NSA verschafft Android-Smartphones mehr Sicherheit

Abgeschlossen

Christoph Puppe

Linux' Rechtemodell – und damit auch das von Android – ist zwar erprobt, bietet aber nur wenige Differenzierungsmöglichkeiten. Das möchte die NSA mit einer Portierung der Konzepte von SELinux auf Googles Mobilplattform ändern. Ein Statusbericht.

Unter Linux erfolgt die Zugriffsteuerung des Betriebssystems nach einem DAC-Modell (Discretionary Access Control). Dies ist zwar erprobt, wird aber dennoch nicht gelobt, denn DAC erlaubt nur recht grobe Unterteilungen. Mandatory Access Control (MAC) hat feinere Regeln und schützt daher die Daten effizienter. Zwar hat Android als Linux-Ableger das DAC-Konzept geerbt, doch die NSA verschafft Android nun MAC-Fähigkeiten, indem sie das auch unter ihrer Ägide entwickelte Security Enhanced Linux (SELinux, siehe „Alle Links") auf Android portiert hat. Auf MAC aufbauend, soll SE Android Betriebssystem und Apps vor Exploits, Trojanern und Ähnlichem schützen. Android ist mit der NSA-Erweiterung von allen Betriebssystemen das mit den meisten Sicherheitsoptionen. Da fast alles Open Source ist, kann jeder nachsehen, ob es Backdoors oder Verwundbarkeiten gibt. Ob dies im Alltag Benutzer und deren Daten schützt, will dieser Artikel klären.

Die National Security Agency (NSA) – früher scherzhaft als „No such Agency" bezeichnet, da sie so geheim war, dass die Regierung sogar die Existenz leugnete – ist seit vielen Jahren stark in die Verbesserung der IT-Sicherheit involviert. Analog zum deutschen BSI veröffentlicht sie Anleitungen zum Absichern von Servern, zertifiziert Sicherheitsverfahren und beteiligt sich aktiv an der Open-Source-Entwicklung. SELinux entstand in Zusammenarbeit mit privaten Partnern. Es ist seit Längerem Bestandteil des Standard-Kernel und ermöglicht den Linux-Einsatz in Umgebungen, in denen Daten unterschiedlicher Sicherheitseinstufungen auf einem Gerät zu verarbeiten sind (Stichwort: Multi Level Security, MLS). Seit Kurzem existiert ein von der NSA entwickeltes Android-Handy mit dem Codenamen Fishbowl. Es verschlüsselt die Sprachdaten, sodass Regierungsangestellte damit selbst geheime Gespräche führen dürfen. Google nutzt dieses Interesse der US-Behörden für eine stärkere Zusammenarbeit und will Android zum sichersten Mobilbetriebssystem machen. Noch in diesem Jahr soll es eine erste Zertifizierung geben, und man strebt einen höheren Sicherheitslevel als BlackBerry an. Zu erwarten ist, dass Google zumindest Teile dieser Entwicklungen in den Standard-Kernel einfließen lässt.

Größenvergleich ohne/mit SE Android

Systembereich	ohne SE	mit SE	Veränderung
boot	3444 kByte	3584 kByte	+140 kByte
system	161 620 kByte	161 668 kByte	+48 kByte
recovery	3776 kByte	3916 kByte	+140 kByte

Quelle: Stephen Smalley, Android Builders Summit 2012

Mengenmäßig hält sich der Mehraufwand für SE Android in Grenzen.

SE Android sieht nach den verfügbaren Informationen seine Bestimmung in der Sicherung des Betriebssystems vor allem gegen Angriffe. Die veröffentlichten Folien sind klar auf das Verhindern von Exploits abgestellt. Stephen Smalley von der NSA zeigte bei der SE-Andoird-Präsentation, wie es drei bekannte Exploits stoppt (siehe „Alle Links").

MAC auf Android und darüber hinaus

Eine andere MAC-Erweiterung für Android ist BizzTrust des SIT, es setzt wie SE Android auf der LSM-API (Linux Security Modules) des Kernel auf. Auch BizzTrust verfolgt das Ziel, Multi-Level-Security auf Android zu ermöglichen – dies allerdings mit dem Fokus auf der Trennung von geschäftlichen und privaten Daten. Damit möchte man Firmen mit hohen Sicherheitsansprüchen einen Android-Einsatz ermöglichen. Da Android Open Source ist, können Benutzer bei beiden Ansätzen die notwendigen Änderungen einpflegen und bei Bedarf den Code analysieren. Für potenzielle Anwender, seien dies Staatsorgane oder Firmen, ein immenser Vorteil: Während sie bei BlackBerry, iPhone oder anderen dem Hersteller mehr oder weniger blind vertrauen müssen, können sie bei diesen beiden MAC-Ansätzen durch eigene Audits sicherstellen, dass das Betriebssystem nur die versprochenen Funktionen enthält und die Programmierer diese auch sicher

umsetzen. Mehr zum Thema Weltentrennung findet sich im Artikel „Schutzhüllen“ [1].

SE Android implementiert MAC im Kernel und definiert gleich die notwendigen Domänen. Darüber hinaus erweitert es das Dateisystem um die für MAC notwendigen Labels. Hier bekommt nicht nur das Subjekt, also meist der agierende Prozess, Rechte auf passive Objekte wie Dateien oder Netz-Sockets. MAC nutzt erweiterte Attribute wie Labels, um per Regel zu entscheiden, ob der Zugriff statthaft ist. Über diese erweiterten Attribute und sehr fein zu definierende Rechte kann der Kernel seine Entscheidungen viel präziser treffen. Allerdings muss ein Mensch all diese Attribute und Regeln erstellen und pflegen. Der damit einhergehende Aufwand hat bis heute die Nutzung von MAC außerhalb von Regierungsstellen größtenteils verhindert.

In die MAC-Vorbereitung auf Android hat das SE-Android-Projekt bereits einige Arbeit investiert, denn schon allein die Grundlagen sind an allen Stellen der Rechteverwaltung zu implementieren. Laut der Webseite haben die Entwickler die notwendigen Schnittstellen in das Dateisystem (Dateien, Dateisystem-Abbilder, Sockets, Verzeichnisse von Apps et cetera), das Installationsprogramm, die Interprozesskommunikation (Binder IPC) und den Startprozess für alle Apps (Zygote) eingefügt.

Damit dies auch praktisch einsetzbar ist, hat das Projekt eine Domain für die System-Apps definiert und einen minimalen Editor programmiert, mit dem der Benutzer die Attribute und Regeln verwalten kann.

SE Android will in der Zukunft mehr als „nur“ MAC implementieren. Wie in den Folien zu sehen, will das Projekt den Fokus auf das Verhindern von Sicherheitslücken setzen. Die NSA hat sich vorgenommen, im Rahmen des Projekts alle Android-Schwachstellen zu identifizieren und zu bereinigen. Damit sind nicht so sehr Verwundbarkeiten im Code gemeint, die zu Exploits führen, sondern eher strukturelle Schwachstellen, die Linux auf das Sicherheitsmodell von Android vererbt hat und die Android Inc. beim Design einbaute.

Derzeit veröffentlicht das Projekt allerdings nur die Absicht auf seinen Seiten, konkrete nächste Schritte sind wohl noch nicht öffentlich. Welche Änderungen sich daraus für den Android-Kernel ergeben, lässt sich derzeit noch nicht absehen. Wer heute schon ein SE Android haben möchte, muss es selbst übersetzen. Basierend auf dem Android Open Source Project (AOSP) kann sich jeder Interessierte den Quellcode per Git laden und in den eigenen Build aufnehmen. Das erstellte Image läuft derzeit laut Aussagen der NSA auf dem Emulator, Samsungs Nexus S und Motorolas Xoom.

Fazit

Für den Alltag eignet sich SE Android noch nicht, aber als Studie und Entwicklungsplattform zeigt es die Richtung, die Google mit Android verfolgt. Es soll so gut geschützt sein, dass Hersteller beziehungsweise Nutzer das Betriebssystem auch in sicherheitskritischen Bereichen einsetzen können. In welchem Umfang Google die Erweiterungen in den Standard-Kernel einfließen lässt, ist leider noch nicht klar. Wahrscheinlich erscheint, dass Google es nutzen wird, um die Sicherheit des Kernels vor Angriffen durch bösartige Apps und andere Malware zu erhöhen.

SE Android bringt bereits eine Domäne für die Apps sowie eine für das Betriebssystem mit. Dies allein verringert schon das Risiko, dass ein im Code von Android gefundener Fehler zu einem erfolgreichen Bruch der durch den Kernel wahrgenommenen Sicherheitsfunktionen führt. Daher ist zu hoffen, dass SE Android bald in den Geräten regulärer Konsumenten zum Einsatz kommt. (avr)

CHRISTOPH PUPPE

ist seit 23 Jahren in der IT-Sicherheit aktiv, IS-Revisor und verantwortet derzeit die technischen Audits bei der HiSolutions AG in Berlin.

Literatur

[1] Christoph Puppe; Mobility; Schutzhüllen; Privates und Geschäftliches auf einem Gerät voneinander trennen; *iX* 4/2012, S. 56

Alle Links: www.ix.de/ix1205110