



Zentrum für sichere Informationstechnologie – Austria Secure Information Technology Center – Austria

A-1040 Wien, Weyringergasse 35
Tel.: (+43 1) 503 19 63-0
Fax: (+43 1) 503 19 63-66

A-8010 Graz, Inffeldgasse 16a
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

<http://www.a-sit.at>
E-Mail: office@a-sit.at

DVR: 1035461

ZVR: 948166612

SICHERHEITSANALYSE - BLACKBERRY OS 5 (VERSION 1.0.2, 19. APRIL 2010)

Diese Studie wurde von A-SIT im Auftrag des Bundeskanzleramts durchgeführt

Dipl.-Ing. Peter Teufl • IAİK • eMail: peter.teufl@iaik.tugraz.at
Dipl.-Ing. Kurt Dietrich • IAİK • eMail: kurt.dietrich@iaik.tugraz.at

Überblick: In diesem Dokument wird auf die Sicherheitsmerkmale von Research In Motion (RIM) *BlackBerry* Smartphones mit *BlackBerry OS 5* eingegangen. Das Smartphone wird dabei mit unterschiedlichen Subsystemen dargestellt. Jedes dieser Subsysteme wird auf etwaige Gefahren, vorhandene/fehlende Sicherheitsfeatures des Smartphones und mögliche technische/organisatorische Gegenmaßnahmen analysiert.

Die Studie ist eine Überarbeitung und Erweiterung der von A-SIT 2004 veröffentlichten Studie „Sicherheitsanalyse – BlackBerry Mobile Data Service“.

Inhaltsverzeichnis

Inhaltsverzeichnis	2
Glossar, Abkürzungen	3
Abschnitt I: Überblick	4
Abschnitt II: Allgemeines zu Smartphones	4
1. Eigenschaften von Smartphones.....	4
2. Angriffe auf das Smartphone.....	5
3. Angriffe vom Smartphone.....	5
Abschnitt III: Subsystem Analyse	7
1. Application Store/Installation von Applikationen	7
1.1 Beschreibung	7
1.2 Gefahren.....	8
1.3 Sicherheitsfeatures.....	8
1.4 Best Practice.....	8
2. Applikationen.....	8
2.1 Browser.....	9
2.2 Mail.....	10
2.3 Andere Applikationen	12
3. Sensoren.....	13
3.1 A-GPS und Kompass	13
3.2 Mikrophon.....	14
3.3 Kamera	15
3.4 Lagesensoren	15
4. Betriebssystem.....	16
4.1 Beschreibung	16
4.2 Gefahren.....	16
4.3 Sicherheitsfeatures.....	16
4.4 Best Practice.....	18
5. Kommunikation	18
5.1 WLAN.....	19
5.2 Bluetooth	19
5.3 VPN	20
5.4 Mobilfunknetzwerk (Daten), Internet.....	21
5.5 Mobilfunknetzwerk (Telefon)	21
Abschnitt IV: Enterprise Server	23
1. BES Policies.....	23
Abschnitt V: Schlussfolgerungen	25
Abschnitt VI: Referenzen	26

Glossar, Abkürzungen

API	Application Programming Interface
ECC	Elliptic Curve Cryptography
EDGE	Enhanced Data GSM Environment
GPRS	General Packet Radio Service
HSDPA	High Speed Downlink Packet Access
IMAP	Internet Message Access Protocol
IPSEC	Internet Protocol Security
L2TP	Layer 2 Tunneling Protocol
PPTP	Point-to-Point Tunneling Protocol
POP	Post Office Protocol
SIM	Subscriber Identity Module
S/MIME	Secure Multi Purpose Mail Extension
PGP	Pretty Good Privacy
SSL, TLS	Secure Socket Layer, Transport Layer Security (TLS bezeichnet die als RFC standardisierte Version von SSL)
UMTS	Universal Mobile Telecommunications System
VPN	Virtual Private Network
WLAN	Wireless Local Area Network

Abschnitt I: Überblick

Die in diesem Dokument beschriebenen Komponenten des *BlackBerry* [28], deren Sicherheitsfeatures und Sicherheitsmängel beziehen sich auf die Version 5 des *BlackBerry OS*. Die getroffenen Aussagen gelten daher nicht in allen Fällen für andere Versionen.

Die Studie teilt den *BlackBerry* in unterschiedliche Subsysteme, beschreibt deren Sicherheitsfeatures und mögliche Gefahren, die in diesen Subsystemen auftreten können. Zusätzlich werden generelle organisatorische und technische Maßnahmen angegeben, die die Wahrscheinlichkeit eines erfolgreichen Angriffs minimieren. Dabei muss auf folgende Punkte geachtet werden:

- Die Sinnhaftigkeit der Umsetzung von einzelnen Maßnahmen hängt vom geplanten Einsatzgebiet des *BlackBerry* ab und vor allem wie kritisch die darauf verarbeitenden Daten sind.
- Um die beschriebenen Gefahren auszunutzen zu können und Angriffe zu entwickeln, sind teils sehr große Aufwände nötig. Im Falle der Nutzung des Smartphones für die Verarbeitung von hochkritischen Daten ist es aber auch wahrscheinlich, dass diese hohen Aufwände für einen Angreifer akzeptabel sind.
- Die beschriebenen Maßnahmen stellen auf keinen Fall fertige Maßnahmen dar, die in eine Security Policy integriert werden können. Sie sollen vielmehr eine Basis darstellen, die zeigt, welche Punkte bei der Erstellung einer Security Policy beachtet werden können/müssen.
- Da die Subsysteme sehr detailliert behandelt werden, empfiehlt es sich, zuerst die Schlussfolgerungen in Abschnitt V: zu lesen.

BlackBerry Geräte verwenden ein proprietäres Betriebssystem über das es nur wenige öffentliche Informationen gibt. Aus diesem Grund ist man bei den meisten in dieser Studie analysierten Komponenten auf Herstellerangaben und allgemeine Aussagen angewiesen, die über die verwendeten Technologien getroffen werden können. Allerdings setzt *RIM* viele Standardprotokolle ein, über die es detaillierte Sicherheitsanalysen gibt.

Die Analysen werden in zwei Abschnitten behandelt. Abschnitt III: geht auf die Subsysteme des *BlackBerry* ein. Abschnitt IV: ergänzt diese Analyse um Sicherheits-Features die mit Hilfe des *BlackBerry Enterprise Servers* (BES) zur Verfügung gestellt werden. Eine Kernkomponente stellen die *BES Policies* dar, die es erlauben, sehr detaillierte Vorgaben zur Funktionalität und den Einstellungen des *BlackBerry* zu definieren. Diese Policies sind Teil des *BES* und werden ebenso in Abschnitt IV: behandelt. Sie spielen bei fast allen analysierten Subsystemen eine wichtige Rolle.

Wir verweisen weiter noch auf eine Studie die das *BlackBerry OS*, das *iPhone OS* und *Windows Mobile* miteinander vergleicht [36].

RIM bietet ein *Mail-Push Service* an das es ermöglicht, Nachrichten und Daten zwischen Firmennetzwerken und Handhelds nahezu ohne Zeitverlust zu synchronisieren. Diese in den letzten Jahren diskutierte und von A-SIT untersuchte Funktion wurde in Bezug auf Erweiterungen, Updates etc. auf den neuesten Stand gebracht (siehe Abschnitt III:2.2).

Abschnitt II: Allgemeines zu Smartphones

1. Eigenschaften von Smartphones

Der Smartphone-Markt wurde in den letzten Jahren durch die Integration von neuen Bedienkonzepten, neuen Technologien und unterschiedlichen Sensoren in Smartphones immer bedeutender. Dabei können heutige Smartphones sowohl in weiten privaten als auch kommerziellen Bereichen angewendet werden. Aufgrund der neuen Technologien und des Einsatzes des Smartphones als Basisplattform für eine Vielzahl von Applikationen ergeben sich

neben den vielen neuen Möglichkeiten auch neue Gefahren, die bei bisherigen Systemen noch keine oder eine geringere Rolle gespielt haben.

2. Angriffe auf das Smartphone

Um die gesamte Funktionalität der neuen Technologien verwenden zu können, benötigen Smartphones hochentwickelte Betriebssysteme und *Application Programming Interfaces* (APIs). Da die Funktionalität der Smartphone Betriebssysteme schon an die von Desktop-Systemen heranreicht, werden typischerweise keine neuen Betriebssysteme entwickelt, sondern bestehende Systeme an das Smartphone angepasst. So handelt es sich beim *iPhone OS* [22] von *Apple* [20] um eine speziell angepasste Version von *Mac OS X* [26]. Bei *Android* [23] dem Smartphone Betriebssystem von *Google* [22] handelt es sich um eine angepasste *Linux* [24] Version und *Microsoft* [21] hat mit *Windows Mobile* [25] auch ein Smartphone Betriebssystem, das auf der Desktop Version von *Windows* basiert. Im Gegensatz dazu hat *Research In Motion (RIM)* beim *BlackBerry* einen anderen Ansatz gewählt. Das verwendete Betriebssystem (*BlackBerry OS*) ist ein proprietäres Betriebssystem das von keiner Desktop Version abgeleitet ist. Dies mag auch damit begründet sein, dass der *BlackBerry* schon seit 2002 auf dem Markt ist. Die Leistung der verwendeten Hardware und die verfügbare Speicherkapazität waren damals viel zu gering, um komplexe Betriebssysteme wie *OS X* oder *Linux* an das Smartphone anzupassen. Das *BlackBerry OS* wird aber von *RIM* konstant weiterentwickelt und an die neuen Anforderungen angepasst. Dies gilt vor allem auch für den privaten Bereich wo *BlackBerrys* dank neuer Multimedia-Funktionalität immer mehr an Bedeutung gewinnen.

Mit der steigenden Komplexität der verwendeten Betriebssysteme und aufgrund der gemeinsamen Code-Basis, können auf Smartphone Betriebssysteme gleiche oder ähnliche Angriffe wie auf Desktop Systeme durchgeführt werden. Zusätzlich stellen Smartphones aufgrund der Kombination von unterschiedlichen Technologien wertvolle Ziele für Angreifer dar:

- **Positionssensoren (Kompass, A-GPS, Lagesensoren):** Viele Smartphones bieten die Möglichkeit, die eigene Position über GPS, WLAN oder die aktuelle Mobilfunkzelle zu bestimmen. Ein erfolgreicher Angriff, der das Auslesen dieser Daten zulässt, stellt einen tiefen Eingriff in die Privatsphäre dar.
- **Kamera:** Für die Multimedia-Funktionalität spielt bei einem Smartphone die Kamera eine wichtige Rolle. Allerdings kann sie bei einem erfolgreichen Angriff auch für das unerlaubte und für den Benutzer nicht ersichtliche Erstellen von Fotos verwendet werden.
- **Mikrophon:** Analog zur Kamera kann ein erfolgreicher Angriff einen großen Eingriff in die Privatsphäre darstellen.
- **Daten:** Aufgrund der Mobilität und der vielfältigen Funktionen werden Smartphones immer mehr in Bereichen eingesetzt, für die vorher Laptops verwendet wurden. Vor allem im geschäftlichen Bereich bedeutet dies, dass nun auch am Smartphone kritische Daten verarbeitet werden (z.B. über eMails, VPN Zugänge oder HTTP/HTTPS Verbindungen). Nun ist die Wahrscheinlichkeit des Diebstahls/Verlusts höher als bei größeren Geräten (z.B. Laptop). Weiters fehlen dem Smartphone oft Sicherheitsfeatures, die auf Desktop Betriebssystemen bereits lange im Einsatz sind (Datenverschlüsselung, Firewalls, Virens Scanner). Beide Punkte erhöhen die Anzahl und die Relevanz der Gefahren, die vor allem beim Verarbeiten von kritischen Informationen auftreten.

Alle vorher genannten Punkte stellen sowohl bei der privaten Verwendung als auch im kommerziellen Einsatz ein ernstzunehmendes Problem dar. Aus diesem Grund ist es von besonderer Wichtigkeit, dass das Smartphone über Sicherheitsfunktionen verfügt, die erfolgreiche Angriffe auf die unterschiedlichen Komponenten so gut wie möglich verhindern. Weiters müssen spezielle organisatorische und technische Maßnahmen etabliert werden, die speziell auf die neuen Gefahren und Möglichkeiten angepasst sind.

3. Angriffe vom Smartphone

Auch bei der Absicherung der eigenen Infrastruktur müssen die neuen Möglichkeiten der Smartphones und auch die damit verbundenen Gefahren beachtet werden. Aufgrund der Mobilität und der vielseitigen Sensoren eignen sich Smartphones auch hervorragend als Werkzeug für einen Angreifer:

- **Spionage:** Sensoren wie Kamera und Mikrophon ermöglichen es einem Angreifer unerlaubt Gespräche aufzuzeichnen oder kritische Daten/Systeme zu fotografieren.

Weiters könnten Smartphones recht leicht an kritischen Stellen positioniert werden und dann aufgezeichnete Daten an Dritte weiterleiten.

- **Angriffe auf das Netzwerk:** Smartphones können mit entsprechender Software dazu verwendet werden, um Daten über Netzwerke zu sammeln. Bei schlechter Absicherung eines WLANs kann das Smartphone dazu benutzt werden, um weitere Informationen über das dahinterliegende Netzwerk zu sammeln und diese für weitere Angriffe zu benützen.

Bei der Absicherung der eigenen Infrastruktur müssen diese Punkte unbedingt beachtet werden und geeignete Sicherheitsmaßnahmen umgesetzt werden.

Abschnitt III: Subsystem Analyse

In diesem Abschnitt werden die einzelnen Subsysteme des Smartphones analysiert. Die Unterteilung ist in der folgenden Abbildung zu sehen. Die folgenden Sektionen behandeln diese Subsysteme und gehen dabei auf folgende Punkte ein:

- (V1) **Gefahren (V für Vulnerabilities):** Es werden die Gefahren für jedes Subsystem analysiert.
- (V2) **Sicherheitsfeatures (S):** Es werden die Sicherheitsfeatures des jeweiligen Subsystems analysiert. Dabei werden auch nicht vorhandene Sicherheitsfeatures angemerkt. Diese sind mit **rot hinterlegt und umrandet**.
- (V3) **Best Practice (M für Measures):** Hier werden organisatorische und technische Maßnahmen vorgeschlagen die bei der Verwendung des Smartphones beachtet werden müssen. Es wird hier ausdrücklich darauf hingewiesen, dass diese Maßnahmen keine komplette Liste darstellen und der Sinn deren Umsetzung vom Einsatzgebiet des Smartphones und der verarbeiteten Daten abhängt. Die vorgeschlagenen Maßnahmen können aber als Basis für weitere detaillierte und an die Verwendung angepasste Richtlinien verwendet werden.

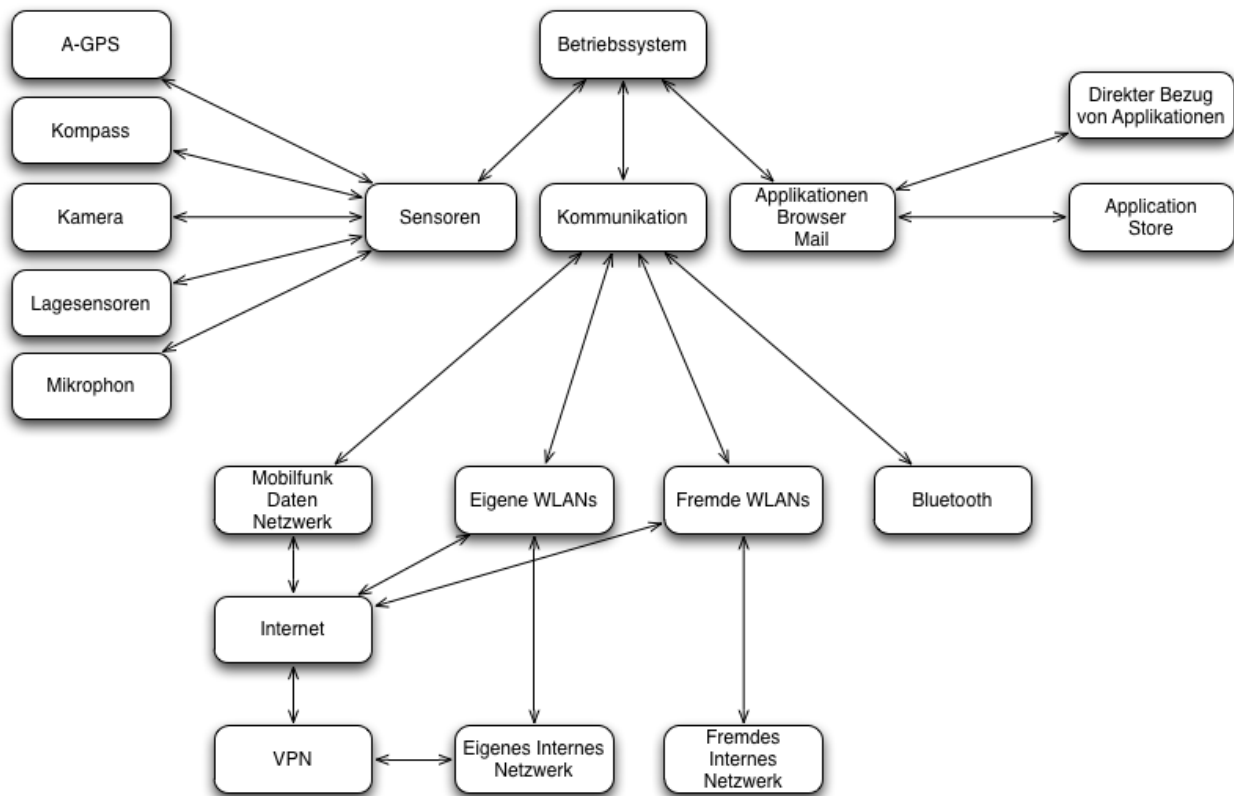


Abbildung 1 - Subsystem Überblick

1. Application Store/Installation von Applikationen

1.1 Beschreibung

Applikationen können direkt über Internet URLs installiert werden. Dies gilt für alle Typen von *BlackBerry* Applikationen (für Details siehe Abschnitt III:4.3.1).

Ähnlich zu den Application Stores von *Apple* (*App Store*) und *Google* (*Android Market*) bietet auch *RIM* einen Application Store für *BlackBerry* Applikationen an – die *BlackBerry App World*.

In Bezug auf die Sicherheit spielen der Freigabeprozess des *App Stores* sowie die dort zur Verfügung gestellten technischen Maßnahmen eine wichtige Rolle. Die etablierten Prozesse und Maßnahmen sollen verhindern, dass bösartige Applikationen von Angreifern eingeschleust werden. Als Beispiel sei hier eine Applikation genannt, die Positionsdaten des Benutzers ausliest und dann ungewünscht an Drittpersonen weiterleitet.

1.2 Gefahren

- (V4) **Einschleusen von bösartigen Applikationen in die BlackBerry App World:** Wenn es einem Angreifer gelingt, eine bösartige Applikation in die *BlackBerry App World* einzuschleusen, dann kann der Angreifer über diese Applikation bösartigen Code nach der Installation am *Smartphone* ausführen. Dies kann zum Verlust von unternehmenskritischen Daten (z.B. eMails) oder zu einer schweren Verletzung der Privatsphäre führen (z.B. das illegale Versenden von Positionsdaten). Beispiele für solche Applikationen gibt es bereits für den von *Apple* zur Verfügung gestellten *App Store* (siehe [10] und [11]). Die dort beschriebenen Gefahren treffen aber auch auf die *App World* von *RIM* zu (siehe auch [12]).
- (V5) **Installation von bösartigen Applikationen:** Es wird auch die Möglichkeit geboten Applikationen direkt über eine URL zu installieren. In diesem Fall wird die *BlackBerry App World* und somit die dort etablierten Freigabeprozesse umgangen. Einem Angreifer bietet sich somit die Möglichkeit, eine bösartige Applikation direkt an den Anwender zu bringen.
- (V6) **Applikationen für Angriffe:** Es gibt Applikationen, deren Funktionalität für bösartige Absichten verwendet werden kann. Als Beispiel seien hier Netzwerk Scanner genannt, die es einem Angreifer ermöglichen, Informationen über ein Netzwerk zu sammeln. So kann damit z.B. ein schlecht abgesichertes WLAN eines Unternehmens untersucht werden und die gesammelten Informationen für weitere Angriffe verwendet werden.

1.3 Sicherheitsfeatures

- (S1) **Widerruf von Applikationen:** Es gibt keine Information von *RIM*, die das Vorhandensein dieser Funktionalität bestätigen. Dies stimmt auch mit dem folgenden Blogeintrag überein, der im Rahmen einer Diskussion über SpyWare auf Smartphones erstellt wurde [12].
- (S2) **Allgemeine organisatorische Maßnahmen:** Im Falle der *BlackBerry App World* werden von *RIM* Richtlinien aufgestellt, die von einem Entwickler eingehalten werden müssen wenn eine Applikation über die *BlackBerry App World* zur Verfügung gestellt werden soll. Für organisatorische und technische Maßnahmen zur Überprüfung der Applikationen wird auf folgende beiden Dokumente verwiesen: [2] und [3]. *RIM* schreibt über den Freigabeprozess folgendes: „*RIM will review a submitted application for content suitability and perform technical testing to ensure the application meets the BlackBerry App World Vendor Guidelines.*“ Über den internen Freigabeprozess und die dort eingesetzten automatischen Verfahren gibt es keine detaillierten Informationen.
- (S3) **Direkter Bezug von Applikationen:** Die Freigabeprozesse der *BlackBerry App World* können umgangen werden, da die Verbreitung von Applikationen auch direkt möglich ist.

1.4 Best Practice

- (M1) **BES Policies:** Es sollten *BES Policies* erstellt werden, die die Installation und das Verwenden von Applikationen regeln. Damit kann auch die Problematik des direkten Bezugs von Applikationen und des etwaigen Ausnützens von Sicherheitslücken im *BlackBerry App World* Freigabeprozess umgangen werden.
- (M2) **Anpassung der Infrastruktur:** Bei der Planung der internen Netzwerkinfrastruktur muss die Gefahr berücksichtigt werden, dass Smartphones von Angreifern für das Beschaffen von Informationen verwendet werden. Hierbei muss bedacht werden, dass deren Verwendung als Angriffswerkzeug aufgrund der Mobilität leichter verheimlicht werden kann.

2. Applikationen

Dieser Abschnitt behandelt die Applikationen eines Smartphones und die möglichen Gefahren, die davon ausgehen. Es werden dabei der Browser und der Email Client getrennt betrachtet, da es sich um die am meisten genutzten Applikationen eines Smartphones handelt.

2.1 Browser

2.1.1. Beschreibung

Der Browser eines Smartphones ist im Prinzip eine unter vielen Applikationen der analog zu diesen für eine bestimmte Aufgabe verwendet wird. In dieser Studie wird aber der Browser aus verschiedenen Gründen getrennt von den anderen Applikationen betrachtet:

- Der Browser ist eine der meist genutzten Komponenten eines Smartphones und wird analog zu den Desktop-Varianten eingesetzt.
- Sicherheitslücken im Browser stellen eine besondere Gefahr dar, da diese unter Umständen durch das Aufrufen von manipulierten Seiten ausgenutzt werden können und einem Angreifer einen recht einfachen Angriffspfad auf das Smartphone ermöglichen.
- Der Browser ist eine komplexe Komponente, die Zugriff auf viele Ressourcen des Smartphones benötigt (z.B. APIs, Dateien). Es ist daher schwer, Technologien wie Sandboxes (siehe 4.3.2) einzusetzen, die den Zugriff auf diese Ressourcen einschränken.
- Der Browser kann für den Zugang zu Webapplikationen des Unternehmens verwendet werden. Die Sicherheit des Browsers hat somit direkten Einfluss auf die Sicherheit dieser Daten.

Der Standard-Browser auf *BlackBerry* Geräten ist der *BlackBerry* Browser. Es können aber auch andere Browser wie der *Opera Mini* [19] installiert werden. In diesem Dokument wird aber nur auf den *BlackBerry* Browser eingegangen.

2.1.2. Gefahren

Die hier genannten Gefahren müssen auch unbedingt zusammen mit den Gefahren zum Abhören oder Manipulieren von Kommunikationsinhalten – (V21), (V22), (V23) in Abschnitt III:5.1 – betrachtet werden.

- (V7) **Sicherheitslücken im Browser:** Etwaige Sicherheitslücken im Browser können von einem Angreifer durch manipulierte Seiten ausgenutzt werden und im schlimmsten Falle zur Übernahme des Smartphones durch den Angreifer führen.
- (V8) **Phishing:** Analog zu Browsern die auf Desktop Systemen benutzt werden, kann der mobile Browser für das Anzeigen von Phishing Seiten genutzt werden, die es zum Ziel haben, Authentifizierungsdaten von Benutzern auszuspionieren. Hier muss darauf geachtet werden, dass sich aufgrund der Smartphone User Interfaces (UI) neue Möglichkeiten zur Darstellung von Phishing Seiten ergeben könnten, die UI Elemente des Smartphones nachbilden.
- (V9) **Einsatz von HTTP:** Prinzipiell gilt für alle Systeme, dass kritische Daten nur verschlüsselt übertragen werden sollen. Dafür wird das HTTPS Protokoll verwendet, das den HTTP Verkehr mit TLS absichert. Aufgrund der Mobilität des Smartphones und dessen Einsatz in fremden, möglicherweise bösartigen WLANs, besteht eine erhöhte Gefahr, dass HTTP Daten abgehört werden. Dies spielt vor allem eine wichtige Rolle, wenn in einem Unternehmen Webapplikationen eingesetzt werden, auf die von Smartphones aus zugegriffen wird.

2.1.3. Sicherheitsfeatures

- (S4) **Fraud Protection:** Es werden keine externen Services (z.B.: *Google* Safebrowsing Feature [32]) für die Erkennung von Phishing Seiten oder Seiten mit Malware verwendet.

2.1.4. Best Practice

- (M3) **BES Policies:** Es sollten *BES Policies* erstellt werden, die die Funktionalität je nach Sicherheitsbedarf einschränken.
- (M4) **Einsatz von VPN:** Um Problemen mit bösartigen Access Points und dem Mitlauschen von HTTP Verkehr zu umgehen, macht es Sinn, zuerst eine VPN Verbindung aufzubauen und darüber den HTTP/HTTPS Verkehr zu tunneln. Damit stehen auch die Sicherheitsmaßnahmen von etwaigen internen Application Firewalls zur Verfügung (z.B. Blacklists von Webseiten, Malware Überprüfung etc.). Der mobile Browser ist somit

einerseits durch die Sicherheitsumgebung des eigenen Netzwerks geschützt und andererseits aufgrund der VPN Verbindung immun gegen Angriffe von etwaigen bösartigen Access Points.

- (M5) **Einsatz von HTTPS:** Ist der Einsatz von VPN nicht möglich, muss bei Verwendung des Browsers an die Möglichkeit von bösartigen Access Points gedacht werden. Diese können zum Mitlauschen von ungesicherten HTTP Verbindungen, für das Weiterleiten auf andere Webseiten und für andere Angriffe verwendet werden. Kritische Informationen dürfen deswegen auf keinen Fall über HTTP Verbindungen übermittelt werden, sondern nur über die mit TLS gesicherten HTTPS Verbindungen.
- (M6) **Gefahren, die auch von Desktop Systemen bekannt sind:** Die Benutzer müssen über die möglichen Gefahren aufgeklärt werden, die auch bei Desktop Systemen auftreten:
- **Phishing:** Benutzer müssen auf die Gefahren hingewiesen werden, die von Phishingseiten ausgehen.
 - **Vertrauenswürdige Seiten:** Benutzer sollen generell auf die Gefahren aufmerksam gemacht werden, die von bösartigen Seiten ausgehen: Ausnutzen von Sicherheitslücken, Phishing etc.
 - **Fremdnetzwerke:** Benutzer sollen auf die Gefahren bei der Verwendung von Access Points hingewiesen werden. Diese werden vor allem aufgrund der geringeren Kosten für den Internetzugriff im Ausland verwendet. Dabei muss bedacht werden, dass Access Points auch von Angreifern mit bösartigen Absichten installiert worden sein können (siehe auch (M4), (M5)).

2.2 Mail

2.2.1. Beschreibung

RIM bietet den Kunden ein *Push-Mail Service* an, das es erlaubt Mailnachrichten, die an ein im Firmennetzwerk registriertes Konto gesendet werden, an ein entsprechend registriertes *BlackBerry* Endgerät weiterzuleiten bzw. vom Endgerät ausgehend über das Firmennetzwerk Mails zu versenden. In Kombination mit dem *Mobilen Daten Service* (MDS) ist es des weiteren möglich, Nachrichten, Kalendereinträge, Adressbücher etc. zwischen BlackBerry Gerät und Firmenkonto automatisch zu synchronisieren ohne dass der Vorgang aktiv vom Benutzer ausgelöst werden muss. Auch das Backup der auf dem Gerät befindlichen Daten kann auf diese Weise erstellt werden. Dabei stellt der *BlackBerry Enterprise Server* die Schnittstelle zwischen dem Handheld und den sich im Firmennetzwerk befindlichen Mailservern (typischerweise MS-Exchange oder Lotus Domino Server) dar. Der BES dient außerdem dazu, Daten an die entsprechenden Einschränkungen die durch die einzelnen Endgeräte entstehen, anzupassen. Dazu gehört beispielsweise das Komprimieren der Daten oder das Konvertieren von PDFs oder Excel-Dateien in ein am Gerät verwendbares Format. Die Verbindung zwischen Handheld und BES ist grundsätzlich gesichert, was sowohl die Vertraulichkeit, Integrität als auch die Authentizität der übertragenen Daten gewährleistet.

2.2.2. Gefahren

- (V10) **Kommunikation wird abgehört:** Wie bei allen mobilen Geräten besteht auch bei BlackBerry Telefonen die Gefahr dass versucht wird, die übertragenen Daten mitzulesen und abzuhören. Dies gilt für alle Arten von übertragenen Daten. In der Vergangenheit wurde vor allem besonderes Augenmerk auf die BlackBerry Infrastruktur gelegt, da über diese die Push Nachrichten übermittelt werden.
- (V11) **Datenverlust durch Diebstahl bzw. Verlust:** Am Gerät gespeicherte Daten können in fremde Hände gelangen. Hier muss anhand der Möglichkeiten, die potentiellen Angreifern zur Verfügung stehen zwischen Hardware- und Softwareattacken unterschieden werden. Dies gilt ebenso für den folgenden Gefahrenpunkt:
- (V12) **Zugang zu Userdaten bzw. der Firmeninfrastruktur:** Ein mit entsprechenden Autorisierungsinformationen ausgestattetes Endgerät ermöglicht es Fremdpersonen, Zugang zur Firmeninfrastruktur des BlackBerry Besitzers und damit Zugriff auf User bzw. firmenspezifische Daten zu erlangen.

2.2.3. Sicherheitsfeatures

Die Verbindung zwischen BlackBerry Endgerät und BES kann verschlüsselt erfolgen. Dafür stehen verschiedene Verfahren zur Verfügung:

- (S5) **Die von RIM entwickelte Lösung via Mail-Push Service:** Dabei kommen zur Verschlüsselung der Kommunikation Algorithmen wie TripleDES bzw. AES zum Einsatz. Alle übertragenen Daten (Nachrichten und Attachments) werden auf diese Weise gesichert – unabhängig vom verwendeten Transportmedium (GSM, Internet etc.). Für die Implementierung dieser Verschlüsselungsalgorithmen an den Endgeräten besitzt RIM eine FIPS-140 Zertifizierung.

Versucht sich nun eine nicht autorisierte Person als ein bestimmter Benutzer auszugeben, um dessen Nachrichten vom Exchange Server abzuholen, so weist ihn der Enterprise Server aufgrund des falschen oder fehlenden Schlüssels zurück. Durch die verwendete Verschlüsselung ist die Verbindung gegen Abhören gesichert.

Bekommt ein Angreifer jedoch ein Gerät in die Hände, so hat er solange Zugriff auf die Daten des Benutzers (Mailbox und Daten am Gerät) bis der Zugang gesperrt wird. Durch Sicherungsmechanismen bei der GSM Übertragung und durch die Verschlüsselung ist es auch nicht möglich, eine bestehende Verbindung zu übernehmen.

Beim Versenden einer Nachricht vom BlackBerry Handheld aus geschieht folgendes: Die Nachricht wird am Handheld verschlüsselt und an den Enterprise Server geschickt. Der BES holt den Schlüssel des Besitzers des Handhelds vom Exchange Server und entschlüsselt die Nachricht. Der Schlüssel des Benutzers befindet sich in so genannten „Hidden Folders“ des Benutzers im Exchange Server Account. Die Nachricht wird nun unverschlüsselt an den Exchange Server weitergeleitet, welcher wiederum die Nachricht dem betreffenden Empfänger zustellt. Empfängt ein Benutzer eine Nachricht in der InBox seines Exchange Server Accounts, so wird der Enterprise Server über die MAPI-Connection informiert, dass eine neue Nachricht vorhanden ist. Ob nun die Nachricht an den Handheld weitergeleitet werden soll, kann durch Filter geregelt werden, die entweder vom Benutzer oder global definiert sind (globale Filterregeln haben Vorrang gegenüber benutzerdefinierten). Die Verbindung zwischen Enterprise Server und Exchange Server kann mittels SSL oder TLS abgesichert werden. Die Nachricht ist somit nur am Enterprise Server und am Exchange Server unverschlüsselt. Entsprechende Maßnahmen zum Schutz dieser Server sind daher notwendig und werden von BlackBerry empfohlen. Die Mail-Push Nachrichten werden dabei über die BlackBerry Infrastruktur verteilt und über BlackBerry Datenzentren in Kanada und Großbritannien, geleitet. Die darüber laufenden Daten zwischen BlackBerry Handhelds und BES sind dabei verschlüsselt, wobei nur die Endpunkte (Handheld, BES) die verwendeten Schlüssel kennen. Eine Entschlüsselung an diesen Knotenpunkten ist somit nicht möglich.

- (S6) **Verbindungen über Standardprotokolle wie HTTPS resp. VPN:** Bei dieser Verbindungsart kommen Standardprotokolle wie SSL/TLS/WTLS/IPSec zum Einsatz.

- (S7) **S/MIME bzw. PGP Support:** Versendete Nachrichten sind auf der Strecke zwischen BlackBerry und BES verschlüsselt. Werden die Mails jedoch an Mail-Server ausserhalb des Firmennetzwerkes gesendet, müssen andere Technologien wie z.B. S/MIME oder PGP verwendet werden. Hierfür gibt es Unterstützung für die BlackBerry Endgeräte in Form eines Softwarepakets für das Versenden von S/MIME oder PGP signierten/verschlüsselten Nachrichten. Dieses Paket bietet eine end-to-end Sicherung der Daten an. Daten bzw. Nachrichten werden am Handheld verschlüsselt und erst wieder beim Empfänger entschlüsselt und nicht an einer Zwischenstation. Allerdings benötigt man dafür ein entsprechendes Zertifikatmanagement und eine PKI Infrastruktur, die sich nach verwendeter Technologie (S/MIME, PGP) und der Verfügbarkeit beim Kommunikationspartner richtet.

Die Installation von Zertifikaten am BlackBerry kann auf verschiedene Arten erfolgen. Nachrichten können (siehe S/MIME Standard) Zertifikate enthalten die vom Benutzer installiert werden können - sofern es die vorgegebene Policy erlaubt. Zertifikate können auch über den Desktop PC, wenn sich das Gerät in der Dockingstation befindet, installiert werden. Zusätzlich kann über den BlackBerry Enterprise Server ein Zertifikatsuchdienst angeboten werden, der das entsprechende Zertifikat sucht, überprüft und über die

drahtlose Verbindung an den Handheld weiterleitet. Der Vertrauensstatus von Zertifikaten kann vom Benutzer selbst bzw. vom Administrator festgelegt werden (je nach Policy). Verschlüsselte Nachrichten die an den BES übermittelt werden, werden wie unverschlüsselte Nachrichten an das BlackBerry Endgerät weitergeleitet. Allerdings kann hier aufgrund der Verschlüsselung keine Formatkonvertierung von etwaigen Attachments durch das MDS durchgeführt werden.

- (S8) **Datensicherheit am Gerät:** Auf die Sicherheit der am Gerät gespeicherten Daten wird in (S9) und (S12) eingegangen.

2.2.4. *Best Practice*

- (M7) **Sicherheit der Daten am Gerät:** Es wird allen Benutzern empfohlen, ihre BlackBerry-Smartphones mit einem Kennwort abzusichern. Das Kennwort muss zum Entsperren und Verwenden des Smartphones eingegeben werden. Über das Menü „Sicherheitsoptionen“ auf dem Smartphone kann die Kennworteingabe aktiviert werden. Die Option kann auch mithilfe der BES-Policy „Password Required“ (Kennwort erforderlich) auf dem BlackBerry Enterprise Server erzwungen werden. Das Smartphone kann so eingestellt werden, dass es entweder in bestimmten Zeitabständen (etwa alle 30 Minuten) automatisch gesperrt oder immer dann gesperrt wird, wenn es sich in der Tasche befindet. Wenn die Option „Content Protection“ (Inhaltsschutz) auf dem Smartphone aktiviert ist, werden die Benutzerdaten auf dem Smartphone mithilfe von AES-256 verschlüsselt. Also, selbst wenn jemand die Benutzerdaten direkt von der Gerätehardware liest, gibt es keine Möglichkeit, die Daten ohne das Smartphone-Kennwort zu entschlüsseln. Ein verloren gegangenes oder gestohlenen BlackBerry-Smartphone kann auch standortfern vom Administrator des BlackBerry Enterprise Server gesperrt oder sogar gelöscht werden, sofern der Server mit dem Smartphone kommunizieren kann. Der Administrator kann außerdem das Kennwort des Smartphones standortfern ändern und Anwendungen auf dem Smartphone löschen.
- (M8) **Auswahl von SSL/TLS Ciphersuites:** SSL und TLS sind Standards, deren Sicherheitseigenschaften relativ gut untersucht wurden. Jedoch sollte bei der Auswahl der verwendete Ciphersuites genaues Augenmerk auf die verwendeten Algorithmen und Schlüssellängen gelegt werden. Ciphersuites die mit EXPORT gekennzeichnet sind, stammen aus Tagen der Export-Beschränkung für starke Kryptographie und sollten nicht mehr verwendet werden. Außerdem sollte der RC4 resp. ARC4 Algorithmus nicht eingesetzt werden, da dieser Algorithmus einige Schwächen aufweist [37], [38].

2.3 *Andere Applikationen*

2.3.1. *Beschreibung*

Die *BlackBerry App World* und auch andere direkte Quellen über Download Links bieten eine große Anzahl an Applikationen die weite private und kommerzielle Bereiche abdecken. Viele dieser Applikationen greifen dabei auf die vom Smartphone zur Verfügung gestellten Sensoren und Technologien zu.

2.3.2. *Gefahren*

- (V13) **Bösartige Applikationen:** Eine bösartige Applikation kann nach deren Installation und dem Ausführen des Benutzers unerlaubt Daten an Dritte übermitteln oder Sicherheitslücken in APIs oder dem Betriebssystem ausnützen und somit das Smartphone übernehmen.
- (V14) **Fehler in der Applikation:** Fehler, die von einem Applikationsentwickler gemacht wurden, können je nach Art des Fehlers von Angreifern ausgenützt werden, um Zugriff auf Daten zu bekommen oder um weitere Angriffe auf das Smartphone durchzuführen.

2.3.3. *Sicherheitsfeatures*

Es muss zwischen unterschiedlichen Sicherheitsaspekten unterschieden werden:

- **Applikationssicherheit in Bezug auf Angriffe:** Hier ist gemeint, wie sicher die Applikation vor einem Angriff ist. Diese Sicherheit kann z.B. durch Bufferoverflows, die durch nicht sorgsame Programmierung des Applikationsentwicklers verursacht wurden, kompromittiert werden. Zum

Großteil gelten hier die allgemeinen Sicherheitsfeatures die vom Betriebssystem selbst geboten werden (siehe Abschnitt III:4.3).

- **Sicherheit in Bezug auf bösartige Applikationen – BlackBerry App World:** Hier sind bösartige Applikationen gemeint, die vom Freigabe Prozess der *BlackBerry App World* nicht als solche erkannt wurden und nach der Installation bösartige Aktivitäten durchführen. Einerseits können solche Applikationen etwaige Sicherheitslücken im Betriebssystem selbst ausnützen. Dies wird durch die Sicherheitsfeatures des Betriebssystems eingeschränkt. Allerdings muss man davon ausgehen dass der Angreifer über diese Features Bescheid weiß und daher die bösartige Applikation entsprechend anpassen kann. Andererseits kann ein Angreifer auch mit den vom Betriebssystem zur Verfügung gestellten APIs auf viele private Daten zurückgreifen, ohne eine Sicherheitslücke auszunützen. Beide Arten von Angriffen sollen durch die Sicherheitsfeatures der *BlackBerry App World* (siehe Abschnitt III:1.3) verhindert werden. Aufgrund der großen Anzahl an Applikationen und der limitierten Möglichkeiten der automatischen Überprüfung von freizugebenden Applikationen ist aber durchaus die Wahrscheinlichkeit gegeben, dass bösartige Applikation nicht erkannt werden (siehe auch Abschnitt III:1).
- **Sicherheit in Bezug auf bösartige Applikationen – Direkter Download:** Hier sind bösartige Applikationen gemeint, die über direkte Download Links angeboten werden. Da dort der Freigabe Prozess der *BlackBerry App World* nicht greift, können hier Applikationen mit bösartigen Absichten den Benutzern angeboten werden.

2.3.4. Best Practice

Generell gelten die gleichen Maßnahmen wie bei Browser (siehe Abschnitt III:2.1) und bei eMail Client (siehe Abschnitt III:2.2). Im Falle von eigenen Applikationen, die für den Zugriff auf Unternehmensdaten verwendet werden, muss bei der Entwicklung der Applikation auf benötigte Sicherheitsfeatures geachtet werden um die verarbeiteten Daten so gut wie möglich abzusichern (Datenverschlüsselung, VPN etc.).

Die Sicherheit im Allgemeinen kann hier maßgeblich durch das Festlegen von *BES Policies*, die die Installation und das Verwenden von Applikationen regeln, erhöht werden.

3. Sensoren

Heutige Smartphones verfügen über unterschiedliche Sensoren die für Applikationen zur Verfügung stehen. In diesem Abschnitt wird auf diese Sensoren, mögliche Missbrauchsszenarien und Gegenmaßnahmen eingegangen.

3.1 A-GPS und Kompass

3.1.1. Beschreibung

Das *Assisted-Global Positioning System* (A-GPS) Modul eines Smartphones ermöglicht die Positionsbestimmung über die Verwendung von unterschiedlichen Technologien:

- **WLAN Access Points:** Verfügbare WLAN Access Points werden mit einer Datenbank verglichen, die über Positionsinformationen dieser Access Points verfügt. Die Datenbanken werden dabei von verschiedenen Anbietern erstellt und zur Verfügung gestellt (z.B. [30]).
- **Mobilfunk Netzwerk:** Dazu wird mit Hilfe der aktuellen Mobilfunkzelle eine Datenbank nach Positionsinformationen abgefragt.
- **GPS:** Die beiden ersten Methoden lassen eine schnelle Positionsbestimmung zu. Da aber damit nur die ungefähre Position bestimmt werden kann, dienen die Methoden nur zur initialen Positionsbestimmung bevor die Position über ein echtes GPS genau bestimmt werden kann. Außerdem ermöglichen sie zumindest eine ungefähre Positionsbestimmung wenn kein GPS Signal vorhanden ist (z.B. in Gebäuden).

Viele Smartphones verfügen auch über einen Kompass, der in Verbindung mit A-GPS vor allem für Augmented Reality Applikationen verwendet wird.

3.1.2. Gefahren

Es muss hier zwischen zwei Gefahren unterschieden werden, die für den Benutzer auftreten können:

- (V15) **Ungewolltes Tracking des Smartphone Users:** Hierbei könnte ein Angreifer die A-GPS Informationen eines Smartphones verwenden, um die Position des Benutzers auszulesen. Dies würde eine schwere Verletzung der Privatsphäre bedeuten.
- (V16) **Fälschung der Positionsinformationen die das Smartphone erhält:** Ein Angreifer könnte die rohen Positionsinformationen fälschen und somit dem Benutzer eine vom Angreifer gewünschte Position zeigen [31].

3.1.3. Sicherheitsfeatures

Der Zugriff auf das A-GPS Subsystem eines Smartphones erfolgt über vom Smartphone Betriebssystem zur Verfügung gestellte APIs. Deren Sicherheit ist kompromittiert, sobald ein Angreifer Zugriff auf das Gerät hat (z.B. durch Ausnutzen einer Sicherheitslücke). Mögliche Angriffsvektoren und Gegenmaßnahmen sind dabei bereits in anderen Subsystemen abgedeckt (z.B. Applikationen, App Store, Schutzfunktionen des Betriebssystems etc.).

3.1.4. Best Practice

Die größte Gefahr stellt hier die Möglichkeit durch einen erfolgreichen Angriff auf die Positionsdaten des Benutzers dar (V15).

Die Gefahr der Fälschung der Positionsinformationen (V16) wird genannt, ist aber für einen Großteil der Smartphone Anwendungsszenarien irrelevant, da erstens der Aufwand für einen erfolgreichen Angriff recht groß ist und zweitens die Genauigkeit der Positionsbestimmung bei Smartphones zu gering für kritische Anwendungen ist, die auf absolut richtige Positionsdaten angewiesen sind.

- (M9) **BES Policies:** Es sollten *BES Policies* erstellt werden, die die Funktionalität je nach Sicherheitsbedarf einschränken. Benutzer müssen sich über die Verwendung A-GPS und den dabei auftretenden Gefahren für die Privatsphäre im Allgemeinen bewusst sein.

3.2 Mikrophon

3.2.1. Beschreibung

Ein Mikrophon wird von jedem Smartphone für die Telefon-Funktionalität benötigt, steht aber typischerweise auch für andere Applikationen zur Verfügung. Gelingt es einem Angreifer Zugriff auf das Smartphone zu erhalten, kann dieses für weiteren Missbrauch verwendet werden.

3.2.2. Gefahren

- (V17) **Mithören von Telefongesprächen:** Bei einem erfolgreichen Angriff auf das Smartphone kann ein Angreifer Zugriff auf das Mikrophon Subsystem des Smartphones erhalten und es für das Mithören von Telefongesprächen missbrauchen.
- (V18) **Mithören von anderen Gesprächen:** Bei einem erfolgreichen Angriff auf das Smartphone kann ein Angreifer Zugriff auf das Mikrophon Subsystem des Smartphones erhalten und das Mikrophon gezielt einschalten, um Gespräche aus der Umgebung abzuhören.

3.2.3. Sicherheitsfeatures

Es gilt gleiches wie für das Subsystem A-GPS und Kompass (Abschnitt III:3.1.3).

3.2.4. Best Practice

- (M10) **Schulung der Benutzer:** Benutzer müssen sich über die möglichen Gefahren bei einem erfolgreichen Angriff auf das Mikrophon Subsystem des Smartphones im Klaren sein.
- (M11) **Einschränkungen für das Benutzen von Smartphones:** Für Räume, in denen vertrauliche Gespräche durchgeführt werden, kann es je nach Vertraulichkeit der Daten

Sinn machen, Smartphones zu verbieten oder nur im ausgeschalteten Zustand zuzulassen. Dadurch lässt sich ein unerwünschtes Mithorchen von Gesprächen vermeiden.

3.3 Kamera

3.3.1. Beschreibung

Die Kamera wird typischerweise von den fix integrierten Applikationen verwendet, die für das Aufnehmen von Fotos und Videos zur Verfügung stehen. Das Kamera Subsystem steht aber auch anderen Applikationen zur Verfügung, um weitere Anwendungsgebiete zu ermöglichen (z.B. Augmented Reality Applikationen). Gelingt es einem Angreifer, Zugriff auf das Smartphone zu erhalten, kann die Kamera für das unerlaubte Aufzeichnen von visuellen Informationen verwendet werden.

3.3.2. Gefahren

(V19) **Unerlaubtes Aufzeichnen von visuellen Informationen:** Bei einem erfolgreichen Angriff auf das Smartphone kann ein Angreifer Zugriff auf das Kamera-Subsystem des Smartphones erhalten und es für das Aufzeichnen von visuellen Informationen (Fotos, Videos) benutzen. Dies ist nur insofern gezielt nutzbar, als die Kamera (ggf. zufällig) auf sensible Inhalte ausgerichtet ist.

3.3.3. Sicherheitsfeatures

Es gilt gleiches wie für das Subsystem A-GPS und Kompass (Abschnitt III:3.1.3).

3.3.4. Best Practice

- (M12) **Schulung der Benutzer:** Benutzer müssen sich über die möglichen Gefahren bei einem erfolgreichen Angriff auf das Kamera-Subsystem des Smartphones im Klaren sein.
- (M13) **Einschränkungen für das Benutzen von Smartphones:** Für Räume oder Bereiche, in denen vertrauliche Informationen visuell erfasst werden können, kann es je nach Vertraulichkeit der Daten Sinn machen, Smartphones zu verbieten oder nur im ausgeschalteten Zustand zuzulassen. Dadurch lässt sich ein unerwünschtes Aufzeichnen von visuellen Informationen verhindern.
- (M14) **BES Policies:** Je nach Verwendung des Smartphones sollten *BES Policies* erstellt werden, die die Funktionalität der Kamera je nach Sicherheitsbedarf einschränken.

3.4 Lagesensoren

Dabei handelt es sich typischerweise um Beschleunigungssensoren, die es ermöglichen, die Lage des Smartphones zu bestimmen. Diese Informationen werden z.B. dazu verwendet, um automatisch eine horizontale oder vertikale Darstellung zu wählen. Weiters können die Informationen für Augmented Reality Applikationen oder für die Steuerung des Smartphones verwendet werden (z.B. Ausführen von Befehlen durch Schütteln).

Im Prinzip gilt hier für Gefahren, Sicherheitsfeatures und Best Practice wie bei dem A-GPS Subsystem. Bei typischen Smartphone Anwendungsbereichen sind die A-GPS Informationen für einen Angreifer wertvoller als die Informationen der Lagesensoren. Allerdings kann es durchaus Szenarien geben, in denen die Informationen der Lagesensoren schützenswert sind und dadurch das Gefahrenpotential höher wird. Etwa gibt eine Lageveränderung zumindest Rückschluss auf Bewegung.

Für weitere Informationen wird auf Subsystem A-GPS und Kompass (Abschnitt III:3.1) verwiesen.

4. Betriebssystem

4.1 Beschreibung

Das Betriebssystem stellt die Kernkomponente eines Smartphones dar. Der Funktionsumfang des Smartphones und vor allem die Sicherheit hängen zu einem großen Teil von dieser Kernkomponente ab. RIM setzt dabei auf die proprietäre Eigenentwicklung *BlackBerry OS*.

4.2 Gefahren

Es werden hier speziell keine Gefahren genannt. Die Sicherheit des Betriebssystems hat aber einen direkten Einfluss auf die Sicherheit der Applikationen und des Smartphones im Allgemeinen. Die relevanten Gefahren werden in den jeweiligen Subsystemen besprochen.

4.3 Sicherheitsfeatures

Die Sicherheit des Smartphones hängt zu einem großen Teil von den Sicherheitsfeatures ab, die vom Betriebssystem angeboten werden.

4.3.1. Applikationstypen

BlackBerry Applikationen werden mit der *Java Micro Edition (Java ME)* [13] entwickelt. Dabei gibt es unterschiedliche Möglichkeiten wie Applikationen zur Verfügung gestellt werden:

- **MIDlets:** Dabei handelt es sich um normale JAR Dateien, die von Java Applikationen verwendet werden. Im Prinzip ist eine JAR Datei eine ZIP Datei, die die vom Java Compiler erstellten Klassen beinhaltet. Es sollte auf jeden Fall Code Obfuscation eingesetzt werden, da sonst der Original Source Code aus den Klassen Dateien extrahiert werden kann. Der Source Code kann zwar auch im Falle von Code Obfuscation extrahiert werden ist dann aufgrund der ersetzten Variablen/Methoden sehr schwer lesbar. Es ist nicht möglich MIDlets zu signieren. Das bewirkt, dass nur auf bestimmte *BlackBerry* APIs zugegriffen werden kann.
- **RIMlets:** *RIMlets* verwenden ein spezielles Dateiformat (COD) von RIM, das das Signieren der Applikation und somit den Zugriff auf alle APIs zulässt. Außerdem kann hier im Gegensatz zu den bei *MIDlets* verwendeten JAR Dateien der Code nicht mehr ausgelesen werden.
- **MIDlets => RIMlets:** Es können auch bestehende *MIDlets* in *RIMlets* konvertiert werden und somit eine Signatur erhalten.

Für eine genaue Auflistung der Vor- und Nachteile der unterschiedlichen Technologien wird auf [8] verwiesen. Für Details zum Erstellen von Signaturen wird auf [9] verwiesen. Um eine Applikation über die *BlackBerry App World* zur Verfügung zu stellen, müssen *RIMlets* (COD Dateiformat) verwendet werden. Die Signatur alleine bewirkt aber noch nicht, dass eine Applikation in die *BlackBerry App World* aufgenommen wird. Dazu sind noch die in (Abschnitt III:1) besprochenen Freigabeprozesse nötig.

Für den direkten Download von Applikationen können sowohl *MIDlets* als auch *RIMlets* erstellt werden, die keinem weiteren Freigabeprozess unterliegen.

4.3.2. Bufferoverflows/Unerlaubter Zugriff auf Ressourcen

Bufferoverflows stellen noch immer ernstzunehmende Sicherheitslücken dar und sind die Ursache für einen Großteil der in den letzten Jahren erfolgten Angriffe. Abgesehen von einem sorgfältigen Programmierstil, der etwaige Buffer Overflows verhindert, gibt es allgemeine Maßnahmen die verhindern, dass diese ausgenutzt werden können.

Es wird hier nur oberflächlich beschrieben wie solche Bufferoverflows ausgenutzt werden können. Für weitere Details wird auf [33] verwiesen:

- Ein gefundener Bufferoverflow kann bewirken, dass ein Angreifer beliebigen Assembler Code einschleusen kann (Code Injection) und diesen ausführen kann.
- Der Angreifer präpariert den einzuschleusenden Code (Shellcode) und fügt die gewünschte Funktionalität hinzu. Ein einfaches Beispiel für diese Funktionalität wäre das Ausführen eines beliebigen Systemkommandos des Betriebssystems.
- Während des Ausführens eines Programms enthält der sogenannte Stack die lokalen Variablen dieses Programms. Durch einen Bufferoverflow ist es dem Angreifer möglich, diese

lokalen Variablen am Stack mit seinem eigenen Code zu überschreiben und diesen zur Ausführung zu bringen.

Es gibt aufgrund des proprietären Betriebssystems leider wenig Details zu Sicherheitsfeatures, die das Ausnutzen von Bufferoverflows verhindern. Allgemein kann folgendes gesagt werden:

- **Java:** Für die Entwicklung von *MIDlets* und *RIMlets* wird *Java* verwendet. Da somit jeder Code in der *Java VM* des *BlackBerry OS* laufen muss, entfallen die typischerweise durch unsorgsam geschriebenen C Code bekannten Buffer Overflows¹.

Folgende Funktionen werden von Betriebssystemen eingesetzt um das Ausnutzen von Bufferoverflows zu verhindern. Da es nur sehr wenige öffentliche Informationen über das *BlackBerry OS* gibt, wird die Funktionalität dieser Technologien hier beschrieben. Es kann aber keine Aussage getätigt werden, ob diese Features im *BlackBerry OS* integriert sind.

- **NX/XN FLAG:** Wie vorher erwähnt kann ein Angreifer durch einen Bufferoverflow beliebigen Code am Stack des laufenden Programms einfügen und dann zur Ausführung bringen. Im Normalfall wird aber am Stack (und auch am Heap) kein Code ausgeführt. Da das Betriebssystem weiß, an welchen Adressen sich der Stack und der Heap befinden, kann es diese Bereiche als lesbar (R), schreibbar (W) aber nicht ausführbar (X) markieren. Stack und Heap sind somit mit den Flags (RW) gekennzeichnet. Ausführbarer Code ist dann nur mehr an den dafür vorgesehenen Teilen möglich (markiert mit (RX)). Moderne Prozessoren unterstützen diese Flags und brechen die Ausführung eines Programms ab, wenn die Instruktionen von Adressbereichen gelesen werden, die nicht über das (X) Flag verfügen. D.h. auch wenn ein Angreifer ausführbaren Code erfolgreich am Stack/Heap einschleust, verhindert das nicht gesetzte (X) Flag die Ausführung des Codes. Das Programm wird dann aufgrund einer Zugriffsverletzung beendet, der Angreifer kann aber den bösartigen Code nicht ausführen. Dem Angreifer bleibt aber immer noch die Möglichkeit andere Funktionen auszuführen, die schon im Speicher des Betriebssystems liegen. Dieser Ansatz wird als *return/libc* Technik bezeichnet. Details dazu werden im nächsten Punkt (ASLR) genannt.
- **Address Space Layout Randomization (ASLR):** Bibliotheken mit unterschiedlichen Funktionen wie das Versenden von SMS, die Steuerung der Kamera, die Berechnung von 3D Grafiken etc. müssen vom Betriebssystem in den Speicher des Smartphones geladen werden. Systemnahe Bibliotheken werden dabei immer benötigt und beim Start des Betriebssystems geladen und sind typischerweise immer an den gleichen Adressen im Speicher zu finden. An diesen Stellen befindet sich der ausführbare Code der Bibliothek. Sind die Adressen der Bibliotheken und deren Funktionen einem Angreifer bekannt, kann dieser nach dem erfolgreichen Ausnutzen eines Buffer Overflows den dort liegenden Code ausführen und somit gewünschte Funktionen ausführen (z.B. Versenden eines SMS, Auslesen der Positionsdaten etc.). ASLR bewirkt dass sich die Bibliotheken immer an zufälligen Stellen im Adressraum befinden. Der Angreifer kann also im Vorhinein nicht wissen, wo er den gewünschten Code finden kann und ist daher bei Vorhandensein des vorher genannten Sicherheitsfeatures (NX/XN Flag) in seinen Möglichkeiten stark eingeschränkt.
- **Sandboxes:** Sogenannten Sandboxes (Sandkasten) erlauben es, Applikationen in einer für sie zugeschnittenen Umgebung laufen zu lassen, die den Zugriff der Applikation auf Ressourcen limitiert. Es gibt z.B. keine Notwendigkeit, dass Applikationen auf bestimmte Systemdateien zugreifen müssen. Im Falle eines ausgenutzten Bufferoverflows und beim erfolgreichen Einschleusen von bösartigem Code kann ein Angreifer trotzdem nicht aus diesen vorgegebenen Sandboxes ausbrechen und erhält damit auch keinen Zugriff auf nicht freigegebene Ressourcen.

4.3.3. Schutzfunktionen

(S9) **Code Signing:** *BlackBerry* Geräte unterstützen Code Signing (siehe 4.3.1).

¹ Die *Java VM* selbst ist in C geschrieben und kann daher Code erhalten, der Buffer Overflows verursacht. Allerdings ist die Wahrscheinlichkeit hier geringer, dass diese ausgenutzt werden.

- (S10) **Datenverschlüsselung:** *BlackBerry* Geräte unterstützen die Verschlüsselung der Daten auf dem Gerät im gesperrten Zustand. Die Vorgaben für diese Verschlüsselung können mit den *BES Policies* gesetzt werden. Dabei spielen neben den Verschlüsselungseinstellungen auch die Passwortrichtlinien eine entscheidende Rolle da die für die Datenverschlüsselung verwendeten Schlüssel mit Hilfe der verwendeten Passwörter abgeleitet werden.
- Interner Speicher:** Es wird ein symmetrischer AES Schlüssel (weilers als KEY-A bezeichnet, Schlüssellängen von 128 bis 256 Bit) verwendet, der die Daten des internen Flash Speichers verschlüsselt wenn das Gerät gesperrt ist. Dieser Schlüssel wird von dem Passwort abgeleitet, das vom Benutzer eingegeben werden muss, um das Gerät zu entsperren. Da KEY-A im gesperrten Zustand nicht vorhanden ist, der *BlackBerry* aber dennoch externe Daten erhalten kann (z.B. eMails), gibt es weiters ein asymmetrisches ECC Schlüssel Paar (KEY-ECC-PRIVATE, KEY-ECC-PUBLIC). Erhält der *BlackBerry* Daten, werden diese mit dem KEY-ECC-PUBLIC verschlüsselt. Der private Schlüssel (KEY-ECC-PRIVATE) zum Entschlüsseln steht im gesperrten Zustand gleich wie KEY-A nicht zur Verfügung. Durch das Eingeben des Passworts wird ein weiterer symmetrischer Schlüssel abgeleitet (KEY-WRAP), mit dem im gesperrten Zustand KEY-A und KEY-ECC-PRIVATE verschlüsselt sind. Beim Entsperrern werden diese beiden Schlüssel mit KEY-WRAP entschlüsselt. Damit können die gespeicherten Daten wieder entschlüsselt werden. Die Sicherheit der Datenverschlüsselung hängt damit direkt von der Sicherheit des verwendeten Passworts ab. Für weitere Details wird auf [39] verwiesen.
- Externer Speicher:** Auch hier ist die Verschlüsselung der Daten möglich.
- (S11) **Löschen der Daten/Remote Wipe:** Es kann festgelegt werden nach wie vielen falschen Passworteingaben der Speicher gelöscht werden soll. Ausserdem bietet der BES einem Administrator die Möglichkeit, das Löschen von Daten aus der Ferne zu initiieren. Dabei muss aber bedacht werden, dass dies vom Angreifer mit einfachen Mitteln und Methoden unterbunden werden kann (z.B. durch Tauschen oder Entfernen der SIM-Karte) und daher keine Garantie für den Erfolg des Löschens gegeben ist.
- (S12) **BES Policies:** Die wichtigste Schutzfunktion stellen *BES Policies* dar. Diese decken alle denkbaren Sicherheitsbereiche des Smartphones ab und können je nach Bedarf detailliert angepasst werden.
- (S13) **Smartcard Reader:** Es gibt die Möglichkeit, Smartcards zu verwenden, die für eine höhere Sicherheit bei kryptographischen Operationen sorgen. Es wird dazu ein *BlackBerry* SmartCard Reader angeboten der über Bluetooth mit dem *BlackBerry* kommuniziert. Ein Beispiel für die Anwendung ist das Signieren/Entschlüsseln von eMails mit Hilfe des S/MIME Standards. Für weitere Informationen wird auf [14] verwiesen.

4.4 Best Practice

- (M15) **Allgemeines:** Bei der Auswahl einer Smartphone-Plattform muss auf die Sicherheitsfeatures des Betriebssystems geachtet werden, da sie die Basissicherheit des ganzen Systems beeinflussen. Im Besondern spielen hier die Sicherheitsfeatures, die beim Ausführen von böartigem Code greifen, eine entscheidende Rolle.
- (M16) **BES Policies:** Um den optimalen Schutz vor Angriffen zu bieten, macht es Sinn, *BES Policies* zu definieren, die die Sicherheit aller *BlackBerry* Komponenten erhöhen.
- (M17) **Datenverschlüsselung:** Wenn kritische Daten am *BlackBerry* verarbeitet werden müssen sollte diese Funktionalität genutzt werden. Es muss dabei auch auf die vorgegebenen Passwortrichtlinien geachtet werden, da die Sicherheit der eingesetzten Schlüssel direkt vom verwendeten Passwort abhängt.

5. Kommunikation

Kommunikation spielt für die Funktionalität eines Smartphones eine zentrale Rolle. Smartphones unterstützen daher unterschiedliche Kommunikationsschnittstellen, die in den folgenden Sektionen analysiert werden.

5.1 WLAN

5.1.1. Beschreibung

Viele *BlackBerry* Modelle bieten wie alle aktuellen Smartphones WLAN Funktionalität und ermöglichen es somit, Netzwerkverbindungen unabhängig von verfügbaren Datendiensten des Mobilfunkproviders herzustellen.

5.1.2. Gefahren

- (V20) **Verwendung als Angriffstool:** Ein Angreifer nutzt das Smartphone als Tool für das Sammeln von Informationen über die Netzwerkinfrastruktur. Bei schlechter Absicherung eines WLANs ist es dem Angreifer dadurch möglich, Details über die dahinterliegenden Netzwerke herauszufinden. Diese Informationen könnten für einen Angriff von dem Smartphone aus oder für die Planung von weiteren Angriffen verwendet werden.
- (V21) **Bösartige WLAN Access Points:** Ein bössartiger WLAN Access Point wird dazu verwendet, um die Kommunikation des Smartphone Benutzers aufzuzeichnen.
- (V22) **Bösartige WLAN Access Points:** Ein bössartiger WLAN Access Point wird für Man-in-the-middle Angriffe verwendet. Der Access Point kann in diesem Fall z.B. DNS Informationen fälschen, um den Benutzer auf andere Seiten umzuleiten, die z.B. für Phishing verwendet werden.
- (V23) **Bösartige WLAN Access Points:** Ein bössartiger WLAN Access Point nutzt etwaige Schwachstellen (z.B. Browser, Netzwerkschnittstellen) in verbundenen Smartphones aus, um das Smartphone unter Kontrolle zu bringen.

5.1.3. Sicherheitsfeatures

- (S14) **WLAN Sicherheit:** Es werden alle aktuellen Authentifizierungsmechanismen unterstützt: Für eine detaillierte Auflistung wird auf [5] verwiesen.

5.1.4. Best Practice

Aus Sicht der internen Infrastruktur:

- (M18) **Interne WLANs:** Bei der Konfiguration und Installation von internen WLANs müssen die neuen Möglichkeiten der Smartphones berücksichtigt werden. Es empfiehlt sich, für Smartphones ein eigenes WLAN einzurichten, das nur die absolut notwendigen Dienste zur Verfügung stellt. Dies ist durch die folgenden Punkte begründet:
 - **Smartphone als Angriffstool:** Aufgrund der Mobilität eines Smartphones kann es recht leicht innerhalb die Reichweite eines internen WLANs gebracht werden.
 - **Gestohlene Smartphones:** Wird ein Smartphone gestohlen und wurden die WLAN Zugangsdaten darauf gespeichert, könnte der Angreifer Zugang zu einem internen WLAN bekommen.

Aus Sicht der Smartphone Sicherheit:

- (M19) **BES Policies:** Es sollten *BES Policies* erstellt werden, die die Verwendung von WLAN regeln.
- (M20) **Schulung der Benutzer:** Die Benutzer müssen auf die Gefahren von bössartigen Access Points aufmerksam gemacht werden.

5.2 Bluetooth

Es konnten keine detaillierten Sicherheitsanalysen über den am *BlackBerry* implementierten Bluetooth Stack gefunden werden. Deswegen werden hier allgemeine Punkte betrachtet. Eine gute Übersicht über sicherheitsrelevante Gefahren und mögliche Gegenmaßnahmen bei der Verwendung von Bluetooth wird in der NIST Studie „Guide to Bluetooth Security“ [35] gegeben.

5.2.1. Gefahren

Es gelten die generellen Gefahren, die im Zusammenhang mit Bluetooth auftreten (siehe [35]).

5.2.2. Sicherheitsfeatures

- (S15) **Bluetooth Stack:** Es werden die Sicherheitsfeatures des Bluetooth Stacks unterstützt.
- (S16) **BES Policies:** Es können Policies definiert werden, die die Verwendung von Bluetooth regeln.

5.2.3. Best Practice

- (M21) **Deaktivieren von Bluetooth:** Generell ist es zu empfehlen Bluetooth nur dann zu aktivieren, wenn es benötigt wird. Dadurch können etwaige Sicherheitsprobleme im Bluetooth Stack nicht ausgenutzt werden.
- (M22) **Allgemeine Maßnahmen:** Für weitere Maßnahmen und generelle Richtlinien wird auf die detaillierte „Guide to Bluetooth Security“ Studie verwiesen [35].
- (M23) **BES Policies:** Es sollten *BES Policies* definiert werden, die nur die absolut notwendige Bluetooth-Funktionalität ermöglichen.

5.3 VPN

5.3.1. Beschreibung

Virtual Private Networks (VPN) spielen im mobilen Bereich eine große Rolle, da sie es dem Benutzer ermöglichen, auf Ressourcen des Heimnetzwerks zuzugreifen, als ob sie direkt in diesem Netzwerk wären. Die VPN Verbindungen werden dabei über eine bestehende Internet Verbindung (WLAN oder Mobilfunk Provider Datendienste) hergestellt.

5.3.2. Gefahren

Siehe Best Practice.

5.3.3. Sicherheitsfeatures

- (S17) **IPSEC:** *BlackBerry* Geräte unterstützen IPSEC und erlauben die Verbindung zu unterschiedlichen VPN Lösungen unterschiedlicher Hersteller. Für eine komplette Liste dieser Hersteller wird auf [5] verwiesen.

- (S18) **L2TP/IPSEC und PPTP:** Diese von Windows Servern verwendeten Protokolle werden nicht unterstützt.

5.3.4. Best Practice

Aus Sicht der internen Infrastruktur:

- (M24) **Eigenes VPN Netzwerk für Smartphones:** Aufgrund der Mobilität des Smartphones muss von einer höheren Diebstahlwahrscheinlichkeit ausgegangen werden. Im Falle von gespeicherten VPN Zugangsdaten oder bei leicht erratbaren Passwörtern steht einem Angreifer der Zugang zum internen Netzwerk und somit zu den dort angebotenen Services zur Verfügung. Es ist daher dringend anzuraten, nur absolut notwendige Services des internen Netzwerks für das Smartphone zur Verfügung zu stellen. Dies kann z.B. durch einen eigenen Netzwerkbereich, der nur an Smartphones vergeben wird, erfolgen. Die von dort aus möglichen Verbindungen sollen durch Firewalls nur auf das absolute Minimum beschränkt werden.

Aus Sicht der Smartphone Sicherheit:

- (M25) **Erhöhung der Sicherheit des Smartphones durch VPN:** Der Einsatz von VPN für Smartphone User bringt unterschiedliche Vorteile:
 - **Schutzfunktionen von internen Firewalls:** Nach dem Aufbau der VPN Verbindung wird die gesamte Netzwerkkommunikation über einen sicheren Kanal zum internen Netzwerk abgewickelt. Dadurch ist der Benutzer in der Lage, interne Services sicher zu benutzen. Weiters können die Vorteile der internen Infrastruktur am Smartphone genutzt werden: Dazu gehört z.B: der Einsatz von Application Firewalls, die Webtraffic auf Malware etc. überprüfen oder Phishing Seiten filtern. Dadurch

können Sicherheitsfeatures, die aufgrund beschränkter Ressourcen am Smartphone fehlen (z.B. Virenschanner), kompensiert werden.

- **Sichere Kommunikation in fremden Netzwerken:** Aufgrund der Mobilität des Smartphones erfolgt der Betrieb des Smartphones in nicht vertrauenswürdigen Umgebungen. Durch den Einsatz von VPN können verschiedene Angriffe vermieden werden (siehe auch (V21), (V22) und (V23)).

5.4 Mobilfunknetzwerk (Daten), Internet

5.4.1. Beschreibung

Die Mobilfunknetzwerke stellen über Technologien wie EDGE, GPRS, UMTS und HSDPA Datenverbindungen zur Verfügung, über die ein Smartphone Zugriff auf das Internet bekommt. Die Kommunikation über das Internet stellt bei Smartphones eine zentrale Komponente dar, die für einen Großteil der Anwendungen eine Rolle spielt.

5.4.2. Gefahren

(V24) **Permanente Internetverbindung:** Typischerweise verbinden sich Smartphones sobald ein dementsprechendes Datennetzwerk vorhanden ist zu diesem Netzwerk und erhalten damit Zugriff auf das Internet. In vielen Fällen erhält das Smartphone dabei eine öffentliche IP Adresse und ist somit auch von überall aus erreichbar. Im Zusammenhang mit anderen Gefahren und möglichen Angriffen auf das Smartphone stellt dies eine Gefahr dar, da ein Angreifer unbemerkt Angriffe starten kann oder im Falle eines übernommenen Smartphones, Daten von diesem aus verschicken kann.

5.4.3. Sicherheitsfeatures

Für den Schutz der Internetverbindung und der offenen Services sind die Sicherheitsfeatures des Betriebssystems und die *BES Policies* von Wichtigkeit (siehe Abschnitt III:4.3 und Abschnitt IV:1).

5.4.4. Best Practice

(M26) **Schulung der Administratoren/Benutzer:** Beide Gruppen müssen sich der Gefahren bewusst sein, die durch die dauernde Internet-Verbindung des Smartphones in unterschiedlichen Netzwerken entstehen.

(M27) **BES Policies:** Auch hier sollten Policies definiert werden, die die Sicherheit der Kommunikation im Internet erhöhen.

5.5 Mobilfunknetzwerk (Telefon)

5.5.1. Beschreibung

Neben den neuen Technologien und Möglichkeiten spielen bei Smartphones das Telefonieren und das Senden/Empfangen von SMS/MMS eine große Rolle. Es wird dafür das Mobilfunknetzwerk des jeweiligen Providers verwendet. Die Applikationen die diese Funktionalität zur Verfügung stellen, laufen gleich wie andere Applikationen in der vom Betriebssystem zur Verfügung gestellten Umgebung und unterliegen deswegen ähnlichen Gefahren.

5.5.2. Gefahren

(V25) **Kommunikationsprozess (Telefon, SMS, MMS, Datendienste):** Bei Smartphone Betriebssystemen wird die Telefonfunktionalität von einem eigenen Prozess zur Verfügung gestellt der parallel zu anderen Diensten läuft. Bei einem erfolgreichen Angriff (z.B. über Browser etc.) auf das Smartphone kann der Angreifer unter Umständen Zugriff auf den Dienst erhalten und somit Zugriff auf Gesprächsdaten/SMS/MMS erhalten.

(V26) **Fehler im Kommunikationsprozess (Telefon, SMS, MMS, Datendienste):** Im Falle von Fehlern in den Telefon/SMS/MMS Applikationen kann diese ein Angreifer über das Mobilfunknetzwerk ausnützen. Es steht damit neben den Internet Verbindungen ein weiterer Angriffsvektor zur Verfügung. Ein Beispiel für so einen Angriff ist unter [34] zu finden.

5.5.3. *Sicherheitsfeatures*

Es greifen hier die Sicherheitsfeatures des Betriebssystems (siehe Abschnitt III:4.3) und die relevanten *BES Policies*.

5.5.4. *Best Practice*

(M28) **Schulung der Benutzer:** Die Benutzer müssen sich über die Gefahren, die durch die Kombination aus unterschiedlichen Technologien auftreten, bewusst sein.

(M29) **BES Policies:** Die Sicherheit sollte auch hier durch das Festlegen von *BES Policies* erhöht werden.

Abschnitt IV: Enterprise Server

RIM bietet für die Konfiguration von *BlackBerry* Smartphones verschiedene Softwareprodukte [6], die sich in den angebotenen Features unterscheiden. Welches Produkt dabei verwendet wird, hängt von der Größe des Unternehmens ab und von den benötigten Features. Es gibt dabei folgende Varianten [7]:

- **BlackBerry® Professional Software:** Es können hier nur 30 Geräte verwaltet werden. Weiters steht nur ein Subset der verfügbaren Policy-Einstellungen zur Verfügung.
- **BlackBerry® Enterprise Server (BES):** Bei dieser Version können alle Policy-Einstellungen vorgenommen werden.
- **Hosted BlackBerry® Services:** Die Funktionalität ist äquivalent zu der des *BES*, aber das Hosting wird nicht vom Unternehmen selbst durchgeführt.

Mit der angebotenen Software können folgende Aufgaben durchgeführt werden:

- Erstellen von detaillierten Sicherheitspolicies, die auf den Geräten umgesetzt werden. Diese Policies können vom Benutzer nicht umgangen werden.
- Push Email Service
- Management von *BlackBerry* Geräten

Es wird nun detaillierter auf die Sicherheitsfeatures des Servers eingegangen:

1. BES Policies

Die *BES Policies* stellen das Kernkonzept der gesamten *BlackBerry* Sicherheit dar. Sie erlauben es, detaillierte Richtlinien zu allen Funktionen und Komponenten des *BlackBerry*s zu erstellen und reichen dabei von detaillierten Vorgaben zur Verwendung von TLS-Verbindungen oder Datenverschlüsselung über Vorgaben zur Verwendung von Kameras, oder A-GPS bis zu Vorgaben zur Verwendung des Telefons und des Internetzugangs.

Die *BES Policies* erlauben es, wirksame technische Gegenmaßnahmen gegen die in den Subsystemen beschriebenen Gefahren zu erstellen. Dadurch können viele Maßnahmen, die bei anderen Smartphones nur organisatorisch umgesetzt werden können (Schulungen, Vorgaben die von Benutzern eingehalten werden müssen), kostengünstig durch sichere technische Maßnahmen ersetzt werden.

Folgende Policy Gruppen, die insgesamt 415 einzelne Policies umfassen, können dabei auf dem Enterprise Server bearbeitet werden:

- **Application Center policy group**
- **BlackBerry Messenger IT Policy group**
- **BlackBerry Smart Card Reader policy group**
- **BlackBerry Unite policy group**
- **Bluetooth policy group**
- **Browser policy group**
- **Camera policy group**
- **Certificate Synchronization policy group**
- **Common policy group**
- **Desktop Only items**
- **Desktop policy group**
- **Device IOT Application policy group**
- **Device Only Items**
- **Documents To Go policy group**
- **Email messaging policy group**
- **Enterprise Voice Client policy group**
- **Firewall policy group**
- **Global items**

- **Instant Messaging policy group**
- **Location Based Services policy group**
- **MDS Integration Service policy group**
- **Memory Cleaner policy group**
- **On-Device Help policy group**
- **Password policy group**
- **PIM Synchronization policy group**
- **PGP Application policy group**
- **RIM Value-Added Applications policy group**
- **S/MIME Application policy group**
- **Secure Email policy group**
- **Security policy group**
- **Security Exclusivity policy group**
- **SIM Application Toolkit policy group**
- **Smart Dialing policy group**
- **TCP policy group**
- **TLS policy group**
- **Wireless Software Upgrades policy group**
- **WTLS policy group**

Abschnitt V: Schlussfolgerungen

Die vorliegende Studie analysiert die Sicherheitsfunktionen des *RIM BlackBerry OS*. Analog zu anderen Smartphones kombinieren *BlackBerry* Geräte unterschiedliche Technologien und integrieren diese in einer Plattform:

- [1] Herkömmliche Mobilfunk Funktionen:
 - a. Telefon
 - b. SMS
 - c. MMS
- [2] Multimedia Funktionalität:
 - a. Kamera
 - b. Mikrophon
 - c. Abspielen von Musik/Videos
- [3] Sensoren:
 - a. Lagesensoren
 - b. A-GPS
- [4] Kommunikation:
 - a. Permanenter Zugriff auf das Internet
 - b. WLAN
- [5] Erweiterbarkeit
 - a. Applikationen in der *BlackBerry App World*

Gerade die Kombination dieser Technologien und das dafür benötigte komplexe Betriebssystem bieten neben neuen Anwendungsgebieten auch neue Gefahren, die beim Einsatz des Smartphones unbedingt bedacht werden müssen. Auch muss die interne Infrastruktur (Netzwerke) an Smartphones angepasst werden.

RIM stellt viele Sicherheitsfunktionen, die prinzipiell das Verarbeiten von kritischen Daten auf den *BlackBerry* Geräten ermöglichen (z.B. Datenverschlüsselung). Eine wichtige Rolle spielt dabei der *BlackBerry Enterprise Server (BES)* und die dort verfügbaren *BES Policies*. Sie erlauben es, sehr detailliert zu definieren, welche Sicherheitsfunktionen am Gerät aktiv sind bzw. welche Funktionen der Benutzer ausführen darf (z.B. Installieren von Applikationen). Die über die Policy vorgegeben Einschränkungen und die gewählte Sicherheitsstufe (z.B. Vorgaben für die Länge von Passwörtern und deren Gültigkeitsdauer) sollten an die am Gerät verarbeiteten Daten angepasst werden.

Allerdings können auch die *BES Policies* und die Sicherheitsfeatures des *BlackBerry OS* nicht alle Angriffe verhindern. Die Restrisiken müssen bei der Entscheidung, welche Daten auf den Geräten verarbeitet werden, unbedingt berücksichtigt werden.

Weiters muss betont werden, dass über das *BlackBerry OS* und den *BES Server* nur sehr wenige vom Hersteller unabhängige Informationen verfügbar sind. *RIM* bietet viele Sicherheitsfunktionen und Features an, die theoretisch sehr gut geeignet sind um Angriffe zu verhindern. Allerdings können Implementierungsfehler nicht ausgeschlossen werden, die von Angreifern durchaus gefunden und ausgenutzt werden können. Aufgrund des proprietären Betriebssystems ist eine unabhängige Überprüfung der vom Hersteller getätigten Aussagen schwer möglich.

Smartphones werden in Zukunft eine immer wichtiger Rolle spielen und dürfen bei der Erstellung von Sicherheitspolicies auf keinen Fall mehr ignoriert werden.

Abschnitt VI: Referenzen

- [1] RIM – BlackBerry App World - <http://na.blackberry.com/eng/services/appworld/> abgerufen am 25.02.2010
- [2] RIM – BlackBerry App World: Vendor Guidelines – abgerufen von <https://appworld.blackberry.com/ismportal/home/guidelines.seam?cid=78460> am 25.02.2010
- [3] RIM – BlackBerry SDK License Agreements – abgerufen von http://na.blackberry.com/eng/legal/SDKLA_english.pdf am 25.02.2010
- [4] RIM – BlackBerry App World Vendor Support – FAQ - abgerufen von <http://na.blackberry.com/eng/developers/appworld/faq.jsp> am 25.02.2010
- [5] RIM - System Requirements and Support for Wi-Fi Enabled BlackBerry Smartphones - [http://na.blackberry.com/eng/atagance/networks/#tab tab wifirequirements](http://na.blackberry.com/eng/atagance/networks/#tab_tab_wifirequirements) am 25.02.2010
- [6] RIM – BlackBerry Business Software – abgerufen von <http://na.blackberry.com/eng/services/business/> am 25.02.2010
- [7] RIM - BlackBerry Software Comparison – abgerufen von [http://na.blackberry.com/eng/services/business/BlackBerry Software Comparison.pdf](http://na.blackberry.com/eng/services/business/BlackBerry_Software_Comparison.pdf) am 25.02.2010
- [8] RIM - C40 Using MIDlets on BlackBerry – abgerufen von [http://na.blackberry.com/developers/resources/C40 Using MIDlets on BlackBerry v3.pdf](http://na.blackberry.com/developers/resources/C40_Using_MIDlets_on_BlackBerry_v3.pdf) am 25.02.2010
- [9] RIM – A60 How and when to sign – abgerufen von [http://na.blackberry.com/developers/resources/A60 How And When To Sign V2.pdf](http://na.blackberry.com/developers/resources/A60_How_And_When_To_Sign_V2.pdf) am 25.02.2010
- [10] Black Hat DC 2010 – Nicolas Seriot – iPhone Privacy – abgerufen von http://seriot.ch/resources/talks_papers/iPhonePrivacy.pdf am 25.02.2010
- [11] Black Hat DC 2010 – Nicolas Seriot – iPhone Privacy Presentation - abgerufen von http://seriot.ch/resources/talks_papers/iPhonePrivacySlides.pdf am 25.02.2010
- [12] Veracode at RSA 2010 – In Which We Dispel Misconceptions - abgerufen von <http://www.veracode.com/blog/2010/02/in-which-we-dispel-misconceptions/> am 25.02.2010
- [13] Oracle – Java ME – abgerufen von <http://java.sun.com/javame/index.jsp> am 26.02.2010
- [14] RIM - BlackBerry Smartcard Reader – abgerufen von <http://na.blackberry.com/eng/atagance/security/products/smartcardreader/> am 26.02.2010
- [15] Apple - iPhone - Download thousands of applications, abgerufen von <http://www.apple.com/iphone/apps-for-iphone/> am 30.06.2009
- [16] Android Market - abgerufen von <http://www.android.com/market/> am 30.06.2009
- [17] BlackBerry App World - abgerufen von <http://mobileapps.blackberry.com/devicesoftware/entry.do?code=appworld> am 30.06.2009

- [18] Developing for iPhone OS 3.1 – abgerufen von <http://developer.apple.com/iphone/> am 25.01.2010
- [19] Opera – Opera Mini – abgerufen von <http://www.opera.com/mini/> am 25.02.2010
- [20] Apple - <http://www.apple.com> abgerufen am 25.01.2010
- [21] Microsoft Corporation – <http://www.microsoft.com> abgerufen am 25.01.2010
- [22] Google - <http://www.google.com/intl/en/about.html> abgerufen am 25.01.2010
- [23] Android - <http://www.android.com/> abgerufen am 25.01.2010
- [24] Linux - <http://www.linux.org/> abgerufen am 25.01.2010
- [25] Windows Mobile - <http://www.microsoft.com/windowsmobile/en-us/default.aspx> abgerufen am 25.01.2010
- [26] Mac OS X Snow Leopard - <http://www.apple.com/macosx/> abgerufen am 25.01.2010
- [27] iPod touch - <http://www.apple.com/ipodtouch/> abgerufen am 25.01.2010
- [28] iPhone - <http://www.apple.com/iphone/> abgerufen am 25.01.2010
- [29] Apple – iPhone – New features in the iPhone 3.1 Software Update – abgerufen von <http://www.apple.com/iphone/softwareupdate/> am 25.01.2010
- [30] Skyhook Wireless - <http://www.skyhookwireless.com/> abgerufen am 26.01.2010
- [31] Nils Ole Tippenhauer, Kasper Bonne Rasmussen, Christina Pöpper, Srdjan Capkun - *iPhone and iPod Location Spoofing: Attacks on Public WLAN-based Positioning Systems* - Technical Report 599 - ETH Zürich - System Security Group - April 2008 – abgerufen von <ftp://ftp.inf.ethz.ch/pub/publications/tech-reports/5xx/599.pdf> am 26.01.2010
- [32] Google Safe Browsing API - <http://code.google.com/apis/safebrowsing/> abgerufen am 26.01.2010
- [33] Aleph One - .oO Phrack 49 Oo. - Volume Seven, Issue Forty-Nine - Smashing the Stack for Fun and Profit – abgerufen von <http://insecure.org/stf/smashstack.html> am 28.01.2010
- [34] cnet - *Researchers attack my iPhone via SMS* - abgerufen von http://news.cnet.com/8301-27080_3-10299378-245.html am 28.01.2010
- [35] NIST – Guide to Bluetooth Security – abgerufen von <http://csrc.nist.gov/publications/nistpubs/800-121/SP800-121.pdf> am 24.02.2010
- [36] J.Gold Associates - Choosing an Enterprise-Class Wireless Operating System: A Comparison of BlackBerry, iPhone and Windows Mobile – abgerufen von http://na.blackberry.com/eng/atagance/get_the_facts/Choosing_an_enterprise-class_wireless_operating_system.pdf am 25.03.2010
- [37] Souradyuti Paul and Bart Preneel - New Weakness in the RC4 Keystream Generator and an Approach to Improve the Security of the Cipher, Fast Software Encryption - FSE 2004, pp245 – 259, abgerufen von: <http://www.cosic.esat.kuleuven.be/publications/article-40.pdf> am 29.03.2010
- [38] Scott R. Fluhrer, Itsik Mantin and Adi Shamir, Weaknesses in the Key Scheduling Algorithm of RC4, Selected Areas in Cryptography 2001, pp1 – 24, – abgerufen von http://www.wisdom.weizmann.ac.il/~itsik/RC4/Papers/Rc4_ksa.ps am 29.03.2010

- [39] Technischer Überblick – Sicherheit - BlackBerry Enterprise Solution
[http://docs.blackberry.com/de-de/admin/deliverables/12191/BlackBerry Enterprise Solution--847262-1116042902-003-5.0.1-DE.pdf](http://docs.blackberry.com/de-de/admin/deliverables/12191/BlackBerry_Enterprise_Solution--847262-1116042902-003-5.0.1-DE.pdf), abgerufen von [http://docs.blackberry.com/de-de/admin/deliverables/12190/Related_resources STO 849766 11.jsp](http://docs.blackberry.com/de-de/admin/deliverables/12190/Related_resources_STO_849766_11.jsp) am 29.03.2010
- [40] RSA SecurID Token für BlackBerry, abgerufen von <http://germany.rsa.com/node.aspx?id=1165> am 29.03.2010