

# Camouflage: Kryptographisches Tarnen und Täuschen

Die Möglichkeit, private Schlüssel zu knacken, ist der wunde Punkt einer Software-gestützten Authentisierung. Physikalische Smart Cards umgehen dieses Problem zwar, bringen aber ihre eigenen Nachteile mit sich. Eine neue Technologie, die kryptographische Camouflage, will „des Pudels Kern“ hinreichend verschleiern.

>> Der Vorteil von Public-Key-Kryptosystemen ist es, dass die Vertrauens entgegenbringende Partei keine Kopie des Private Keys des Users besitzen muss. Im Gegensatz dazu muss bei Passwortsystemen serverseitig eine Möglichkeit, das Passwort zu verifizieren, vorgesehen werden – woraus wiederum das Passwort abgeleitet werden kann. In einer idealen Situation würde eine starke Authentisierung des Users zur Nicht-Abstreitbarkeit führen bzw. zu der Tatsache, dass der User wirklich der Eigentümer des Private Keys ist. Während das

sers. Diese Art von Programmen wird käuflich (!) angeboten, um vergessene Passwörter wiederherzustellen.

## Hardware Smart Cards

Eine andere Möglichkeit zum Schutz eines Private Keys ist die Hardware Smart Card. Statt den Private Key auf der Festplatte eines Rechners zu speichern, wird er in einem Microchip (umgeben von einer Plastikkarte) sicher aufbewahrt. Der Microchip schützt vor Auslesen des Private Keys, bis der User sich mit einer PIN gegenüber der Smart Card authentisiert. Einen noch höheren

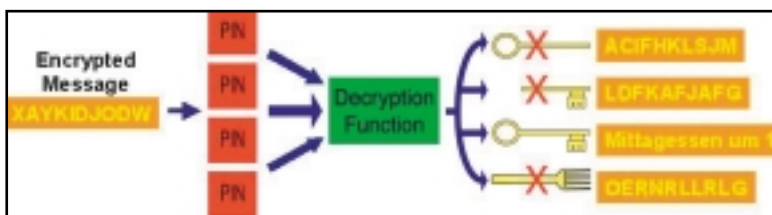
Inkompatibilitäten zwischen den einzelnen Smart-Card-Herstellern.

## Software Smart Cards

Eine neue Technologie zur Authentisierung verspricht Abhilfe: Cryptographic Camouflage. Bei diesem Ansatz wird der Private Key in einem Software-Container, der Software Smart Card, gesichert. Dieses mittlerweile patentierte Verfahren basiert darauf, den Private Key unter tausenden anderen, unechten, jedoch plausibel aussehenden Private Keys zu verbergen (camouflieren). Ein Hacker, der versucht, den Container über z.B. eine Brute-Force-Angriffe anzugreifen, wird viele plausible Private Keys entschlüsseln. Der richtige Private Key kann unter der Menge der falschen aber nur herausgefunden werden, indem er diese Private Keys zur Authentisierung gegenüber dem zuständigen Server benutzt. Dieser Authentisierungsserver erkennt mehrfache Authentisierungsversuche und kann die entsprechende Software-Smart-Card sperren.

Die Idee der Cryptographic Camouflage erklärt sich wie folgt: Normalerweise bestehen zu verschlüsselnde Daten aus verifizierbarem Plaintext, d.h. die Daten sind mit genügend Strukturen versehen, die für einen Krypto-Experten ersichtlich machen, ob er den richtigen Schlüssel zur Dekodierung benutzt hat. Wird beispielsweise der deutsche Text „Mittagessen um 1“ mit dem DES-Verfahren und einem Schlüssel „A“ kodiert und danach mit einem anderen Schlüssel „B“ dekodiert, so

Abb. 1: Private Keys haben bestimmte mathematische Charakteristiken, die Hacker ausnutzen können (z.B. RSA oder ungerade Zahlen). Hier weiß der Hacker, wann die Nachricht dekodiert wurde.



für die Vertrauens entgegenbringende Partei angenehm ist, trägt der User stets die Last, seinen Private Key sicher aufzubewahren.

Schutz bieten Kryptokarten mit einem kryptographischen Prozessor in der Smart Card.

Normale PC-Umgebungen sind im Gegensatz zu Server-Umgebungen eher als unsicher einzustufen (BSI-Schutzklasse D) – trotzdem speichern Microsofts IE, AOLs Netscape-Browser und andere PKI-Software-Hersteller die Private Keys mit Passwortschutz lokal auf dem PC ab. Kommt ein Hacker in den Besitz einer solchen Datei mit einem Private Key, kann er durch Dictionary-Angriffe das Passwort herausfinden. Das Crackprogramm „ncrack“ entschlüsselt z.B. Passwörter des Netscape-Brow-

Smart Cards werden erfolgreich auf diversen Gebieten eingesetzt, z.B. in Handys, Debit- und Kreditkarten, usw. Bisher wenig erfolgreich waren Smart Cards allerdings im Internet. Eine breite Verteilung von Smart-Card-Readern und die nötigen Investitionen hierfür bremsen diese Technologie. Die Forderung nach Mobilität (Roaming), und entsprechende Treiber für diverse Betriebssysteme zur Verfügung zu stellen, hat sich in der Praxis als sehr schwierig herausgestellt. Hinzu kommen im Detail unterschiedliche Standards und

entsteht nur ein Wirrwarr von zufälligen Zeichen und kein logischer Text. Diesem Prinzip folgend, kann ein Hacker, ohne den Originaltext zu kennen, den gesamten Schlüsselraum (PIN-Space) absuchen, bis der richtige Plaintext vorliegt und demnach der gültige Schlüssel verwendet wurde. Um einer solchen intensiven Suchattacke zu entgehen, muss der Schlüsselraum extrem groß gewählt werden.

Enthalten dagegen alle Dekodierungen die gleiche Struktur wie der Originaltext, kann der Hacker nicht mehr zwischen der richtigen und den vielen anderen plausiblen Möglichkeiten unterscheiden. In diesem Fall muss der Schlüsselraum nicht übermäßig groß gewählt werden, da der gültige Schlüssel unter ebenfalls plausibel wirkenden anderen (aber falschen) camoufliert wurde. In unserem Beispiel (siehe

nen Hashwert des Passwortes. Stattdessen wird bei der Camouflage ein Partial Hash oder Secure Hash verwendet.   
 ■ Verschlüsseln von Signaturen. Besitzt ein Hacker den Key-Container, signierte Daten und die Signatur, so kann er durch Ausprobieren den richtigen Private Key herausfinden, der zur Signatur passt. Zum Vermeiden dieser Attacke wird der Hash der Daten, nicht deterministisch sondern randommäßig aufgefüllt. Signaturen von gleichen Daten sind also niemals gleich.

Erweitert man das Konzept der Cryptographic Camouflage, so kann außer der Authentisierung an jedem Ort von jedem Gerät aus auch der sichere Transport von Third-Party-Zertifikaten erreicht werden. Damit sind Zertifikate nach X.509.v3 für Applikationen (PKI-enabled applications) sicher auch über das Internet zu transportieren und nach

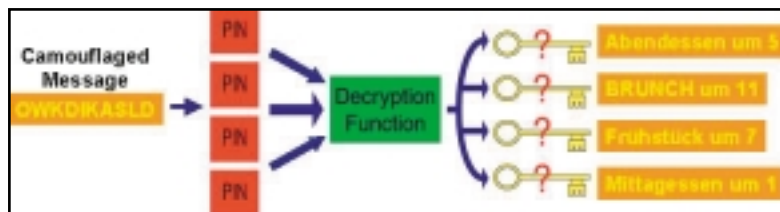


Abb. 2) werden also beim Durchprobieren der PIN-Space (Passworte) stets deutsche Sätze (Schlüssel) erzeugt.

Abb. 2: Bei der Camouflage-Technologie produziert das Durchprobieren aller PINs als Eingabe für die Decryption-Funktion immer sinnvolle Schlüssel als Ausgabe. Hier weiß der Hacker nicht, wann die Nachricht dekodiert wurde.

Zur Camouflage von Schlüsselwerten bedient man sich der Standard-Algorithmen DSA und RSA. Zusätzlich müssen weitere Maßnahmen getroffen werden, da diese Algorithmen zwar Encryption und Signaturen erzeugen können, aber noch keine Camouflage. Diese Maßnahmen sind:

- Keine Strukturen mit dem PIN (Passwort) verschlüsseln, sondern vor der Encryption eliminieren. (RSA-Keys sind z.B. immer ungerade. Diese Information kann etwa durch Weglassen der 1er-Bits entzogen werden.)
- Den Public Key verschlüsseln. Auch der User kennt seinen eigenen Public Key nicht. Mit dem Public Key wird kein verifizierbarer Plaintext verschlüsselt (Verhindern der Known-Signature-Attacke).
- Geheimhaltung des PINs. Dieser Aspekt erscheint als selbstverständlich, aber viele Key-Container enthalten ei-

erfolgter positiver Authentisierung vom User zu verwenden. CSP (Microsoft) und PKCS#11 werden als Programmschnittstelle verwendet. Damit eignet sich die Software-Smart-Card als Ergänzung zur physischen Smart Card für den Einsatz in der digitalen Welt des Internets.

Entwickelt wurde die Cryptographic Camouflage von der Firma Arcot unter Beratung durch die Kryptographie-Spezialisten Bruce Schneier, Taher ElGamal und Martin Hellmann.

|                 |                        |
|-----------------|------------------------|
| <b>Kontakt:</b> | Arcot Deutschland GmbH |
|                 | Andreas Gatz           |
|                 | Feringastr. 6          |
|                 | D-85774 München        |
|                 | Tel. 0049-89-99216-402 |
|                 | Fax 0049-89-99216-200  |
|                 | andreas.gatz@arcot.com |
|                 | www.arcot.com          |

:profil

## Firmenprofil

„Secure e-Business anywhere“ lautet das Motto des 1997 gegründeten US-Unternehmens. Seit 2001 ist Arcot - mit Sitz in München - auch in Deutschland, Österreich und der Schweiz aktiv. Arcot bietet reine Softwarelösungen zur starken Authentisierung. Mögliche Anwendungen sind: Zugangskontrolle, Secure E-Mail, Authentifizierung und Administration für E-Paymentsysteme, B2B Extranets, Web Portale und Virtual Private Networks. Das Thema „Sicherheit des Private Keys“ wird durch einen revolutionären und weltweit patentierten Ansatz namens „Cryptographic Camouflage“ gelöst. Hohe Bedienungsfreundlichkeit, Sicherheit auf Hardware-Niveau, Unabhängigkeit bei der Wahl der Endgeräte, ressourcenschonende Implementierung und vor allem auch höchst mögliche Kosteneffizienz zeichnen die Produkte aus.

An Arcot beteiligt sind unter anderem die Firmen Oracle, Novell, First Union Bank, SEB Bank und Visa International.