Ammar Alkassar, Steffen Schulz, Christian Stüble

# Sicherheitskern(e) für Smartphones: Ansätze und Lösungen

## Vom Mikrokern bis zu Capabilities – Verschiedene Lösungsansätze für die App-Trennung und -Kontrolle.

Dieser Artikel beschreibt die verschiedenen, heute verfolgten theoretischen und praktischen Lösungsansätze zur Trennung von Informationen aus unterschiedlichen Sicherheitsstufen. Ein typisches Anwendungsziel ist beispielswiese die Verwendung eines einzelnen Smartphones für die berufliche und private Nutzung.

### 1 Einleitung

Smartphones sind zu einem Eckpfeiler der mobilen Informationsgesellschaft geworden. Sie erlauben klassischen PIM-Anwendungen und neuen Applikationen(Apps) den Zugriff auf Unternehmensanwendungen zu jeder Zeit und an jedem Ort.

**Ammar Alkassar**

ist Vorstandschef des Sicherheitsspezialisten Sirrix AG in Saarbrücken und Vorstandsmitglied im IT-Sicherheitsverband TeleTrusT.

E-Mail: alkassar@sirrix.com

**Steffen Schulz**

ist Doktorand am Lehrstuhl für Systemsicherheit der TU Darmstadt. Er befasst sich dort mit neuen Ansätzen im Bereich Betriebssystemsicherheit und Trusted Computing.

E-Mail: steffen.schulz@trust.cased.de

**Christian Stüble**

ist Technikvorstand bei der Sirrix AG in Bochum. Er ist Spezialist u.a. für Betriebssystemsicherheit und Trusted Computing mit zahlreichen Publikationen auf diesem Gebiet.

E-Mail: stueble@sirrix.com

Darüber hinaus werden zukünftige transaktionsbasierte Anwendungen, wie sie beispielsweise im Zuge der Einführung des neuen Personalausweises (nPA) oder für das kontaktlose elektronische Bezahlen mittels NFC entwickelt werden, von Smartphones bedient werden können. Doch die damit verbundenen Risiken (Datenverlust durch Diebstahl oder Verlust) führen meist dazu, dass das volle Potential heutiger Smartphones nicht genutzt werden kann.

Durch den Einsatz von Virtualisierung und Isolation und unter Nutzung von speziell auf mobile Endgeräte ausgerichtete Sicherheitstechnologien ist es möglich, eine sichere und vertrauenswürdige Nutzung sensitiver Daten und Anwendungen in heterogenen Einsatzumgebungen wie Unternehmen oder Behörden zu gewährleisten. Die strikte Trennung von „unsicheren“ und „sicheren“ Bereichen (und „Apps“) werden dabei so realisiert, dass die eingesetzten Geräte in ihren Funktionen und der Benutzbarkeit nicht beschnitten werden.

Für die Realisierung solcher sicheren mobilen Plattform wurden in den vergangen Jahren verschiedenen Ansätze entwickelt. Diese unterscheiden sich in Komplexität und Anforderungen teilweise erhebliche und adressieren unterschiedliche Sicherheitsstufen und -ziele.

In diesem Artikel skizzieren wir die wichtigsten konzeptionellen Ansätze und zeigen Technologien von bereits im Einsatz befindlichen und in Zukunft zu erwartenden Lösungen.

#### 1.1 Smartphones & Sicherheit

Smartphones sind heute nicht nur weit verbreitet und werden intensiv genutzt, sie sind aus dem privaten und beruflichen Alltag kaum noch wegzudenken.

Während Smartphones lange unstrukturiert beruflich eingesetzt worden sind, gewinnen Sie heute zunehmend auch im großflächigen Einsatz in Unternehmen und Behörden an Bedeutung. Voraussetzung hierfür ist die Erfassung der Risiken und deren Einordnung in die Gesamtrisikoabschätzung der Unternehmens-IT.

Risiken wie Verlust oder Diebstahl durch Gelegenheitsangreifer können heute mit Sicherheitslösungen adressiert werden, die von den Smartphone-Herstellern entwickelt und von sogenannten Mobile-Device Management (MDM) Systemen zentral gesteuert werden.

Dafür haben die Hersteller in ihren Betriebssystemen standardisierte Funktionen integriert, die es beispielsweise ermöglichen, verloren gegangene Geräte remote zu deaktivieren oder zu löschen, verpflichtende Kennwortrichtlinien zu setzen und die Installation von Applikationen zu beschränken.

Diese Funktionen lassen sich dann durch die MDM-Systeme auch unternehmensweit zentral steuern. Typische Beispiele sind Afaria (Sybase), MobileIron und Ubitex.

Auch die sichere (verschlüsselte und authentisierte) Nutzung von Unternehmensressourcen kann heute durch VPN-Zugänge realisiert werden (Data at move). Dies umfasst den Zugang zu Diensten wie Unternehmensmail, Kalender und Kontakten als auch Web-basierten Unternehmensdiensten wie CRM.

Während lange Zeit VPN-Zugänge durch das unsichere Shared-Secret-Verfahren umgesetzt wurden, gelten heute zentral verwaltete, Zertifikat-basierte Systeme als Mindeststandard bei der Anbindung von mobilen Geräten an zentrale Unternehmensressourcen.

Da die einfachen Schutzmechanismen der Smartphonehersteller und der meisten MDM-Anbieter, z.B. Remote-Löschen und Deaktivieren, nicht ausreichen gegen gezielte Angriffe auf Unternehmenswerte, bieten immer mehr Hersteller Lösungen zur Verschlüsselung der auf dem Smartphone gespeicherten Daten an (Data at rest). Dabei soll verhindert werden, dass vertrauliche Daten wie Kontakte, Nachrichten oder Mails, die sich auf dem mobilen Gerät befinden, bei Verlust oder Diebstahl in unautorisierte Hände gelangen – auch wenn keine Remote-Löschung beispielsweise mehr möglich ist.

## 2 Neue Herausforderungen

Während sich mobile Geräte wie Smartphones in rasantem Tempo ihren Weg in die Unternehmen und Behörden bahnen, kristallisieren sich drei Herausforderungen heraus, deren Adressierung durch adäquate Sicherheitslösungen essentiell für den ökonomischen Einsatz in Unternehmen sein wird:

### 2.1 Bring-Your-Own-Device (BOYD)

Smartphones sind heute vollwertige und leistungsfähige kleine Computer – und kosten mindestens so viel. Der Druck auf die Unternehmen, die privaten Geräte für den Unternehmenseinsatz zu öffnen, wird auch aus Kostengesichtspunkten dazu führen, dass Unternehmen ihre Strategien anpassen. Bisher etablierte Strategien, unternehmensweit einheitliche Geräte vorzuschreiben, die sich gut in die Infrastruktur einbinden lassen, von der hauptsächlich Anbieter wie RIM mit BlackBerry profitiert haben, sind heute kaum noch durchsetzbar. Unternehmen verlangen heute nach Lösungen, die Mobilgeräte unterschiedlicher Hersteller sicher managen und die es erlauben, dass der Nutzer weiterhin seine privaten Anwendungen parallel betreibt – ohne dass es das Sicherheitsrisiko für die Unternehmensdaten erhöht.

### 2.2 Neue, transaktionsbasierte Dienste

Kein anderer persönlicher technischer Gegenstand hat heute eine Verbreitung gefunden wie Mobilfunkgeräte – weltweit und auch in Entwicklungs- und abgelegen Regionen. Damit werden Mobilgeräte zu einem wichtigen Anker für viele neue Dienste insbesondere auch Authentifizierungs- und Bezahldienste. Die Sicherheitsanforderungen solcher Dienste erfordern die Durchsetzung von Sicherheitszielen, die auch gegenüber dem Benutzer des Mobilgerätes eingehalten werden müssen (ein Benutzer hätte beispielsweise ein Interesse daran, den Wert seines digitalen Portemonnaies zu erhöhen).

### 2.3 Schadsoftware

Viren, Trojaner und andere Schadsoftware stellen nach ihrem wirtschaftlichen Schaden bereits heute die größte Sicherheitsgefahr bei stationären Rechnern dar. Mit Hinblick auf die erhebliche Bedeutung von Smartphones und der zunehmenden Anzahl einzelner Vorfälle ist absehbar, dass ein wirksamer Schutz mobiler Geräte vor Schadsoftware eine Schlüsselvoraussetzung für deren breiten Einsatz im Unternehmens- und Behördenumfeld sein wird.

Der wirksame Schutz gegen Schadsoftware adressiert dabei auch die beiden erstgenannten Herausforderungen: Sowohl die Zulassung privater und beruflicher Anwendungen auf dem gleichen Gerät, als auch die Nutzung des Gerätes für geldwerte Dienste wird die Attraktivität von Angriffen erheblich erhöhen. Bereits heute wird Schadsoftware in erheblichem Umfang gezielt eingesetzt, um Rechner auszuspähen (bspw. Ausspähen von Kreditkarteninformationen oder zum Abhören von verschlüsselten Telefonaten).

## 3 Vertrauenswürdige Systeme und Sicherheitskerne

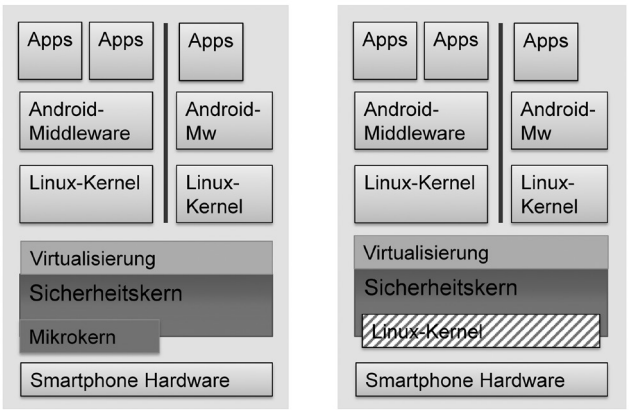
Damit wird die Vertrauenswürdigkeit eines mobilen Systems zu einer wichtigen Grundeigenschaft, die gegenüber den beteiligten Akteuren belegbar sein muss. Die Akteure können über unterschiedliche (Sicherheits-)Interessen verfügen: Gerätenutzer (mal in der Eigenschaft als Mitarbeiter und mal als Privatnutzer), das Unternehmen/Behörde, der Hersteller des Gerätes, des Systems und der Software und der Betreiber weiterer Dienste (z.B. Bezahldienste).

Die Erfahrungen der letzten Jahre haben bereits bei nicht-mobiler IT gezeigt, dass die bisherigen reaktiven Ansätze für IT-Sicherheit (bspw. Reaktion *nach* Virenbefall) den aktuellen Herausforderungen nicht gewachsen sind. Adäquate Sicherheit erfordert einen proaktiven Ansatz, der sowohl ein Sicherheitsmodell definiert als auch deren Umsetzung in dem IT-System nachweist. Dies ist Grundlage für vertrauenswürdige Systeme.

Die Umsetzung eines solchen Ansatzes ist auf Basis großer monolithischer Plattformen schwierig. Daher gilt heute die Aufteilung in Sicherheitsdomänen, deren strenge Isolation und die Informationsflusskontrolle zwischen ihnen sowie deren Integritätsprüfung als entscheidender Ansatz zur Entwicklung vertrauenswürdiger Systeme [7].

Diese Aufgabe wird von sogenannten Sicherheitskernen übernommen, die folgende Kernaufgaben umsetzten:

**Abb. 1 | Ansätze mit Mikrokern (links) und Linux-Kern (rechts)**




- Isolation kritischer Komponenten: Damit soll sichergestellt werden, dass unterschiedliche Bereiche strikt voneinander getrennt werden können. So kann beispielsweise verhindert werden, dass sich Benutzer (unabsichtlich) Viren und Trojaner über eine private Anwendung einfangen, die dann Zugriff auf Unternehmensressourcen erlangt.
- Kontrolle aller Informationsflüsse zwischen den Komponenten sowie Kontrolle des Zugriffs von Komponenten auf Hardwareschnittstellen. Die umfassende Kontrolle an den Schnittstellen der Komponenten erleichtert einerseits die Informationsverarbeitung innerhalb der Komponente und verhindert andererseits, dass Informationen aus Unternehmensressourcen (absichtlich oder unabsichtlich) „geleaked" werden. Auf die Kontrolle können sich alle beteiligten Akteure verlassen, sodass weder das Unternehmen Zugriff auf private Daten, noch privat installierte Apps Zugriff auf Unternehmensdaten bekommen.
- Integritätsprüfung der verwendeten Komponenten. Damit wird sichergestellt, dass nur autorisierte und integere Komponenten auf bestimmte Daten zugreifen und diese verarbeiten dürfen. Ein Teilaspekt hiervon ist das sichere Laden des Betriebssystems. Ein weiterer Teilaspekt ist die sichere GUI. Diese ist beispielsweise unerlässlich, wenn vertrauliche Daten vom Benutzer abgefragt werden, wie etwa die PIN.

Derzeit sind zwei Common Criteria Schutzprofile bekannt, die die wesentlichen Sicherheitsanforderungen an ein höherwertiges sicheres mobiles Gerät adressieren können:

- Separation Kernel Protection Profile (SK-PP). Das SK-PP wurde im Auftrage der NSA entwickelt und ist nicht zertifiziert. Entwicklungen können bis EAL6 auf Basis dieses PP evaluiert werden. Neben Anforderungen an den Sicherheitskern enthält dieses Schutzprofil insbesondere Anforderungen bzgl. des Entwicklungs- und Konfigurationsmanagement.
- High-Assurance Security Kernel Protection Profile (HASK-PP) [4]. Das HASK-PP ist im Auftrage des BSI entwickelt worden und von diesem nach EAL5 AUG zertifiziert. Im Gegensatz zum SK-PP enthält dieses Sicherheitsprofil auch eine Integritätsprüfung der Komponenten.

Beispiele für ein nach dem HASK-PP entwickelter Sicherheitskern ist der durch das BMWi entwickelte TURAYA™ Security Kernel. Beispiel für einen nach dem SK-PP entwickelten Kern ist INTEGRITY™ von Greenhills Software. Für einen ausführlicheren Vergleich zwischen den o.g. Schutzprofilen siehe z.B. [8].

## 4 Implementierungen und Lösungen

Hauptziel einer sicheren mobilen Plattform ist die Isolation von Apps und die Kontrolle der Informationsflüsse zwischen ihnen. Aus technischer Sicht kommen dafür im Wesentlichen drei Lösungsansätze in Betracht:

- Mikrokern-basierte Sicherheitsarchitektur
- Sicherheitsarchitektur basierend auf Standardkomponenten
- Trennung auf Middleware-Ebene mittels Capabilities

Im Folgenden werden diese drei Lösungsaspekte insbesondere im Hinblick auf Sicherheit, Einsatz in Produktivumgebungen und Wirtschaftlichkeit verglichen.

### 4.1 Mikrokern-basierte Sicherheitsarchitektur

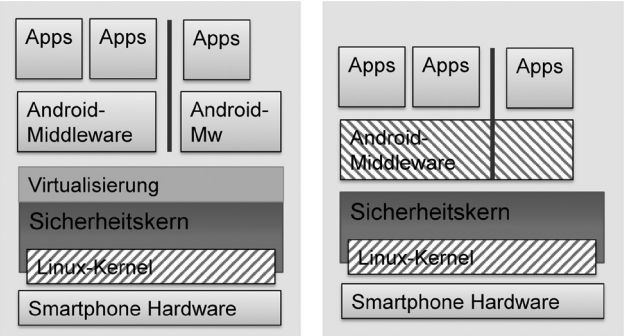
Dieser Lösungsansatz besteht im Wesentlichen aus zwei Kernkonzepten: Ein minimaler, Mikrokern-basierter Sicherheitskern setzt die Isolations- und Informationsflussregeln zwischen parallel ausgeführten Instanzen des Smartphonebetriebssystems durch (vgl. Abbildung 1). Die Betriebssysteminstanzen bestehen aus virtualisierten Betriebssystemkernen, auf denen jeweils die Middleware und die Apps ausgeführt werden. Bei diesem Lösungsansatz sind nur der Sicherheitskern und die Smartphone Hardware sicherheitskritisch, da die virtualisierten Betriebssysteminstanzen selbst die Sicherheitsregeln nicht umgehen können. Zur Virtualisierung der Smartphone Betriebssysteme können verschiedene Technologien verwendet werde:

Bei der Hardware-unterstützten Virtualisierung bietet die CPU erweiterte CPU-Kommandos, mit denen der Sicherheitskern eine effiziente Virtualisierung erreichen kann. Ein typisches Beispiel hierzu sind die für mobile Plattformen vorgesehenen x86-Architekturen.

Bei der sogenannten Para-Virtualisierung wird hingegen der Betriebssystemkern so modifiziert, dass er statt auf der CPU, die Funktionen des Sicherheitskerns nutzt. Paravirtualisierung ist im Allgemeinen effizienter und flexibler als hardware-basierte Virtualisierung, verlangt jedoch eine umfangreiche Modifikation des paravirtualisierten Kernels. Beide Ansätze lösen noch nicht unmittelbar das Problem des gleichzeitigen Hardware-Zugriffs durch die Gastsysteme. Das hierfür erforderliche Multiplexing hat sich aufgrund von oftmals nur in Binärform vorliegenden Treibern, kaum verfügbarer Hardware-Spezifikationen und der schnellen Hardware-Entwicklungszyklen als unerwartet hoher, langfristiger Kostenfaktor erwiesen. Auch die Wiederverwendung von Treibern durch Einsatz einer dedizierten „Treiber-Domäne" stellt oft nur eine unbefriedigende Lösung dar, da die resultierende quasi-monolithische Architektur wesentliche Sicherheitsmerkmale eines echten Sicherheitskernels verspielt und ggf. weiterhin mit Performance-Problemen zu kämpfen hat, etwa in Bezug auf die in Smartphones heute essentielle 3D-Grafik.

Aus Sicherheitssicht bietet eine Mikrokern-basierte Sicherheitsarchitektur im Vergleich zu den anderen Lösungsansätzen klare Vorteile: Aufgrund der geringen Komplexität des Sicherheitskerns und der damit einhergehenden Reduktion möglicher Fehlerquellen ist eine Common Criteria Zertifizierung nach EAL5 (und höher) oder sogar eine formalen Verifikation der Korrektheit im Bereich des Realisierbaren [6]. Andererseits zeigen die Erfahrungen mit der Entwicklung von Mikrokern-basierten Sicherheitskernen, dass mit einem erheblichen Entwicklungsaufwand, speziell im Bereich der Treiberentwicklung, gerechnet wer-

**Abb. 2 | Ansätze mit Container (links) und Capabilities (rechts)**




den muss. In Zusammenhang mit den kurzen Produktzyklen im Smartphonebereich und der geringen Verfügbarkeit technischer Spezifikationen entstehen hierdurch langfristig erhebliche Zusatzkosten.

Ein bekanntes Beispiel für die Umsetzung dieser Architektur mittels Para-Virtualisierung ist das EU-Projekt TECOM[1], bei dem mehrere Linux-instanzen auf dem TURAYA-Sicherheitskern auf einem PikeOS Mikrokern ausgeführt werden. Eine der weltweit ersten Lösung auf kommerzieller Standardhardware (dem Nokia N900) ist das BSI-Projekt MoTrust Mobile [1], welches den TURAYA-Sicherheitskern zusammen mit dem OKL4-Mikrokern verwendet, um mehrere Android-Instanzen parallel auszuführen.

Ein weiteres Beispiel ist L4Android [5], dass einen erweiterten L4-Mikrokern nutzt und dessen grundsätzliche Funktionsweise auf einem x86-Developerboard vorgeführt wurde.

### 4.2 Sicherheitskern basierend auf Standardkomponenten

Mobilfunkgeräte, insbesondere Smartphones verwenden heute Hardwareplattformen, die in kurzen Zeitabständen wechseln. Damit sind ressourcen-intensive Mikrokern-basierte Ansätze, bei denen Hardware-spezifische Treiber angepasst bzw. neu entwickelt werden müssen, oftmals wenig wirtschaftlich.

Daher wurden alternative Ansätze entwickelt, in denen bei der Realisierung des Sicherheitskerns auf Standardkomponenten zurückgegriffen wird (vgl. Abbildung 1 rechts).

Neben der hardwarebasierten Virtualisierung auf geeigneten Hardwareplattformen bietet sich hier im Zusammenhang mit Android die Paravirtualisierung eine Userspace-Virtualisierung in Form von User-Mode Linux (UML) oder Linux Lguest an. Bei diesem Ansatz macht man sich zu Nutzen, dass das virtualisierte (Android-) Betriebssystem und der zugrunde liegende Betriebssystemkern des Sicherheitskerns identische Schnittstellen benutzen, wodurch eine sehr effiziente und ressourcensparende Virtualisierung realisierbar ist.

Aufgrund der höheren inhärenten Komplexität eines solchen Sicherheitskerns ist die Erfüllung gegebener Sicherheitsanforderungen deutlich aufwändiger als bei einem Mikrokern-basierten Sicherheitskern.

1 http://www.tecom-project.eu/

Allerdings wurde in der Vergangenheit bereits mehrfach gezeigt, dass Linux-basierte Systeme zumindest in der Common Criteria Evaluierungsstufe EAL4 zertifizierbar und unter bestimmten Voraussetzungen auch für den Einsatz im Verschlusssachenbereich zulassbar sind.

Sicherheitslösungen mit einer solchen Sicherheitsarchitektur haben sich im Desktop-Bereich etabliert. Beispiele sind Trusted-Desktop von Sirrix, Trusted Virtual Environment von General Electric und SINA Virtual Workstation von Secunet.

In der Praxis kann das verbleibende Risiko durch regelmäßige Sicherheits Patches weitgehend minimiert werden.

Aus technischer Sicht ist die Entwicklung eines Linux-basierten Sicherheitskerns wesentlich kosteneffizienter zu realisieren als bei Mikrokernen, da auf eine große Anzahl existierender und stabil funktionierender Komponenten und insbesondere Treiber zurückgegriffen werden kann, die von den Herstellern bereits für die jeweilige Plattform optimiert wurden. Weiterhin ist es heutzutage üblich, dass Hersteller ihre Entwicklerplattformen mit einem funktionierenden Linux ausliefern.

Für Linux-basierte Sicherheitskerne auf Smartphones gibt es bisher wenig verfügbare Beispiele. Einen vielversprechender Ansatz verfolgt zurzeit die TU Darmstadt mit der Sirrix AG [12]:

Basierend auf Linux vServer Container-Virtualisierung wird für den TURAYA/Linux Sicherheitskern eine Virtualisierung von Android-Umgebungen entwickelt. Dabei wird die sich im Server-Bereich bereits etablierte vServer-Virtualisierung um Smartphone-spezifische Hardware-Komponenten wie SIM-Karte, Touch-Interface und vor allem 3D-Grafik erweitert. Das Ziel dieses Ansatzes besteht darin, die bei einem Android-System oftmals in Binärform enthaltenen Linux-Treiber direkt weiterverwenden zu können, ohne wie bspw. im Mikrokern-Ansatz üblich bei jedem Zugriff eine Umleitung durch eine spezielle Treiber-Domain zu benötigen, was oftmals mit Performance-Einbußen und umfassender Entwicklungsarbeit verbunden ist. Die Durchsetzung der Sicherheitsregeln findet dabei ausschließlich im Linux-Kern selbst statt, sodass die Android-Middleware unmodifiziert bleiben kann und nicht vertrauenswürdig sein muss.

### 4.3 Capabilities-basierte Lösung

Die Erfahrung zeigt, dass eine komplette Trennung von Anwendungswelten oftmals nicht erwünscht und auch nicht hinreichend ist: Für eine bessere Benutzbarkeit wird meist erwartet, dass etwa Termine und Kontakt-Datenbank, aber auch scheinbar einfache Funktionen wie Drag&Drop die Domänen-Isolation überschreiten können. Weiterhin benötigen sichere Smartphones und andere Endgeräte aus Anwendersicht nicht nur eine „sichere Domäne“ mit etwa Online-Banking oder Firmen-VPN-Anwendung, sondern es muss langfristig ein „Defense-in-Depth“-Ansatz verfolgt werden, bei dem etwa eine eMail-Anwendung vor Fehlfunktionen in Browser oder Terminverwaltung innerhalb der gleichen Domäne geschützt ist. Ein bereits im akademischen Bereich stark verfolgter Ansatz ist daher die Analyse und Erweiterung von Smartphone Middleware und App-Isolationsmechanismen [2,9], sowie insbesondere auch die Anpassung und Integration erweiterter Linux Access Control-Mechanismen wie Tomoyo oder SELinux [10].

Der Ansatz wurde im Rahmen des BizzTrust-Projekts in Kooperation von der TU Darmstadt, dem Fraunhofer SIT und der Sirrix AG ausgebaut, um Gruppen von Anwendungen durch in

die Android-Middleware eingeführte Zugriffskontrollmechanismen voneinander zu trennen [11].

Auf diese Weise können wiederum die für Endkunden konzeptuell leicht verständlichen Anwendungs-Domänen implementiert werden, ohne jedoch den Betriebssystem-Kern zu modifizieren oder gar eine zusätzliche Kontrollschicht wie im Mikrokern-Ansatz einzuführen.

Die Lösung erlaubt durch die sehr gute Performance eine Vielzahl logischer Domänen und große Flexibilität in der Kommunikation zwischen Domänen. Wesentlicher Nachteil ist jedoch, dass es sich um einen Blacklist-Ansatz handelt bei dem jede mögliche Kommunikation in der Analyse vorhergesehen und behandelt werden muss. Außerdem wird auch die Android-Middleware derzeit noch stark weiterentwickelt, wenn auch der resultierende Implementierungsaufwand bisherigen Erfahrungen nach nicht mit dem Problem der Treiberabhängigkeit im Virtualisierungs- und vor allem im Mikrokern-Ansatz vergleichbar ist.

## 5 Secure Bootstrap & Risiko Baseband

Bestimmte Sicherheitsziele können durch den Sicherheitskern nur mit Unterstützung sicherer Hardwarekomponenten realisiert werden. Hierzu gehört beispielsweise das „Secure Boot" sowie Sicherheitsziele, die auch gegen den Benutzer durchgesetzt werden müssen.

Neben den proprietären Lösungen der Hersteller von Mobilfunk-Chipsets wie TI's M-Shield[2] oder SecureMSM[3] von Qualcomm, existieren auch standardisierte Verfahren wie das Mobile Trust Module (MTM) der Trusted Computing Group, das sich aber bisher nicht durchsetzen konnte. Die erste MTM-Implementierung wurde im Rahmen des Projektes TECOM durch Infineon, Sirrix AG und Gemalto entwickelt und wird von der Sirrix AG kommerziell lizensiert.

Auch beim Einsatz eines Sicherheitskerns darf die Hardware nicht aus der Risikobetrachtung ausgeklammert bleiben: Ähnlich zu den DMA-Angriffen bei stationären Systemen können Schwächen in der Hardware der Mobilfunkgeräte für Angriffe genutzt werden.

Dabei stehen die Baseband-Komponenten im besonderen Fokus, da sie heute in Smartphones weitestgehend als mächtige, programmierbare und updatefähige Komponenten realisiert sind. Interessante Aufschlüsse dürfte das BMBF-Projekt SMOG – „Schutz mobiler Endgeräte vor Angriffen über die Luftschnittstelle" (SMOG)[4] geben.

2 focus.ti.com/pdfs/wtbu/ti_mshield_whitepaper.pdf

3 www.qualcomm.com/solutions/.../security

4 www.pt-it.pt-dlr.de/de/2615.php

## Literatur


[1] Selhorst, Stüble, Gnaida, Feldmann: „MoTrust.Embedded – Eine vertrauenswürdige Sicherheitsplattform für Smartphones" 12th German IT Security Congress, Bonn-Bad Godesberg, May 2011.

[2] Sven Bugiel, Lucas Davi, Alexandra Dmitrienko, Thomas Fischer, Ahmad-Reza Sadeghi, Bhargava Shastry: Towards Taming priviledge escalation attacks on Android. Annual Network & Distributed System Security Symposium (NDSS), Februar 2012

[3] Luigi Catuogno, Hans Löhr, Mark Manulis, Ahmad-Reza Sadeghi, Christian Stüble und Marcel Winandy: Trusted Virtual Domains: Color Your Network. Datenschutz und Datensicherheit (DuD) 5/2010, pp. 289-294, Gabler Verlag, 2010.

[4] Sirrix AG: High-Assurance Security Kernel Protection Profile (EAL5), according to the Common Criteria v3.1 R2, 2007, zertifiziert durch das Bundesamtfür Sicherheit in der Informationstechnik (BSI) 2008.

[5] Matthias Lange, Steffen Liebergeld, Adam Lackorzynski, Alexander Warg, Michael Peter: „L4Android: A Generic Operating System Framework for Secure Smartphones", In proceedings of the 2011 ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices, Chicago, IL, USA, Oct 2011

[6] Eyad Alkassar, Mark A. Hillebrand, Wolfgang Paul und Elena Petrova: Automated Verification of a Small Hypervisor. In Proceedings of "Verified Software: Theories, Tools, Experiments"; Lecture Notes in Computer Science, 2010, Volume 6217/2010, 40-54, Edinburgh, Scotland.

[7] Ahmad-Reza Sadeghi, Christian Stüble, Norbert Pohlmann: European Multilateral Secure Computing Base – Open Trusted Computing for You and Me; Datenschutz und Datensicherheit (DUD) 9/2004, Vieweg Verlag, pp. 548-554, 2004.

[8] Hans Löhr, Ahmad-Reza Sadeghi, Christian Stüble, Marion Weber, Marcel Winandy: Modeling Trusted Computing Support in a Protection Profile for High Assurance Security kernels; Proceedings der TRUST 2009, Oxford.

[9] Peter Hornyack, Seungyeop Han, Jaeyeon Jung, Stuart Schechter, and David Wetherall: „These Aren't the Droids You're Looking For": Retroffiting Android to Protect Data from Imperious Applications. ACM Conference on Computer and Communication Security (CCS), Oct 2011

[10] Stephen Smalley: The Case for SE Android, National Security Agency (NSA), 2011

[11] Sven Bugiel, Lucas Davi, Alexandra Dmitrienko, Stephan Heuser, Ahmad-Reza Sadeghi, Bhargava Shastry : Practical and Lightweight Domain Isolation on Android. In: Proceedings of the 1st ACM CCS Workshop on Security and Privacy in Mobile Devices (SPSM), ACM Press, Oct 2011.

[12] Soeren Heisrath, Christian Stüble: Sirrix AG Technical Report No 12/1102, August 2011.