Sichere Authentifizierung im Internet

Mit der SmartCard durch den Passwort-Dschungel

Persönliche Daten im Internet sind zu einem Handelsgut der virtuellen Welt geworden und nehmen einen immer höheren Stellenwert in unserer Gesellschaft ein. Die Flut an persönlichen Daten ergibt sich aus der Nutzung vieler, verschiedener Internet-Dienste. Aus der Masse der persönlichen Daten entsteht die Möglichkeit von Profilbildung und Tracking einzelner Personen. Daher gilt es, die persönlichen Daten vor unauthorisiertem Zugriff zu schützen. Besondere Herausforderungen für diese Aufgabe sind unter anderem keine gemeinsame Infrastruktur für die Identifikation/Authentikation der Nutzer der Internet-Dienst-Anbieter, das Fehlen von Landesgrenzen im Internet, unterschiedliche Rechtsräume und -auffassungen sowie ein eingeschränktes Unrechtsbewusstsein der Internet-Nutzer in der virtuellen Welt.

Der Passwortmechanismus ist zurzeit das meistverwendete Verfahren zur Verifikation der Identität, von Nutzern bei Internet-Diensten. Grundsätzlich bringt der Einsatz eines Passwortmechanismus zahlreiche Sicherheitsprobleme mit sich. Mit der steigenden Anzahl von genutzten Internet-Diensten wird die Sammlung von Passwörtern des Nutzers immer größer. Probleme, die hier in der Breite auftreten, sind die Verwendung von qualitativ schlechten Passwörtern, die Verwendung eines guten Passworts für unterschiedliche Dienste oder die Übertragung von Passwörtern im Klartext in http-Sessions oder in E-Mails. Häufig vorkommende Angriffsmethoden auf den Passwortmechanismus sind Trojanische Pferde mit Key-Logger-Funktionen auf den Zugangs-Computern (PC, Notebook, SmartPhone, Internet-Café-Rechner, …), Phishing-Webseiten und/oder Social Engeneering [1].

SmartCard als Schlüssel zum Internet

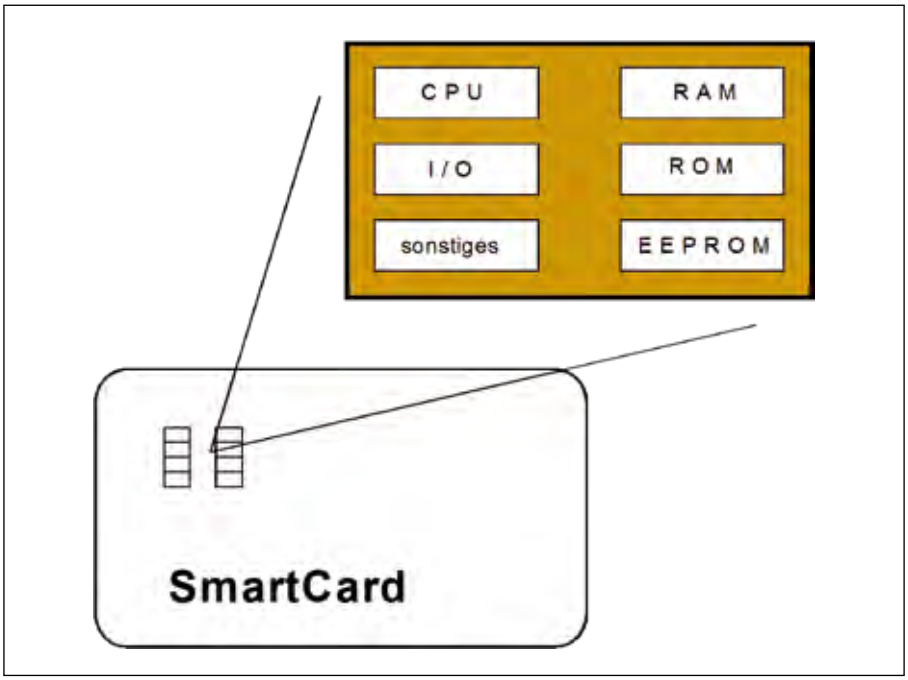
Seit Jahren ist die SmartCard ein bewährtes elektronisches Sicherheitsmedium im Banken- und Kreditkarten-Umfeld. Jedoch ist auffällig, dass die SmartCard nur in wenigen Einsatzbereichen zur Verifikation eines Nutzers verwendet wird.

Eine SmartCard ist eine Plastikkarte in der genormten Größe einer EC-Karte (86 x 54 x 0,76 mm), in die ein Computer-System integriert ist und die dem Nutzer Sicherheitsdienstleistungen zur Verfügung stellt. Ein SmartCard-Computer enthält: eine CPU, RAM- und ROM-Speicher, ein „schlankes" Betriebssystem im ROM, eine I/O-Schnittstelle, über die die gesamte Kommunikation stattfindet (Kontaktflächen oder kontaktloses Interface), ein EEPROM, auf dem die geheimen Schlüssel, zum Beispiel ein privater RSA-Schlüssel oder andere symmetrische Schlüssel, sowie persönliche Daten (Passwörter etc.) sicher gespeichert sind. Eine weitere Komponente in einer SmartCard kann zum Beispiel ein Co-Prozessor sein, der eine symmetrische oder eine asymmetrische Verschlüsselung sehr schnell durchführt.

Die SmartCard wird in der Regel durch eine PIN geschützt. Wenn ein Nutzer die Sicherheitsfunktionen in Anspruch nehmen will, muss er seine SmartCard mithilfe seiner persönlichen PIN aktivieren. Verliert der Nutzer seine SmartCard, kann ein Finder diese nicht verwenden, da er die PIN nicht kennt. Kennt jemand die individuelle PIN eines anderen Nutzers, kann er keinen Nutzen daraus ziehen, sofern er nicht auch die SmartCard besitzt. Außerdem kann ein Nutzer seine PIN jederzeit ändern. Die Sicherheit einer SmartCard beruht also auf Wissen (PIN) und Besitz (Karte). Geheime Schlüssel verlassen die SmartCard nie. Alle geheimen Operationen finden direkt in der SmartCard statt. Schlüssel können benutzt werden, ohne sie zu kennen. Geheime Daten sind manipulationssicher in der Karte gespeichert … [2].

Die Verifikation der Identität des Nutzers wird in den meisten Fällen durch die digitale Signatur einer Challenge (zum Beispiel Zufallszahl), die in der SmartCard mit einem geheimen Public-Key-Schlüssel durchgeführt wird (Challenge-Response-Verfahren), wird realisiert. In der Regel steht dafür eine Public-Key-Infrastruktur (PKI) zur Verfügung [3].

Die Sicherheitsverfahren auf der Basis einer PKI mit Public-Key-Verfahren, Zertifikaten, Sperrlisten usw. ist für einen Angreifer,



der den Kommunikationsablauf verfolgen kann, in der Regel nicht zu knacken. Dennoch gibt es auch hier Restrisiken, die es zu beachten gilt. Wird ein SmartCard-Leser ohne eine Tastatur verwendet (Klasse-1-Leser), dann wird die PIN zur Aktivierung der SmartCard auf dem Computer eingelesen und dem SmartCard-Leser gesendet. Hier besteht das Risiko, dass der Computer mit einem Trojanischen Pferd mit Key-Logger-Funktionalität verseucht ist, der die PIN-Eingabe mitliest und dann in der Lage ist, die Smartcard zu manipulieren, wenn zum Beispiel der Nutzer die SmartCard im SmartCard-Leser lässt.
Mit einem sogenannten Klasse-2-Leser, der eine Tastatur im SmartCard-Leser integriert hat, kann ein solcher Angriff verhindert werden. Noch sicherer ist ein Klasse-3-Leser, der zusätzlichen neben eigenen Sicherheitsfunktionen noch ein eigenes Display im Leser integriert hat, auf dem nicht manipulierbare Anzeigen für den Nutzer ausgegeben werden können.

Passwortmechanismus vs. SmartCard-System

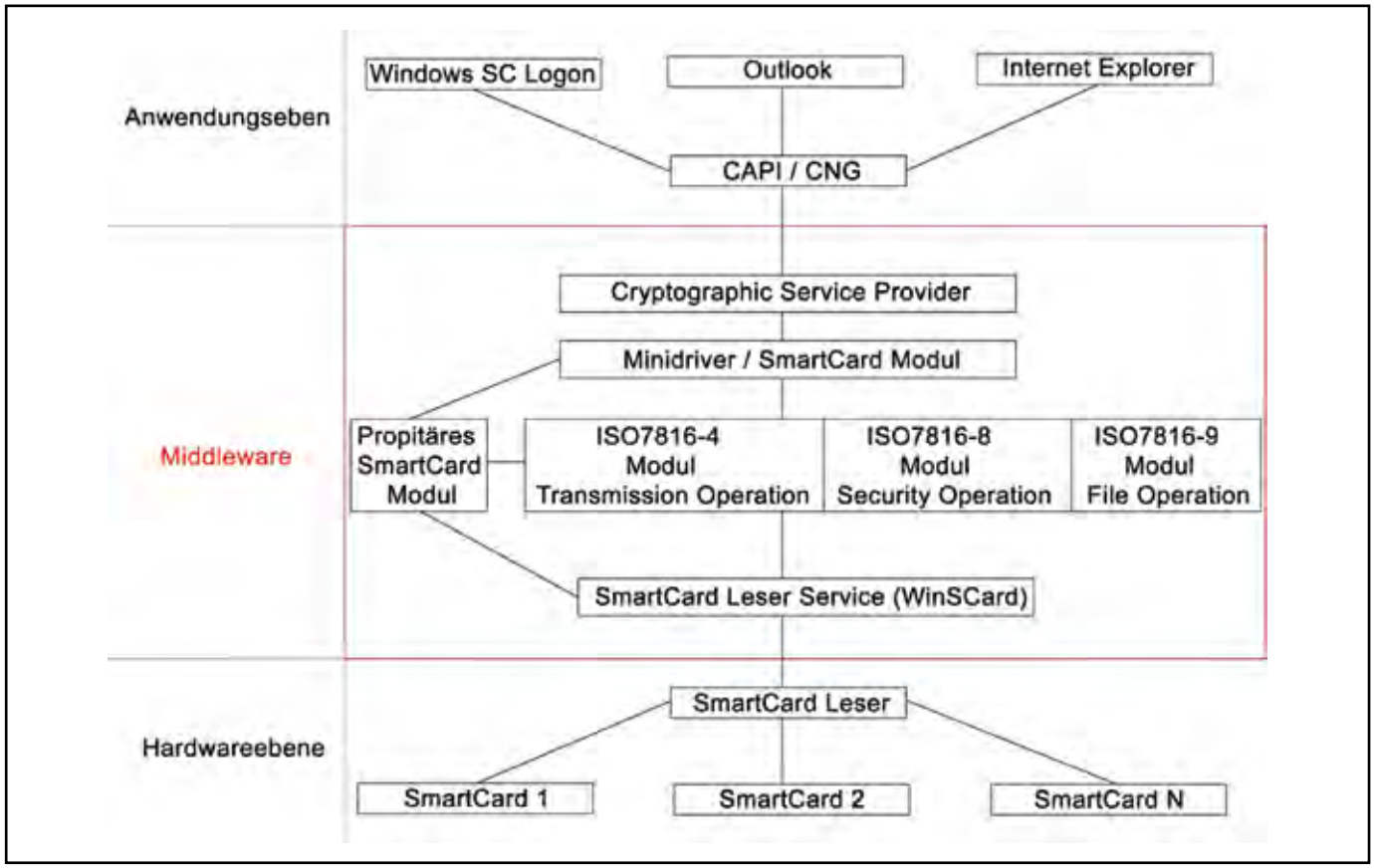
Der direkte Vergleich der Sicherheitsaspekte von Passwortmechanismen und SmartCard-Systemen zeigt, dass ein SmartCard-basierendes System deutlich sicherer ist, aber auch sehr viel mehr Geld kostet. Jeder Nutzer braucht eine SmartCard und einen SmartCard-Leser. Da es keine gemeinsame Infrastruktur gibt, müsste für jede Anwendung eine eigene SmartCard verwendet werden. Ein Kernproblem liegt momentan also in dem eingeschränkten Angebot an SmartCard-gestützten Lösungen. Aus diesem kleinen Angebot an Lösungen folgt, dass es eine geringe Nutzerzahl und somit auch eine geringe Verbreitung von SmartCard-Lesern gibt.

Ein weiteres Problem, das aus dem dürftigen Angebot an SmartCard-gestützten Diensten resultiert, ist die Standardisierung von Komponenten in dem SmartCard-System. Momentan besteht Kompatibilität unterschiedlicher SmartCards nur in weit verbreiteten und bewerten Anwendungen, wie zum Beispiel bei der EC-Karte. Um die Verbreitung von SmartCards voranzutreiben, müssen für die bestehenden Schnittstellen weitere Anwendungen spezifiziert werden, die es ermöglichen, diverse SmartCards für eine Anwendung ohne Zusatzaufwand einzusetzen.

Um diese Vielfalt an Spielräumen von SmartCards zu managen und proprietäre Entwicklungen zu unterstützen, werden Middleware-Systeme für die Integration von SmartCard-Anwendungen verwendet. Diese Middleware-Systeme sind modular strukturiert und haben so die Fähigkeit, proprietäre Module, wie SmartCard-Treiber, die von den SmartCard-Herstellern geliefert werden, einfach einzubinden. Im Rahmen eines Forschungsprojektes hat sich das Institut für Internet-Sicherheit mit der Realisierung eines solchen Middleware-Systems beschäftigt.

Abhilfe durch noch mehr Standardisierung?

Die International Organization for Standardizion (ISO) hat sehr grundlegende Standards im Bereich der SmartCards hervorgebracht. Ein Großteil der Standards für SmartCards ist in den ISO 7816-1 bis ISO 7816-15 definiert. Die ISO 7816-1 bis 3 standardisieren die physikalischen Eigenschaften sowie die Kommunikationsprotokolle zwischen SmartCard und SmartCard-Leser. Diese Standards werden von der SmartCard-Branche ausnahmslos und erfolgreich umgesetzt und genutzt.



Eine bestehende Inkompatibilität betrifft die Kommunikationseinheiten auf der Anwendungsebene. Diese Kommunikationseinheiten (APDUs) haben indirekt mit der Kommunikation zwischen SmartCard und SmartCard-Leser zu tun. Standard-APDUs sind in der Lage, maximal 256 Byte an Daten in einem Befehl zu transportieren. Diese relativ kleine Datenmenge reicht für die Mehrzahl der möglichen Befehle aus und wird von allen Komponenten unterstützt. Da aber immer größere Datenmengen auf SmartCards gespeichert werden können, wurden extended APDUs eingeführt. Diese sind in der Lage, bis zu 65.536 Byte an Daten zu transportieren, was zu einem Geschwindigkeitsgewinn beim Austausch der Daten führt.

Die APDUs müssen vom Treiber des SmartCard-Lesers umgesetzt werden, um diese verständlich zu verschicken. Sowohl APDUs als auch extended APDUs sind in der ISO 7816-4 standardisiert. Dennoch werden extended APDUs nicht von allen SmartCard-Lesern und SmartCards unterstützt, was in der Praxis immer wieder zu Problemen führt.

Die Komplexität von SmartCards liegt im Card Operating System (COS). Die ISO 7816-4 bis -9 standardisieren ein COS. Hier werden die APDUs, Befehle und Lebenszyklen für SmartCards definiert. Dabei handelt es sich um Befehle für minimale Sicherheits- und Dateioperationen. Hier lassen die Standards leider einen großen Spielraum, der dazu führt, dass proprietäre Befehle verwendet werden. Ähnliche Probleme gibt es auch bei dem Dateilayout von SmartCards. Viele SmartCard-Hersteller verwenden proprietäre SmartCard- und Dateistrukturen. Dadurch ist es für Anwendungen nicht einfach möglich, Daten von der SmartCard anzufordern oder auf diese zu schreiben, solange die Anwendung keine genaueren Informationen über die Struktur der SmartCard hat.

Um diesem Problem entgegenzuwirken, gibt es die ISO 7816-15, die auf dem PKCS#15-Standard der RSA Labs basiert. Hier wird eine einheitliche Struktur definiert, die Auskunft darüber gibt, an welchem Ort sich bestimmte Daten auf der SmartCard befinden. Um die Nutzung transparent zu machen, besteht zusätzlich die Möglichkeit, Daten über sprechende Labels zu referenzieren. Auch bei der ISO 7816-15/PKCS#15-Struktur gibt es SmartCard spezifische Probleme. COS verfügen im Gegensatz zu Betriebssystemen nur in den seltensten Fällen über eine dynamische Speicherverwaltung und Dateilängen. Aus diesem Grund werden die meisten Daten mit festen Längen erzeugt. Soll eine Anwendung Daten in der PKCS#15-Struktur von unterschiedlichen SmartCards schreiben oder lesen, muss sichergestellt sein, dass die Datengröße auf den eingesetzten SmartCards einheitlich ist. Es besteht noch Bedarf an Standardisierung in diesem Bereich.

Eine SmartCard statt 100 Passwörtern

Die Verifikation von Identitäten auf der Basis von SmartCard-Lösungen ist deutlich sicherer als der Passwortmechanismus. Passwortmechanismen sind in einer vernetzten Informations- und Wissensgesellschaft im Hinblick auf die erzielbare Sicherheit her schon lange nicht mehr ausreichend! Die geringe Verbreitung von SmartCards im Bereich der Verifikation von Identitäten lässt sich auf die hohen Kosten bei der Umsetzung einer Public-Key-Infrastruktur und von SmartCard-Leser zurückführen, sowie auf die Kompatibilitätsprobleme verschiedener SmartCard-Lösungen.

Ziel muss es sein, durch präzise Standards, Spielräume und somit proprietäre Entwicklungen weitestgehend zu verhindern. Dies scheint eine triviale Lösung zu sein, doch verfolgt eine internationale Standardisierung, wie die ISO, im Gegensatz zu industriellen Spezifikationen, das Ziel, Interessen aller am Prozess Beteiligten zu vereinigen. Dieser Prozess kostet nicht nur viel zu viel Zeit und Geld durch die Mitarbeit an Standards, sondern die Ergebnisse sind am Ende oft Kompromisse, die wieder proprietäre Lösungen möglich machen.
Große Hoffnung wird in die Einführung des neuen Personalausweises (nPA) im Herbst gesetzt. Durch den neuen Personalausweis wird in einem Zeitraum von wenigen Jahren jeder Bürger in Deutschland eine SmartCard mit ID-Funktionalität besitzen – sehr viele davon auch geeignete SmartCard-Leser. Unklar ist noch, ob die SmartCard-Leser für den nPA kontaktbehaftete SmartCards lesen können. Der nPA selber hat eine kontaklose Schnittstelle.

Die SmartCards sind ein geeignetes Sicherheits-Modul für Personen und könnten noch sehr viele Sicherheitsdienstleistungen erfüllen. Aus diesem Grund sollten wir SmartCard-Anwendungen weiter fördern, denn sie unterstützen uns angemessen bei der IT-Sicherheit. ■

[1] M. Linemann, N. Pohlmann: „Sicher im Internet – Tipps und Tricks für das digitale Leben", Orell Fuessli Verlag, 2010
[2] W. Effing, W. Rankl: Handbuch der Chipkarten: „Aufbau – Funktionsweise – Einsatz von Smart Cards", Hanser Fachbuch, 5. Auflage, 2008
[3] C. Adams, S. Lloyd: „Understanding Pki: Concepts, Standards, and Deployment Considerations", Addison-Wesley Longman, 2. Auflage, 2002

Prof. Dr. Norbert Pohlmann,
Informatikprofessor für Verteilte Systeme und Informationssicherheit, Leiter des Instituts für Internet-Sicherheit – if(is) an der Fachhochschule Gelsenkirchen (www.internet-sicherheit.de).

Markus Hertlein,
forscht im Rahmen seiner Bachelor-Thesis im Bereich „Middleware für SmartCard-Anwendungen" im Institut für Internet-Sicherheit an der Fachhochschule Gelsenkirchen.