Zusammenfassung

Im Gegensatz zu fast allen anderen Aspekten unseres täglichen Lebens ist die Kontrolle des Zugangs zu und der Verbreitung von privaten Daten durch den Einsatz von Computersystemen *nicht* einfacher geworden. Ist Information auf einem Blatt Papier oder einem klassischen, chemisch entwickelten Film noch relativ einfach zu kontrollieren – dem Medium kann vertraut werden, dass es sich exakt so verhält, wie es der Benutzer erwartet – gilt dies nicht uneingeschränkt für Daten, die auf heutigen Computersystemen gespeichert und verarbeitet werden: Der Benutzer hat keinerlei Garantie bezüglich Verhalten und Sicherheit des Systems. Ansätze dies zu ändern resultierten in der Forschung der vergangenen Jahre vielfach im vollständigen Überbordwerfen bestehender Architekturen; ein Migrationspfad von existierenden Systemen hin zu besser kontrollierbaren Umgebungen ist daher häufig lang und nicht in jedem Fall gegeben.

Angesichts dessen beschäftigt sich die vorliegende Arbeit mit der Frage, wie und unter welchen Bedingungen die Kontrolle über private Daten auf *existierenden* Computersystemen verbessert werden kann. Der Autor argumentiert, dass zumindest drei Vorbedingungen erfüllt sein müssen, damit grundsätzlich die Möglichkeit besteht, Kontrolle über die auf einem Computersystem gespeicherten und verarbeiteten Daten zu behalten: proaktive Erforschung potentieller Angriffsvektoren, Kenntnis der genauen Funktionsweise des zu schützenden Systems durch dessen Analyse und, auf basierend auf beidem, die Verfügbarkeit von Erkennungs- und, wenn möglich, Schutzmechanismen. Am Beispiel des offensiven Potential des scheinbar harmlosen SVG-Datenformats zeigt die vorliegende Arbeit, wie proaktive Schwachstellenforschung dazu geeignet ist, neuartige Schutzmaßnahmen zu entwickeln, bevor Angreifer sich global existierende Mängel in existierenden Standards und Software zu Nutze machen können. Die Arbeit beschäftigt sich im Weiteren mit der Analyse der kryptographischen Protokolle des Sofortnachrichtendiensts TextSecure, um auf Basis der vollständigen Kenntnis des Systems eine Aussage über die tatsächlich gebotene Sicherheit zu treffen. Auffälligkeiten in der Verwendung kryptographischer Primitive werden aufgezeigt, ebenso wie daraus resultierende Angriffe und wie diese zu verhindern sind. Im Folgenden behandelt die Arbeit die dritte oben genannte Bedingung für den Erhalt der Kontrolle über auf Computersystemen gespeicherte Daten: Die Fähigkeit Angriffe zu erkennen, ihren Effekt zu begrenzen und sie nach Möglich zu verhindern. Unter diesem Aspekt wird ein System vorgestellt, dass auf Basis heuristischer Methoden und maschinellem Lernen die Erkennung von Schadcode auf Webseiten direkt im Browser des Benutzers erlaubt. Relevante Elemente bösartiger Webseiten können hierbei so modifiziert werden, dass der Angriff nicht zur Ausführung kommt. Die vorgestellten Techniken haben dabei ein weiteres Anwendungsfeld – die Natur der zu schützenden Daten ist hier schlussendlich unter technischen Aspekten nicht maßgeblich – die vorliegenden Arbeit legt den Fokus jedoch auf den Erhalt der Kontrolle über private Daten.

Bis zu diesem Punkt hat sich die vorliegende Arbeit auf die nachträgliche, systemerhaltende Integration von Schutzmaßnahmen fokussiert. Gerade jedoch in Technologiefeldern, die fester Bestandteil des täglichen Lebens sind, wie z.B. mobile Kommunikationsnetze oder individuelle Mobilität, ist es mit dem nachträglichen Erweitern existierender Systeme um Sicherheitskomponenten nicht getan. Ist die Verwendung einer Technologie für den Benutzer (nahezu) alternativlos, darf Sicherheit und der Schutz privater, persönlicher und personenbeziehbarer Daten kein Additiv, sondern muss integraler Bestand der Technologie sein, ohne in funktionalen Einschränkungen zu resultieren. Wie dieses Ziel zu erreichen ist, wird am Beispiel der im Aufbau befindlichen Ladeinfrastruktur für Elektrofahrzeuge verdeutlicht. Die vorliegende Arbeit zeigt, wie die authentische Übermittlung von abrechnungsrelevanten Daten sichergestellt und dennoch verhindert werden kann, dass ein detailliertes Bewegungsprofil jedes einzelnen Benutzers anfällt.