Security and Trust Architectures for Protecting Sensitive Data on Commodity Computing Platforms

Marcel Winandy

- Kurzfassung -

Viele Computer-Anwendungen benötigen eine sichere Ausführungsumgebung, um die Vertraulichkeit und Integrität ihrer Daten zu schützen. Obwohl es bereits verschiedene Ansätze in der Kryptographie und in der Anwendungssicherheit gibt, schlagen diese in der Praxis letztendlich fehl aufgrund unsicherer Betriebssysteme und falscher Annahmen bezüglich der Vertrauenswürdigkeit der zugrunde liegenden Plattformen.

Die Entwicklung sicherer Betriebssysteme war und ist immer noch ein komplexes Problem. In der Vergangenheit entwickelte sich deshalb die Idee des *Sicherheitskerns*: Alle relevante Sicherheitsfunktionalität wurde innerhalb eines kleinen Kerns implementiert, der folgende Eigenschaften hatte: komplette Kontrolle über alle Objekte; Selbstschutz gegen Manipulation; und geringe Codegröße zur Erleichterung einer formalen Verifikation. Es stellte sich jedoch heraus, daß selbst die Konstruktion einer solchen kleinen vertrauenswürdigen Basis in der Praxis bereits aufwendig und schwierig war. Zudem wiesen frühe Implementierungen eine sehr schlechte Performanz auf. Daher ist die Idee des Sicherheitskerns nie in die Entwicklung von Standardbetriebssystemen eingeflossen.

In dieser Dissertation präsentieren wir Sicherheitsarchitekturen, die in der Lage sind, sensible Daten auch auf gewöhnlichen (PC-)Computerplattformen zu schützen. Die Integration von *Trusted Computing* Technologie in heutige Standardplattformen erlaubt die Einbettung zusätzlicher Sicherheitsfunktionen direkt in die Hardware. Außerdem besitzen moderne Prozessoren hardware-seitig unterstützte Virtualisierungstechnologie. Basierend auf diesen Funktionalitäten, sowie neuer Ergebnisse zur Konstruktion von Mikrokernen, verwenden wir die Idee der Sicherheitskerne wieder und entwerfen Sicherheitsarchitekturen, die Endbenutzer verwenden können, um ihre Systeme und ihre Daten gegen eine Vielzahl von Bedrohungen zu schützen.

Ein erster Beitrag dieser Arbeit ist die Verbesserung von Sicherheitsarchitekturen, die Virtualisierung verwenden. Ein wichtiger Aspekt in diesem Kontext ist die Virtualisierung von Hardware-Sicherheitsmodulen wie die des Trusted Platform Module (TPM). Wir präsentieren daher das *property-based vTPM*, ein flexibles und datenschutz-erhaltendes virtuelles TPM. Es integriert verschiedene Ansätze zur Ermittlung des Integritätszustandes einer Plattform und zur Erstellung von kryptographischen Schlüsseln. Dies ermöglicht einen flexibleren Umgang mit Softwareupdates und Migration von virtuellen Maschinen bei gleichzeitiger Beachtung der erforderlichen Sicherheitseigenschaften.

Ein weiterer Beitrag ist der Entwurf und die Implementierung einer Sicherheitsarchitektur gegen Phishing-Angriffe, d.h. Angriffe, die versuchen Passwörter eines Benutzers zu stehlen. Die Hauptidee hierbei ist ein *trusted password wallet (TruWallet)*, das sich anstelle des Benutzers um den Login-Vorgang auf Webseiten kümmert. Dazu speichert TruWallet sicher alle Passwörter des Benutzers und führt die Login-Vorgänge aus. Im Gegensatz zu anderen Ansätzen liefert TruWallet Schutz gegen die stärkste Art des Phishing-Angriffs, nämlich gegen Phishing-Malware, die auf dem Rechner des Anwenders läuft.

Wir zeigen ferner eine Sicherheitsarchitektur, um über mehrere Plattformen hinweg gemeinsam genutzte Informationen zu schützen. Diese Architektur basiert auf dem Konzept von *Trusted Virtual Domains (TVDs)* und realisiert im wesentlichen eine verteilte Informationsflußkontrolle. Wir erweitern dieses Konzept über die übliche Verwendung in Rechenzentren hinaus und beziehen auch Plattformen von Endanwendern ein. Um deren spezielle Anforderungen zu berücksichtigen, entwerfen wir eine transparente Verschlüsselung von mobilen Datenträgen (z.B. USB-Sticks), die konform zu einer gegebenen Informationssicherheitspolitik arbeitet. Außerdem evaluieren wir eine vollständige Implementierung des TVD-Konzepts auf einem existierenden Desktop-Betriebssystems.

Schließlich schauen wir uns einige besondere Anwendungsszenarien an, die zwar ebenfalls eine vertrauenswürdige Plattform benötigen, aber nicht notwendigerweise einen permanent laufenden Software-Sicherheitskern. Dazu nutzen wir die erweiterten Funktionen moderner Hauptprozessoren, um eine sichere Ausführungsumgebung bereitzustellen, auf der wir einen *Unidirectional Trusted Path (UTP)* realisieren, d.h. einen vertrauenswürdigen Kommunikationspfad in nur eine Richtung: vom lokalen Anwender zu einer entfernten Partei. Wir evaluieren eine vollständige Implementierung dieses Ansatzes und zeigen, daß UTP eine Alternative für CAPTCHAs sein kann und daß man damit eine sichere Transaktionsbestätigung für Online-Einkäufe realisieren kann.