CanSecWest: Angreifbare Schutzmechanismen

Sandkästen

Bernd Wernerus

Anfang März lockte im kanadischen Vancouver die CanSecWest, eine der wichtigsten Konferenzen für angewandte Sicherheit. Erfolgreiche Angriffe auf Sandboxes oder TPMs demonstrierten, dass auch etablierte Sicherheitsmechanismen nicht zwangsläufig unüberwindbar sind.

Gleich zwei Vorträge bei der Sicherheitskonferenz CanSecWest beschäftigten sich mit Sandboxen, die in vielen Sicherheitsarchitekturen und -systemen etabliert sind: „Sandbox Escapes: When the Broker is Broken" von Peter Vreugdenhil sowie „Reflecting on Reflection – Exploiting Reflection Vulnerabilities in Managed Languages" von James Forshaw. Ersterer erklärte anschaulich, wie die Sandbox im Adobe Reader, die wiederum auf der Chrome-Sandbox basiert, analysiert und geknackt werden kann. Hierzu verfolgte Vreugdenhil die Aufrufe der innerhalb der Sandbox zur Verfügung stehenden Funktionen bis hin zum Weiterleiten in den Betriebssystemkern. James Forshaw ging in seinem Vortrag auf die Sandboxen von Managed Languages am Beispiel von Java und .NET ein. Hier zeigte er, welche Sicherheitsprobleme für eine Sandbox durch die Sprachfunktionen Reflection oder Delegates entstehen: Verschiedene interne Methoden der Sprachen können benutzt werden, um aus einer Sandbox auszubrechen, wenn die Sicherheitsprüfungen für Reflection oder Delegates unzureichend oder fehlerhaft implementiert sind.

Die Sicherheit von Trusted Module Platforms (TPM) thematisierten die Vorträge von Yuriy Bulygin, Oded Horovitz und Steve Weis. Sie zeigten Angriffe auf den Sicherheits-Chip auf verschiedenen Ebenen. Bulygin belegte, dass der heutzutage gängige Einsatz von Festplattenverschlüsselung auch in Verbindung mit einem TPM nicht automatisch sicher ist. Vielmehr muss auch die Entschlüsselung sicher erfolgen und darf beispielsweise nicht transparent stattfinden, sondern erst nach einer erfolgreichen Prä-Boot-Authentifizierung.

Kein Garant für Sicherheit

Horovitz und Weis beschäftigten sich mit der Sicherheit von TPMs im Allgemeinen und zeigten, dass auch diese keinen 100%-Schutz für die darin enthaltenen Schlüssel bietet. Darüber hinaus stellten sie weitere Möglichkeiten vor, ein System über Hardwareschnittstellen zu übernehmen – unter anderem, wie man mit präparierten PCI-Karten direkt auf den Hauptspeicher zugreifen kann. Hierzu verwendeten sie eine PCI-Steckkarte, die wiederum als eigenständiges System mit eigenem Linux-OS funktioniert.

Als wenig geeignet für Paranoiker, die Missbrauch von in Geräten eingebauten Kameras befürchten, erwies sich der Vortrag „Smart TV Security" von SeungJin Lee. Er zeigte, dass aktuelle Smart-TVs die gleichen Sicherheitsschwächen wie Smartphones der ersten Generation aufweisen: Angreifer können mit relativ wenig Aufwand das System über verschiedene Schnittstellen übernehmen und steuern. In SeungJin Lees Demonstration verwendete das System eine veraltete Browser-Engine und brachte Zugriff auf den App-Store des Herstellers mit. Einige Apps daraus wurden auf dem System im Root-Kontext ausgeführt und konnten nativen Code ausführen.

Obendrein ließ sich auf dem Smart-TV ein Rootkit installieren, mit dem das Gerät mittels des eingebauten Mikrofons sowie der eingebauten Kamera seine Umgebung überwachen kann, ohne dass der Benutzer das merkt. (ur)