

Passwörter oder Smartcards zur Absicherung von Portalen?

Prof. Dr. Johannes Buchmann

Technische Universität Darmstadt

Online Portale sind weit verbreitet. Sie haben unzählige Anwendungen, zum Beispiel E-Banking, E-Commerce und E-Government. In [1] findet sich folgende Definition.

Ein Portal ist [...] eine Applikation, welche basierend auf Webtechnologien einen zentralen Zugriff auf personalisierte Inhalte sowie bedarfsgerecht auf Prozesse bereitstellt. Charakterisierend für Portale ist die Verknüpfung und der Datenaustausch zwischen heterogenen Anwendungen über eine Portalplattform. Eine manuelle Anmeldung an den in das Portal integrierten Anwendungen ist [...] nicht mehr notwendig, es gibt einen zentralen Zugriff über eine homogene Benutzungsoberfläche. Portale bieten die Möglichkeit, Prozesse und Zusammenarbeit innerhalb heterogener Gruppen zu unterstützen.“

Da Portale Zugang zu sicherheitskritischen Daten und Anwendungen bieten, muss dieser Zugang sorgfältig abgesichert werden. Dazu werden verschiedene Techniken eingesetzt. In diesem Beitrag werden zwei Techniken verglichen: der Zugangsschutz durch Benutzernamen und Passwort mit der Access Control mittels kryptographischer Smartcards.

Die Absicherung eines Portals mit Passwörtern funktioniert so: Verwendet wird eine kryptographische Hashfunktion. Sie bildet Passwörter auf Hashwerte fester Länge ab. Üblich sind 160-Bit oder 256-Bit Hashwerte. Die Hashfunktion ist öffentlich bekannt. Jeder kann den Hashwert eines vorgelegten Passworts berechnen. Es ist aber unmöglich, aus einem Hashwert das entsprechende Passwort zu rekonstruieren. Beim Portal sind die Hashwerte der Passwörter aller Berechtigten gespeichert. Meldet sich ein Teilnehmer beim Portal an, wird er aufgefordert, sein geheimes Passwort einzugeben. Das Portal berechnet daraus den Hashwert und vergleicht ihn mit dem Eintrag in der Datenbank. Stimmt der Hashwert, gewährt das Portal Zugang und sonst nicht.

Der Zugangsschutz mit Passwörtern somit funktioniert durch „Proof of knowledge“. Nur wer beweisen kann, dass er ein Geheimnis – das Passwort - kennt, erhält Zugang zum Portal.

Die Absicherung mit Chipkarten ist technisch anspruchsvoller. Jeder Teilnehmer hat eine Chipkarte. Sie enthält einen geheimen Signaturschlüssel. Das Portal kennt den zugehörigen öffentlichen Verifikationsschlüssel. Meldet sich ein Teilnehmer beim Portal an, wird er aufgefordert, seine Chipkarte in den Leser zu stecken. Der Leser fordert den Benutzer auf, eine PIN einzugeben. Die richtige PIN autorisiert den Kartenleser, die Chipkarte zu benutzen. Das Portal schickt der Chipkarte eine Zufallszahl. Die Chipkarte signiert diese Zahl mit ihrem geheimen Signaturschlüssel und schickt die Signatur an das Portal. Dort wird die Signatur verifiziert. Ist sie korrekt, erhält der Teilnehmer Zugang zum Portal.

Der Zugangsschutz mittels Chipkarten steht auf zwei Säulen: „Proof of knowledge“: der Anmeldende beweist, dass er die richtige PIN zur Chipkarte kennt und „Proof of possession“: den Anmeldende beweist, dass er die Chipkarte besitzt, weil nur sie die richtige Signatur berechnen kann. Der geheime Signaturschlüssel kann nicht aus der Chipkarte ausgelesen werden. Daher gibt es ihn nur einmal.

Die Absicherung mit Passwörtern hat sich in der Vergangenheit als unsicher erwiesen. Die Absicherung mit Smartcards ist deutlich sicherer. Dies wird im Folgenden erläutert.

Ein Passwort kann – beabsichtigt oder unbeabsichtigt – an einen oder mehrere Personen weitergegeben werden. Das geschieht auf vielfältige Weise. Passwörter werden von ihren Besitzern absichtlich weitergegeben, damit andere Personen Tätigkeiten im Namen des Passwortinhabers durchführen können. Diese anderen können dann das Passwort ihrerseits weitergeben. Passwörter werden aber auch unbeabsichtigt verbreitet. Sichere Passwörter sind nämlich schwer zu behalten. Sie werden an unsicheren Orten aufbewahrt. Dort können sie von Dritten leicht gefunden werden. Passwörter sind außerdem Phishing-Angriffen ausgesetzt. Passwörter werden auch in Phishing-Angriffen systematisch gesammelt. Dazu werden Benutzer in gefälschten Emails oder Webseiten, die anscheinend von autorisierter Stelle kommen, aufgefordert, ihr Passwort einzugeben. Das Passwort kann dann missbraucht werden, ohne dass der Passwortinhaber das bemerkt. Von solchen Angriffen waren schon zahlreiche Portale betroffen, zum Beispiel die Postbank (<http://www.heise.de/security/news/meldung/49049>), die Commerzbank (<http://www.heise.de/newsticker/meldung/59766>) und Ebay (<http://www.heise.de/security/artikel/54271>).

Allen diesen Vorgängen ist gemeinsam, dass einzelne Passwörter vielen anderen bekannt werden können, ohne dass die rechtmäßigen Besitzer dies bemerken, geschweige denn Kontrolle darüber haben.

Eine weitere Angriffsmöglichkeit auf Passwörter besteht darin, sie auf dem PC des Anwenders abzufangen, wenn sie benutzt werden. Dafür werden so genannte Trojaner verwendet. Das sind Computerprogramme, die sich als harmlos tarnen, in Wirklichkeit aber darauf warten, dass ein Benutzer ein Passwort eingibt und das Passwort dann an den Angreifer schicken. Solche Trojaner sind weit verbreitet. Man braucht sie nicht neu zu programmieren. Man kann sie von erfahrenen Programmierern kaufen, die auch noch Support anbieten (siehe z.B. <http://www.eweek.com/article2/0,1895,1942497,00.asp>). Von einem solchen Angriff war zum Beispiel AOL betroffen. In (<http://www.heise.de/newsticker/meldung/14958>) kann man lesen: „Der Trojaner befällt das System eines AOL-Users, um dessen User-ID und Passwort bei dem Online- Dienst zu stehlen und an den Autor des Schädlings weiterzuleiten. Diese Trojaner-Variante verbreite sich schnell, da sie die Fähigkeit habe, sich selbst per E-Mail zu verbreiten.“

Die beschriebenen Gefahren bestehen bei Smartcard-Authentisierung nicht. Nur eine Person kann die Smartcard besitzen und sie für den Zugang benutzen. Der geheime Signaturschlüssel

kann nicht aus der Smartcard ausgelesen werden. Weitergabe der Zugangsdaten an viele Personen ist ausgeschlossen. Phishing-Angriffe sind sinnlos. Trojaner versagen, solange die geheime PIN über die gesicherte Tastatur des Lesegeräts eingegeben wird. Selbst wenn der rechtmäßige Eigentümer die Karte verliert oder wenn sie gestohlen wird, wird das schnell auffallen. Jeder Benutzer hat zu jedem Zeitpunkt Kontrolle darüber, ob ein Dritter in seinem Namen Zugang erhalten kann.

Über den Angriff auf einzelne Passwörter hinaus wurden in jüngerer Zeit Möglichkeiten gefunden, Verzeichnisse der Hashwerte aller Passwörter anzugreifen. Gerät ein solches Verzeichnis in die Hände eines Angreifers, beschafft sich der Angreifer eine sog. Rainbow Tabelle, also eine Tabelle mit allen zulässigen (oder wahrscheinlichen) Passwörtern und deren Hashwerten. Moderne Computer sind so leistungsfähig, dass sie solche Tabellen berechnen können. Für jeden Hashwert aus dem gestohlenen Hashwertverzeichnis kann der Angreifer in der Rainbow Tabelle das richtige Passwort finden und benutzen. Rainbow Tabellen kann man ganz offiziell kaufen, etwa unter <http://www.rainbowtables.net/products.php>. Von solchen Rainbow Angriffen waren schon Sicherheitslösungen namhafter Hersteller betroffen, zum Beispiel Cisco Pix Passwörter, MySQL 3.x/4.x Passwörter, Oracle DB, Windows Lanman (siehe <http://www.objectif-securite.ch/research/websec06.pdf>). Gegen Chipkarten sind Rainbow Angriffe nicht möglich. Als Signaturverfahren wird typischerweise das RSA-Verfahren verwendet. Die geheimen RSA-Signaturschlüssel haben aktuell eine Länge von 1024 Bits. Brute Force Angriffe sind ausgeschlossen. Auch die besten Spezialangriffe versagen.

Chipkarten sind nicht nur sicherer. Sie ermöglichen zusätzliche Anwendungen. Einige Beispiele:

- Bei Verwendung von Chipkarten ist jede Anmeldung am Portal und jeder Zugriff auf anmeldepflichtige Anwendungen Dritten gegenüber nachweisbar. Die Verwendung der Chipkarte ist nämlich nicht abstreitbar. Passwörter bieten keine Nichtabstreitbarkeit.
- Eine Chipkarte kann Zugang zu unterschiedlichen Portalen ermöglichen. Die Portale müssen nur den öffentlichen Schlüssel des Benutzers kennen. Die Kenntnis dieses Schlüssels eröffnet keine Möglichkeit, den geheimen Schlüssel des Benutzers zu finden. Sind die Portale mit Passwörtern abgesichert, wird aus Sicherheitsgründen für jedes neue Portal ein neues Passwort gebraucht. Die Administration vieler Passwörter ist aber für den Benutzer deutlich aufwändiger als die einer einzigen Chipkarte. Außerdem kann die Ausgabe und Verwaltung der Chipkarten bei einer besonders gesicherten von den Portalen unabhängigen Institution (Trustcentern) erfolgen. Das vereinfacht die Administration noch weiter und macht die Sicherheit besser einschätzbar.
- Chipkarten können verwendet werden, um Email Kommunikation abzusichern. Sie garantieren die Vertraulichkeit, Authentizität und Nichtabstreitbarkeit der Emails und leisten damit einen Beitrag zur Unterscheidung von gewünschten Mails und Spam Mails.

Das Fazit ist: Die Verwendung von Passwörtern ist zu unsicher, um die sensiblen Daten und Anwendungen hinter Portalen zu schützen. Die Sensibilität der Portale wird mit der Komplexität der Anwendungen steigen, zu denen die Portale Zugang gewähren. Angriffe auf passwortgeschützte Portale sind mit moderatem Aufwand schon heute möglich und werden in den nächsten Jahren noch einfacher werden. Zugangsschutz mit Chipkarten ist wesentlich sicherer und wird es in der Zukunft auch bleiben. In komplexen Anwendungen vereinfachen Chipkarten die Abläufe und bieten Zusatznutzen. Also sind Chipkarten das Mittel der Wahl für die Absicherung von Portalen.

[1] Thorsten Gurzki et al.: »*Was ist ein Portal?*« *Definition und Einsatz von Unternehmensportalen*

Weitere Informationen zum Thema Trojaner:

Von Kai Raven SPIEGEL ONLINE - 27.06.2000 <http://kai.iks-jena.de/miniwahr/pc-wanzen.html>
Original von <http://service.spiegel.de/digas/servlet/find/ON=spiegel-82775>

Einer der ersten mächtigen und erweiterbaren Trojaner war Sub7 (manchmal auch SubSeven), der auch Keylogger Funktionalität integriert:

F-Secure Virus Descriptions: SubSeven <http://www.f-secure.com/v-descs/subseven.shtml>

Weiteres Trojaner-Beispiel (Auf Description klicken):
<http://www.sophos.com/security/analyses/trojpwsql.html>

Microsoft Technet Note zu Remote Access Trojans aus dem Jahre 2002:
<http://www.microsoft.com/technet/security/alerts/info/virusrat.msp>

Do-It-Yourself Spyware Kit Sells for \$20: <http://www.eweek.com/article2/0,1895,1942497,00.asp>

US DoJ: Queens Man Sentenced to 27 Months' Imprisonment on Federal Charges of Computer Damage, Access Device Fraud and Software Piracy <http://www.cybercrime.gov/jiangSent.htm>

Weitere Informationen zum Thema Passwort-Cracking:

John The Ripper (UNIX Password Cracker): <http://www.openwall.com/john/>

Ophcrack 2 (Windows password cracker, using Rainbow table TMT0):
<http://ophcrack.sourceforge.net/>

Philippe Oechslin: Password Cracking: Rainbow Tables Explained <https://www.isc2.org/cgi-bin/content.cgi?page=738>

kommerzieller Anbieter von Rainbow Tables: <http://www.rainbowtables.net/products.php>

Über FlexSecure

Die FlexSecure GmbH ist einer der führenden Anbieter von innovativen Sicherheitslösungen in der Informationstechnologie. In enger Kooperation mit namhaften Forschungsinstituten entwickelt FlexSecure eSecurity-Anwendungen zur Autorisierung, Authentifizierung, Integritätsprüfung und Verschlüsselung auf der Basis von digitalen Signaturen.

Seit dem Gründungsjahr 2000 hat sich FlexSecure zu einem international anerkannter Vorreiter für sichere Informationen und sichere Identität in der digitalen Informationsgesellschaft entwickelt.

Lösungen von FlexSecure sorgen dafür, dass elektronische Geschäftsprozesse in Unternehmen sowie öffentlichen Institutionen sicherer, einfacher und wirtschaftlicher werden. So liefert Flexsecure z.B. die Zertifizierungstechnologie für den neuen Reisepass. Weitere Kunden sind u.a. das Bundesamt für Sicherheit in der Informationstechnologie (BSI), die Bundesnetzagentur, das Zweite Deutsche Fernsehen und das Deutsche Gesundheitsnetz.