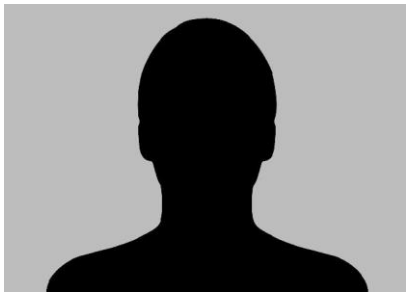
Zürcher Hochschule
für Angewandte Wissenschaften

School of Engineering

InIT Institut für angewandte Informationstechnologie

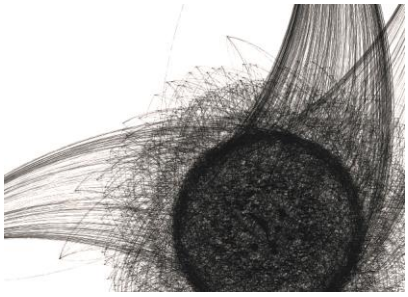
FirmwareDroid - Security Analysis of the Android Firmware Eco-System



Diplomand/in
Thomas Sutter

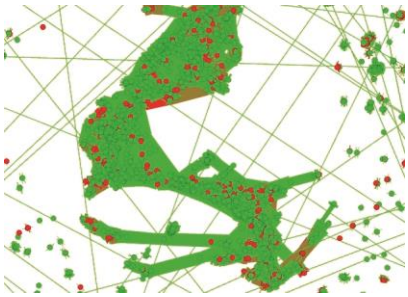
Dozent/in
Bernhard Tellenbach

Das Android Open Source Project (AOSP) ist das wohl am häufigsten verwendete Betriebssystem für Smartphones und IoT-Geräte weltweit. Sein Marktanteil und seine hohe Anpassungsfähigkeit machen Android zu einem interessanten Betriebssystem für viele Entwickler. Heutzutage wird Android-Firmware in Smartphones, Fernsehern, Smartwatches, Autos und anderen Geräten von verschiedenen Anbietern und Herstellern verwendet. Die schiere Menge an Android-Firmware und -Geräten macht es für Sicherheitsanalysten schwierig, potenziell schädliche Anwendungen zu erkennen. Der Fakt, dass viele Hersteller Apps von Drittanbietern in ihre Firmware einbinden, macht es zudem schwierig, Android Firmware zu analysieren. Vorinstallierten Apps haben in der Regel mehr Berechtigungen als Standard-Apps und können vom Benutzer nicht einfach entfernt werden. In den Medien wurde in den letzten Jahren über mehrere Fälle berichtet, in denen vorinstallierte bösartige Apps in Android Firmware gefunden wurde. Medienberichte behaupten, dass vorinstallierte Malware wie Chamois und Triade in der Lage waren, mehrere Millionen Geräte zu infizieren. Solche Fälle zeigen die Notwendigkeit besserer Strategien zur Analyse von Android Firmware.



Ausschnitt eines Fuzzy-Hashing Clusters mit mehreren Tausend Android apps.

In dieser Studie haben wir das Android-Firmware-Ökosystem auf verschiedene Arten analysiert. Es wurde ein Datensatz mit mehreren Tausend Android-Firmware-Archiven erstellt und aufgezeigt, dass mehrere Terabytes an Firmware-Daten im Web darauf warten, analysiert zu werden. Wir entwickeln einen Webservice namens FirmwareDroid zur Analyse von Android-Firmware-Archiven und vorinstallierten Apps und automatisieren den Prozess des Extrahierens und Scannens vorinstallierter Apps mit state-of-the-art Open-Source-Tools.



Ausschnitt eines Fuzzy-Hashing Clusters mit bösartigen Android apps dargestellt in rot.

Als Ergebnis dieser Studie wird aufgezeigt, dass viele vorinstallierte Apps tatsächlich eine Bedrohung für Android-Nutzer darstellen. In der Studie wurden mehr als 900.000 Apps analysiert und wir geben den Lesern einzigartige Einblicke in das Android Firmware Eco-System. Es wird gezeigt, wie mehrere tausend Malware-Samples mit Scannern wie VirusTotal, AndroGuard, und APKiD entdeckt werden konnten. Zudem wird aufgezeigt, wie Fuzzy-Hashing-Algorithmen genutzt werden können, um Ähnlichkeiten zwischen Binärdateien zu erkennen. Wir erläutern die Herausforderungen der dynamischen Analyse von vorinstallierten Android-Apps und diskutieren die Grenzen von Fuzzy-Hashing-Algorithmen zur Ähnlichkeitserkennung von Binärdaten.