MoTrust-TCG: Manipulationsschutz für mobile Signaturanwendungen mittels „Trusted Computing“

Ammar Alkassar
Sirrix AG , SB
a.alkassar@sirrix.com

Utz Gnaida
BSI, Bonn
utz.gnaida@bsi.bund.de

Thomas Quirin
Sirrix AG , Bochum
t.quirin@sirrix.com

Zusammenfassung: Gängige Betriebssysteme sind nach wie vor anfällig gegen die verschiedensten Arten von Schadsoftware. Die punktuellen Verbesserungen der Systeme haben die inhärenten Schwächen nicht zu lösen vermocht, wie die regelmäßig veröffentlichten Sicherheitslücken zeigen. Andererseits erfordern bestimmte Anwendungen – beispielsweise solche mit rechtsverbindlichen Transaktionen – den garantierten Ausschluss böswilliger Manipulationen. Dieser Kurzbeitrag zeigt, wie mit Hilfe von Trusted Computing-Mechanismen im Zusammenspiel mit einem High-Assurance Sicherheitskern eine Plattform für vertrauenswürdige Anwendungen auf mobilen Systemen realisierbar ist. In der konkreten Anwendung wird dabei nicht nur eine Signaturanwendung in einer geschützten Umgebung ausgeführt. Zudem werden Informationen über die Integrität des signierenden Systems integriert, die später bei der Verifikation der Signatur eine verlässliche Aussage über die Vertrauenswürdigkeit der Signaturanwendung zum Zeitpunkt der Signaturerstellung möglich macht.

1 Einleitung

Die Bedeutung des “Mobile Computing” hat in den letzten Jahren für Anwendungen aller Bereiche erheblich zugenommen - und ist dabei, selbst diejenigen Bereiche, die bisher stationären Systemen wie Workstations und Terminals zugeschriebene wurde, zu überholen. Gleichzeitig wird die vom Bundeskabinett initiierte eCard-Strategie [eCard05] mittelfristig dazu führen, dass die Verbreitung von Anwendungen, die auf eine vertrauenswürdige Einsatzumgebung angewiesen sind, stark ansteigen wird. Im Umfeld der elektronischen Gesundheitskarte (eGK) und des elektronischen Personalausweises (ePA) stellt die elektronische Signatur (eSig) – insbesondere die qualifizierte (QES) – eine solche besonders schützenswerte Anwendung dar.

Insbesondere die Effizienzsteigerung durch Abschaffung von Medienbrüchen und die gleichzeitige durch den Gesetzgeber geschaffene Rechtssicherheit haben zur Attraktivität der QES beigetragen. Von zentraler Bedeutung sind hierbei die hohen technischen und organisatorischen Anforderungen, auf denen die rechtliche Aussagekraft der QES unter anderem fußt.

Die zukünftige Entwicklung wird in starkem Maße mobile elektronische Signaturen in den Fokus rücken, für die eine breite Palette neuer Anwendungsmöglichkeiten mit deutlichem Mehrwert für alle beteiligten Nutzer existiert.

Mobile elektronische Signaturen fassen Anwendungen mit Signaturerstellung und -verifikation auf einem mobilen elektronischen Gerät wie Notebook, Smartphone, PDA oder Handy zusammen.

Untersuchungen der letzten Jahre (u. a. [GnBr03, Lang06]) haben bei Signaturanwendungen allerdings eklatante Sicherheitsmängel mit einem erheblichen Bedrohungspotenzial entdeckt, für die es auch gegenwärtig keine im Praxiseinsatz effektiven Schutzmaßnahmen gibt. Angreifer könnten damit beispielsweise signierte Dokumente erzeugen, die niemals durch den Benutzer autorisiert wurden.

Im Ergebnis bleibt es dem Anwender überlassen, wie er sicher stellt, dass die verwendete Signaturanwendung vor Manipulation etwa durch Schadsoftware effektiv geschützt wird, womit dieser regelmäßig überfordert ist.

MoTrust-TCG beschreibt einen Lösungsansatz, der die folgenden beiden Kernkonzepte vertrauenswürdiger Systeme einsetzt: Strenge Isolation der Prozesse und Beglaubigung („Attestierung“) der Plattform, wodurch eine Aussage über die Vertrauenswürdigkeit des Gesamtsystems getroffen werden kann. Beide Konzepte sollen zur Demonstration der Machbarkeit mit Hilfe der Plattform TURAYA in Form von Prototypen am Beispiel einer Signaturanwendung auf einem mobilen System umgesetzt werden. Hierbei wird aus Gründen der Verfügbarkeit zunächst ein Notebook-Computer mit Trusted Platform Module [TPM] verwendet, in einer späteren Phase des Projekts soll dann ein ultramobiles System (Mobiltelefon bzw. PDA) eingesetzt werden. Die Plattform TURAYA (http://www.turaya.de) ist ein Sicherheitskern mit Trusted Computing-Unterstützung. Unter einem vertrauenswürdigen System versteht man dabei eines, das sich erwartungsgemäß verhält, insbesondere im Hinblick auf die Erfüllung bestimmter Sicherheitseigenschaften.

Dabei wird das bisherige Benutzerbetriebssystem von den Signaturanwendungen und den Visualisierungskomponenten getrennt und der gegenseitige Zugriff beschränkt und kontrolliert. Einer Malware oder gar Crimeware, die möglicherweise das Benutzerbetriebssystem infiziert hat, wird damit effektiv jegliche Möglichkeit genommen, die Signaturanwendung zu manipulieren. Gleichzeitig werden die Kommunikationsverbindungen zwischen den einzelnen Komponenten geschützt. Dies umfasst die Kommunikation zwischen Signaturanwendung und Benutzer (“Trusted Path”) genauso wie die Kommunikation zwischen Signaturanwendung und beispielsweise einer Signaturkarte (“Trusted Channel”).

Durch dieses fundamentale Schutzprinzip werden sowohl die Signier- (“Trusted Signer”) als auch die Verifizierkomponenten (“Trusted Viewer”) geschützt.

Die Beglaubigung des Systems ermöglicht in einem zweiten Schritt die Verknüpfung einer Signatur mit dem System, auf dem es erzeugt worden ist, und dessen Konfiguration. Damit wird bei der Erzeugung einer Signatur nicht nur das Dokument signiert, sondern auch ein Nachweis angehängt, der es einem Verifzierer zu einem späteren Zeitpunkt ermöglicht, verlässlich nachzuvollziehen, auf was für einem System die Signatur erzeugt worden ist.

Er kann beispielsweise feststellen, dass die Signatur auf einem geschützten oder ungeschützten System erzeugt worden ist, und darauf basierend entscheiden, ob er die Signatur akzeptieren möchte oder nicht. Für einen Einsatz in der Praxis ist dann allerdings ein geeignetes Konzept zur Einbeziehung einer vertrauenswürdigen Instanz ("Trusted Third Party") erforderlich, beispielsweise durch eine Public-Key Infrastruktur (PKI), auf die in dieser Studie nicht näher eingegangen wird.

Im Ergebnis steht damit eine Architektur bereit, die geeignet ist, inhärente Schwächen besonders schützenswerter Anwendungen wie elektronische Signaturen auf mobilen Endgeräten zu beseitigen. So kann der vorliegende Lösungsansatz das Vertrauen der Benutzer in diese wichtigen Anwendungen und damit die Akzeptanz wirkungsvoll erhöhen.

2 Trusted Computing und Sicherheitskern

Bestehende Computerplattformen können aktuellen Sicherheitsanforderungen nicht mehr genügen. Dies verdeutlicht die große Anzahl von Sicherheitslücken und Angriffe von Viren, Würmer und Trojaner. Die konzeptionellen Schwächen der Plattformen konnten in den letzten Jahren nicht verbessert werden. Betroffen sind Windows, sowie auch auf Unix basierende Plattformen. Für ultramobile Plattformen wie Windows Mobile oder Symbian ist eine im Grundsatz vergleichbare Tendenz festzustellen.

2.1 Sicherheitskern und Isolation von Prozessen

Eine inhärente Schwäche gängiger Betriebssysteme ist deren monolithische Struktur, mögliche Sicherheitslücken gefährden sehr schnell die Sicherheit des gesamten Systems. Die für die Sicherheit einer Anwendung relevanten Codeteile, die so genannte Trusted Computing Base (TCB), umfasst dabei schnell das gesamte System mit mehreren Millionen Zeilen Code. Sicherheitseigenschaften hierfür zu *garantieren* ist praktisch unmöglich. Die Sicherheitsverbesserungen beschränken sich daher meist auf die Schließung punktueller Sicherheitslücken.

Die Lösung bildet ein kompakter Sicherheitskern [HASK2007], der kritische Komponenten vom restlichen Betriebssystem trennt und eine strenge Prozess- und Speicherbereichsisolierung durchsetzt. Eine solche Sicherheitsplattform, Turaya [ASSS05], wurde im Rahmen des Projektes European Multilaterally Secure Computing Base (EMSCB) entwickelt. Turaya ist eine offene, mehrseitige sichere Sicherheitsplattform, die in der Lage ist, Sicherheitsrichtlinien verschiedener Parteien eines IT-Systems unter Ausschluss von Konflikten durchzusetzen.

2.2 Trusted Computing

Eine weitere Grundanforderung an vertrauenswürdigen Plattformen ist deren Fähigkeit, verbindliche Aussagen über die eigene Integrität zu treffen.

Dies ist durch softwarebasierte Mechanismen alleine nicht möglich. Erforderlich ist ein manipulationsfreier Sicherheitsanker, der die verschiedenen Systemkomponenten (BIOS, Bootsektor, Betriebssystemkern, etc) überprüfen kann. Die Trusted Computing Group (TCG) hat mit dem Trusted Platform Module [TPM] einen solchen, hardwarebasierten Sicherheitsanker spezifiziert, der bereits zu einem großen Anteil in heutigen Rechnersystem integriert ist.

Das TPM ähnelt einer Smartcard, mit sicheren Mechanismen zur Erzeugung, Verarbeitung und Speicherung kryptographischer Schlüssel. Im Gegensatz zu einer Smartcard ermöglicht ein TPM (mit einem entsprechen angepassten BIOS) allerdings einen vertrauenswürdigen Bootvorgang („ Authenticated Boot“), der die Integrität des Systems erfasst und in der Lage ist, einem anderen, möglicherweise entfernten, System die eigene Softwarekonfiguration und den Status nachzuweisen („Remote-Attestation“).

3. Gefährdungen elektronischer Signaturanwendungen

“Ein System ist nur so sicher wie sein schwächstes Glied es ist”. Dies gilt auch und insbesondere für besonders schützenswerte Systeme wie Signatursysteme. Die hohen Anforderungen an die Signaturinfrastruktur, an die Chipkarten und an die Schlüsselerzeugung sind von nur begrenztem Wert, wenn der Benutzerrechner so “löchrig” ist, dass dort mit lohnenswertem Aufwand zu signierende Daten manipuliert werden können, ohne dass sich der Benutzer effektiv davor schützen kann. Wie einleitend bereits erwähnt, haben Untersuchungen [GnBr03, Lang06] gezeigt, dass die heute verfügbaren Signaturanwendungskomponenten keinen ausreichenden Schutz gegen realistische Angriffsszenarien bieten. Dies birgt insbesondere im Hinblick darauf, dass mit Hilfe dieser Komponenten in der Regel qualifizierte elektronische Signaturen erzeugt werden, die handschriftlichen Unterschriften gleichgestellt und in einem Rechtsstreit nicht ohne Weiteres abstreitbar sind, ein äußerst hohes Risikopotenzial, das dem Nutzer auferlegt wird und weshalb die Akzeptanz von elektronischen Signaturen nur schleppend zunimmt.

Kernproblem ist dabei die mangelnde Vertrauenswürdigkeit der Ein-/Ausgabekanäle sowie die unsichere Kommunikation der Komponenten untereinander, die möglichen Angreifern zahlreiche Angriffsflächen bieten:

- PIN oder Passphrase wird während der Eingabe ausgespäht
- WYSIWYS-Prinzip verletzt: Der Nutzer signiert tatsächlich andere Inhalte als ihm vor dem Signaturvorgang dargestellt werden oder signiert Inhalte, die er nicht kennt.
- Ein Signaturvorgang erfolgt außerhalb der Kontrolle des Nutzers
- Die Verifizierung und/oder Validierung ergibt ein unrichtiges Ergebnis

4. Realisierung einer vertrauenswürdigen Signaturumgebung

Um eine sichere Kommunikation zwischen den Komponenten zu gewährleisten, müssen zwei zentrale Konzepte umgesetzt werden. Zum einen garantiert das Konzept des "Trusted Channel" eine sichere Kommunikation zwischen den einzelnen Soft- und Hardwarekomponenten. Zum anderen ist ein "Trusted Path", ein vertrauenswürdiger Kanal zwischen dem Benutzer und einer Softwarekomponente, notwendig.

Mit Hilfe des Sicherheitskerns Turaya werden kritische Softwarekomponenten isoliert und der Datenfluss zwischen den Komponenten kontrolliert. Zur Realisierung einer vertrauenswürdigen Signaturanwendung werden vier isolierte Compartments eingerichtet:

- eine Arbeitsumgebung (signierte Dokumente werden hier empfangen und gehalten)
- ein Trusted Signer (eine Signaturerzeugungskomponente)
- ein Trusted Viewer (Anwendung zur Anzeige des Dokuments und des Signaturverifikationsergebnisses)
- ein Kontrollserver (überprüft/verwaltet die Verbindung zwischen den einzelnen Compartments und stellt die Vertraulichkeit der ausgetauschten Daten sicher)

Durch Trusted Booting wird Turaya mit den vier erläuterten Compartments gestartet und in einen definierten Zustand gebracht. Anschießend wird das zu signierende Dokument in ein geeignetes Format (PDF/A) gewandelt, das die Gefahr einer unterschiedlichen Darstellung der Inhalte reduziert. Danach wird es in der Signaturerzeugnungskomponente digital unterschrieben und im Trusted Viewer angezeigt. Erst nach Überprüfung des Dokuments auf Manipulation durch den Benutzer wird das signierte Dokument der Arbeitsumgebung übergeben.

Ferner ist es möglich, dem Empfänger des Dokumentes nachzuweisen, dass das Dokument vor dem Signieren dem Benutzer auf vertrauenswürdige Weise dargestellt wurde. Dies erfolgt mit Hilfe eines Plattformzertifikates, in dem ein Abbild (Hash) aller kritischen Systemkomponenten, der Signaturanwendung sowie der Signatur des Dokuments enthalten ist und welches durch den Sicherheitsanker (TPM) signiert wird. Es „attestiert" so den Zustand des IT-Systems während des Signiervorgangs. Der Empfänger kann sich das signierte Dokument im Trusted Viewer darstellen lassen und die Signatur überprüfen. Durch Nachfrage bei einem Verzeichnisdienst kann er ggf. nachschlagen, ob das erzeugende IT-System sich in einem vertrauenswürdigen (d. h. bekannten) Zustand zum Zeitpunkt des Signaturvorganges befunden hat.

5. Fazit

Das vorgestellte Konzept erlaubt mit Hilfe von Trusted Computing-Mechanismen und der Turaya-Architektur vertrauenswürdige Signaturen zu erstellen und zu verifizieren. Das bei Signaturanwendungen für den manuellen Betrieb zu fordernde "What You See Is What You Sign"-Prinzip wird realisiert durch eine Überprüfungsmöglichkeit des zu signierenden Dokuments über einen vertrauenswürdigen Pfad durch den Benutzer. Manipulationen am Dokument vor oder während des Signaturvorgangs lassen sich damit weitgehend ausschließen. Außerdem wird der Empfänger in die Lage versetzt, verlässliche Aussagen über den Zustand des signierenden Systems zu erhalten.

Literaturverzeichnis

[ASSS05] Ammar Alkassar, Marcel Selhorst, Ahmad-Reza Sadeghi, Chris Stüble: Towards Secure Computing Platforms with Open-Source and Trusted Computing. In: Tagungsband zum 9. Deutschen IT-Sicherheitskongress. Bad Godesberg : SecuMedia Verlag, Mai 2005

[eCard05] BUNDESREGIERUNG: Chipkarten-Strategie der Bundesregierung (eCard-Strategie). http://www.bmwi.de/BMWi/Redaktion/PDF/E/ecard-strategie,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf, 2005

[GnBr03] Utz Gnaida, Jürgen Brauckmann: Jürgen: Sichere Signaturinfrastruktur - Risikoananalyse. interne, unveröffentlichte Studie, Bundesamt für Sicherheit in der Informationstechnik, 2003

[HASK07] Protection Profile for a High-Assurance Security Kernel (HASK-PP). To be published, March 2008

[Lang06] Hanno Langweg: Malware Attacks on Electronic Signatures Revisited. In: Sicherheit, 2006, S. 244–255

[SG97] Gesetz zur digitalen Signatur, Artikel 3 des Gesetzes „Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste", 1997

[TPM] TRUSTED COMPUTING GROUP (TCG): TCG Specification Architecture Overview. https://www.trustedcomputinggroup.org/groups/TCG_1_4_Architecture_Overview.pdf, 2007