Veröffentlicht in: Tagungsband des 3. Internationalen Kongress "Sichere Identität", Berlin, Fraunhofer, 2011, Seite 40-44.

SumoDacs: Absicherung des mobilen Zugriffs auf Unternehmensanwendungen mit einer manipulationsresistenten Smartcard

Michael Decker
AIFB, Karlsruher Institut für Technologie (KIT)

Dr. Bernhard Kölmel
CAS Software AG, Karlsruhe

1 Einleitung

Der Einsatz mobiler Computer (z.B. Smartphones & Netbooks) in Verbindung mit drahtloser Datenkommunikation (z.B. UMTS, WLAN) bietet ein großes Potential für die Unterstützung von Geschäftsprozessen mit mobilen Aktivitäten. Allerdings bringt der Einsatz dieser Technologien auch besondere Sicherheitsprobleme mit sich: ein mobiler Computer kann durch Unachtsamkeit oder Diebstahl in die Hände Unbefugter geraten oder die drahtlose Datenkommunikation könnte abgehört werden. Gerade *kleine und mittelständische Unternehmen (KMU)* können nicht die Ressourcen für die Implementierung von entsprechenden Sicherheitsmaßnahmen aufbringen und verzichten daher oft ganz auf mobile Lösungen und den damit einhergehenden Produktivitäts- und Qualitätsgewinnen.
Vor diesem Hintergrund wurde das SumoDacs-Projekt[1] initiiert: Ziel des Projektes ist die Entwicklung eines auch für KMU geeigneten Software-Frameworks zur Absicherung des mobilen Zugriffs auf Unternehmensanwendungen. Eine wesentliche Komponente von SumoDacs ist die Verwendung einer sog. Security-Smartcard (auch „Hardware-Token“): hierbei handelt es sich um eine spezielle Smartcard für Sicherheitsfunktionen, die in verschiedenen für mobile Endgeräte geeigneten Bauformen vorhanden ist (z.B. (Mikro-)SDCard, USB-Stick) und u.a. sensitive kryptographische Daten (z.B. private Schlüssel) sicher speichert. Diese Smartcard kann den Schutz dieser Daten auch dann noch aufrechterhalten, wenn es in die Hände eines Angreifers gelangt. Das vom Token sicher verwahrte Schlüsselmaterial ist Grundlage für die Authentifizierung im Rahmen des Aufbaus einer mobilen Verbindung zu einer Anwendung (z.B. CRM- oder ERP-System) im sicheren Unternehmensnetzwerk. Eine tokenbasierte bietet gegenüber einer herkömmlichen rein passwortbasierten Authentifizierung mehrere Vorteile, die im Beitrag erörtert werden. Weiter kann das Token auch mit dem mobilen Computer erfasste Daten sicher speichern, wenn diese wegen mangelnder Konnektivität nicht sofort hochgeladen werden können („Tresor-Funktion“).

[1] Das Akronym steht für „Secure Mobile Data Access“; die Webseite findet sich unter http://www.sumodacs.de

Der vorliegende Beitrag ist wie folgt aufgebaut: im folgenden Kapitel 2 wird zunächst die Gesamtarchitektur vorgestellt, bevor dann im dritten Kapitel die Rolle der Smartcards für die Absicherung des mobilen Datenzugriffs erklärt wird. Im vierten Kapitel wird mit der kontextabhängigen Zugriffskontrolle ein weiteres Konzept vorgestellt, mit dem im Projekt mobilspezifische Sicherheitsherausforderungen adressiert werden. Der Beitrag endet mit einer kurzen Zusammenfassung und einem Ausblick.

2 Architektur

In Abbildung 1 ist die Gesamtarchitektur von SumoDacs dargestellt. Diese Architektur teilt die Komponenten in drei Zonen auf: **Zone I** ist das interne Netzwerk der Unternehmung, in dem die mobil anzusprechenden Unternehmensanwendungen betrieben werden; diese Netzwerkzone wird als vertrauenswürdig eingestuft. **Zone II** ist eine sog. *„Demilitarisierte Zone“ (DMZ)*, die Zone I vom öffentlichen Internet durch eine innere und äußere Firewall abschirmt und somit als Sicherheitspuffer fungiert. Das öffentliche Internet ist **Zone III**; es handelt sich hierbei insbesondere auch um drahtlose Zugangsnetze wie etwa GPRS, UMTS oder öffentliche WLANs.

In Zone I werden die Unternehmensanwendungen betrieben, auf die mobil zugegriffen werden soll. Beispiele für solche Anwendungen sind etwa CRM-/ERP-Systeme oder Dokumentenserver. Bei der überwiegenden Anzahl der Systeme wird es sich um Altanwendungen handeln, die also ohne Berücksichtigung eines mobilen Zugriffs implementiert wurden. SumoDacs sieht deshalb sog. Wrapper vor, mit denen die relevanten Funktionen dieser Systeme eingebunden und mit dem SumoDacs-Sicherheitsserver in der DMZ (Zone II) verbunden werden. Eine weitere Komponente in Zone I ist die Administrations-Konsole, mit der das SumoDacs-System konfiguriert und überwacht wird.

In der „mittlere Zone“ befindet sich der Sicherheitsserver, der verschiedene Funktionen für das Gesamtsystem bereitstellt. Seine Hauptaufgabe ist die Vermittelung der Anfragen aus der unsicheren Zone III an die entsprechende Anwendung in Zone I. Bevor solch eine Anfrage über einen Wrapper an eine Anwendung weitergereicht wird, muss eine Authentifzierung des mobilen Clients durchgeführt werden. Die Daten werden vor der Übertragung im unsicheren Internet auch auf Anwendungsebene verschlüsselt, so dass der Sicherheitsserver ebenfalls Ver- und Entschlüsselung vornehmen muss. Weiter kann er mobil-spezifische Berechtigungsmodelle auf die anwendungsspezifischen Berechtigungsmodelle abbilden, wozu er mit einer „Policy“-Komponente ausgestattet ist. Er kann mit der „Store & Forward“-Komponente auch an Clients zurückzugebende Daten zwischenspeichern, falls die Internetanbindung gerade nicht zu Verfügung steht, etwa weil sich der mobile Nutzer gerade in einem „Funkloch“ befindet.

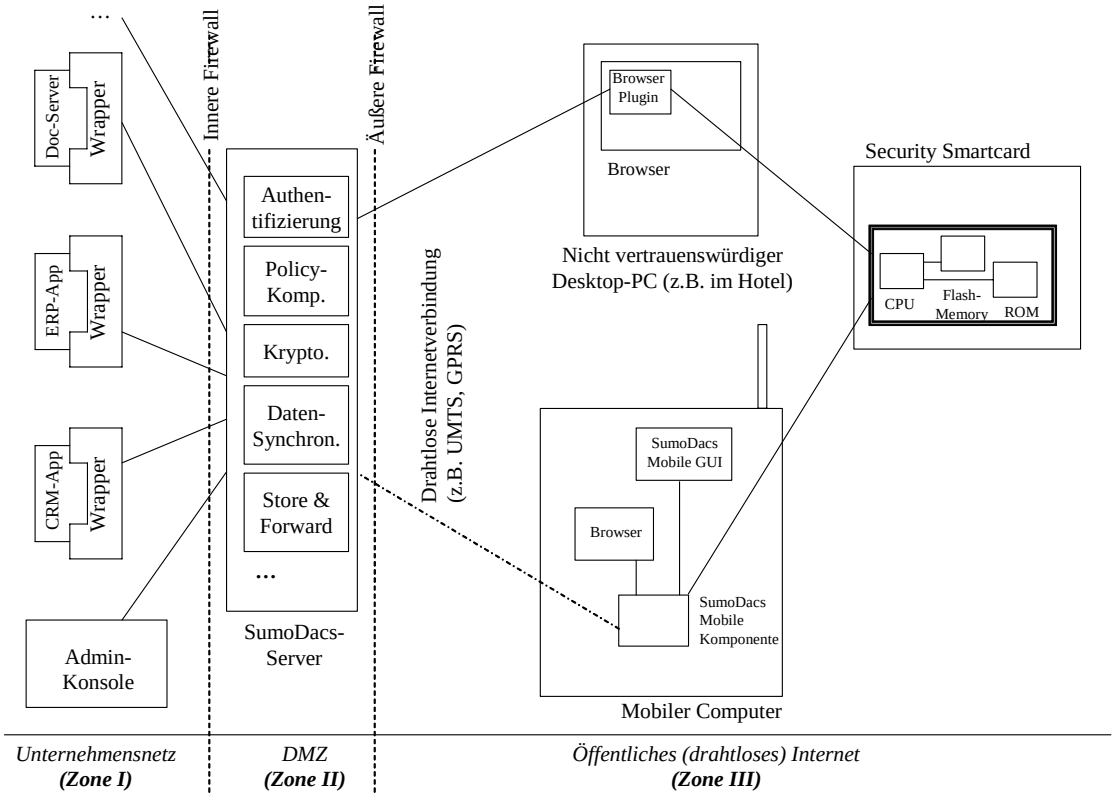

Abbildung 1: Gesamtarchitektur von SumoDacs

Die dritte Zone ist das öffentliche Internet, von dem aus drahtlos und drahtgebunden von den mobilen Computern auf die Unternehmensanwendungen zugegriffen werden soll. Insbesondere der drahtlose Zugriff bringt Sicherheitsrisiken mit sich, da viele gängige Verfahren (z.B. GPRS, WLAN) nicht ausreichend gegen Angriffe geschützt sind. Auf dem mobilen Computer wird eine spezielle Laufzeitumgebung benötigt, um die Smartcard anzusprechen und die Absicherung der mobilen Client-Anwendung zu realisieren. Weiter ist in Zone III noch ein nicht vertrauenswürdiger Desktop-PC eingezeichnet, der ebenfalls für den mobilen Zugriff verwendet werden; es kann sich hierbei um einen Rechner in einem Internet-Café, einem Hotel oder bei einem Kunden handeln. SumoDacs sieht auch die Verwendung eines solchen „Kiosk“-Rechners vor, bei dem dann auf die Unternehmensanwendung mit einer Webanwendung zugegriffen wird, wobei über ein spezielles Browser-Plugin mit der Smartcard kommuniziert wird.

3 Smartcard-basierte Sicherheit

Eine wesentliche Rolle im Gesamtkonzept von SumoDacs spielt die Verwendung einer speziellen Smartcard mit den mobilen Computern. Damit diese möglich ist, muss die Smartcard in Bauformen vorliegen, die das Anschließen an einen mobilen Computer erlauben, also vor allem als (μ)SDCard oder als USB-Stick. Diese Smartcard ist insbesondere auch gegen direkte Manipulationen gesichert, kann also bestimmte Sicherheitseigenschaften auch noch dann

aufrecht erhalten, wenn ein Angreifer in ihren Besitz gekommen ist und diese in einem Labor manipulieren kann.

Die Smartcard implementiert mehrere sicherheitsrelevante Funktionen, insbesondere die Ver- und Entschlüsselung von Daten mit symmetrischer und asymmetrischer Kryptographie, wobei die geheimen/privaten Schlüssel dabei nicht die Karte verlassen. Dies erfordert, dass die Schlüssel selbst auf der Karte erzeugt werden können, wofür ein integrierter Zufallsgenerator notwendig ist. Neben Schlüsselmaterial kann die Karte auch in einem bestimmten Umfang beliebige Daten sicher speichern; hierauf wird zurückgegriffen, wenn mit dem mobilen Computer erfasste Daten etwa wegen eines „Funklochs" nicht sofort zum Back-End übertragen werden können („Secure Caching"). Neben Verschlüsselungsfunktionen implementiert die Karte auch geeignete Hash-Funktionen (z.B. SHA-256), um digitale Unterschriften erzeugen zu können. Weiter beinhaltet die Smartcard noch eine sichere Zeitquelle, was für bestimmte kryptographische Protokolle notwendig ist.

Smartcards bieten im Vergleich zu herkömmlichen mit Passwörtern arbeitenden Authentifizierungsverfahren ein deutlich größeres Maß an Sicherheit, da herkömmliche Passwörter oft angreifbar sind, auch häufig vergessen werden oder gar schriftlich notiert werden. Eine Authentifizierung unter Verwendung eines von der Smartcard sicher gekapselten privaten oder geheimen Schlüssels bietet erheblich mehr Sicherheit, da solche Schlüssel mehr Information beinhalten (z.B. 128-Bit für symmetrische Verfahren) als Passwörter, die sich ein Mensch merken kann. Dieser Schlüssel sollte zusätzlich durch ein herkömmliches Passwort geschützt sein, so dass eine *„Zwei-Faktor-Authentifizierung" (2FA)* vorliegt.

Mögliche Vorkehrungen für die Erlangung von Manipulationsresistenz von Smartcards umfassen ein spezielles Layout der Leiterbahnen, um die Analyse unter einem Elektronenmikroskop erheblich zu erschweren oder die Verwendung von Dummy-Rechenoperationen, um auf Zeit- und Stromverbrauchsmessungen basierende Seitenkanal-Attacken zu verhindern. Eine andere Klasse von Angriffen beruht darauf, durch bewusst unzulässige Betriebsbedingungen (z.B. Stromspannung, Taktfrequenz, Temperatur) Fehlfunktionen zu provozieren, bei denen die Smartcard eigentlich geheime Daten (insb. Schlüsselmaterial) ausgibt. Werden solche Angriffe von der Smartcard erkannt dann schaltet sie sich ab oder löscht sogar die auf ihr gespeicherten Daten. Für weitere Ausführungen zu diesem Thema sei auf [KöKu99] verwiesen.

Angriffe auf in spezieller Hardware implementierte Sicherheitsfunktionen sind erheblich aufwändiger als Angriffe auf Software oder Netzwerke, da hierzu eine teure Laborausstattung notwendig ist. Ist ein solcher Angriff einmalig tatsächlich geglückt, so ist für eine Wiederholung des Angriffs auf eine zweite Smartcard fast der gleiche Aufwand zu betreiben; Angriffe auf Hardware skalieren also viel schlechter als Angriffe auf Software. Im Projekt werden Security-Smarcards aus der *CodeMeter*-Produktlinie des Projektpartner *WIBU Systems* verwendet, die als USB-Stick (CmStick) und als (μ)SDCard (CmCard) zur Verfügung stehen[2].

[2] siehe http://wibu.com/codemeter.php

Die Entwicklung dieser Smartcards ist NICHT Gegenstand des Projekts, sondern lediglich deren softwaretechnische Integration sowohl auf Client- als auch Server-Seite.

4 Kontextabhängige Zugriffskontrolle

Die Zugriffskontrolle eines (verteilten) Informationssystems ist eine Sicherheitsfunktion, die entscheidet, ob ein bestimmter Nutzer eine bestimmte Operation (z.B. Lesen, Schreiben) auf einer bestimmten Ressource (z.B. Datei, Datenbankobjekt) durchführen darf oder nicht. Für diese Entscheidung wird bei herkömmlicher Zugriffskontrolle im Wesentlichen die Identität des Nutzers sowie Eigenschaften der Ressourcen berücksichtigt. Bei Verwendung von mobilen Computern kann aber ein zusätzlicher Sicherheitsgewinn erzielt werden, wenn geeignete Kontext-Parameter von der Zugriffskontrollkomponente ausgewertet werden.
Unter „Kontextinformation“ im Sinne des *Mobile Computing* handelt es sich um jegliche zur Laufzeit des Systems in expliziter Form verfügbare Information, die vom System ausgewertet werden kann, um die Interaktion mit dem Nutzer zu unterstützen [Dour04]. Hierunter versteht man zunächst Sensor-Messungen, anhand deren etwa der aktuelle Aufenthaltsort des Nutzers oder die Umgebungshelligkeit ermittelt werden kann. Aber auch durch „Software-Sensoren“ ermittelte Daten können als Kontext herangezogen werden, etwa die aktuelle (Orts-)Zeit, Parameter der Netzanbindung (Sicherheit, Qualität) oder Einträge im persönlichen Terminkalender des Nutzers.
Die Grundidee der kontextabhängigen Zugriffskontrolle ist es nun, für das jeweilige Szenario geeignete Kontextparameter auch für die Zugriffsentscheidung zu berücksichtigen. Es könnte etwa festgelegt werden, dass auf bestimmte Dokumente nur vom Firmengelände oder Inland aus zugegriffen werden darf [Deck11]. Wird nun über ein Ortungsverfahren festgestellt, dass diese Bedingung vom mobilen Nutzer derzeit nicht erfüllt ist, so verweigert der SumoDacs-Server die Weiterleitung der entsprechenden Anfrage. Die Änderung von Gehaltseinträgen in der entsprechenden Tabelle gegen Mitternacht ist verdächtigt und sollte deshalb unterbunden werden. Auch im Kalender eingetragene Termine können zur Erhöhung der Sicherheit ausgewertet werden: ist für das aktuelle Datum ein Urlaubstag eingetragen, so sollten Zugriffe auf sensitive Geschäftsdaten unterbunden werden; ist hingegen ein Termin vor Ort bei Kunde A eingetragen, so sollte es mit dem mobilen Computer nicht möglich sein, die Daten von einem anderen Kunden B einzusehen, insbesondere wenn A und B zueinander in Konkurrenz stehen. Ebenfalls denkbar ist es, die Art der Authentifzierung, das aktuell verwendete Endgerät (Kiosk-PC oder persönliches Endgerät mit bestimmter Sicherheitsausstattung?) und die Absicherung der (drahtlosen) Internetverbindung als Eingangsparameter für die Zugriffskontrolle zu berücksichtigen. Auch der Status eines Dokuments („Freigegeben“/“Gesperrt“) kann eine Vorbedingung für einen mobilen Zugriff auf dieses sein.

5 Zusammenfassung und Ausblick

Im Beitrag wurde der im Rahmen des SumoDacs-Projektes verfolgte Ansatz für die Realisierung eines sicheren mobilen Zugriffs auf Unternehmensanwendungen beschrieben. Eine zentrale Rolle spielen hierbei Smartcards in für mobile Computer geeigneten Bauformen zur Kapselung wichtiger Sicherheitsfunktionen sowie eine kontextabhängige Zugriffskontrolle.
Eine nahe liegende Weiterentwicklung des beschriebenen Ansatzes ist es, die Unternehmensanwendungen gem. des Konzeptes des „Cloud Computing" in den Rechenzentren spezialisierter Anbieter auf virtualisierter Hardware zu betreiben und per Internet darauf zuzugreifen. Dieser Ansatz verspricht gerade für KMU erhebliche Kostenvorteile. Allerdings müssen hierzu sensible Firmendaten in fremde Hände gegeben werden. Der naive Ansatz, die Daten vor der Migration in die Cloud einfach komplett zu verschlüsseln ist nicht sinnvoll, da der Cloud-Anbieter in diesem Falle die Daten nicht mehr verarbeiten könnte. Der mobile Client müsste bei Anfragen also die kompletten verschlüsselten Daten herunterladen, um den relevant Datensatz zu finden, was natürlich in keiner Weise praktikabel ist. Die Auflösung dieses „Datenschutz-Paradoxons" ist eines der Hauptziele des Projektes MimoSecco[3], das gerade vom SumoDacs-Konsortium in Angriff genommen wurde. Ein im Projekt verfolgter Ansatz ist es etwa, die Daten so auf verschiedene unabhängige Cloud-Anbieter zu verteilen, so dass keiner alleine aus den bei ihm vorgehaltenen Daten Nutzen ziehen könnte.

Literatur

[Deck11] M. Decker: *Location-Aware Access Control: Scenarios, Modeling Approaches, and Selected Issues.* Kapitel 7 in (S. Ahson, & M. Ilyas, Hrsg.): Location-Based Services Handbook: Applications, Technologies, and Security. CRC-Press, Boca Raton, FL, USA, Seite 155-187.

[zdne08] zdnet.de: Warum Firmen Mobilität nutzen oder nicht nutzen. http://www.zdnet.de/it_business_strategische_planung_mittelstand_nutzt_potenzial_mobiler_loesungen_nur_teilweise_story-11000015-39197997-2.htm, Meldung vom 29.10.2008.

[Dour04] P. Dourish: *What we talk about when we talk about context.* Personal Ubiquitous Computing, Band 8, Nummer 1, Seite 19-30.

[KöKu99] O. Kömmerling, & Markus G. Kuhn: *Design Principles for Tamper-Resistant Smartcard Processors*. Proceedings of the USENIX Workshop on Smartcard Technology (Smartcard '99), Chicago, Illinois, USA, 1999, Seite 9-20.

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen *01IS09035C* gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

[3] „Middleware for Mobile and Secure Cloud Computing"; siehe auch http://www.mimosecco.de