Sichere Plattform zur Smartphone-Anbindung auf Basis von TNC

Prof. Dr. Kai-Oliver Detken[1] · Günther Diederich[2] · Stephan Heuser[3]

[1]DECOIT GmbH, Fahrenheitstraße 9, D-28359 Bremen
detken@decoit.de

[2]Hochschule Bremen, Flughafenallee 10, D-28199 Bremen
guenther.diederich@hs-bremen.de

[3]Fraunhofer Institute for Secure Information Technology, Rheinstraße 75, D-64295 Darmstadt
stephan.heuser@sit.fraunhofer.de

Zusammenfassung

Unternehmen stellen heute große Anforderungen an die Mobilität und Flexibilität ihrer Arbeitnehmer. Der Anspruch, auch über die Unternehmensgrenzen hinweg mit Daten verschiedener Betriebe arbeiten zu können, birgt jedoch auch neue Herausforderungen und Risiken. Er führt zu einer Ausdehnung der digitalen Unternehmensgrenzen, von traditionellen Perimeter-Einrichtungen bis hin zu den mobilen Endgeräten der Arbeitnehmer. Neben der obligatorischen Kontrolle von Benutzerdaten brauchen Unternehmen die Gewissheit, dass sensible Firmendaten, die sich im Netz sowie auf den Geräten selbst befinden, nicht durch kompromittierte oder gefährdete Endgeräte bedroht werden. Zu diesem Zweck ist ein Mechanismus erforderlich, der den Zustand der Endgeräte vor dem Zugriff auf kritische Ressourcen erfassen und gegebenenfalls angemessen reagieren kann. Der vorliegende Beitrag beschreibt die im VOGUE-Forschungsprojekt entwickelten Lösungen, um diese Lücke zu schließen. Im Rahmen des Projekts werden die Möglichkeiten des Einsatzes von Trusted-Computing-Konzepten auf mobilen Endgeräten in einem Business-Intelligence-Szenario untersucht. Dazu wird eine Sicherheitsarchitektur für mobile Endgeräte und die Infrastruktur definiert, die es ermöglichen soll, die vorher definierten Sicherheitsanforderungen zu erfüllen. So soll mobilen Geräten in verschiedenen Einsatzumgebungen der sichere Zugriff auf Ressourcen unterschiedlicher Unternehmen ermöglicht werden.

1 Generisches Anwendungsszenario

Kontinuierliche Geschäftsentscheidungen und kooperative Wettbewerbsfähigkeit setzen IT-Systeme voraus, die Geschäftsdaten erheben und verarbeiten können. Diese Business-Intelligence(BI)-Systeme zielen darauf ab, zuvor verteilte und fragmentierte Daten aus verschiedenen Teilen eines Unternehmens zu kombinieren, zu analysieren und zu bearbeiten, um die Informationen zu verbessern, auf deren Grundlage strategische Entscheidungen getroffen werden. Die erhöhte Verfügbarkeit und Leistung mobiler Systeme erlaubt eine flexible Datenerhebung und -verarbeitung vor Ort und erweitert auf diese Weise BI zur mobilen Business

P. Schartner · J. Taeger (Hrsg.) · DACH Security 2011 · syssec (2011) pp-pp.

Intelligence. Darüber hinaus stehen hierbei Erhebung und Vorverarbeitung vermehrt als IT-Dienst zur Verfügung. Dementsprechend erfordert der Einsatz von BI-Werkzeugen auf mobilen Geräten (Mobiltelefonen, Netbooks, Smartphones) eine sichere Anpassung an verschiedene physikalische und netzspezifische Umgebungen (z.B. unterschiedliche drahtlose Kommunikation und heterogene Server-Infrastrukturen) sowie veränderliche Arbeitsumgebungen (z.B. Software- oder Sicherheitsanforderungen).

Das Beispiel in Abb. 1 wurde als generisches Szenario in VOGUE entwickelt und setzt sich zusammen aus verschiedenen realen Szenarien. Es zeigt verschiedene IT-Infrastrukturen, die einen Service-Mitarbeiter betreffen, wenn er ein mobiles Gerät für eine sichere Verbindung zur BI-Plattform eines Kundenunternehmens verwendet. Initial nutzt der Mitarbeiter die Infrastruktur des Dienstleistungsunternehmens und ist mit seinem mobilen Endgerät ein Teil dieser Infrastruktur. Der Mitarbeiter hat hier System- und Datenzugriffe entsprechend der Sicherheitsrichtlinie seines Arbeitgebers. Der sichere Einsatz und der sichere Betrieb des Gerätes erfolgt dabei entsprechend eines standardisierten Informationssicherheitsmanagements (z.B. ISO27001).

Im Rahmen der Auftragsbearbeitung wird das mobile Endgerät zudem außerhalb der sicheren Infrastruktur des Dienstleisters verwendet, z.B. im Unternehmensnetz des Kunden. Um nach der Auftragsbearbeitung im Unternehmensnetz wieder Zugriff auf das Netz des Dienstleisters zu erhalten, muss das mobile Gerät vertrauenswürdig sein, d.h. die Sicherheitsanforderungen des Dienstleistungsunternehmens im vorgeschriebenen Umfang erfüllen (z.B. Versionsstand des Betriebssystems, der Anti-Viren-Software, der Firewall und der Sicherheitseinstellungen). Um dies festzustellen, wird der Zustand des mobilen Endgeräts unter Verwendung von Trusted Network Connect (TNC) vor seiner Rückkehr ins Netz des Dienstleisters überprüft [TCG07a]. Sollten diese Anforderungen nicht erfüllt sein, kann ein sicher abgetrennter Bereich im Netz, eine sog. Quarantänezone, verwendet werden, um den vertrauenswürdigen Zustand wieder herzustellen (z.B. durch Rücksetzen von Konfigurationen oder Aktualisierung von Software) [DDN10].

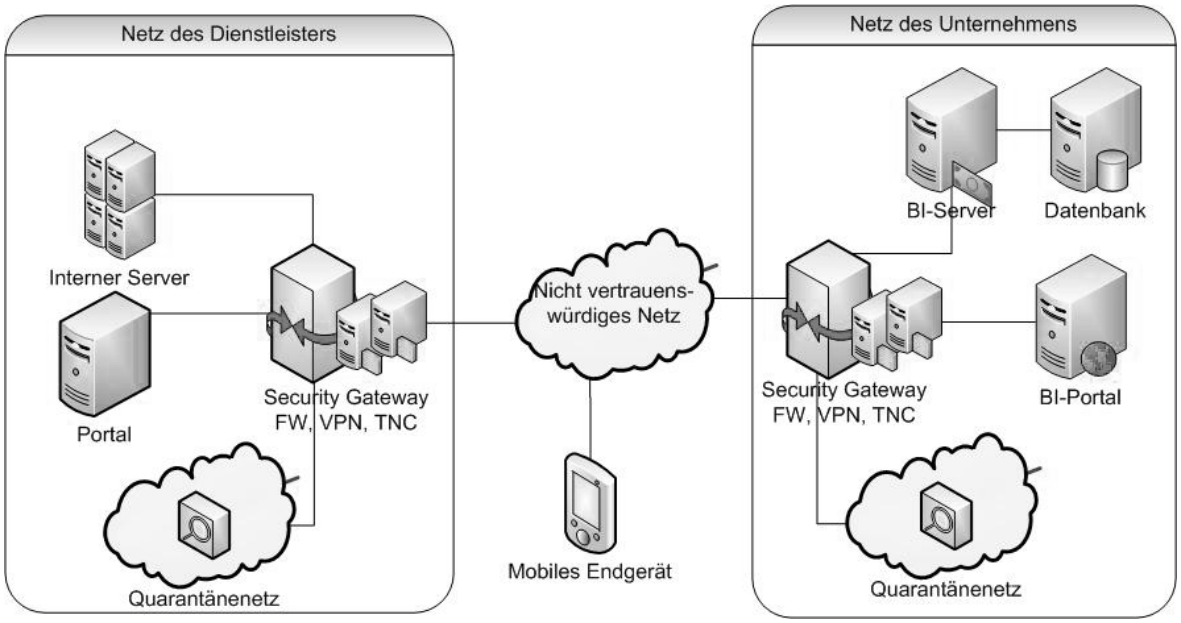

Abb. 1: Unterschiedliche Sicherheitsanforderungen in mobilen BI- Infrastrukturen [DeDiNo10]

Nimmt der Service-Mitarbeiter die Tätigkeit für den Kunden wieder auf oder setzt diese fort, verlässt der Mitarbeiter hierfür die Infrastruktur seines Arbeitgebers und verbindet sich mit dem Netz des Kundenunternehmens. Dieses unterliegt ebenfalls einem standardisierten Informationssicherheitsmanagement, unterscheidet sich jedoch in den verwendeten Sicherheitsrichtlinien (z.B. sicherheitsrelevante Einstellungen, Softwareanforderungen). Daher muss der Mitarbeiter die entsprechenden, vordefinierten Sicherheitsrichtlinien seines mobilen Endgerätes wechseln. Anschließend nimmt er zunächst Verbindung zum Sicherheits-Gateway des Kundenunternehmens auf und authentifiziert sich. Das Sicherheits-Gateway überprüft die Authentifizierung und vergleicht die Informationen zum Systemzustand des mobilen Endgerätes mit den Sicherheitsanforderungen des Kundenunternehmens. Für den Fall, dass dem mobilen Endgerät unabdingbare Sicherheitsmerkmale fehlen (z.B. VPN-Client, aktuelle Fassung der Sicherheitsrichtlinie), wird das mobile Endgerät nur mit einer Quarantänezone verbunden, in der fehlende Daten oder Software zur Verfügung gestellt werden können und die Überprüfung wiederholt werden muss.

Wenn der Zustand des Clients der Sicherheitsrichtlinie des Kundenunternehmens entspricht, wird eine sichere VPN-Verbindung zwischen dem mobilen Endgerät und einem Portal der BI-Lösung in der DMZ des Kundennetzes aufgebaut. Unter Verwendung der Dienste des BI-Portals hat der Mitarbeiter eingeschränkten Zugriff auf die BI-Plattform im Intranet des Kundenunternehmens. Der Zugriff des Mitarbeiters ist auf jene Systemdienste beschränkt, die zur Erfüllung seines Vertrages erforderlich sind, z.B. einen Auftrag abrufen, auf auftragsrelevante Daten zugreifen, Ergebnisse abliefern (neue Daten, Berichte) oder eigene offene Aufträge schließen. Die wesentlichen Herausforderungen in diesem Anwendungsszenario betreffen das sichere Wechseln von Sicherheitseinstellungen durch nicht-privilegierte Nutzer, das Management der Quarantänezonen und Netzzugehörigkeiten, die zuverlässige Zusammenstellung und sichere Übertragung des Zustands des mobilen Endgerätes sowie die Anwendungsfreundlichkeit und Transparenz der entsprechenden Funktionen. Das Management der zwei Quarantänezonen muss, mit Blick auf die Kontrolle des mobilen Endgeräts, den unterschiedlichen Rollen des Mitarbeiters im Dienstleistungs- und Kundenunternehmen entsprechen. Das Dienstleistungsunternehmen, als tatsächlicher Eigentümer des mobilen Endgerätes, wird z.B. wesentliche Software-Updates wie Betriebssystem- und Anti-Virensoftware-Updates zur Verfügung stellen, während jegliche kundenspezifische Software, z.B. der VPN-Client, vom Kundenunternehmen zur Verfügung gestellt wird. Fordert beispielsweise ein mobiles Endgerät mit einer veralteten Virendatenbank eine Verbindung zum Kundennetz an, wird die Verbindung verweigert und der Mitarbeiter darüber informiert, dass er sich mit dem Netz seines Arbeitgebers (des Dienstleisters) verbinden und seine Virendatenbank aktualisieren muss, bevor eine Verbindung zum Kundennetz gestattet wird.

Solche zusätzlichen Sicherheitsanforderungen wirken sich auf die Verfügbarkeit von Netzwerkverbindungen aus und in Folge dessen auf die Anwendungsfreundlichkeit des mobilen Endgerätes. Daher müssen die entsprechenden Sicherheitsmaßnahmen sorgfältig implementiert werden. Erlaubt man z.B. gleichzeitig eine Verbindung in beide Quarantänenetze, kann dies helfen, häufige Wechsel zwischen den beteiligten Netzen zu vermeiden und die Herstellung des erforderlichen Systemzustandes kann dem Nutzer als ein einziger Prozess präsentiert werden.

2 Bedrohungsanalyse

Ein mobiles Endgerät, welches Zugriff auf die Infrastruktur von verschiedenen Unternehmen hat (siehe Abb. 1), unterliegt verschiedenen Bedrohungen. Im Folgenden werden exemplarisch solche Bedrohungen aufgelistet:

B.1. Aufgrund von Sicherheitslücken des Betriebssystems, der Middleware oder der Java Virtuellen Maschine (z.B. im Falle von Android) kann Schadsoftware auf dem mobilen Endgerät eingeschleust werden. Falls beispielsweise der Betriebssystemkern eine Sicherheitslücke enthält, kann Schadsoftware diesen unterwandern (Rootkit).

B.2. Kompromittierte mobile Kommunikationsendgeräte haben das Potential das gesamte Unternehmensnetz zu gefährden. Falls ein solches Gerät im Unternehmensnetz integriert wird, kann es als Ausgangpunkt für die Verbreitung von Schadprogrammen auf andere Netzwerkkomponenten oder die Durchführung von weiteren Angriffen benutzt werden, z.B. Denial-of-Service Angriffe. Zusätzlich kann das kompromittierte mobile Endgerät Spoofing-Attacken durchführen, indem es dem Netz eine falsche Identität vorspielt.

B.3. Ein Angreifer schneidet Informationen mit, welche zwischen einem Endgerät (BI-Client) und dem Unternehmensserver (BI-Server) versendet werden, oder verändert diese Daten nicht autorisiert.

B.4. Ein Mitarbeiter installiert eine Applikation (App) auf dem mobilen Endgerät im Widerspruch zur Sicherheitsrichtlinie, die für das mobile Endgerät festgelegt worden ist. Enthält die Anwendung Schadsoftware oder besitzt sie zu umfassende Rechte (Zugriff auf Kontaktdaten, Geo-Daten etc.), können Sicherheitseinstellungen unbefugt geändert oder auf sensible Daten unbefugt zugegriffen werden. Hierdurch sind Integrität, Vertraulichkeit und Verfügbarkeit des Endgerätes sowie der darauf befindlichen Unternehmensdaten und Applikationen gefährdet

B.5. Ein Mitarbeiter überschreibt die aktuell gültige Sicherheitsrichtlinie auf dem mobilen Endgerät, ohne dass er hierzu autorisiert ist.

B.6. Durch temporären oder dauerhaften Verlust eines mobilen Endgerätes können die drauf gespeicherten, sensiblen Unternehmensdaten für unbefugte Dritte zugänglich sein.

B.7. Der Service-Dienstleister versucht einen nicht autorisierten Zugriff auf das Unternehmensnetz zu erhalten.

In folgenden Abschnitten werden nun Sicherheitsanforderungen an eine vertrauenswürdige Plattform für mobile Endgeräte beschrieben, welche den eben genannten Bedrohungen begegnen.

3 Sicherheitsanforderungen

Für das VOGUE-Szenario, bei dem Nutzer mit mobilen Geräten vertrauenswürdigen Zugang zu Ressourcen eines fremden Netzes erhalten sollen, müssen vier grundlegende Sicherheitsanforderungen erfüllt sein. Geräte und Nutzer müssen zuverlässig authentifiziert werden können. Die Authentizität ausgetauschter, sowie während des Szenarios erzeugter Daten und damit die Integrität derselben während der gesamten Kommunikationsbeziehung muss sichergestellt werden. Weiterhin muss für diese Daten die Anforderung der Vertraulichkeit gegeben sein und schließlich muss durch eindeutige Richtlinien ein vertrauenswürdiger Zustand von Systemen definiert sein.

Aus diesen grundsätzlichen Sicherheitsanforderungen lassen sich funktionale Anforderungen bzgl. geforderter Sicherheitsmechanismen ableiten. Diese sind:

A.1. Abgesicherter, kontrollierter Zugriff auf die IT-Infrastruktur, mit

A.2. Geeigneter Authentisierung der Identität des Access Requestors (AR)

A.3. Vertrauenswürdige, mobile Identitäten (des Gerätes sowie des Nutzers), Identitätsmanagement

A.4. Vertrauliche und authentische Kommunikation zwischen mobilem Gerät und Infrastruktur bzw. der Zielressourcen

A.5. Authentische Kontrollierbarkeit des Gerätezustands

A.6. Richtlinienkonformität des Zustands des Geräts: Anforderungen an Konfiguration, hinreichendes Patchlevel, notwendige Sicherheitssoftware, wie zum Beispiel Firewalls.

A.7. Datensicherheit: Auf dem mobilen Endgerät vorhandene Firmen-, Nutzer- und Plattformdaten (z.B. Adressbuch, Sicherheits-Credentials, E-Mail- und Multimedia Archive oder Sicherheitsrichtlinien) müssen vor nicht autorisierten Zugriffen geschützt werden. Zusätzlich sollen Schutzmaßnahmen gegen Offline-Attacken definiert werden.

A.8. Isolierung und automatische Sanierung: Endgeräte die die Sicherheitsrichtlinien des Unternehmensnetzes nicht erfüllen konnten, sollten vom Rest des Netzes zuverlässig isoliert werden und unter Quarantäne gestellt werden. Wenn erlaubt, sollten kompromittierte mobile Endgeräte, die zu einer Quarantänezone umgeleitet wurden, dort mit den notwendigen Sicherheitsupdates versehen werden. Um die Bemühung für die Ausführung solch einer Strategie, besonders in großen Unternehmen zu verringern, muss der Sanierungsprozess automatisiert sein.

Diese Anforderungen lassen sich nur durch eine Kombination unterschiedlicher Technologien erfüllen. Dazu werden in der Architektur TNC (Trusted Network Connect), VPN (Virtual Private Network) und RADIUS (Remote Authentication Dial In User Service) unter Einsatz geeigneter Richtliniendefinitionen in ein ganzheitliches Netzkonzept integriert.

4 Überblick über die VOGUE-Systemarchitektur

Wie bereits in der Szenario-Beschreibung erklärt, ist das zentrale Thema des Projekts ein Nutzer der im Auftrag eines Unternehmens, mit einem mobilen Gerät Zugriff zu Ressourcen eines weiteren Unternehmens erhalten soll. Nachdem zunächst über einen VPN-Gateway mit Benutzernamen und Passwort der eingeschränkte Zugang zum fremden Netz gewährt wird, ist als nächster Schritt die Identität des mobilen Geräts anhand des entsprechenden Zertifikats zu prüfen (Remote Attestation). Daraufhin ist festzustellen, welche Richtlinien auf dem mobilen Gerät erfüllt sind und inwiefern diese für den Zugriff auf die gewünschten Ressourcen ausreichen oder angepasst werden müssen. Durch Einsatz eines Quarantänenetzes sollen gegebenenfalls Änderungen der Eigenschaften des Geräts (wie zum Beispiel Versionen der Firewall- und Virenschutzsoftware) ermöglicht werden und somit eine Anpassung hinsichtlich der Richtlinien durchsetzen. Erst wenn die Richtlinien (Policys) glaubhaft überprüft wurden, können die Zugriffsrechte des mobilen Geräts auf die geschützten Ressourcen erweitert werden. Eine Übersicht über die einzelnen Rollen und Entitäten, die im VOGUE[1]-Projekt Beachtung finden, gibt Abb. 2.

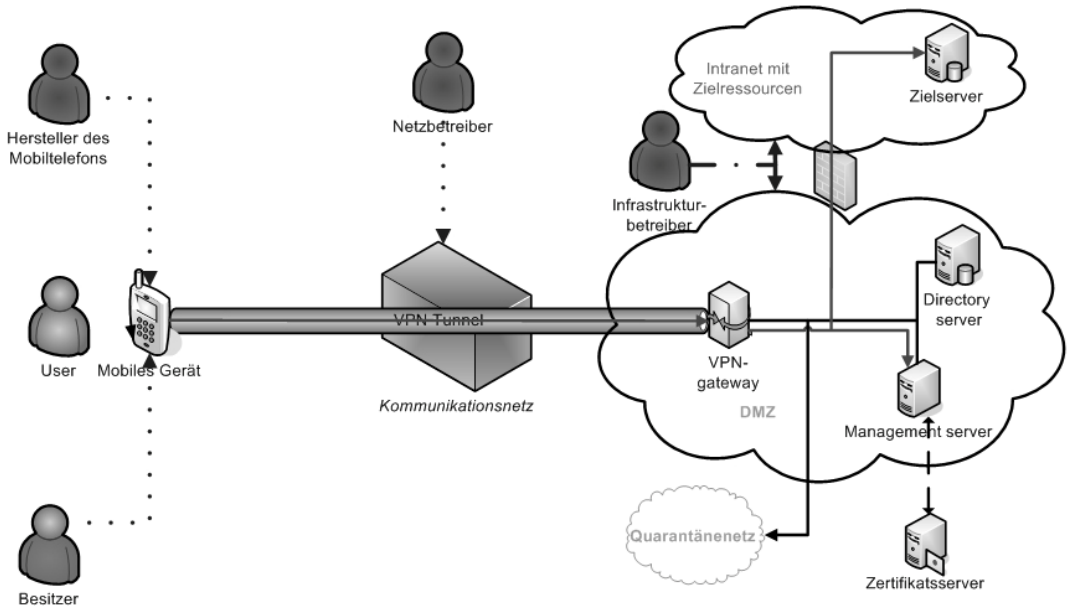

Abb. 2: Übersicht Rollen und Entitäten der VOGUE-Architektur

Durch die Anwendung von mobilen Geräten in fremde Netze und der daraus resultierenden Einflüsse verschiedener Rollen, ergeben sich besondere Anforderungen an die Strategie der Sicherheitsrichtlinien. Nicht nur das Gerät für sich, sondern zusätzlich auch der Nutzer des Geräts müssen verifiziert und gegebenenfalls eingeschränkt werden. In VOGUE wird dies durch eine Aufteilung der Kontrollmechanismen der Richtlinie und somit durch eine zusätzliche Richtlinienkontrolle auf dem mobilen Gerät ermöglicht. So soll allen Partnern ermöglicht werden, Einfluss auf die sicherheitskritischen Einstellungen des mobilen Geräts zu erhalten. Nur dadurch wird eine Vertrauensbeziehung zwischen der Infrastruktur und dem Nutzer möglich. Bei diesem Ansatz ist es wichtig, die Richtlinien in einer einheitlichen und eindeutigen Semantik zu verfassen, um Kohärenz zu gewährleisten.

[1] URL: http://www.vogue-project.de

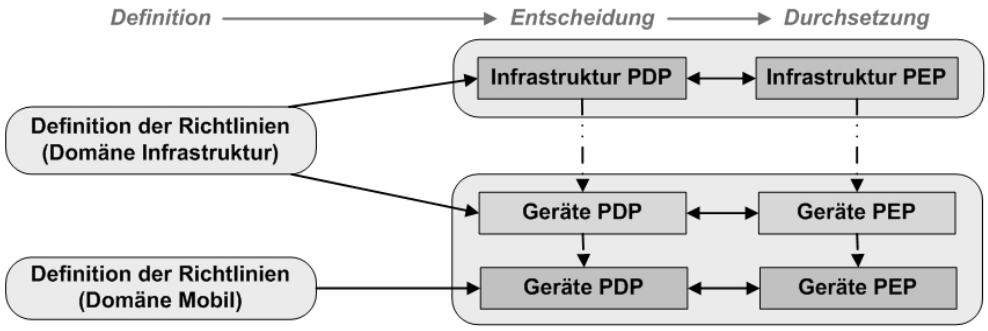

Abb. 3: Aufteilung von PEP und PDP auf Gerät bzw. Infrastruktur

Abb. 3 zeigt die Teilung der Richtliniendomänen in Infrastruktur und Gerät. Dabei steht PDP für Policy Decision Point, also die Instanz, die Informationen erhält und gegen die Richtlinie prüft. Die Durchsetzung der Richtlinien wird durch die Policy Enforcement Points (PEP) erreicht, die außerdem zum Sammeln der nötigen Information dienen. Die Entscheidung und Durchsetzung von Richtlinien bzgl. Infrastrukturressourcen muss auf Infrastrukturseite geschehen. Entsprechend müssen die Richtlinien der mobilen Domäne auf dem mobilen Gerät entschieden und durchgesetzt werden. Im Falle des Einsatzes von Software und Daten auf dem mobilen Gerät, deren Nutzung insbesondere auch nach bzw. ohne Zugang zur Infrastruktur (durch den PEP derselben) unter der Einhaltung der entsprechenden Richtlinien erfolgen soll, ist es also zusätzlich nötig, dass Richtlinienentscheidungen der Infrastrukturdomäne auch auf dem Gerät repräsentiert sind.

Eine detaillierte Grobarchitektur der in VOGUE kombinierten Dienste zur Ermöglichung vertrauenswürdiger Zugriffe auf fremde Unternehmensnetze gibt Abb. 4. Die Architektur lässt sich zunächst in Komponenten der Infrastruktur und in die des mobilen Geräts gliedern. Als mobiles Endgerät könnte ein Smartphone mit einem Linux-basierten Betriebssystem, wie beispielsweise Google Android, zum Einsatz kommen.

Zur Absicherung der Kommunikation eines mobilen Endgeräts mit einer Infrastruktur können Virtual Private Networks (VPN) eingesetzt werden. Diese übernehmen die Prüfung des Nutzers mittels sicherer Authentifizierungsverfahren sowie die Sicherung der Vertraulichkeit und der Integrität von ausgetauschten Nachrichten zwischen zwei VPN-Endpunkten durch geeignete kryptographische Verfahren. Für die Realisierung des VPN werden somit die Komponenten „VPN-Client“ und „VPN-Gateway“, sowie ggf. auf Infrastrukturseite eine entsprechende Management-Architektur (wie beispielsweise ein Zertifikatsserver, ein AAA-Server und ein Verzeichnisdienst) benötigt. Auf dieser Verbindung basierend können daraufhin weitere Eigenschaften des mobilen Geräts geprüft bzw. nachgewiesen werden. Um den aktuellen Zustand des Endgeräts glaubwürdig messen und erfassen zu können, wird Trusted Network Connect (TNC) eingesetzt. Dabei ist hervorzuheben, dass TNC unabhängig von VPN ist. Letzteres ermöglicht nur die verschlüsselte, authentifizierte Kommunikation zwischen den Komponenten des mobilen Endgeräts und der Infrastruktur, es wäre also auch eine andere Technologie einsetzbar.

Hat sich der Benutzer authentifiziert, wird mittels TNC Remote Attestation geprüft, ob sich das Endgerät in einem vertrauenswürdigen Zustand befindet. Ein vertrauenswürdiger Zustand ist ein solcher in dem die Software des Endgeräts einer auf der Infrastrukturseite festgelegten Richtlinie entspricht. Eine solche Richtlinie kann verschiedene Programme erlauben oder

verbieten, Versionsnummern vorschreiben oder Datenzugriffsrechte festlegen. Für diese Überprüfung werden die Komponenten „TNC-Client“ und „TNC-Server“ benötigt. [TCG07a]

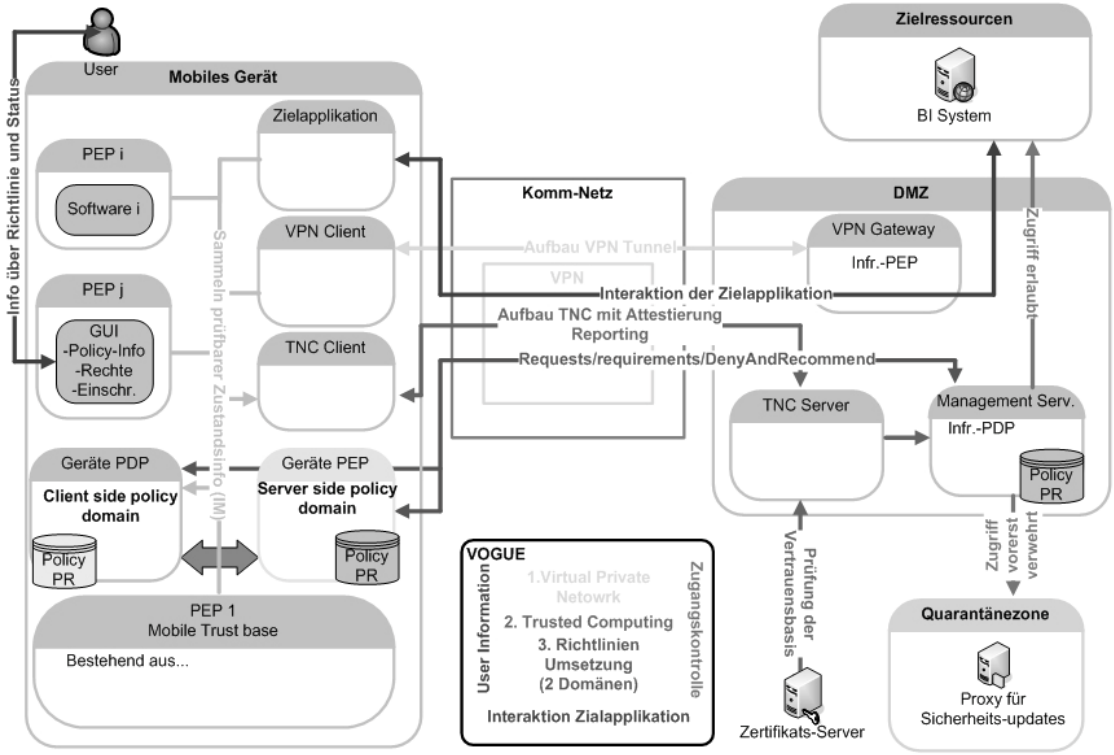

Abb. 4: Grobarchitektur

Wird im Rahmen der Attestierung der Zustand des Endgeräts als unsicher bewertet, beispielsweise aufgrund von veralteter sicherheitsrelevanter Software, erhält das Gerät keinen Zugriff auf die Zielressourcen, sondern wird in einem Quarantänenetz isoliert. Dies kann auf Seiten des VPN-Gateways beispielsweise mittels eines Paketfilters realisiert werden. Innerhalb des Quarantänenetzes kann das Endgerät mithilfe einer Softwareverteilungslösung auf den geforderten aktuellen Stand gebracht werden. Anschließend kann das Gerät gemäß den Spezifikationen von TNC eine erneute Attestierung anfordern.

Für die Richtlinienentscheidung bzw. -durchsetzung ergibt sich eine Ambivalenz. Es müssen in den Policy Decision Points (PDP) die von den beiden Domänen „Mobil“ und „Infrastruktur“ vorgegebenen Richtlinien evaluiert bzw. und durch die Policy Enforcement Points (PEP) entsprechend durchgesetzt werden. Der Entscheidungspunkt der Richtlinien der Domäne „Mobil“ gibt den kleinsten gemeinsamen Nenner der Sicherheitsanforderungen der verschiedenen Domänen vor. Policys der Domäne „Infrastruktur“, die nicht mit den Policys der Domäne „Mobil“ vereinbar sind, können folglich nicht umgesetzt werden. Dies ist sinnvoll, da der Eigentümer des Endgeräts letztendlich die Kontrolle über das Gerät behalten muss. In solchen Situation muss infrastrukturseitig der Zugang zu den Zielressourcen verweigert werden.

Sind alle Voraussetzungen erfüllt, erhält der Nutzer des mobilen Endgeräts mithilfe der Infrastruktur Zugriff auf die gewünschte Zielapplikation und somit auf die Zielressourcen. Während des gesamten Prozesses vom Aufbau der VPN-Verbindung bis zum Zugriff auf die Zielressourcen muss der aktuelle Zustand des Verbindungsaufbaus dem Benutzer jederzeit deutlich gemacht werden. Außerdem muss dem Nutzer jederzeit klar sein, welche Richtlinien auf

seinem Gerät erfüllt sind, bzw. welche Einschränkungen er möglicherweise für die Dauer des Zugangs zur fremden Infrastruktur hinnehmen muss. Nur so kann gewährleistet werden, dass der Benutzer des Endgeräts Vertrauen in das Gesamtsystem hat.

5 Sicherheitslösung

Für das mobile Endgerät wurde im VOGUE-Projekt die Fähigkeit des „Secure Boot“ angenommen: Ein solches Verfahren setzt eine lokale Verifizierung von auszuführendem Code auf dem Endgerät voraus. Mittels Secure Boot wird gewährleistet, dass auf dem Endgerät ein vom Herausgeber zertifizierter Betriebssystemkernel gestartet wird, dessen Authentizität und Integrität gesichert ist. Durch diese Annahme wird der Bedrohung B.1 (Sicherheitslücken im Betriebssystem) entgegengewirkt, sofern ein Mechanismus für Updates des Software Stacks vorgesehen ist. Abb. 5 schildert die mehrstufige Sicherheitsarchitektur für die in VOGUE eingesetzten Android-Plattformen. [DFSD10]

Die in VOGUE eingesetzten Erweiterungen sind gestrichelt umrandet. Die Isolation der einzelnen installierten Applikationen wird auf Anwendungsebene durch die Dalvik VM und die übliche Linux Prozessverwaltung gewährleistet. Der Android Package Installer, der für die Installation von Anwendungen zuständig ist, weist jeder neuen Anwendung jeweils eine individuelle User ID zu. Somit wird auf Dateisystemebene der exklusive Zugriff auf die privaten Daten jeder einzelnen Anwendung sichergestellt. Auf dieser Ebene sind der integrierte VOGUE VPN/TNC Client und die einzelnen Integrity Measurement Collector Komponenten (IMC), welche das Einsammeln von Integritätsdaten im Rahmen eines TNC Handshakes übernehmen, angesiedelt.

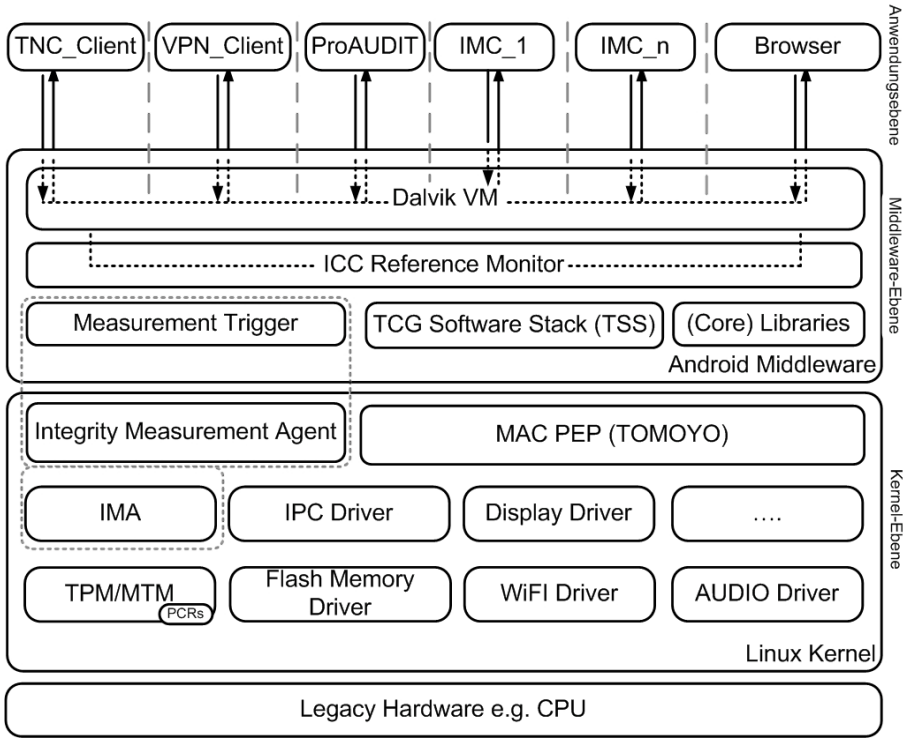

Abb. 5: Übersicht der VOGUE Sicherheitskomponente für mobile Geräte[2]

[2] Android Developer: http://developer.android.com/guide/basics/what-is-android.html

Auf Middleware-Ebene ist der für die Nutzung des TPM Emulators erforderliche Trusted Software Stack (TSS) angesiedelt. Dieser abstrahiert die Kommunikation mit dem TPM und kann von Anwendungen direkt genutzt werden. In VOGUE kommt hier der in die Dalvik VM integrierte Measurement Trigger zum Einsatz. Sobald eine Android-Anwendung gestartet werden soll, wird mittels der auf Kernelebene angesetzten Integrity Measurement Architecture (IMA) [SZJD04] eine Messung des die Anwendung kapselnden Application Packages (apk) durchgeführt und diese mittels des TPM gesichert im Stored Measurement Log abgelegt. Anhand dieses Stored Measurement Log und den Integritätsdaten aus dem TPM kann im Rahmen des TNC Handshakes der aktuelle Zustand bezüglich der gestarteten Anwendungen durch Remote Attestation überprüft werden.

Zusätzlich wurde die Dalvik VM um die Möglichkeit zur lokalen Verifikation von Anwendungen erweitert. Hier wird ein Whitelist-basierter Ansatz verwendet. Policy Decision und Enforcement Point befinden sich hier auf dem Endgerät selbst. Anwendungen, die von der Infrastrukturseite vorgeschrieben werden, mit der lokalen Richtline aber nicht vereinbar sind, führen zu einer Konfliktsituation, die gesondert behandelt werden muss. Es ist hervorzuheben, dass die Auflösung dieses Sonderfalls in VOGUE nicht genauer betrachtet wird. Wie zuvor beschrieben hat der geräteseitige Policy Decision Point in diesem Fall Anwendungsvorrang vor der infrastrukturseitig geforderten Policy. Aufbauend auf dem TNC Stack ist jedoch eine Update-Funktionalität der geräteseitigen Policy denkbar. Hierbei ist besonders auf die Authentizität des Updates der geräteseitigen Policy zu achten. Diese darf nur von dafür zugelassenen Entitäten, beispielsweise dem Arbeitgeber als Eigentümer des Smartphones, erfolgen.

Im Linux Kernel ist der TPM Device Driver angesiedelt, der die Kommunikation zwischen TSS und TPM übernimmt. Das in VOGUE emulierte TPM läuft im Userspace als Linux Prozess im Hintergrund. Es ist hervorzuheben, dass sich die hier beschriebene Architektur mit einem echten TPM einsetzen lässt, sofern die Plattform über ein solches verfügt. So können auf aktuellen ARM Entwicklungsboards I²C TPMs angebunden und verwendet werden.

Ebenfalls auf Kernel-Ebene ist das Mandatory Access Control Framework TOMOYO angesiedelt. Durch entsprechende Policys, die im Rahmen des TNC Handshakes auf das Gerät überspielt werden könnten, können einzelne Anwendungen über das Android Permission Model hinaus in ihren Rechten eingeschränkt werden. So kann beispielsweise unabhängig von den Permissions der Zugriff auf externe Speichermedien generell untersagt werden.

Die Bedrohung B.2 beschreibt den Zugriff auf ein Unternehmensnetz mit einem kompromittierten Endgerät. Daraus ergeben sich die Anforderungen A.1 (kontrollierter Zugriff auf die IT-Infrastruktur), A.2 (Authentisierung des Access Requestors), A.5 (Kontrollierbarkeit des Gerätezustands) und A.6 (Richtlinienkonformität des Zustands des Endgerätes). Um diesen Bedrohungen zu begegnen wird im Kontext von VOGUE Trusted Network Connect (TNC) eingesetzt. Die TNC-Spezifikationen beschreiben eine Architektur zur sicheren Attestierung des Zustands eines Systems über ein Netz. In VOGUE ist hier das Ziel, den Zugriff auf Ressourcen an den Zustand des Endgeräts zu binden und kompromittierte Systeme vor dem Zugriff auf sicherheitskritische Ressourcen zu erkennen. Diese authentische Kontrollierbarkeit des Gerätezustands erfüllt die Anforderung A.5 (Authentische Kontrollierbarkeit des Gerätezustands). Kompromittierte Endgeräte können so frühzeitig erkannt und isoliert werden. Dazu werden die übermittelten Attestierungsdaten mit Referenzwerten verglichen, die in Form einer Richtlinie hinterlegt worden sind. Endgeräte, die nicht den Sicherheitsrichtlinien der Inf-

rastruktur entsprechen, werden in einem Quarantänenetz isoliert und können dort durch den Einsatz einer Softwareverteilungslösung in einen sicheren Zustand überführt werden. Somit ist Anforderung A.8 (Isolation und Sanierung) erfüllt. Der TNC-Server dient hier als Policy Decision Point (PDP), und ein Paketfilter auf Seiten des VPN-Gateways als Policy Enforcement Point (PEP).

Die verschlüsselte Datenübertragung innerhalb des VPN-Tunnels richtet sich gegen Bedrohung B.3 (Mitschnitt von schützenswerten Informationen). Hier müssen sichere Verfahren zur Authentifizierung von Benutzern eingesetzt und aktuelle Verschlüsselungsalgorithmen zur Absicherung der Vertraulichkeit der übertragenen Daten verwendet werden. Des Weiteren ist die Sicherung der Nachrichtenintegrität erforderlich. Sind diese Voraussetzungen erfüllt, kann die Anforderung A.4 (vertrauliche Kommunikation) abgedeckt werden.

Im Rahmen von VOGUE wird die Verbindung zum TNC Server durch eine TLS Session getunnelt (IF-T/TLS). Dadurch ist die VOGUE Implementierung nur von einer bestehenden TCP/IP Verbindung abhängig. Optional kann an dieser Stelle eine weitere Authentifizierung eingesetzt werden. Um Proxy-Angriffe verhindern zu können, sollten im Rahmen der VPN-Verbindung und der IF-T-TLS-Verbindung die gleichen Credentials eingesetzt werden. Der Performanceeinfluss der doppelten Verschlüsselung (VPN und TLS) ist beim Einsatz einer modernen Smartphone-Plattform vernachlässigbar. Die Bedrohung B.4 beschreibt externe Anwendungen, die entgegen der Sicherheitsrichtlinie des Unternehmens von einem Mitarbeiter auf seinem Endgerät installiert werden. In AP 3.1 wurden mehrere Möglichkeiten diskutiert, um möglichen Sicherheitsproblemen, die sich daraus ergeben können, zu begegnen. Zum einen kann durch ein lokales, vertrauenswürdiges Policy Enforcement auf dem Endgerät die Installation derartiger Anwendungen verhindert werden. Zum anderen könnte der Zugriff auf geheime Informationen, die auf dem Gerät verschlüsselt hinterlegt werden, mit Hilfe von Trusted Computing an den Zustand des Endgeräts gebunden werden.

Innerhalb des VOGUE-Projektes wurden Richtlinien auf verschiedenen Ebenen der Architektur definiert, die auf dem Gerät umgesetzt werden müssen, um einen definierten geräteseitigen Sicherheitszustand durchzusetzen. Das Policy Enforcement muss dabei Teil der Vertrauenskette des Endgeräts sein, um sicher gehen zu können, dass es sich korrekt verhält und nur die gewünschten Richtlinien durchgesetzt werden. Zudem gilt es zu beachten, dass neue Richtlinien nur von autorisierten Institutionen (beispielsweise im Rahmen der Softwareverteilung) auf das Endgerät gelangen dürfen. Im Rahmen von VOGUE werden ein MAC Policy Framework auf dem mobilen Endgerät sowie eine Softwareverteilungslösung zur Verteilung bzw. Löschung von infrastrukturseitig vorgegebenen Anwendungen eingesetzt. Dabei kann es sich beispielsweise um zu installierende Anti-Malware Software oder zu entfernende bzw. zu aktualisierende Software handeln. Des Weiteren kann die Software-Update Lösung auch zur Distribution von Richtlinien für das lokale Policy Enforcement auf dem Gerät eingesetzt werden. Auf diese Weise kann der Bedrohung B.6 (Überschreiben der Sicherheitsrichtlinie) begegnet und die Erfüllung von Anforderung A.6 (Richtlinienkonformität des Zustands des Geräts) abgesichert werden.

TNC schreibt die Nutzung eines sicheren Vertrauensankers auf dem Endgerät nicht explizit vor. Um einen mit aktuell eingesetzten Network-Admission-Control-Lösungen, wie Cisco NAC[3] oder Microsoft NAP[4], vergleichbaren Sicherheitsstandard zu gewährleisten ist dies ent-

[3] URL: http://www.cisco.com/web/DE/products/security/nac_home.html

sprechend nicht notwendig. In VOGUE wird zusätzlich eine Emulation eines Hardware-Vertrauensankers (Trusted Platform Module) eingesetzt, um zeigen zu können, wie mittels Remote Attestation ein zusätzlicher Sicherheitsgewinn erreichbar ist. Durch die Nutzung eines Vertrauensankers, der ein erhöhtes Sicherheitsniveau bietet (beispielsweise ein TPM), und der Integrity Measurement Architecture [SZJD04] kann bereits auf Kernelebene festgestellt werden, welche Anwendungen aktuell auf dem Gerät laufen. Eine Repräsentation dieser Informationen, Stored Measurement Log (SML) genannt, wird durch das TPM abgesichert auf dem Gerät abgelegt und mittels Remote Attestation auf Basis von TNC an die Infrastruktur übertragen und dort ausgewertet. Das TPM sorgt dabei für den Schutz der Integrität des SML.

Neben einem infrastrukturseitig vorgeschrieben Patch Level und MAC Policys ist eine Richtlinie denkbar, welche den Zugang zu schützenswerten und daher verschlüsselten Informationen, die auf dem Endgerät hinterlegt sind, an einen zuvor definierten sicheren Systemzustand bindet. Die Umsetzung der Richtlinie setzt voraus, dass der Systemzustand auf dem Gerät selbst korrekt erfasst werden kann. Sofern ein sicherer Vertrauensanker auf dem Mobilgerät zum Einsatz kommt und als Schlüsselspeicher eingesetzt wird, lässt sich dieses Ziel unter Beachtung von Annahme A.1 (korrekte Implementierung des Vertrauensankers) erreichen. Die Durchsetzung dieser Richtlinie durch den Vertrauensanker in Verbindung mit der Bindung der benötigten Schlüssel an einen Systemzustand begegnet Bedrohung B.6 (Datenverlust durch Abhanden gekommene Endgeräte) und erfüllt Anforderung A.7 (unberechtigter Zugriff auf lokale Ressourcen).

Der Zugriff nicht autorisierter Benutzer auf Unternehmensnetze wird in Anforderung B.7 beschrieben. Der Zugriff auf das Unternehmensnetz über beliebige Infrastrukturnetze muss an die Identität des Benutzers des mobilen Endgeräts gebunden werden. In VOGUE wird dazu die VPN Infrastruktur des Konsortialpartners NCP und ein Radius Server eingesetzt. Anhand der hier hinterlegten Informationen können Nutzer sicher authentifiziert werden. So kann der Zugriff unberechtigter Nutzer auf Unternehmensdaten, die nicht auf dem Endgerät hinterlegt worden sind, verhindert werden. Der Radius Server fungiert hier als infrastrukturseitiger Policy Decision Point (PDP), das VPN-Gateway als Policy Enforcement Point (PEP). Die Anforderung A.3 (vertrauenswürdige mobile Identitäten) kann so erfüllt werden. [KRS+10]

6 Ausblick

Im Rahmen des vom BMBF geförderten Verbundprojekts VOGUE werden die Möglichkeiten des Einsatzes von Trusted-Computing-Konzepten auf mobilen Endgeräten untersucht. Die im Rahmen von VOGUE entworfene Sicherheitsarchitektur kann die vorher definierten Anforderungen erfüllen und so den entsprechenden Bedrohungen begegnen. Der zentrale Ansatz ist hierbei die authentische Attestierung des Zustands des Endgeräts gegenüber der Infrastruktur. Im Gegensatz zu den bisher verfügbaren, proprioritären NAC-Lösungen, wie Cisco NAC und Microsoft NAP, basiert der VOGUE-Ansatz auf der standardisierten TNC-Architektur und quelloffenen Software-Komponenten. Diesen Vorteil hat auch Microsoft erkannt, weshalb man sich mit der TNC Working Group auf IF-TNCCS-SOH geeinigt hat, um eine höhere Kompatibilität der Standards zu schaffen. Dazu muss auch der Zustand der Komponenten der TNC-Architektur vertrauenswürdig nachweisbar sein, weshalb eine auf der Annahme eines

[4] URL: http://technet.microsoft.com/en-us/network/bb545879

Secure Boots gründende Vertrauenskette in die Architektur integriert wurde. In Verbindung mit bereits etablierten Standardtechnologien, wie MAC Policy Enforcement und VPN, kann so der Sicherheitsstandard beim unternehmensübergreifenden Einsatz von mobilen Endgeräten weiter erhöht werden.

Danksagung

Das VOGUE-Projekt (http://www.vogue-project.de) ist ein gefördertes BMBF-Projekt mit einer Laufzeit von zwei Jahren, das im Oktober 2009 seine Arbeiten begonnen hat und im September 2011 endet. An dieser Stelle möchten sich die Autoren beim BMBF für die Unterstützung der Forschungsarbeiten bedanken. Ebenso gilt der Dank den Partnern des Projektes, die durch ihre Beiträge und Arbeiten diesen Bericht erst ermöglicht haben.

Literatur

[DDN10] K.-O. Detken, G. Diederich, A. Nowak: Vertrauenswürdiger mobiler Zugriff auf Unternehmensnetze im VOGUE-Projekt. D.A.CH Security 2010: Bestandsaufnahme, Konzepte, Anwendungen und Perspektiven, Herausgeber: Peter Schartner, Edgar Weippl; syssec Verlag; ISBN-13: 978-3-00-031441-4; Wien 2010

[DFSD10] K.-O. Detken, H. S. Fhom, R. Sethmann, G. Diederich: Leveraging Trusted Network Connect for Secure Connection of Mobile Devices to Corporate Networks. In: Communications: Wireless in Developing Countries and Networks of the Future; IFIP World Computer Congress (WCC), Ana Pont, Guy Pujolle, S.V. Raghavan (Eds.), Springer publishing house, Brisbane, Australia 2010

[KRS+10] Kuntze, Rieke, Sohr, Mustafa, Diederich, Sethmann, Detken: Secure mobile business information processing. In: IEEE/IFIP International Symposium on Trusted Computing and Communication (TrustCom), IEEE/IFIP EUC 2010, 11.-13. December, Hong Kong, China 2010

[Schm06] M. Schmiedel: Entwicklung einer Client-/Server-basierten Software für die Prüfung der Vertrauenswürdigkeit von Netzwerkkomponenten. Masterarbeit im Fachbereich Informatik an der FH Hannover, Hannover 2006

[SZJD04] R. Sailer, X. Zhang, T. Jaeger, L. van Doorn: Design and implementation of a TCG-based integrity measurement architecture. In: proceedings of the 13th conference on USENIX Security Symposium – Volume 13 (SSYM'04), Vol. 13., USENIX Association, Berkeley, CA, USA 2004

[TCG07a] Trusted Computing Group, TCG Specification Architecture Overview, Revision 1.3, March 2007

[TCG07b] Trusted Computing Group, TNC IF-IMV Specification v1.2, February 2007

[TCG09] Trusted Computing Group, TNC IF-TNCCS Specification v1.2, May 2009

[Westh10] Johannes Westhuis: Integration von Trusted Computing Technologien in die Android-Plattform. Masterarbeit im Studiengang Angewandte Informatik in der Abteilung Informatik der Fakultät IV an der Fachhochschule Hannover, 19. August 2010, Hannover 2010