffern und Sonderzeichen.

Passwörter speichern

Es ist ratsam, sich das Passwort nur zu merken und es keinesfalls aufzuschreiben und gemeinsam mit dem Login an der glei-

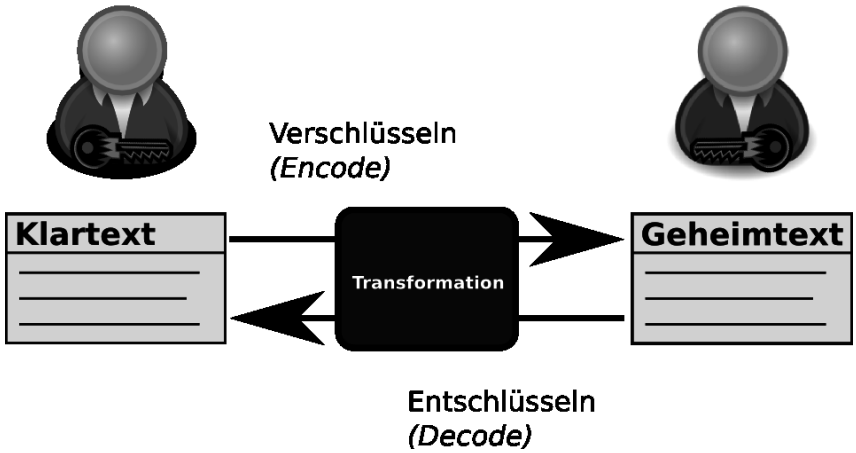


Abbildung 1: Schlüsselaustausch bei symmetrischen Verfahren

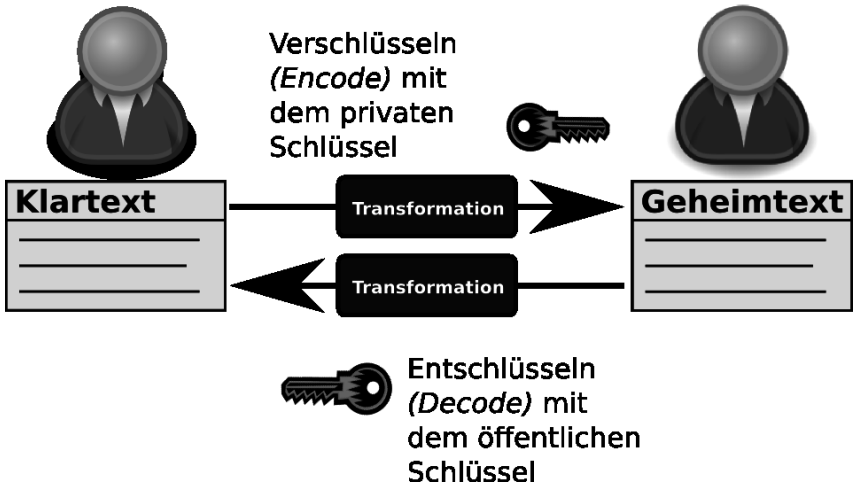


Abbildung 2: Schlüsselaustausch bei asymmetrischen Verfahren



Abbildung 3: Login an einem Debian GNU/Linux-System

chen Stelle aufzubewahren, beispielsweise in einem Textfile mit den Zugangsdaten. Doch je mehr Paare aus Benutzername und Passwort zusammenkommen, umso geringer wird die Überschaubarkeit der Zugangsdaten. Viele Anwender neigen daher dazu, ähnliche oder identische Passwörter für ihre unterschiedlichen Zugänge zu vergeben, was der Sicherheit abträglich ist.

Abhilfe kann ein sogenannter digitaler Schlüsselbund schaffen, der beispielsweise fester Bestandteil des Webbrowsers ist. Alternativen stellen eine App im Smartphone oder Mobiltelefon sowie die Softwarelösungen Gnome Keyring (*Gnome Keyring* 2011, siehe Abb. 4), KeepAss (*KeePass Password Safe* 2012) und KWallet für KDE dar.

Diese Software kann von verschiedenen Anwendungen genutzt werden, um vertrauliche Informationen zu speichern. Die Zugangsdaten können zu einem »virtuellen Schlüsselbund« hinzugefügt werden. Der gesamte Schüsselbund wird mit einem einzigen Passwort gesichert. Somit reduziert sich zwar der Erinnerungsaufwand lediglich auf die Zugangsdaten zum Schlüsselbund, bedingt aber gleichzeitig eine integere und zuverlässigere Speicherung des Schlüsselbundes. Die Zugangshürde bildet das Passwort zum Schlüsselbund. Ist diese Hürde überwunden, liegen alle Zugangsdaten des Schlüsselbunds offen.

Um die Sicherheit zu erhöhen und die Gefahr des Erratens und »Knackens« von Passwörtern zu erschweren, sollten sie ausreichend lang sein und aus mindestens sechs Zeichen bestehen. Empfehlenswert ist eine Kombination aus Buchstaben, Ziffern und Sonderzeichen ohne Verwendung der Umlaute. Letztere sind nicht auf jeder Tastatur sofort auffindbar und in jedem Zeichensatz des Computersystems verfügbar.

Generell gilt, dass Passwörter nicht erratbar sein sollen, aber trotzdem einfach zu merken sind. Grundlage können beispielsweise die Anfangsbuchstaben eines Satzes sein:

```
Pure Vernunft darf
niemals siegen Tocotronic
2006
```

2006 ist das Jahr der Veröffentlichung und liefert gemäß der oben formulierten Bedingungen die Ziffer im Passwort `PVdnsT2`.

Bewertung der vorgestellten Lösung

Das generelle Risiko bei dieser Kombination aus Login und Passwort ist vergleichsweise hoch, da Zugangsdaten schlicht und einfach in Vergessenheit geraten, gestohlen und der Schutz bei gesteigerter Rechenleistung der Computersysteme in überschaubarer Zeit gebrochen werden kann. Die Beachtung der obigen Hinweise verringert das Risiko.

Empfehlenswert ist auch, das Passwort in regelmäßigen Abständen zu ändern und nicht bei allen Benutzerkonten das gleiche Passwort zu verwenden. Häufig werden Passworte zu kurz gewählt oder sind zu leicht erratbar. Daher sind inzwischen bei vielen Dienstleistern Prüfverfahren im Einsatz, die die Stärke des gewählten Passwortes anzeigen und den Nutzer vor schwachen Zeichenfolgen warnen.

Zum bevorzugten Aufbewahrungsort für Passwörter zählen in der Praxis neben dem gelben Klebezettel am Monitor oder unter der Tastatur auch Notizbücher und Merklisten. Einträge im Adressbuch des Mobiltelefons sind ebenfalls sehr beliebt, aber nur bedingt sicher und beispielsweise über das

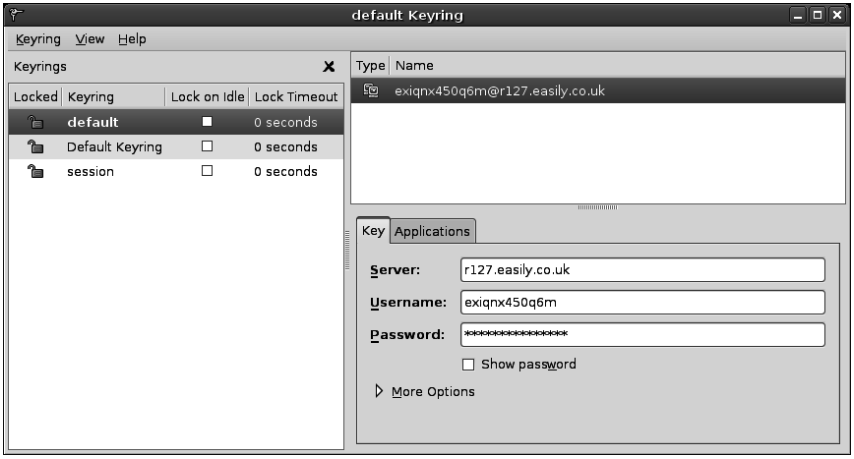


Abbildung 4: Eintragung eines Datensatzes zu einem Schlüsselbund

Bluetooth-Protokoll aus der Ferne problemlos auslesbar.

Der bereits oben beschriebene digitale Schlüsselbund ist nützlich. Er wird jedoch nur lokal auf dem System gespeichert und ist somit nur so sicher, wie das System, auf dem er abgelegt wird. Ein Zugriff aus der Ferne ist nicht ohne weiteres möglich.

Eine Art Safe für Passwörter versprechen hingegen verschiedene kommerzielle Onlinedienste, beispielsweise Clipperz oder LastPass (*Clipperz* 2011; LastPass 2011). Diese Onlinedienste sind nur so sicher, wie es der Anbieter ermöglicht und es die gesetzlichen Bedingungen am Standort des Anbieters überhaupt zulassen (*Patriot Act* 2011) und die damit verbundenen Zugriffsrechte im Rahmen der Terrorabwehr in den USA). wie möglich zu wählen. Als biometrische Verfahren stehen der Scan des Fingerabdrucks oder der Iris des menschlichen Auges zur Wahl.

Als weitere Variante steht die sogenannte Zwei-Faktor-Authentifizierung zur Verfügung. Dabei kommt zu den Zugangsdaten ein weiteres Geheimnis hinzu (der zweite Faktor). Mit diesem zusätzlichen Wissen wird der berechtigte Besitz der Zugangsdaten gegenüber einem Dritten bestätigt.

Bauformen

Um die Handhabbarkeit im Alltag zu vereinfachen und die generelle Akzeptanz der Verfahren zu erhöhen, kommen verschiedene Hardwarekomponenten zum Einsatz. Dazu zählen neben Karten mit Magnetstreifen auch Chipkarten (Speicherkarten und Smartcards), electronic Token (eToken) in verschiedenen Varianten und PGP-/GPG-USB-Speicher.

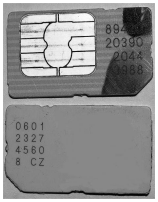


Abbildung 5: Simkarten für mobile Geräte

Chipkarte

Eine Chipkarte ist eine Kunststoffkarte mit einem integriertem Schaltkreis. Chipkarten mit Speicherbaustein heißen Speicherkarten, mit Prozessor, Speicher und einem Betriebssystem hingegen Smartcard oder Mikroprozessorkarte (*Chipkarten* 2011; Rankl und Effing 2008). Diese Karten kommunizieren mit einem Kartenlesegerät gemäß dem PC/SC-Standard (*The PC/SC Workgroup* 2011).

Smartcards kommen heute beispielsweise als Geldkarte, Personalausweis, Krankenversicherungskarte oder SIM-Karte im Mobiltelefon zum Einsatz. Der IT-Dienstleister Oracle verwendet beispielsweise Smartcards im Rahmen seines Produkts Virtual Desktop Infrastructure (VDI) (*Oracle Virtual Desktop Infrastructure* 2011). Dabei dient die Karte zur Identifikation für die Benutzersession und ermöglicht auch einen »fliegenden« Wechsel zwischen den verschiedenen SunRay-Terminals im Netzwerk (siehe Abb. 6).

eToken

eToken steht als Abkürzung für electronic Token und bezeichnet eine Smartcard mit integriertem Cryptoprozessor (siehe Abb. 7). Die Daten zur Autorisierung sind auf dem eToken gespeichert – das gilt jedoch nicht für den zweiten Faktor, der i.d.R. ein Zahlencode ist. Die Kommunikation zum Lesesystem und die Stromversorgung erfolgt über die USB-Schnittstelle, ggf. ergänzt um eine Batterie für eine Token-interne Uhr. Bekannte Hersteller dieser Lösung sind beispielsweise SafeNet/Aladdin, TeleSec sowie der Deutsche Sparkassen-Verlag (*Deutscher Sparkassen-Verlag* 2011; *SafeNet Inc.* 2011; *Telesec* 2011).

Anwendungsfelder

Neben der Autorisierung bei Webanwendungen (Mozilla Firefox und Thunderbird) kommen eToken bisher erfolgreich bei der Fernadministration (OpenSSH, rdesktop, OpenVPN), der Festplattenverschlüsselung (truecrypt, GnuPG, eCryptfs Linux File System, Linux Disk Encryption Integration) und beim Zugriff auf Datenbanken (MySQL) zum Einsatz (Barlev 2011; *eToken unter Linux* 2011).

Diese Lösung bietet mehrere Vorteile gegenüber der Methode aus Login und Passwort. Auf dem eToken wird ein Teil der Zugangsdaten abgelegt, die PIN kommt als externe Zusatzinformation dazu. Durch den Cryp-



Abbildung 6: Oracle Sun Ray 3 Plus mit Smartcard



Abbildung 7: eToken-Varianten von SafeNet/Aladdin

toprozessor ist eine starke Verschlüsselung gegeben und ein Kopieren der darauf gespeicherten Zugangsdaten nicht möglich.

Im Alltag erweist sich ein eToken als recht praktisch, da es von der physischen Größe her problemlos an den Schlüsselbund des Benutzers passt und somit portabel ist. Gegenüber Witterungseinflüssen ist es unempfindlich, auch ein Spülgang in der Waschmaschine führt nicht unbedingt zu Beeinträchtigungen in der Benutzbarkeit.

Aus Sicht des Systemadministrators helfen eToken, den Aufwand bei der Verwaltung von Freigaben und Zugriffsrechten zu reduzieren. Durch die Verwendung der USB-Schnittstelle ist für den Einsatz keine zusätzliche Hardware in Form von Lesegeräten erforderlich. Wird ein Zugang ungültig oder geht ein eToken verloren, bleibt nur die Sperrung des eTokens im eToken-Verbund durch den Systemadministrator und ggf. einer gleichzeitigen Initialisierung und Ausgabe eines neuen eToken an den Benutzer.

Ein Schwachpunkt ist die recht überschaubare Dokumentation und die Unterstützung nur für ausgewählte Software. Das erschwert in vielen Fällen die flächendeckende Einführung des an und für sich guten Konzepts.

OpenKubus

OpenKubus beschreibt sich als »einfaches Framework für sicherere Authentifizierung mittels automatisch generierter One-Time-Pads« (*OpenKubus-Projekt* 2011). Es ähnelt einem USB-Stick und dem bereits oben vorgestellten eToken und wird ebenso über die USB-Schnittstelle mit dem Hostsystem verbunden (siehe Abb. 8). OpenKubus wird von den Betriebssystemen Windows, Linux und MacOS X als zusätzliche USB-Tastatur erkannt.

Das Hardwarelayout des OpenKubus ist frei verfügbar. Es kann daher herstellerunabhängig auf Korrektheit überprüft werden. Zur Integration in eigene Programme stehen Bibliotheken für die Programmiersprachen C, Perl und PHP bereit, ebenso ein passendes Server- und PAM-Modul für UNIX-basierende-Systeme.

YubiKey

Der YubiKey wird von dem amerikanisch-schwedischen Unternehmen yubico (*Yubico* 2011) angeboten. Es ist ein sogenannter OTP-Token, der wiederum über die USB-Schnittstelle mit dem Hostsystem kommuniziert. Auf dem Hostsystem wird keine zusätzliche Software benötigt, um den YubiKey einzusetzen – dieser funktioniert betriebssystemunabhängig.

Der YubiKey generiert bei jedem Aufruf ein One Time Password (OTP), welches gegen einen YubiKey-Server validiert wird. Mit diesem Ergebnis lässt sich gegenüber einem Dritten prüfen, ob die Zugangsdaten für ein Login von einem Berechtigten stammen. Dieser weist sich beim Login mit dem YubiKey als berechtigte Person aus. Partner der YubiKey-Verifikation sind derzeit u.a. der Email-Dienst Fastmail, der Passwortverwalter LastPass, Google Apps und der Sicherheitsdienst Symantec VIP.

Der YubiKey wird von einer ganzen Reihe von OpenSource-Projekten unterstützt, beispielsweise dem Debian-Projekt, Fedora/RedHat, dem IMAP-Mailclient Round Cube und dem Content Management System Joomla. Für die genannten Distributionen stehen auch fertige Pakete bereit, so daß

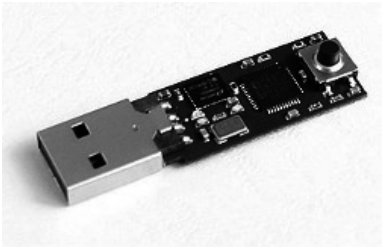


Abbildung 8: Platine des OpenKubus



Abbildung 9: OTP-Token YubiKey

eine eigene Infrastruktur zur Autorisierung eingerichtet werden kann.

GPFCryptoStick der German Privacy Foundation

Die Non-Profit-Organisation German Privacy Foundation (GPF) hat einen eigenen USB-Stick mit OpenPGP-Smartcard entwickelt – den GPFCryptoStick (siehe Abb. 10). Dieser funktioniert mit den Betriebssystemen Microsoft Windows, GNU/Linux und Mac OS X (*Informationsseite zum CryptoStick* 2011; *Wiki zum GPFCryptoStick der German Privacy Foundation* 2011).

Der GPFCryptoStick enthält 3 voneinander unabhängige RSA-Schlüssel (unterschreiben, verschlüsseln, authentifizieren) mit einer Länge von bis zu 4096 Bit. Die Schlüsselerzeugung kann auf der Karte erfolgen, alternativ können bereits existierende Schlüssel auf den GPFCryptoStick hinzugefügt werden. Die privaten Schlüssel können den GPFCryptoStick nicht verlassen.

Der GPFCryptoStick ist für eine optimale Kompatibilität mit offener Software ausgelegt, beispielsweise GnuPG, Mozilla Thunderbird/Enigmail, OpenSSH, Linux PAM, OpenVPN und Mozilla Firefox. Auch bei der Verschlüsselung von Datenträgern kann der Stick zum Einsatz kommen.

mobileTAN

Banken setzen für die Autorisierung von Transaktionen beim Onlinebanking verstärkt auf die Kombination verschiedener Übertragungswege, beispielsweise über das mobileTAN-Verfahren (auch smsTAN genannt). Login und Transaktionsbestätigung werden dabei über unterschiedliche Kanäle zwischen dem Kunden und der Bank ausgetauscht.

Zuerst erfolgt die Anmeldung im Onlinebanking mit der Kontonummer als Benutzername und einem selbstgewählten Passwort. Die Transaktion wird mit einer dritten Komponente bestätigt, der Transaktionsnummer (TAN). Diese TAN wird an die Mobilfunknummer des Benutzers (Bankkunde) als SMS versendet, dieser bestätigt mit der an ihn übermittelten TAN die Transaktion.

Viele Banken versprechen sich von dieser Vorgehensweise eine höhere Sicherheit, da die eindeutigen Identifikationsmerkmale der Transaktion (Betrag, Kontonummer und BLZ des Empfängers) über einen zusätzlichen Kommunikationskanal übertragen werden. Zudem ist die TAN zeitlich nur begrenzt gültig.

Nachteilig wirkt sich die benötigte Mobilfunkanbindung aus, wenn an dem aktuellen Standort keine Netzabdeckung vorhanden ist. Zudem sind viele Gebäude so abgeschirmt, dass kein Funkempfang möglich ist.

Wird die Transaktion von einem Smartphone ausgelöst, verringert sich die Sicherheit. Die SMS wird an das gleiche Gerät gesendet, von dem auch die Transaktion ausgelöst wird. Somit entfällt der zusätzliche Kanal.

Fazit

Aus den obigen Betrachtungen wird ersichtlich, dass für die Speicherung von Zugangsdaten ausgereifte Alternativen zum »Zettelmodell« bereitstehen. Diese Möglichkeiten einzusetzen heißt aber auch, sich mit



Abbildung 10: CryptoStick der German Privacy Foundation

den Technologien zu beschäftigen. Es ist zum Nutzen aller Beteiligter.

Über den Autor

Frank Hofmann hat Informatik an der Technischen Universität Chemnitz studiert. Derzeit arbeitet er im Büro 2.0 (http://www.buero20.org) – einem Berliner Open-Source Experten-Netzwerk – als Dienstleister mit Spezialisierung auf Druck und Satz (http://www.efho.de). Seit 2008 koordiniert er das Regionaltreffen der Linux User Groups aus der Region Berlin-Brandenburg.

Er zählt zu den Mitbegründern und Trainern der Wizards of FOSS UG (haftungsbeschränkt) & Co. Schulungen KG (http://www.wizards-of-foss.de). Die Trainings zu OpenSource-Spezialthemen richten sich an Experten, die ihr Wissen spezifisch festigen und vertiefen möchten.

Literaturverzeichnis

Barlev, A. (2011). Einsatzbereiche von eToken. Zugriff am 24. Januar 2011, unter http://alon.barlev.googlepages.com/open-source

Chipkarten. (2011). Zugriff am 29. August 2011, unter http://www.itwissen.info/definition/lexikon/Chipkarte-chip-card.html

Clipperz. (2011). Zugriff am 30. August 2011, unter http://www.clipperz.com

Deutscher Sparkassen-Verlag. (2011). Zugriff am 14. September 2011, unter http://www.sparkassenverlag.de

eToken unter Linux. (2011). Zugriff am 24. Januar 2011, unter http://www.etokenonlinux.org/et/Applications_for_eToken

Gnome Keyring. (2011). Zugriff am 29. August 2011, unter http://live.gnome.org/GnomeKeyring

Hofmann, F. (2012). Sichere Benutzer-Authentifikation an sensiblen IT-Systemen. *Magdeburger Journal zur Sicherheitsforschung*, *2*, 270–284. Zugriff am 20. November 2012, unter http://www.wissens-werk.de/index.php/mjs

Informationsseite zum CryptoStick. (2011). Zugriff am 30. August 2011, unter http://www.crypto-stick.org/

KeePass Password Safe. (2012). Zugriff am 2. Juli 2012, unter http://keepass.info/

LastPass. (2011). Zugriff am 30. August 2011, unter http://lastpass.com/

OpenKubus-Projekt. (2011). Zugriff am 30. August 2011, unter http://code.google.com/p/openkubus/

Oracle Virtual Desktop Infrastructure. (2011). Zugriff am 24. Januar 2011, unter http://www.oracle.com/us/technologies/virtualization/061153.html

Patriot Act. (2011). Zugriff am 14. September 2011, unter http://de.wikipedia.org/wiki/USA_PATRIOT_Act

Rankl, W. & Effing, W. (2008). *Handbuch der Chipkarten* (5. Auflage). München: Carl Hanser Verlag.

SafeNet Inc. (2011). Zugriff am 14. September 2011, unter http://www.safenet-inc.de

Telesec. (2011). Zugriff am 14. September 2011, unter http://www.telesec.de/

The PC/SC Workgroup. (2011). Zugriff am 23. Januar 2011, unter http://www.pcscworkgroup.com/

Wiki zum GPFCryptoStick der German Privacy Foundation. (2011). Zugriff am 30. August 2011, unter https://www.privacyfoundation.de/wiki/GPFCryptoStick

Yubico. (2011). Zugriff am 10. September 2011, unter http://yubico.com

Abbildungen und Quellen

1 Schlüsselaustausch bei symmetrischen Verfahren (Quelle: Frank Hofmann, eigenes Werk, entnommen den Unterlagen zur Vorlesung „Einführung in Kryptographie und Netzwerksicherheit“ an der Beuth-Hochschule für Technik, Berlin, Sommersemester 2012) 273

2 Schlüsselaustausch bei asymmetrischen Verfahren (Quelle: Frank Hofmann, eigenes Werk, entnommen den Unterlagen zur Vorlesung „Einführung in Kryptographie und Netzwerksicherheit“ an der Beuth-Hochschule für Technik, Berlin, Sommersemester 2012) 273

3 Login an einem Debian GNU/Linux-System (Quelle: Frank Hofmann, Debian GNU/Linux, eigene Sammlung) 274

4 Eintragung eines Datensatzes zu einem Schlüsselbund (Quelle: GNOME, karderio, entnommen der WikiMedia http://de.wikipedia.org/wiki/GNOME_Keyring, 29. August 2011) 276

5 Simkarten für mobile Geräte (Quelle: Kirk, entnommen der WikiMedia http://de.wikipedia.org/wiki/SIM_Karte, 29. August 2011) 277

6 Oracle Sun Ray 3 Plus mit Smartcard(Quelle: Oracle/Sun Ray 3 plus, entnommen von http://edwinfriesen.nl/content/?p=371, 23. Januar 2011) 278

7 eToken-Varianten von SafeNet/Aladdin Quelle: SafeNet/Aladdin, entnommen von Wikimedia http://en.wikipedia.org/wiki/File:EToken_6_models.jpg, 2. Juli 2012 278

8 Platine des OpenKubus Quelle: OpenKubus-Projekt, entnommen von http://code.google.com/p/openkubus/, 23. Januar 2011 280

9 OTP-Token YubiKey ((Quelle: Yubico Ltd., entnommen von http://yubico.com, 15. Mai 2012) 280
10 CryptoStick der German Privacy Foundation(Quelle: German Privacy Foundation, entnommen http://www.privacyfoundation.de/crypto_stick/, 23. Januar 2011) . 282