Privacy-Preserving Protokolle und Anwendungen für vertrauenswürdige Plattformen

Hans Löhr, Oktober 2011

Kurzzusammenfassung. Der *Schutz der Privatsphäre* ist eine essentielle Vorbedingung für eine funktionierende freie und demokratische Gesellschaft. Aktuelle Trends in der Informations- und Kommunikationstechnologie – insesondere, das Auslagern von IT-Diensten, Berechnungen und Datenspeicher in die ,,Cloud" – stellen große Herausforderungen für den Schutz der Privatsphäre der Endbenutzer dar. *Trusted Computing (TC)* ist ein Paradigma in der IT-Sicherheit, in welchem eine Kombination von vertrauenswürdiger Hard- und Software verwendet wird, um die Sicherheit des Gesamtsystems zu verbessern. Da die Sicherheit eines Systems eine notwendige Vorbedingung für effektiven Schutz der Privatsphäre ist, kann TC-Technologie hier Vorteile bringen. Jedoch führt vertrauenswürdige Hardware wie das Trusted Platform Module (TPM) auch eindeutige Bezeichner und kryptografische Schlüssel ein, die wiederum zu neuen Privacy-Problemen führen können.

Diese Dissertation behandelt Sicherheit und Privatsphäre in verschiedenen Anwendungsszenarien und auf unterschiedlichen technischen Ebenen. Die wissenschaftlichen Beiträge dieser Arbeit beinhalten mehrere kryptografische privacy-preserving Protokolle sowie TC-basierte Sicherheitsarchitekturen welche zum Datenschutz und für die Wahrung der Privatsphäre eingesetzt werden können. Insbesondere beinhaltet diese Dissertation folgendes:

Wir schlagen zwei kryptografische Verfahren für untrennbare privacy-preserving Multi-Coupons vor, die ein elektronisches Äquivalent zu Couponheftchen aus Papier darstellen. Das erste Verfahren erzwingt die Einlösung der Coupons in einer vorbestimmten Reihenfolge, wohingegen das Zweite dem Benutzer erlaubt, die Coupons in beliebiger Reihenfolge einzulösen und außerdem das Erste verallgemeinert, so dass mehrere kooperierende ,,Händler" unterstützt werden. Beide Lösungen bieten Unverknüpfbarkeit von Benutzertransaktionen, ähnlich wie bei existierenden Couponheftchen aus Papier.

Wir stellen zwei Protokolle für *property-based attestation (PBA)* vor, die einem Verifizierer beweisen, dass eine Plattform eine gegebene Eigenschaft bietet, ohne die genaue Plattformkonfiguration offen zu legen. Das erste PBA-Protokoll verwendet Zertifikate einer vertrauenswürdigen Partei, die Konfigurationen mit einer bestimmten Eigenschaft zertifiziert. Basierend hierauf beweist die Plattform dem Verifizierer, dass ihre aktuelle Konfiguration die gewünschte Eigenschaft bietet. Das zweite Protokoll benötigt keine Zertifizierungsstelle. Hier beweist die Plattform dem Verifizierer, dass ihre Konfiguration in einer Menge akzeptierter Konfigurationen enthalten ist. Beide Protokolle benutzen eine vertrauenswürdigen Hardwarekomponente: ein leicht modifiziertes TPM.

Wir zeigen, wie die Standardprotokolle *Transport Layer Security (TLS)* und *Direct Anonymous Attestation (DAA)* kombiniert werden können, um anonym authentifizierte, sichere Kommunikationskanäle zu erhalten. Ein Vorteil dieser Lösung ist, dass DAA von aktuellen TPMs unterstützt wird, welche die Authentifizierungs-Credentials per Hardware schützen. Daher können legitime Benutzer, im Gegensatz zu reinen Softwarelösungen, nicht einfach diese Credentials kopieren und weitergeben.

Wir stellen eine *Sicherheitsarchitektur für verteiltes Rechnen* vor, welche die Verwendung von Standard-Grid-Lösungen in virtuellen Maschinen erlaubt, die auf einer vertrauenswürdigen Virtualisierungsschicht laufen. Hierzu wird ein TPM in Verbindung mit Virtualisierungstechnologie verwendet, um Vertraulichkeit und Integrität von Grid-Berechnungen und -Daten zu erreichen. Außerdem schlagen wir ein Verfahren zur *offline Attestierung* vor, wobei Kunden ihre Grid-Jobs durch (von Grid-Providern veröffentlichte) sogenannnte ,,attestation tokens" an sichere Plattformen binden können.

Mit *Trusted Privacy Domains* wird ein umfassendes Framework zum Schutz privater Daten eingeführt, das in vielen Szenarien, u.a. im Cloud-Computing, eingesetzt werden kann. Technisch basieren diese Privacy Domains auf dem Konzept der Trusted Virtual Domains (TVDs), welche zur Durchsetzung und zum Management von Privacy-Policies genutzt werden. Hier führen wir Sicherheitsprotokolle ein, um TVDs auf einer Plattform zu etablieren und um virtuelle Maschinen (,,Compartments") in eine TVD aufzunehmen. Diese Protokolle garantieren, dass alle Plattformen und virtuellen Maschinen einer TVD der TVD-Policy entsprechen. Außerdem präsentieren wir eine TVD-Implementierung auf OpenSolaris sowie eine Schlüsselmanagement-Lösung um mobile Speichergeräte in einer TVD transparent zu verschlüsseln. Des weiteren wird skizziert, wie Privacy Domains helfen können, Patientendaten in der ,,E-Health-Cloud" zu schützen.

Um die Authentifikationsdaten von Benutzern von Web-Services zu schützen schlagen wir eine Sicherheitsarchitektur vor, die auf TC und Virtualisierung basiert. Hierbei speichert ein *vertrauenswürdiges ,,Wallet" (TruWallet)* die Authentifikationsdaten und führt automatische Logins durch. Darüber hinaus zeigen wir, wie ein *mobiles* Wallet die Sicherheit in E-Health-Szenarien verbessern kann.