Aktuelle Grenzen der mobilen Sicherheit

Paschalis Papagrigoriou

EMPELOR GmbH
papagrigoriou@empelor.ch

Zusammenfassung

Dieser Beitrag gibt eine Übersicht über den Stand der Regulierung und der Technik sowie einen Ausblick auf Lösungsansätze und Weiterentwicklungen im Bereich der mobilen Sicherheit.

1 Herausforderungen für mobile Sicherheit

Alle benutzen mit ihren Smartphones und Tablets ganz selbstverständlich das mobile Internet. Angetrieben wird diese Entwicklung von den Angeboten der Dienstleister, den sich im Wettbewerb ständig verringernden Kosten für mobile Kommunikation, dem Streben nach Flexibilität, Wettbewerbsvorteilen und Ortsunabhängigkeit sowie von den omnipräsenten und unter Ausnutzung einer weit fortgeschrittenen Überwachung des Kommunikationsverhaltens individuell zugeschnittenen Angeboten der Industrie an die Verbraucher. „Wir tratschen zwar miteinander – doch in einem Kontext, in dem wir gleichzeitig füreinander als Reklameflächen dienen." schreibt der Medienwissenschaftler Mark Andrejevic im Kapitel „Facebook als neue Produktionsweise" der „Wirklichkeit 2.0" [KeMT12] über die „Generation Facebook" und ergänzt „Wir könnten dies als die formale Unterordnung des Sozialen unter kommerzielle Diktate bezeichnen."

Der Wunsch der Nutzer mobiler IT-Infrastruktur nach mehr Mobilität und dynamischem Einsatz von Ressourcen zur Kostenoptimierung geht einher mit der Aufgabe der Privatheit und der wachsenden Bereitschaft zunehmend jüngerer Benutzergruppen, ihr Leben einer möglichst großen Internet-Gemeinde und damit praktisch jedem transparent zu machen. Dieses Transparenzangebot wird auch von den staatlichen Stellen begrüßt, die z.B. sofort eine völlig legale und kostengünstige Möglichkeit zur Identifizierung von des Übertretens von Verkehrsregeln Verdächtigten anhand ihrer Präsenz in „sozialen" Netzwerken entdeckt haben.

Weit kritischer ist zu sehen, dass über „öffentlich" verfügbar gemachte Informationen hinaus auch auf vermeintlich nicht-öffentliche Informationen und Kommunikation mit vergleichsweise einfachen Mitteln zugegriffen werden kann. Eine solche Möglichkeit bieten zahlreiche gefährliche „Apps" für Smartphones [HrSA14]. Untersuchungen [Kell12] [ThKa10] zeigen, wie gefährlich die Smartphone-Apps [Fryb13] mittlerweile geworden sind. Als kriminell ist auch der Einsatz von sogenannten IMSI Catchern anzusehen, die auch online bestellt werden können [Disc14]. Worum es sich dabei handelt, lässt sich beispielsweise in der Wikipedia nachlesen [Wiki14]: *„An IMSI catcher is essentially a false mobile tower acting between the target mobile phone(s) and the service providers real towers. As such it is considered a Man In the Middle (MITM) attack. It is used as an eavesdropping device used for interception and tracking*

P. Schartner · P. Lipp (Hrsg.) · D•A•CH Security 2014 · syssec (2014) 298-303.

of cellular phones and usually is undetectable for the users of mobile phones. ... The IMSI catcher masquerades as a base station and logs the IMSI numbers of all the mobile stations in the area, as they attempt to attach to the IMSI-catcher. It allows forcing the mobile phone connected to it to use no call encryption (i.e., it is forced into A5/0 mode), making the call data easy to intercept and convert to audio". Das damit verbundene Gefährdungspotential begegnet dem Nutzer von mobiler Kommunikation und von über das mobile Internet abgewickelten Prozessen wie *Mobile Commerce*, *Mobile Banking* und Einsatz von *Mobile Wallets* in unterschiedlichen Formen und Ausprägungen: es beginnt mit dem Bruch der Privatsphäre über das Ausspähen von geistigem Eigentum und Geschäftsgeheimnissen bis hin zum klassischen Identitätsdiebstahl zu Betrugszwecken.

Stellen wir also die Frage, wer in diesem Szenario was beiträgt oder beitragen könnte, um die offensichtlich fehlende Sicherheit für Wirtschaftsunternehmen ebenso wie für Verbraucher herzustellen.

An erster Stelle wird man die Möglichkeit dazu bei den Anbietern im Ökosystem der mobilen Kommunikation suchen. Was leisten die Anbieter – Endgerätehersteller, Netzbetreiber, Cloud-Dienstleister und Anbieter mobiler kommerzieller Prozesse? Die Antwort fällt ernüchternd aus, betrachtet man es vom Ergebnis her. Niemand unter den Mainstream-Anbietern hat bisher geeignete Verfahren und Gerätschaften anzubieten, die das oben skizzierte Szenario ernsthaft in Richtung ausreichender Sicherheit zu verändern in der Lage sind.

2 Konventioneller Ansatz und Scheitern

Spezialisten wie die Anbieter von Software zum Device Management gaukeln der Wirtschaft vor, dass damit der Einsatz beliebiger und wahlfrei auch aus dem Privatbereich mitgeführter Endgeräte („BYOD" – Bring Your Own Device) zu schützenswerten Unternehmenszwecken gefahrlos möglich sei. Ähnliches gilt für Viren-Bekämpfer und Hersteller von Geräten, die den Bankkunden glauben machen wollen, dass damit ihre Online-Überweisungen ausschließlich dort ankommen, wo es der Kunde vorsieht und auch nur in der angegebenen Höhe. Der wahre Hintergrund des akzeptierten Versagens dieser Mechanismen (PIN/TAN, SMS-Banking, u.ä.) ist, dass es für die Bank unter dem Strich wirtschaftlicher ist, übertriebene Sorgfaltspflichten den Kunden aufzuerlegen, der für Betrugsschäden selbst aufkommen soll, oder sich gegen Schäden durch Cyber-Kriminalität zu versichern, als sich um ein teureres sicheres mobiles oder stationäres *online Banking* zu bemühen.

Daran schließt sich die Frage an, welche Vorkehrungen der Staat für seine Bürger trifft. Mit Spezialversionen von Smartphones, die im Wege der Virtualisierung von Betriebssystemen und Schnittstellen gleichsam „unangreifbar" gemacht werden, geht der Staat das Gefährdungspotential für seine eigenen Organvertreter an. Darüber hinaus beschränkt er sich auf Empfehlungen, wie die Wirtschaft und die Bürger mit den Bedrohungen umgehen sollten (siehe z.B. die „BSI-Empfehlungen zur Cyber-Sicherheit" [BSI14]), um sich schließlich selbst auf die Seite der potentiellen Bedroher und Privatsphären-Verletzer zu stellen, indem er selbst den Einsatz von Ausspähungsmitteln („Staats-Trojaner") erlaubt. Der Einsatz verschlüsselter Kommunikation zur Wahrung von Grundrechten auf Vertraulichkeit und Integrität macht Bürger und Unternehmen nicht zu Terroristen und Gefährdern [Adel13, Teil 2]. Doch gerade das verantwortungslose Ändern von Gesetzen [Adel13, Teil 1] und die Schaffung von „legalen backdoors" öffnen gefährliche Lücken und stellen eine offene Einladung zum Missbrauch dar [SRF13].

Eine weitere berechtigte Frage ist die, was von den Interessenvertretern der Verbraucher zu erwarten sein könnte. Adressieren wir damit die Repräsentanten der parlamentarischen Demokratie, dann gilt das zuvor Gesagte. Nehmen wir die Verbraucherschützer ins Visier, so treffen wir in erstaunlichem Umfang deckungsgleiche Empfehlungen an, wie wir sie schon von den damit beauftragten staatlichen Stellen erhalten haben („Es gibt keine Sicherheit ohne Zutun des Benutzers"). Empfehlungen zur Online-Sicherheit im Allgemeinen und zur Gefahrenvermeidung beim Online-Banking werden z.B. von verbraucher-sicher-online [OnBa13] gegeben, wobei die Mitverantwortlichkeit des Nutzers explizit betont wird:

„*Vertiefung im Thema Online-Banking … **Für die technische Sicherheit sind auch Sie verantwortlich** … Wenn Sie von der Bank bereitgestellte Geräte wie Geldautomaten, Kontoauszugsdrucker oder Überweisungsterminals benutzen, kümmert sich die Bank um deren Sicherheit. Beim Online-Banking sind Sie selbst für die Sicherheit des genutzten Computers verantwortlich. Wenn Sie durch Schadprogramme auf Ihrem Computer Geld verlieren, dann könnte die Bank Sie in die Pflicht nehmen.*"

Wo liegen dann denn überhaupt noch Chancen, unsere Privatsphäre zurückzuerhalten?

Ist das mobile Internet eine Fehlentwicklung?

Stellen wir Forderungen an die Hersteller, Sicherheits-Hardware einzubauen, so stoßen wir auf den Widerstand, dass die Geräte doch bitte „sexy" sein müssen, damit der Konsument sie freudig aus dem Regal nimmt. Stimmt – die Geräte sollen Spaß machen. Um das sicherzustellen, muss die Sicherheit dort angesiedelt werden, wo auch die Schwachstellen sind. „Software kann man nicht mit Software schützen" ist eine Erkenntnis, die so alt ist wie inzwischen bereits der Umstand, dass die IT in den Händen und Taschen der Verbraucher gelandet ist.

Dedizierte Hardware ist das Zauberwort. Die bisher betriebene „Geräte-Härtung" widerspricht in den meisten Fällen diametral der Hersteller-Philosophie, womit sie nicht mehr zukunftsfähig sein kann. Die kurzen Lebenszyklen der Geräte und der Weg, den neue Geräte über das Konsumenten-Segment in das Business nehmen, verhindern, dass die Hersteller sich hier in Richtung mehr Sicherheit bewegen können.

3 Ein neues Lösungskonzept

Will man mit dem Mobiltelefon zahlen und evtl. noch weitere Geschäftsvorfälle steuern, so macht man es de facto zum Geldschrank. Im Hinblick auf die derzeitig üblichen Sicherheitsmechanismen steht dessen Tür weit offen oder ist im besten Fall mit einem Klebeband gesichert.

Einen Schlüssel zu verwenden bedeutet, dass es ein Werkzeug gibt, das vom Geldschrank getrennt ist. Also ist die Lösung eine vom Smartphone oder Tablet getrennte Hardware, die dem Gesamtsystem Sicherheitsanker hinzufügt, die die Hersteller bewusst weglassen.

Was muss die dedizierte Sicherheits-Hardware können und bewirken?

- Für die Wirtschaft muss sie bezahlbar sein – das ist sofort der Fall, wenn dem Investment in Sicherheits-Zusatzgeräte die immensen Schäden gegenübergestellt werden, die den Unternehmen Tag für Tag aus Industriespionage und Betrug erwachsen.
- Sie muss unauffällig und einfach bedienbar sein.
- Sie muss von den Endgeräte-Herstellern unabhängig sein, sich also über Standards damit verbinden lassen, ohne dass durch Einschränkungen eines einzelnen Herstellers dessen

Geräte zur „No-Go Area“ werden – was sofort die Akzeptanz empfindlich beeinträchtigen würde.

- Sie muss Online-Banking so unterstützen, dass der Bankkunde sicher sein kann zu sehen, was er unterschreibt – also auf einem separaten sicheren Display.
- Sie muss den Einsatz von Kreditkarten und anderen Zahlungsmitteln so zulassen, dass keine Anpassungen im Prozess nötig werden und eine moderne POS-Infrastruktur unverändert genutzt werden kann.
- Möglichst ein Gerät stellt alle Sicherheitsmechanismen zur Verfügung wie PKI-Zertifikate für sicheres E-Mail (ideal mit S/MIME), sicheren Zugang zum Firmen-VPN und sichere Sprachübertragung mit verschlüsseltem VoIP einschließlich des Übergangs in Festnetze.
- Die Sicherheits-Hardware sorgt dafür, dass auf dem Smartphone oder Tablet ein geschützter Datenbereich eingerichtet ist, der ohne die Sicherheits-Hardware und den Identitätsnachweis des berechtigten Benutzers unzugänglich ist.

Die Herausforderung besteht vornehmlich darin, den Spannungsbogen zwischen der eingesetzten Technologie (das „Womit“) mit dem Streben nach hoher Funktionalität („Was“) und möglichst viel Komfort („Wie“) so aufzubauen, dass kein Element zerreißt.

Beginnend von den auf ein Sicherheitsgerät üblichen Funktionen (siehe Abbildung 1) muss eine Sicherheits-Hardware eine Vielzahl von Anforderungen erfüllen.

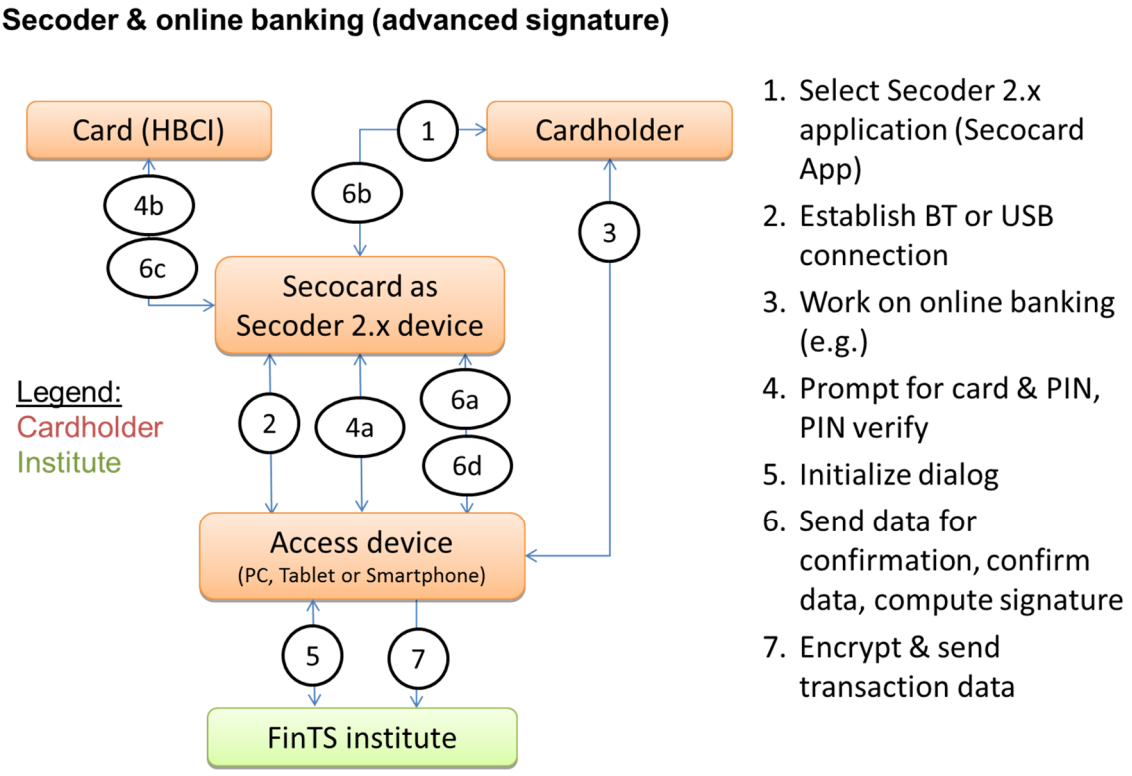

Abb. 1: online Banking & Signaturanwendung

Eine multifunktionale Umgebung für eine dedizierte Hardware-Architektur zeigt die folgende Abbildung:

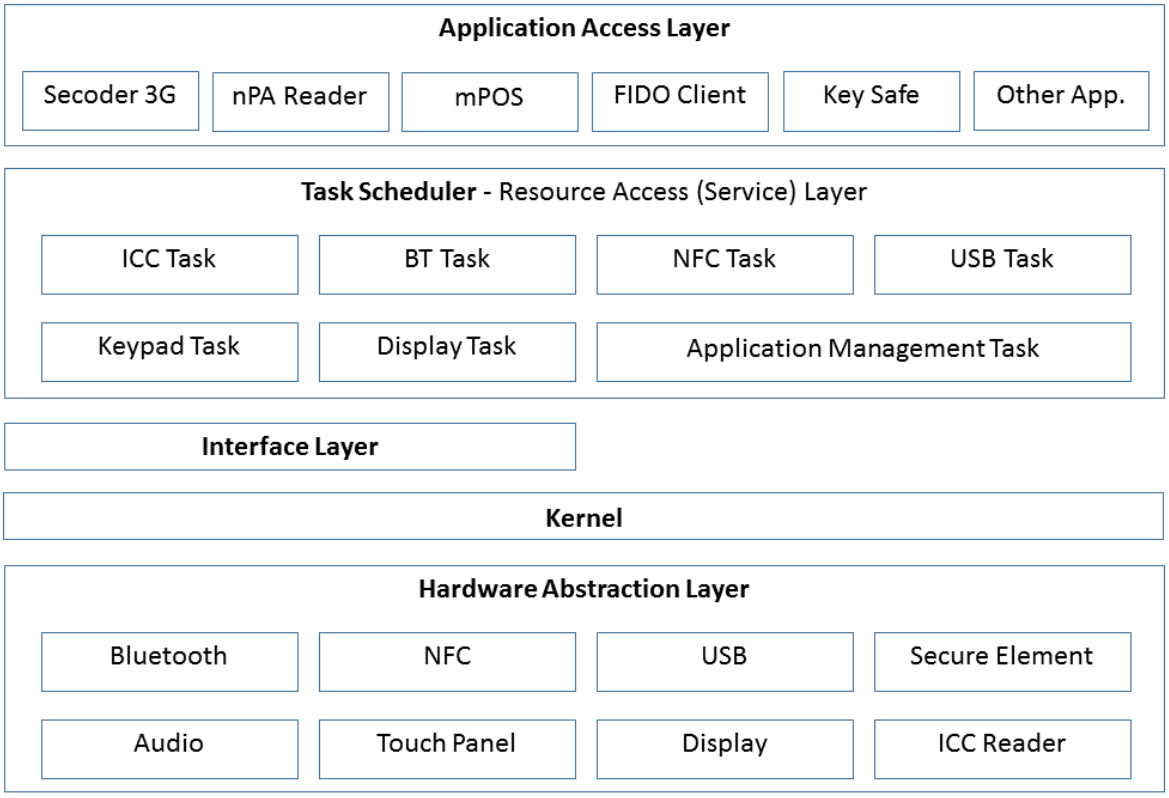

Abb. 2: Übersicht der Architektur

Die sicherheits-relevante Hardware kann als "Hardware Abstraction Layer" präsentiert werden und über das Internet oder mit Hilfe von Middleware als verbundenes Gerät verwendet werden. Sie integriert eine Reihe von funktionalen Bausteinen wie ein eingebettetes Sicherheitsmodul, einen berührungsempfindlichen Bildschirm, Audio-Unterstützung und Komponenten für state-of the-art-Kommunikation mit marktverfügbaren mobilen Geräten. Als Übertragungswege können NFC, Bluetooth (Smart Bluetooth oder Bluetooth Low Energy) und USB zum Einsatz kommen.

Nicht erforderlich aus Kosten-, aber auch aus Sicherheitsgründen sind Module für die WLAN- oder GSM-Konnektivität.

Die Kosten sind ein wesentlicher Faktor bei der Auswahl des idealen Equipments insbesondere für ein geschäftlich genutztes Sicherheitsgerät (z.B. im Handel) und für Transaktions-Vorgänge. Bezahldienstleister und Banken sind daher gut beraten, bei der POS/mPOS-Ausstattung höherwertige, das bedeutet auch mit mehr Funktionalität und Anwendernutzen ausgestattete Lösungen zu geringeren Kosten anzubieten. Mit einer dedizierten Sicherheitshardware können beispielsweise Kreditkarten-Schemes und -Acquirer den Händlern eine POS-Hardware anbieten, die den vollständigen Schutz einer wesentlich teureren, dedizierten POS-Lösung mit sich bringt und zusammen mit den jeweils aktuellsten Smartphones und Tablets funktioniert. Der Einzelhändler kann sein Mobilgerät zu jeder beliebigen Zeit gegen ein neueres, schickeres Modell austauschen, während sein POS/mPOS-System unverändert damit funktioniert und nicht

nur die Kartenakzeptanz sicherstellt, sondern auch seine Online-Banking-Transaktionen abarbeitet und, sofern erforderlich, auch seine Kommunikation mit seiner Bank oder mit wichtigen Geschäftspartnern und Kunden effektiv gegen jede Form des Abhörens abschottet.

Literatur

[Adel13] S. Adelmann: Terroristen und Gefährder, 18. April 2013. http://www.crn.de/netzwerke-tk/artikel-99027-2.html, zuletzt aufgerufen am 24.7.2014.

[Adel13] S. Adelmann: Die Negierung des Datenschutzes, 18. April 2013. http://www.crn.de/netzwerke-tk/artikel-99027.html, zuletzt aufgerufen am 24.7.2014.

[BSI14] Bundesamt für Sicherheit in der Informationstechnik: Cyber-Sicherheit. https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/cyber-sicherheit_node.html, zuletzt aufgerufen am 24.7.2014.

[Disc14] DISCOVERY telecom: Advanced 3G IMSI/IMEI/TMSI Catcher. http://www.discoverytelecom.eu/catalog/2196.html, zuletzt aufgerufen am 24.7.2014.

[Fryb13] M. Fryba: Facebook übernimmt Kontrolle des Smartphones – Albtraum für Datenschützer und Nutzer. http://www.crn.de/netzwerke-tk/artikel-98906.html, zuletzt aufgerufen am 24.7.2014.

[HrSA14] Hauptrisiko bei den Smartphones: Die Apps. http://sicherheitskultur.at/mobile_security.htm#apps, zuletzt aufgerufen am 24.7.2014.

[Kell12] T. Kelly: Free apps 'can spy on texts and calls': Smartphone users warned of privacy dangers, updated 27. Februar 2012. http://www.dailymail.co.uk/sciencetech/article-2106627/Internet-firms-access-texts-emails-pictures-spying-smartphone-apps.html, zuletzt aufgerufen am 24.7.2014.

[KeMT12] P. Kemper, A. Mentzer, J. Tillmanns: Wirklichkeit 2.0, RECLAM Taschenbuch Nr. 20266, 2012.

[OnBa13] Online-Banking: Wie Sie Gefahren meiden. http://www.verbraucher-sicher-online.de/artikel/online-banking-wie-sie-gefahren-meiden, zuletzt aufgerufen am 24.7.2014.

[SRF13] Schweizer Radio und Fernsehen: Bundesrat erlaubt Staatstrojaner im Internet, 28. Februar 2013. http://www.srf.ch/news/schweiz/bundesrat-erlaubt-staatstrojaner-im-internet, zuletzt aufgerufen am 24.07.2014.

[ThKa10] S. Thurm, Y.I. Kane: Your Apps Are Watching You, 17. Dezember 2010. http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html?mod=e2tw#, zuletzt aufgerufen am 24.07.2014.

[Wiki14] Wikipedia: IMSI-catcher. http://en.wikipedia.org/wiki/IMSI_catcher, zuletzt aufgerufen am 24.07.2014.