F A C H H O C H S C H U L E W E D E L

S E M I N A R A R B E I T

in der Fachrichtung

Wirtschaftsinformatik

Seminar:

IT-Sicherheit
Wintersemester 2012/2013

Thema:

Mobile Sicherheit

Philipp Bonfigt (winf9006)

Seminarleiter: Prof. Dr. Gerd Beuster

Inhaltsverzeichnis

Abbildungsverzeichnis

1. Einführung

Mobile Endgeräte weisen gegenüber stationären Geräten wesentliche Unterschiede auf, welche auch für die IT-Sicherheit von Bedeutung sind. So werden häufig andere Schnittstellen für Kommunikation und Datenaustausch verwendet, welche angreifbar sind, falls keine entsprechenden Sicherheitsmaßnahmen getroffen werden. Auch ist z.B. ein Diebstahl durch den kleineren Formfaktor und dem Betrieb in ungesicherten Umgebungen weitaus wahrscheinlicher. Die „Mobile Sicherheit“ beschäftigt sich daher damit, den sicheren Betrieb mobiler Endgeräte zu gewährleisten.

Im Folgenden werden die verschiedenen Angriffsvektoren mobiler Endgeräte am Beispiel eines Smartphones erläutert. Einen Überblick soll die folgende Abbildung geben.

Abb. 1: Smartphone Angriffsvektoren[1]

[1] Grafik entnommen aus Heider J.: Smartphone-Sicherheit im betrieblichen Einsatz

Smartphones sind für Angreifer ein lohnenswertes Ziel, da häufig vertrauliche Geschäftsdaten darauf gespeichert sind. Bei einer Studie des Forschungsinstitutes Dynamic Markets sollen mehr als 90 Prozent der Befragten angegeben haben, dass sie „vertrauliche Geschäftsinformationen und Dokumente auf ihren Geräten speichern“[2].

Gleichzeitig ist ein rasanter Anstieg der Anzahl an verwendeten mobilen Endgeräten zu beobachten. Als Beispiel zeigt die nachfolgende Abbildung die Entwicklung der Anzahl an Smartphone-Nutzern in Deutschland.

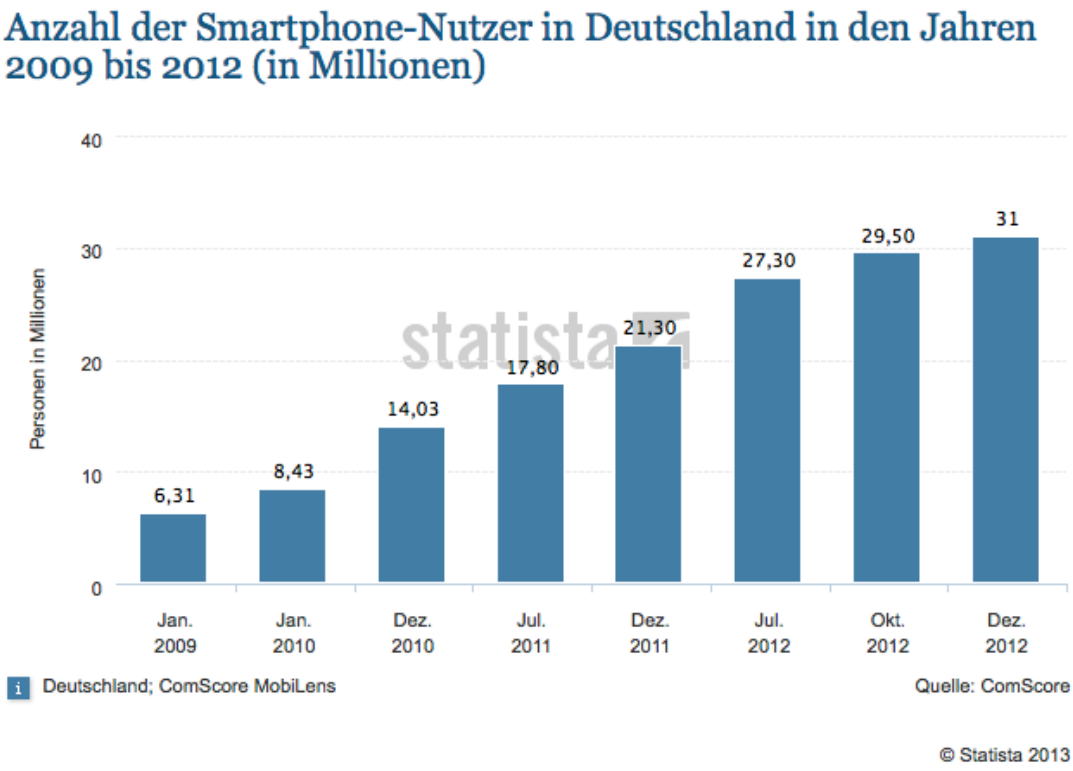

Abb. 2 Smartphone-Nutzer in Deutschland[3]

[2] vgl. Kabodt F.: Riskanter Umfang mit vertraulichen Daten auf mobilen Endgeräten

[3] Grafik entnommen von der Internetseite statista.de, die Daten wurden von folgender Studie verwendet: Mohamud A., Block B.: 2013 Future in Focus – Digitales Deutschland

2. Logische Angriffsvektoren

Unter dem Begriff „logische Angriffsvektoren“ fasst man alle Angriffsvektoren zusammen, die Angriffe auf logischer Ebene ermöglichen. Dabei werden Sicherheitslücken im Betriebssystem und in den Anwendungen des Smartphones genutzt. Angriffe die solche Angriffsvektoren nutzen sind dadurch gekennzeichnet, dass sie aus der Ferne ausgeführt werden können, bzw. der Angreifer sich nicht in der Nähe des Geräts befinden muss.

2.1. Kommunikationsdienste

Einen wesentlichen Bestandteil von Smartphones sind die Kommunikationsdienste. Sie ermöglichen dem Benutzer auch unterwegs in Kontakt zu bleiben. Neben SMS und der Telefonie ist die Nutzung von Internetdiensten, wie E-Mail, Instant-Messenger oder VoIP mittlerweile selbstverständlich. Allerdings können diese Dienste auch dazu genutzt werden einen Angriff durchzuführen[4]. Besitzt der Angreifer die Kontaktdaten des Smartphone-Nutzers für einen dieser Dienste, kann er über diesen Nachrichten versenden. Hierbei versucht der Angreifer seine wahre Identität zu verschleiern und sich gegenüber dem Empfänger als eine vertraute oder bekannte Person auszugeben. Mit dem gewonnenen Vertrauen fordert der Angreifer den Empfänger z.B. dazu auf bestimmte Informationen zu offenbaren oder einen der Nachricht angehängten Schadcode auszuführen. Diese Vorgehensweise ist vor allem beim E-Mail Dienst unter dem Begriff Phishing bekannt. Sie kann aber genauso auch auf andere Kommunikationsdienste übertragen werden.

Ein grundlegendes Problem beim Austausch von Nachrichten ist es, die Vertraulichkeit sicherzustellen. Die von den Kommunikationsdiensten versendeten Datenpakete können theoretisch an jedem Punkt des Übertragungsweges mitgelesen werden. Daher sollte darauf geachtet werden, dass ausgetauschte Nachrichten ausreichend verschlüsselt sind.

2.2. Browser

Der Web-Browser ist auf Smartphones eine Anwendung, die sehr häufig verwendet wird. Viele Web-Seiten wurden daher mit Stylesheets für die Darstellung auf mobilen Endgeräten angepasst. Die Internetseiten enthalten einen zunehmend dynami-

[4] vgl. Heider J., El Khayari R., 2012: Geht Ihr Smartphone fremd?, S. 2

scheren Inhalt. Um client-seitige Dynamik ausreichend zu unterstützen sind hierfür entsprechende Standards erforderlich, die zunehmend komplexer werden. Die zunehmende Komplexität macht es wahrscheinlich, dass Sicherheitslücken entstehen[5].

Über diese versuchen Angreifer Sicherheitsmechanismen des mobilen Endgeräts auszuhebeln und so weiteren Zugriff zu erhalten. So kann der Smartphone-Nutzer z.B. per E-Mail auf eine Internetseite gelockt werden, die so manipuliert ist, dass das Smartphone automatisch einen kostenpflichtigen Anruf tätigt, den der Nutzer nicht abbrechen kann. Bei einer entsprechend teuren Rufnummer kann auf diese Weise ein finanzieller Schaden entstehen[6].

2.3. Baseband Prozessor

In den letzten Jahren wurde vermehrt die Möglichkeit von Angriffen auf mobile Endgeräte über den Baseband-Prozessor diskutiert[7]. Aufgrund der Aktualität dieses Themas ist dieser Abschnitt etwas ausführlicher gestaltet.

2.3.1. Mobilfunk-Basisstation

Der wesentliche Unterschied von Mobilfunknetz und Festnetz besteht darin, dass die Endgeräte über Funk kommunizieren. Daher besteht das Mobilfunknetz aus einer flächendeckenden Anzahl von Funkzellen, die jeweils durch eine sog. Basisstation versorgt werden. Ein mobiles Endgerät stellt zur Kommunikation also zunächst eine Funkverbindung zu einer Basisstation her, die das empfangende Signal anschließend über eine Kabelverbindung zur nächsten Vermittlungsstelle im Netz weiterleitet. Diese Konstellation wird in Abbildung 1 dargestellt.

[5] vgl. Heider J., El Khayari R., 2012: Geht Ihr Smartphone fremd?, S. 2
[6] vgl. o.V.: iPhone ruft automatisch Abzock-Nummer an
[7] vgl. Weinmann R.-P.: Baseband Attacks

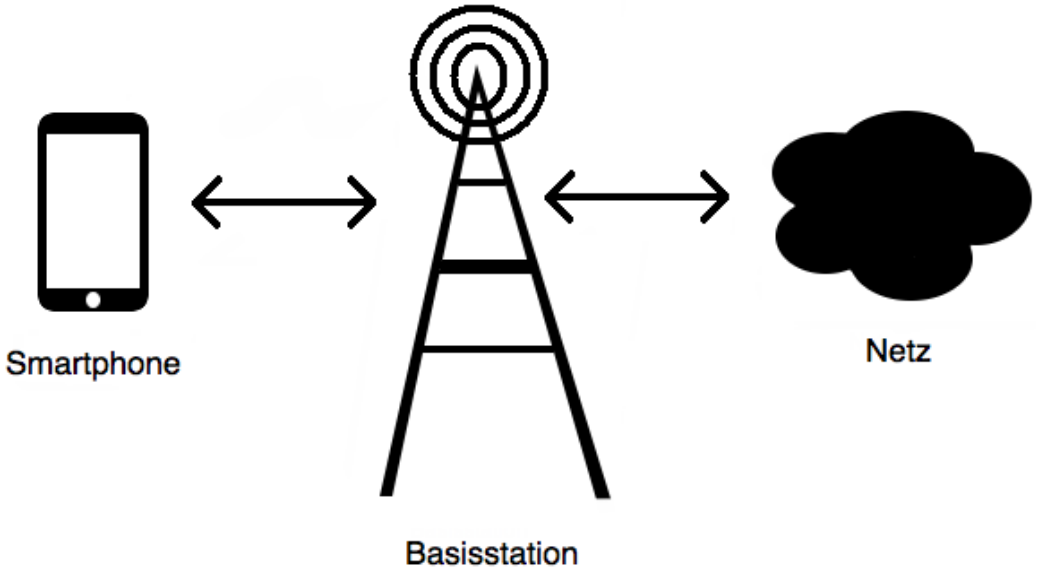

Abb. 3 Mobilfunkkommunikation

2.3.2. Funktion des Baseband-Prozessors

Der Prozessor eines Smartphones lässt sich grob in einen Applikationsprozessor und den Baseband-Prozessor unterteilen. Auf dem Applikationsprozessor werden das Betriebssystem und die Anwendungen ausgeführt. Der Baseband-Prozessor kodiert und dekodiert die Datenströme, die zur Basisstation gesendet bzw. von ihr empfangen werden.

2.3.3. Das Prinzip des Angriffs und die Auswirkungen

Für einen Angriff stellt der Angreifer nun selbst eine manipulierte Basisstation zur Verfügung (dies ist heute mit einem überschaubaren Mitteleinsatz und OpenSource-Lösungen wie z.B. OpenBTS realisierbar)[8]. Damit ist ein Man-in-the-middle-Angriff zwischen mobilem Endgerät und einer Basisstation möglich. Hierbei wird der Umstand ausgenutzt, dass mobile Endgeräte sich immer mit der nächstliegenden Basisstation verbinden. Der Benutzer hat darüber keine Kontrolle. Durch so einen Angriff hat der Angreifer zunächst die Möglichkeit alle übertragenden Daten mitzulesen. Dies ist gefährlich wenn unverschlüsselte Daten ausgetauscht werden. Der Angriff erhält aber eine noch größere Tragweite, wenn Sicherheitslücken in der Firmware des Baseband-Prozessors existieren. Über diese kann der Angreifer

[8] vgl. Weinmann R.-P.: Baseband Attacks, S.1

Schadcode auf dem Smartphone zur Ausführung bringen, indem er diesen in manipulierten Datenpaketen mit Hilfe der manipulierten Basisstation an das Gerät sendet. Sicherheitslücken in der Firmware sind allerdings nicht leicht zu finden. Wenn der Quellcode zur Firmware vorliegt, kann dieser durchsucht werden. Ansonsten besteht noch die Möglichkeit mittels Reverse-Engineering[9] die Binärdateien eines Firmware-Updates auszuwerten. Der Aufwand kann sich aber lohnen, da es mit manipulierten Datenpaketen z.B. möglich sein kann eine bestimmte Person zu überwachen, indem Kamera oder Mikrofon kontrolliert werden. Auch die Position könnte mit Hilfe des GPS-Empfängers verfolgt werden. Angreifer können die manipulierte Basisstation an einem beliebigen Ort platzieren. Orte an denen sich viele Menschen aufhalten oder besonders vertrauliche Gespräche geführt werden können dabei eine hohe Erfolgsquote für Angriffe dieser Art bedeuten. Als Smartphone-Nutzer kann man sich gegen diese Art von Angriffen kaum wehren. Daher wird insbesondere an die Hersteller mobiler Endgeräte appelliert die Firmware des Baseband-Prozessors auf Sicherheitslücken untersuchen und diese zu schließen.

2.4. Smartphone Apps

Mit Hilfe von zusätzlich installierbaren Apps kann die Funktionalität von mobilen Endgeräten erweitert werden. Diese sind meist über einen sogenannten Store des jeweiligen Betriebssystems erhältlich. In den Stores von Apple iOS und Android existiert ein riesiges Angebot an Apps. Die Preise sind oft sehr niedrig oder die Anwendungen werden über Werbe-Einblendungen finanziert. Mit den geeigneten Entwicklungsumgebungen ist es recht einfach eine Anwendung zu programmieren. Die Schwierigkeit besteht eher darin die App gegen Angriffe zu schützen. Die Schwierigkeit, die Sicherheit einer App zu gewährleisten und der Preisdruck in den App-Stores begründen, warum viele der vorhandenen Anwendungen immer wieder Sicherheitslücken aufweisen[10]. Als Smartphone-Nutzer sollte man daher darauf achten, ob eine App ausreichend geprüft oder zertifiziert wurde.

Anwendungen können auch von Angreifern absichtlich so entwickelt werden, dass diese eine Backdoor für Hacker darstellen. Anwendungen dieser Art tauchen auch immer wieder in den offiziellen Stores auf. Insbesondere die Installation von Anwen-

[9] vgl. Weinmann R.-P.: Baseband Attacks, S. 3
[10] vgl. Heider J., El Khayari R., 2012: Geht Ihr Smartphone fremd?, S. 3

dungen anderen Quellen sollte vermieden werden, da diese Apps nicht auf Schadcode überprüft werden.

In Bezug auf den Datenschutz gibt es auch eine Vielzahl an Anwendungen in den App-Stores, die bestimmte Daten, wie z.B. Standortdaten oder Kontakte an den Gerätehersteller, Provider oder Anbieter von Analysediensten weiterleiten ohne das der Smartphone-Nutzer dies mitbekommt.

2.5. Multimedia-Player

Oft werden Multimedia-Inhalte, wie mp3- oder PDF-Dateien auf Smartphones verwendet. Ein Multimedia-Player, der in der Lage ist diese komprimierten Datenströme zu verarbeiten ist auf dem Gerät meist bereits vorinstalliert. Es gibt aber auch von Drittanbietern viele Anwendungen mit gleicher Funktion. Die Verarbeitung der Datenströme kann allerdings mit Sicherheitslücken behaftet sein[11]. Diese nutzen Angreifer aus, um Schadcode zur Ausführung zu bringen. Hierzu muss eine Multimedia-Datei jedoch zunächst entsprechend manipuliert werden und anschließend auf dem Gerät geöffnet werden. Hierbei gab allerdings auch einen Fall in dem iPhone-Nutzer eine Sicherheitslücke in der Verarbeitung von PDF-Dokumenten bewusst nutzten, um einen Jailbreak durchzuführen[12].

2.6. Fernwartung

Wenn Unternehmen ihren Mitarbeitern für die Arbeit Smartphones zur Verfügung stellen, sind sie meist auch mit dem Problem konfrontiert die Sicherheit der mobilen Endgeräte zu gewährleisten. Insbesondere bei Unternehmen kann durch den Verlust vertraulicher Daten ein hoher finanzieller Schaden entstehen. Um dieses Risiko zu verringern gibt es für das sog. Mobile-Device-Management bestimmte Fernwartungs-Tools, die es erlauben die Geräte der einzelnen Mitarbeiter zentral zu verwalten[13]. So können aus der Ferne die Sicherheitskonfigurationen durchgeführt werden und wichtige Updates installiert werden. Auch können die Smartphones regelmäßig auf unerwünschte Anwendungen untersucht werden und diese per Fernlöschung vom Gerät entfernt werden. Für die Fernwartung muss auf dem mobilen Endgerät eine Schnittstelle bereitgestellt werden. Diese kann allerdings auch angreifbar sein.

[11] vgl. Heider J., El Khayari R., 2012: Geht Ihr Smartphone fremd?, S. 3
[12] vgl. Bachfeld D., Mulliner C.: Mobile Bedrohungen
[13] vgl. Heider J., El Khayari R., 2012: Geht Ihr Smartphone fremd?, S. 3

Verschafft sich ein Angreifer die nötigen Zugangsdaten oder kann er die Sicherheitsbarrieren umgehen, erhält er so ebenfalls die Kontrolle über das Gerät.

2.7. Anwender

In vielen Fällen nutzen Angreifer aber auch den Umstand aus, dass die Nutzer der mobilen Endgeräte zum Teil wenig Hintergrundwissen über die mobile Sicherheit besitzen. Es wird versucht den Nutzer zu täuschen[14]. So kam es bereits vor, dass Angreifer einen unechten Warnhinweis auf einer Webseite platziert haben, der beim Bestätigen Schadcode auf dem Gerät installierte[15]. Auch können Fehlentscheidungen bei den Sicherheitseinstellungen der mobilen Endgeräte getroffen werden. Unkenntnis über mögliche Verschlüsselung oder Sperrcodes können Angriffe vereinfachen. Anwendern sollte daher zumindest Basiswissen über mobile Sicherheit vermittelt werden, um das Risiko eines Angriffs zu verringern.

2.8. Homebanking

Um ein sicheres Homebanking zu ermöglichen, setzen die meisten Kreditinstitute ein oder mehrere TAN-Verfahren ein. Neben dem Anmelde-Passwort muss der Nutzer bei diesen Verfahren für jede durchzuführende Transaktion seine Identität durch die Eingabe einer Transaktionsnummer nachweisen. Die TAN wird dem Nutzer unabhängig vom Anmelde-Passwort zur Verfügung gestellt. Allgemein wird diese Art von Verfahren als Two-Factor-Authentication bezeichnet. Das relativ aktuelle „Mobile TAN“-Verfahren (kurz mTAN) ermöglicht es dem Nutzer sich mit Hilfe seines Mobiltelefons zu verifizieren. Prinzipiell erhält der Nutzer dabei die TAN per SMS von der Bank. Ein Angriff ist also insbesondere dann möglich, wenn der Angreifer das mobile Endgerät in seinen Besitz gebracht hat. Doch auch ohne Diebstahl ist das Verfahren angreifbar. Der GSM-Standard auf dem deutsche Mobilfunknetze basieren, verwendet für die sichere Kommunikation eine Stromverschlüsselung. Die verwendeten Chiffren A5/1 und A5/2 können mit ein wenig Hardwareaufwand fast in Echtzeit entschlüsselt werden[16][17]. Das QR-TAN Verfahren wird als eine sichere Alternative zum mTAN-Verfahren vorgeschlagen[18].

[14] vgl. Heider J., El Khayari R., 2012: Geht Ihr Smartphone fremd?, S. 3
[15] vgl. Lerg A.: Zeus-Trojaner attackiert deutsche Online-Banking-Nutzer
[16] vgl. Weinmann R.-P.: Baseband Attacks, S. 1

3. Physische Angriffsvektoren

Die zweite Kategorie unter der Angriffsvektoren zusammengefasst werden können ist die der physischen Angriffsvektoren. Diese ermöglichen Angriffe auf physischer Ebene und sind vom Angreifer in den meisten Fällen nur dann durchführbar, wenn dieser das Smartphone für eine kurze oder längere Zeit in seinen Besitz gebracht hat. Die Angriffsvektoren ermöglichen hardwarenahe Angriffe auf das Gerät bzw. Angriffe auf die einzelnen Komponenten, wie z.B. Speicher- oder SIM-Karte. Auf diese Weise können Sicherheitsmechanismen auf logischer Ebene umgangen werden.

3.1. Drahtlose Schnittstellen

Drahtlose Schnittstellen eines Smartphones ermöglichen die Kommunikation bzw. den Datenaustausch zwischen zwei Geräten über eine Funkverbindung. Bekannte Schnittstellen sind hierbei Bluetooth, NFC oder WLAN. Diese Schnittstellen ersetzen eine sonst notwendige Kabelverbindung, werden allerdings auch nur für kurze Distanzen verwendet werden. Aus diesem Grunde lässt sich ein Angriff nur aus der Nähe durchführen. Der Angreifer versucht dabei über diese Schnittstellen manipulierte Dateien zu versenden, welche bereits beim Empfang auf dem Smartphone verarbeitet werden, ohne dass die Datei vom Nutzer geöffnet wird[19]. Dabei werden mögliche Fehler bei der Empfangsverarbeitung ausgenutzt um Schadcode auszuführen. Beispielsweise können so Nutzerdaten und Passwörter ausgelesen werden. Diese Informationen können wiederum für einen weiteren Angriff verwendet werden.

Da der Datenverkehr meist über Funk stattfindet kann die Kommunikation zudem leicht mitgelesen werden. Daher ist es wichtig, dass eine ausreichende Verschlüsselung verwendet wird. Die WEP-Verschlüsselung kann mit einfachen Mitteln geknackt werden und schützt daher nur wenig vor Angriffen.

Heutzutage werden an vielen öffentlichen Orten frei nutzbare WLAN-Hotspots für den Internetzugang angeboten. So experimentiert der VHH derzeit mit WLAN in

---

[17] vgl. Starnberger G, Froihofer L, Goeschka K: QR-TAN: Secure Mobile Transaction Authentication S. 579

[18] nähere Informationen in der Quelle Starnberger G, Froihofer L, Goeschka K: QR-TAN: Secure Mobile Transaction Authentication

[19] vgl. Heider J., El Khayari R., 2012: Geht Ihr Smartphone fremd?, S. 4

öffentlichen Verkehrsmitteln[20]. Auch die Deutsche Telekom plant die Anzahl ihrer Hotspots mit Hilfe der Kunden deutlich zu steigern. Hierbei sollen sich die Kunden untereinander über WLAN gegenseitig ihren Internetzugang zur Verfügung stellen[21]. Allerdings sollte man bei der Nutzung öffentlicher Hotspots vorsichtig sein, denn Angreifer haben ebenfalls die Möglichkeit einen eigenen Hotspot zu betreiben, der von anderen nicht zu unterscheiden ist. Es ist lediglich die frei wählbare SSID sichtbar, die z.B. „kostenlose Internetverbindung“ lauten kann. Smartphone-Nutzer, die so einen Hotspot als Internetzugang nutzen, ahnen nicht, dass der gesamte Datenverkehr vom Angreifer mitgelesen wird. Bei öffentlichen Hotspots sollte daher darauf geachtet werden, dass vertrauliche Daten ausschließlich verschlüsselt ausgetauscht werden.

3.2. Speicherkarten

Für die Erweiterung des Speicherplatzes statten viele Smartphone-Hersteller das Gerät mit einem Schacht für eine Speicherkarte aus. Obwohl dieser zwar meist erst nach dem Entfernen des Akkus erreichbar ist, lässt sich eine enthaltene Speicherkarte mit nur wenigen Handgriffen herausnehmen bzw. hinzufügen. Dies eröffnet Angreifern die Möglichkeit binnen kurzer Zeit direkt auf die Speicherkarte zuzugreifen. Aus diesem Grunde ist es wichtig, dass der Inhalt der Speicherkarten verschlüsselt ist. Meist ist das aber nicht der Fall. Auch wenn der Inhalt auf logischer Ebene geschützt ist, kann er auf diesem Wege ausgelesen werden[22].

Um die Daten zwischen Computer und Smartphone abzugleichen, kann der Nutzer diese Geräte z.B. über die USB-Schnittstelle miteinander verbinden. Dabei wird auch auf den Inhalt der Speicherkarte zugegriffen. Bei einer Evil-Maid-Attack[23] kann der Angreifer einen Computer-Virus auf der Speicherkarte platzieren, welcher dann bei der nächsten Synchronisation den PC befällt. Hierzu genügt es, dass das Smartphone für kurze Zeit vom Nutzer entfernt wird (ohne das dieser das bemerkt), oder das Gerät unbeobachtet vom Nutzer liegen gelassen wird. Daher sollten Nutzer besonders in ungesicherter Umgebung auf ihr Smartphone achten.

[20] vgl. o.V.: Mobil ins Internet
[21] vgl. Heuzeroth T.: Telekom überzieht das Land mit Hotspot-Teppich,
[22] vgl. Heider J., El Khayari R., 2012: Geht Ihr Smartphone fremd?, S. 4
[23] ein Angriff, bei dem das Gerät in Abwesenheit des Nutzers manipuliert wird

3.3. SIM-Karte

Mit Hilfe einer SIM-Karte kann sich der Nutzer im Mobilfunknetz identifizieren. Sie ermöglicht die Teilnahme am Mobilfunknetz über mobile Telefon- oder Datenanschlüsse. Damit eine unbefugte Verwendung verhindert werden kann, besteht die Möglichkeit die SIM-Karte mit einem PIN-Code zu schützen. Dieses System gilt bis heute als sicher.

Auch wenn der Angreifer nicht direkt auf die SIM-Karte zugreifen kann, besteht die Möglichkeit mit Hilfe einer Hardwaremanipulation den Datenaustausch zwischen der SIM-Karte und dem Smartphone mitzulesen[24]. Hierzu wird im Rahmen eines Evil-Maid-Angriffs ein Mikrocontroller zwischen diese Komponenten platziert. Verwendet der Benutzer sein mobiles Endgerät anschließend weiter, lassen sich Daten, wie PIN, Telefonbucheinträge, Anruflisten und Kurznachrichten aus der Kommunikation herauslesen. Der Mikrocontroller ist außerdem in der Lage Kurznachrichten zu versenden und Anrufe umzuleiten, ohne dass der Benutzer davon etwas mitbekommt. Um sich gegen solche Angriffe zu schützen, wird eine Versiegelung des Geräts empfohlen.

3.4. Hardware-Schnittstellen

Etwas aufwendiger gestalten sich Angriffe über die Hardware-Schnittstellen, die sich auf den Hauptplatinen der mobilen Endgeräte befinden. Dazu muss das Gerät komplett in seine Einzelteile zerlegt werden. Nach der Zerlegung sind die Schnittstellen und Speicherbusse frei zugänglich[25]. Durch den direkten Zugriff auf die einzelnen Komponenten können Sicherheitsmechanismen auf Software-Ebene, wie Sperrcodes oder –muster umgangen werden. Einen wirkungsvollen Schutz bietet hierbei nur die vollständige Verschlüsselung des Geräts. Dadurch wird sichergestellt, dass an keiner Stelle des Smartphones Daten in Klartext vorliegen. Dadurch wird ein Angriff dieser Art unwirksam.

[24] vgl. Heider J., El Khayari R., 2012: Geht Ihr Smartphone fremd?, S.4
[25] ebd.

3.5. Speicher

Auf die gleiche Art, wie sich der Angreifer Zugriff auf Hardware-Schnittstellen verschafft, kann er auch auf den Inhalt des internen Speichers zugreifen[26]. Auf diesem sind vor allem das Betriebssystem und installierte Anwendungen gespeichert. Ist der interne Speicher nicht ausreichend verschlüsselt, kann der Angreifer das Betriebssystem manipulieren und Sicherheitsmechanismen, die auf logischer Ebene existieren aushebeln, sodass diese beim Booten des Gerätes nicht mehr vorhanden sind und der Angreifer auf weitere Daten zugreifen kann.

3.6. Firmware

Als Firmware wird das Betriebssystem eines Smartphones bezeichnet. Dieses unterscheidet sich von Betriebssystemen normaler PCs oder Notebooks darin, dass es vom Hersteller genau an die einzelnen Komponenten des Geräts angepasst wurde. Die Firmware ist daher fester Bestandteil des Geräts und wird vom Hersteller vorgegeben. Im Gegenzug erwartet der Benutzer dafür, dass alle Funktionen des Geräts mit der installierten Firmware problemlos funktionieren. Mit Updates wird das Betriebssystem funktional, aber auch sicherheitstechnisch auf den neusten Stand gebracht. Sicherheitslücken in der Firmware können auf diese Weise geschlossen werden. Durch die notwendige Anpassung der Firmware an das Gerät kommt es aber häufig vor, dass für ältere Geräte keine Updates für die Firmware mehr entwickelt werden. So gibt es viele Smartphones, deren Betriebssysteme veraltet sind und Sicherheitslücken enthalten.

Davon abgesehen hat ein Angreifer, der physischen Zugriff auf das mobile Endgerät erlangt, die Möglichkeit die Firmware zu manipulieren[27]. Mit einer manipulierten Firmware kann der Angreifer die volle Kontrolle über das Smartphone erlangen, den Benutzer aus der Ferne überwachen sowie gespeicherte Daten auslesen.

Der sog. Jailbreak bezeichnet eine Firmware-Manipulation von iOS-Geräten, die ein Benutzer absichtlich durchführt, um Beschränkungen des Betriebssystems aufzuheben, wie z.B. die Bindung an den offiziellen App-Store als einzige Quelle für zusätzliche Apps. Ein Jailbreak ist jedoch als kritisch anzusehen, da hierbei wichtige Sicherheitsfunktionen abgeschaltet werden können.

---

[26] vgl. Heider J., El Khayari R., 2012: Geht Ihr Smartphone fremd?, S. 4
[27] ebd. S. 5

3.7. USB

Um Daten mit dem Computer zu synchronisieren, oder den Akku aufzuladen, besitzen Smartphones meistens eine USB-Schnittstelle. Hardwarenahe Protokolle können es dem Angreifer ermöglichen über die USB-Schnittstelle auf das Smartphone zuzugreifen[28]. Auf diesem Wege kann die Firmware ausgetauscht werden oder können Daten aus dem internen Speicher ausgelesen werden. Aufgrund der Tatsache, dass das Laden des Akkus und der Datenaustausch über eine gemeinsame USB-Verbindung erfolgt, sollte man vorsichtig bei öffentlichen Ladestationen sein. Angreifer könnten eine Ladestation so manipulieren, dass während des Ladens die Daten des Geräts ausgelesen werden.

[28] vgl. Heider J., El Khayari R., 2012: Geht Ihr Smartphone fremd?, S. 5

4. Umgang mit Mobilen Sicherheitsrisiken

Heutzutage ist ein Alltag ohne mobile Endgeräte kaum noch vorstellbar. Dennoch bestehen noch immer viele Sicherheitsrisiken. Um diese einzudämmen und Smartphones auf diesem Wege im Allgemeinen sicherer zu machen, werden verschiedene Lösungsansätze verfolgt[29]. Deren Umsetzung könnte auch zuverlässigen Schutz für sicherheitskritische Anwendungsfälle bieten. Dazu zählen Bring-your-own-device-Lösungen oder Authentifizierungs- und Bezahldienste. Auch ein wirksamer Schutz gegen Schadsoftware, wie z.B. Viren und Trojaner könnte dadurch realisiert werden.

Insbesondere das Thema Bring-your-own-device spielt für Unternehmen eine große Rolle. Bisher wird der Einsatz privater Endgeräte im Unternehmensumfeld aus Sicherheitsgründen vermieden, da z.B. zusätzlich installierte Apps eine Sicherheitslücke darstellen können, wodurch der Schutz von gespeicherten Unternehmensdaten nicht mehr gewährleistet wird. Daher wird auch die Verwendung vom Dienst-Geräten für private Zwecke nicht erlaubt. Dies führt dazu, dass viele Nutzer mindestens zwei Smartphones (ein privates und ein Dienst-Gerät) verwenden. Durch die Kosten mobiler Endgeräte besteht auch aus ökonomischer Sicht ein Interesse daran, ein einzelnes Smartphone beruflich und privat zu Nutzen.

Für diesen Anwendungsfall muss die Vertrauenswürdigkeit des Systems gegenüber dem Unternehmen und dem Gerätnutzer (als Privatnutzer oder Mitarbeiter) belegbar sein[30]. „Die Aufteilung in Sicherheitsdomänen, deren strenge Isolation und die Informationsflusskontrolle zwischen ihnen sowie deren Integritätsprüfung“ gilt als „entscheidender Ansatz zur Entwicklung vertrauenswürdiger Systeme“[31].

[29] vgl. Alkassar A., Schulz S., Stüble C., 2012: Sicherheitskern(e) für Smartphones
[30] ebd. S.176
[31] ebd.

Blackberry hat auf den Bedarf an BYOD-Lösungen reagiert und stellt unter dem Namen „Balance Technology“ eine technische Lösung zur Verfügung[32]. Private Daten und Unternehmensdaten werden in voneinander getrennten Bereichen abgelegt (siehe Abb. 4). Der Datenaustausch zwischen privaten und beruflichen Bereichen kann dabei vom Unternehmen mit Hilfe von Richtlinien eingeschränkt bzw. komplett verhindert werden. Während der Bereich mit den Unternehmensdaten standardmäßig verschlüsselt ist, kann auch der Bereich der privaten Daten verschlüsselt werden. Die Technik ermöglicht, dass Unternehmen nur den Unternehmensbereich verwalten können und bei privaten Apps wie z.B. facebook oder Spielen die Unternehmensdaten nicht gefährdet werden.

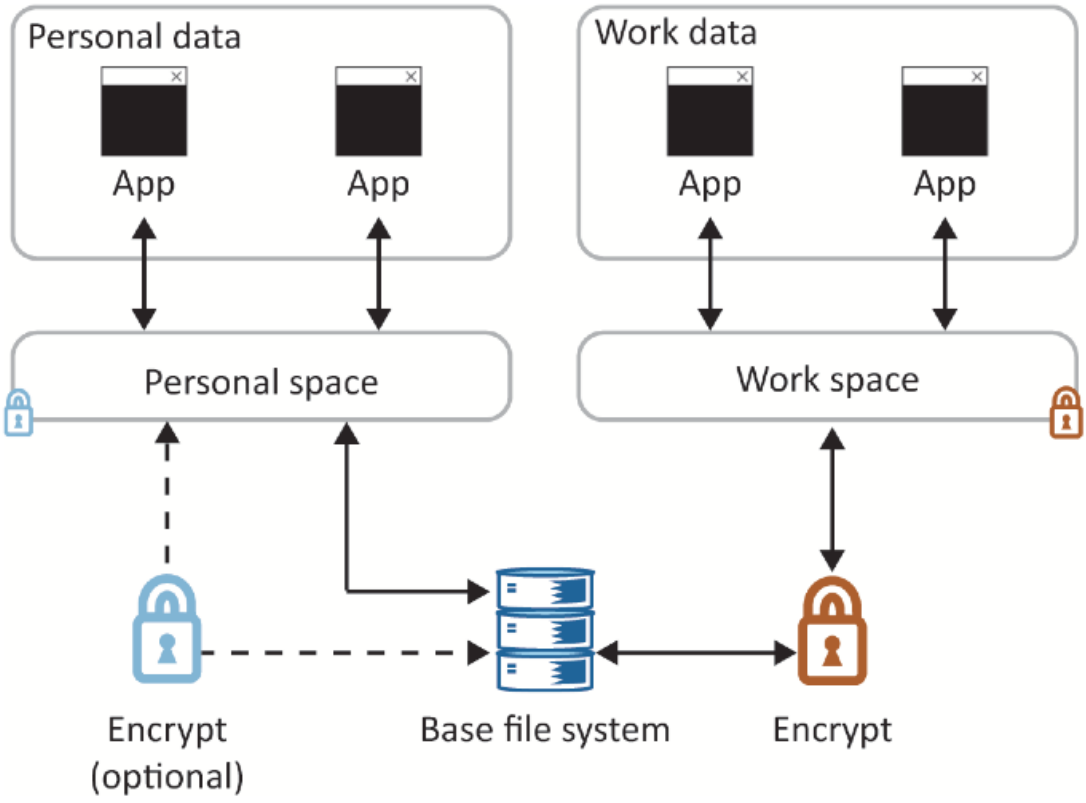

Abb. 4 Blackberry Balance Technology[33]

[32] o.V. 2013: Blackberry Enterprise Service 10, S. 44

[33] Grafik entnommen aus o.V. 2013: Blackberry Enterprise Service 10, S. 45

Für das Smartphone-Betriebssystem Android gibt es unterschiedliche Ansätze. Einer davon nennt sich BizzTrust und wird vom Fraunhofer SIT entwickelt. Dieser basiert auf einem Sicherheits-Framework[34], welches eine „anwendbare und leichte Domänentrennung für Android ermöglicht, um unautorisierten Datei-Zugriff und Kommunikation zwischen Anwendungen unterschiedlicher Vertrauens-Ebenen zu vermeiden“[35]. Dabei werden private und berufliche Daten und Anwendungen auf Middleware- und Kernelebene isoliert (siehe Abb. 5).

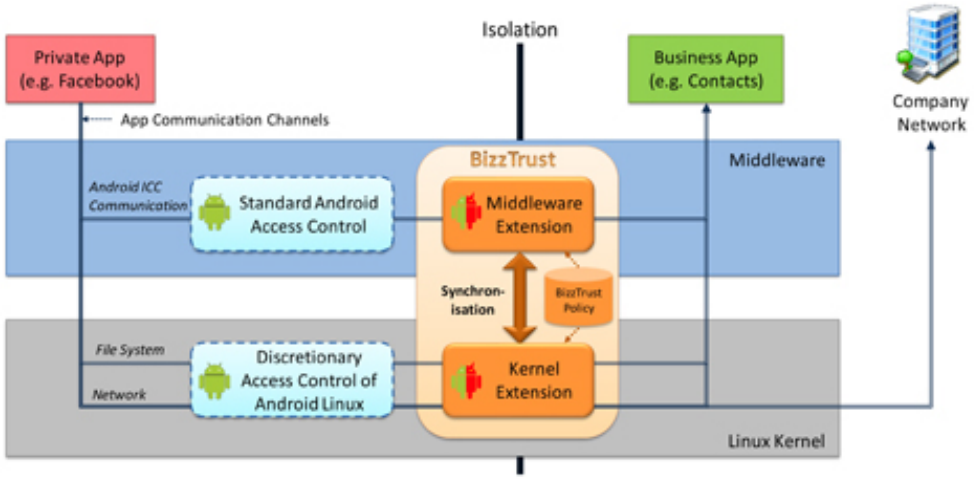

Abb. 5 BizzTrust Technologie[36]

[34] vgl. Bugiel S., u.a., 2011, Practical and Lightweight Domain Isolation on Android
[35] ebd. (eigene Übersetzung)
[36] Grafik entnommen aus o.V., o.J.: BizzTrust - Technology

5. Fazit

Durch die Vielzahl an Angriffsvektoren wird deutlich, dass mobile Endgeräte eine große Angriffsfläche bieten. Es kann aber ein Großteil der möglichen Angriffe verhindert werden, wenn die richtigen Sicherheitsmaßnahmen getroffen werden.

Auf logischer Ebene sollten Hersteller auf eine sichere Firmware achten. Apps von Drittanbietern sollten geprüft oder zertifiziert sein. Generell wird die Sicherheit des Geräts aber vor allem vom Benutzer bestimmt, da dieser in der Regel die Entscheidungen über die Installation von Anwendungen, Updates oder die Konfiguration von Sicherheitseinstellungen trifft. Daher gilt: Je mehr Hintergrundwissen ein Benutzer besitzt und er sich über die potentiellen Gefahren bewusst ist, desto sicherer kann der Betrieb mobiler Endgeräte sein.

Auch auf physikalischer Ebene kann die mobile Sicherheit verbessert werden. So können direkte Datenzugriffe durch eine vollständige und zeitgemäße Verschlüsselung des mobilen Endgeräts (und der enthaltenen Speicherkarte) verhindert werden. Beim Betrieb in öffentlichen Umgebungen ist erhöhte Vorsicht geboten. Unbefugter Zugriff sollte immer mit einem Sperrcode erschwert werden.

Zusammenfassend sind viele Dinge für den sicheren Betrieb mobiler Endgeräte zu beachten. Im Vergleich zum Nutzen dieser Geräte ist das jedoch ein Aufwand der sich lohnt.

6. Literaturverzeichnis

Alkassar A., Schulz S., Stüble C., 2012: Sicherheitskern(e) für Smartphones: Ansätze und Lösungen, in DuD: Datenschutz und Datensicherheit 36 (2012), Nr. 3, Seiten 175-179, Springer Gabler Verlag: Heidelberg, Internet: http://www.informatik.tu-darmstadt.de.de/fileadmin/user_upload/Group_TRUST/PubsPDF/dud_sicherheitskerne.pdf, Abruf: 2013-04-20

Bugiel S., u.a., 2011, Practical and Lightweight Domain Isolation on Android, Technische Universität Darmstadt, Fraunhofer SIT, Darmstadt, Deutschland, Internet: http://www.trust.informatik.tu-darmstadt.de/fileadmin/user_upload/Group_TRUST/PubsPDF/spsm18-bugiel.pdf, Abruf: 2013-04-21

Heider J., El Khayari R., 2012: Geht Ihr Smartphone fremd?, in DuD: Datenschutz und Datensicherheit 36 (2012), Nr. 3, Seiten 155-160, Springer Gabler Verlag: Heidelberg, Internet: https://www.sit.fraunhofer.de/fileadmin/dokumente/artikel/DuD-Artikel_geht_ihr_Smartphone_fremd.pdf, Abruf 2013-04-07

Heider J., 2011: Smartphone-Sicherheit im betrieblichen Einsatz, in 54. DFN-Betriebstagung 15.03.2011, Berlin, Internet: https://www.dfn.de/fileadmin/3Beratung/Betriebstagungen/bt54/forum-mobileit-heiderEnterprise_Smartphones.pdf, Abruf 2013-04-03

Mohamud A., Block, B., 2013: 2013 Future in Focus – Digitales Deutschland, Reston, Virginia, USA: comScore Inc., 2013, Internet http://www.comscore.com/ger/Insights/Presentations_and_Whitepapers/2013/2013_Future_in_Focus_Digitales_Deutschland, Abruf 2013-04-03

Starnberger G, Froihofer L, Goeschka K, 2009: QR-TAN: Secure Mobile Transaction Authentication, in International Conference of Availability, Reliability and Security, Vienna, Austria: Vienna University of Technology, Institute of Information Systems, Internet: https://guenther.starnberger.name/publications/ares09_qrtan.pdf, Abruf: 2013-04-16

Weinmann R.-P., 2012: Baseband Attacks: Remote exploitation of memory corruptions in cellular protocol stacks, in USENIX Workshop on Offensive Technologies (WOOT'12), Bellevue, Washington, USA, 2012, Internet https://www.usenix.org/system/files/conference/woot12/woot12-final24.pdf, Abruf 2013-04-03

Ergänzende Quellen

Bachfeld D., Mulliner C., 2010: Mobile Bedrohungen – Spionageangriffe und Abzocke auf Android und iPhone, Internet: http://heise.de/-1103471, Abruf: 2013-04-07

Heuzeroth T., 2013: Telekom überzieht das Land mit Hotspot-Teppich, Internet: http://www.welt.de/wirtschaft/webwelt/article114106920/Telekom-ueberzieht-das-Land-mit-Hotspot-Teppich.html, Abruf: 2013-04-07

Kabodt F., 2007: Riskanter Umfang mit vertraulichen Daten auf mobilen Endgeräten, Internet http://www.areamobile.de/news/6633-studie-riskanter-umfang-mit-vertraulichen-daten-auf-mobilen-endgeraeten, Abruf 2013-04-07

Lerg A., 2012: Zeus-Trojaner attackiert deutsche Online-Banking-Nutzer, Internet: http://www.t-online.de/computer/sicherheit/id_58525278/banking-trojaner-zeus-in-the-mobile-attackiert-smartphones-.html, Abruf: 2013-04-07

o.V., 2011: Fakten zum Thema Technik – Wie das mobile Telefonieren funktionert, Telekom Deutschland GmbH, Internet: http://www.telekom.com/static/-/9982/1/fakten-mobilfunktechnik-si, Abruf: 2013-04-07

o.V., 2008: iPhone ruft automatisch Abzock-Nummer an, Die Welt, Internet: http://www.welt.de/wirtschaft/webwelt/article2756659/iPhone-ruft-automatisch-Abzock-Nummer-an.html, Abruf: 2013-04-07

o.V., 2012: Mobil ins Internet: 25 Busse bieten kostenloses WLAN, Hamburger Abendblatt, Internet: http://www.abendblatt.de/hamburg/article111795300/Mobil-ins-Internet-25-Busse-bieten-kostenloses-WLAN.html, Abruf: 2013-04-07

o.V., 2009: BSI-Kongress: Preis für Beitrag zu Handy-Manipulation, Heise Security, Internet: http://heise.de/-219071, Abruf: 2013-04-07

o.V., 2013: Introduction to Blackberry Balance Technology, Internet: http://resources.infosecinstitute.com/intro-to-blackberry-balance-technology/, Abruf: 2013-04-21

o.V. 2013: Blackberry Enterprise Service 10, Internet: http://docs.blackberry.com/en/admin/deliverables/49294/BlackBerry_Device_Service_6.2_Security_Technical_Overview_en.pdf, Abruf: 2013-04-21

o.V., o.J.: BizzTrust - Technology, Internet: http://www.bizztrust.de/en/technology.html, Abruf: 2013-04-21

Theiss B., 2012: Die 4. Snapdragon-Generation im Detail, Internet: http://www.connect.de/ratgeber/vierte-generation-des-snapdragon-prozessors-1250411.html, Abruf: 2013-04-07