SWITCHcert Report zu aktuellen Trends im Bereich IT-Security und Privacy

Oktober 2014

SWITCH

I. Same procedure as last time? Fingerabdrucksensor im neuen iPhone 6 mit gleicher Technik geknackt wie beim Vormodell

Apple hat Grund zur Freude: Nach eigenen Angaben wurden am ersten Verkaufswochenende mehr als 10 Millionen Exemplare des neuen iPhone 6 verkauft und damit eine neue Rekordmarke geknackt. Weniger Freude dürfte dagegen die Tatsache machen, dass auch der neue – gemäss heise.de: alte – Fingerabdrucksensor bereits wieder geknackt ist – und zwar mit der gleichen Technik, mit der sich auch schon das Touch ID im Vorgängermodell z.B. vom Chaos Computer Club austricksen liess.

Auch Lookout-Blogger Marc Rogers hat Touch ID geknackt, kommt aber in seinem Blogbeitrag zu einem ambivalenten Schluss: «Touch ID is great for locking the iPhone, and it will keep most people out, but when it comes to really sensitive data, you should consider another security measure.» Dieser Einschätzung liegen mehrere Fakten zugrunde: So sperrt Touch ID den Zugang zu einem iPhone 6 nach 5 missglückten Versuchen. Eine höhere Auflösung und ein grösseres Abtastfeld sollen zudem dazu führen, dass ein funktionierender Spoof, also ein falscher Fingerabdruck, deutlich mehr Kenntnisse, Geduld und Akuratesse braucht. Andererseits öffnet Touch ID – und so-

mit auch ein überlisteter Sensor – aber den Zugang zu Apps von Drittanbietern, wie z.B. zum Passwort-Safe 1Password und zum kontaktlosen Bezahlen via Apples neuer NFC-Bezahlfunktion Apple Pay. Das Knacken eines iPhone 6 hat für seinen rechtmässigen Besitzer also unter Umständen weit gravierendere Folgen als beim Vorgänger.

Während Apple den Einsatz von Touch ID mit einem hohen Mass an Bequemlichkeit bei gleichzeitig hoher Sicherheit begründet, bleibt jenseits aller Sicherheitsbedenken in Bezug auf Einzelfunktionen die grundsätzliche Frage nach Sinn und Risiko des Einsatzes von biometrischen Sicherungen offen. Siehe dazu auch unseren Security-Report zu diesem Thema von September 2013: Die dort zitierte Warnung des Hamburger Datenschützers Johannes Caspar, dass biometrische Daten nicht löschbar seien und man deshalb keine solche Daten hinterlassen sollte, wenn es nicht unbedingt sein muss, hat nach wie vor Aktualität und Gültigkeit.

Nachzulesen unter:

http://www.inside-it.ch/articles/37692

http://www.heise.de/security/meldung/Fingerabdrucksensor-des-iPhone-6-ueberlistet-2399891.html

http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid

https://blog.lookout.com/blog/2014/09/23/iphone-6-touchid-hack

http://arstechnica.com/security/2014/09/fake-fingerprint-fools-iphone-6-touch-id-why-its-not-so-serious

http://www.switch.ch/export/sites/default/all/cert/downloads/secrep/_files_secrep/Sec-Report_September_2013.pdf

II. Alles andere als eine Luftnummer: Drohnen, Ballone und offene Sicherheitsfragen

Folgt man den Analysten der amerikanischen Luftfahrt-Forschungsfirma Teal Group, dann werden die Verkäufe militärischer und ziviler Drohnen in den nächsten 10 Jahren ein Volumen von über 89 Milliarden USD (ca. 86 Mrd. Franken) jährlich erreichen. Ein erheblicher Anteil an diesen Zahlen wird (in des Wortes wahrstem Sinn) auf das Konto von Amazon, DHL und anderer Logistik-Dienstleister gehen. Dazu kommen Internet-Anbieter, die mit Drohnen (Facebook) bzw. Ballonen (Google) das Internet in bis anhin nicht vernetzte Regionen der Welt bringen möchten. Und schliesslich sorgen neben dem Militär auch Geheimdienste, Polizei, Journalisten, Filmer, Fotografen und Privatleute für steigendes Verkehrsaufkommen im Luftraum.

Zivile unbemannte Flugkörper oder UAVs (unmanned aerial vehicles), bzw. seit kurzem RPA (remotedly piloted aircraft), werden heute bereits zur Versorgung oder für Such-und-Rettungseinsätze von Menschen in unzugänglichen Gebieten eingesetzt, wie etwa auf Haiti oder in Bhutan. DHL startete vor kurzem die testweise Paketzustellung der 12 km vom Festland entfernt gelegenen Nordseeinsel Juist. Und Facebook wird 2015 Drohnen testen, die unterversorgten Regionen Internetzugang bringen sollen. Noch weiter gediehen ist Googles Projekt «Loon»: Gemäss eigenen Angaben wird man 2015 ein ganzes Land im Dauerbetrieb mit Internet aus Ballonen versorgen, die in 20 km Höhe über der Erde fahren. Das Spektrum der unbemannten Fluggeräte reicht vom einfachen hobbymässig geflogenen Quadrocopter bis hin zur zivil genutzten Global Hawk mit einer Flugzeit von 40 Stunden und einer Reichweite von 20.000 km.
Während die technische Entwicklung also rasant voran schreitet, sind viele Fragen wie Schutz vor Spionage, öffentliche Sicherheit, Sicherheit der von Drohnen gesammelten bzw. übertragenen Daten ebenso ungeklärt wie die nach dem Schutz der Privatsphäre. Die NASA entwickelt gemeinsam mit dem Start-Up Airware derzeit ein automatisiertes Flugverkehr-Kontrollsystem das in vier bis fünf Jahren den Flugverkehr von Drohnen überwachen und steuern soll. Die meisten zivilen UAVs sind jedoch relativ einfach zu hacken und zu kapern. Auch finden sich vermehrt Berichte über Abstürze von Drohnen. Aktuellstes Beispiel: Der bis dato ungeklärte Absturz einer der beiden 30.000-Franken-Drohnen der Zürcher Polizei am 3. Oktober dieses Jahres.

Nachzulesen unter:

http://www.tagesanzeiger.ch/zuerich/stadt/Drohne-der-Polizei-ist-abgestuerzt/story/25181885

http://www.zeit.de/digital/internet/2014-09/drohnen-hacken-gps-star-wars

http://www.tagesschau.de/wirtschaft/post-drohne-alltag-101.html

http://resources.infosecinstitute.com/privacy-security-issues-usage-civil-drones

http://futurezone.at/digital-life/nasa-entwickelt-flugverkehr-kontrollsystem-fuer-drohnen/85.522.462

http://futurezone.at/digital-life/facebook-startet-bald-internet-drohnen-tests/87.507.428

https://www.steigerlegal.ch/2014/07/10/drohnen-schweiz-verschaerft-regeln-per-1-august-2014

http://www.heise.de/tr/artikel/Google-Projekt-Internet-per-Ballon-auf-der-ganzen-Welt-2403375.html

III. Googles Transparenzbericht bescheinigt Schweizer Behörden zunehmenden Datenhunger

Im Vergleich zu den fast 32.000 Aufforderungen zur Herausgabe von Kundendaten, mit denen sich Google gemäss des jüngst herausgegebenen Transparenzberichts im 2. Halbjahr 2013 konfrontiert sah, nehmen sich die 124 Anfragen Schweizer Behörden schon beinahe mickrig aus. Dennoch steckt auch in dieser kleinen Zahl eine gewisse Brisanz, denn sie liegt um mehr als die Hälfte höher als in der vorangegangenen Vergleichsperiode. Vor allem aber liegt der Anstieg deutlich höher als der globale Durchschnitt. Laut Googles Transparency Report haben Regierungsbehörden im Rahmen polizeilicher Ermittlungen weltweit 15% mehr Auskunftsgesuche vorgelegt, die Anfragen der US-Regierung stiegen um 19%, die der deutschen Behörden um 44%.
Dabei bemüht sich Google nach Auskunft von Richard Salgado, Director for information security and law enforcement matters, Auskünfte nur dann zu erteilen, wenn alle rechtlichen Grundlagen dafür eingehalten wurden. Dennoch mussten in etwa der Hälfte aller Fälle Daten herausgegeben werden.

Nachzulesen unter:

http://www.computerworld.ch/marktanalysen/studien-analysen/artikel/schweizer-behoerden-wollen-immer-mehr-von-google-wissen-66425/

http://www.forbes.com/sites/emmawoollacott/2014/09/16/google-piles-pressure-on-congress-with-latest-transparency-report/

http://www.handelsblatt.com/technologie/it-tk/it-internet/anfragen-bei-google-und-facebook-deutsche-behoerden-sind-besonders-neugierig/9772564.html

http://de.statista.com/infografik/844/auskunftsersuchen-zu-nutzerdaten-von-behoerden-und-gerichten-bei-google/

IV. Wenn der Hacker durch den Kühlschrank kommt: Wie steht es um die Sicherheit im Internet der Dinge?

Armbänder, Autos und Kühlschränke haben auf den ersten Blick wenig miteinander zu tun. Im Zeitalter von Wearables, Connected Car-Konzepten und Smart Homes aber sind sie alle miteinander vernetzt. Cisco schätzt die Zahl vernetzter Geräte im Jahr 2020 auf rund 50 Milliarden. Weil aber alles, was vernetzt ist, auch gehackt werden kann, lohnt sich ein Blick auf die Sicherheitslage. Und die ist alles andere als beru-

higend. So musste z.B. David Jacoby von Kapersky Lab erkennen, dass er zwar alle gängige IT gut geschützt hatte, eines seiner Netzwerkgeräte aber in Form eines versteckten Root-Zugangs mit der einstelligen Ziffer 1 als Passwort potenziellen Angreifern gegenüber offenstand wie ein Scheunentor. Die Frage heisst also: Wie gut sind Wearables, Smart Homes und Connected Cars gegen Missbrauch geschützt? Denkbare Bedrohungsszenarien lassen sich nämlich ohne Mühe finden.

Wearables: So könnte z.B. das Nike FuelBand oder die Apple Watch eines CEOs von dessen Konkurrenzunternehmen oder auch «nur» einem Headhunter angezapft werden, um ein Bild vom Gesundheitszustand der Führungskraft zu bekommen und damit die Chancen für eine feindliche Übernahme abzuschätzen oder dessen Voraussetzungen für die Übernahme einer neuen Aufgabe verlässlicher als in Gesprächen zu prüfen. Das eigene Unternehmenscontrolling könnte derweil anhand der Daten aus der Golfuhr ermitteln, wann die Kader eben nicht im Büro waren.

Smart Home: «Nest» ist ein kleines KI-Gerät, das die Aktivitäten der Bewohner eines Hauses aufzeichnet und aus den Daten Programme zur Steuerung von Licht, Heizung etc. erstellt und speichert – gehackt und ausgelesen eine praktische Arbeitshilfe für Einbrecher oder Kidnapper. Und wenn das Badezimmer wie Philips´ Apothecary allmorgendlich die Gesundheitsdaten seiner Nutzer aufzeichnet, ist es nur noch ein kleiner Schritt dahin, dass die Krankenversicherung gegen Prämienvergünstigung einen Transmitter einbaut, um Wohl- und Fehlverhalten mit Prämienauf- und -abschlägen bzw. Leistungszu- und -absagen zu sanktionieren.

Connected Car: In abgespeckter Form geschieht dies heute bereits mit Drive-Recordern von Autoversicherern – selbstverständlich in legalem Rahmen und mit Zustimmung der Nutzer. Was aber, wenn eifersüchtige Ehemänner oder betrogene Ehefrauen Brems- und Gaspedale des Connected Cars von Nebenbuhlern manipulieren können? Oder wenn ein 20 Jahre alter Bashbug in vernetzten Autos ausgenützt werden kann? Ein Ereignis wie «Shellshock» hätte in diesem Kontext plötzlich eine völlig neue Bedeutung.

Nachzulesen unter:

http://www.heise.de/security/meldung/Internet-der-Dinge-Die-Zahnbuerste-als-Gefahr-2400670.html

http://www.golem.de/news/smarthome-die-ifa-wird-zur-messe-der-sicherheitsluecken-1408-108841.html

http://www.golem.de/news/internet-der-dinge-ameisengrosse-radios-sollen-die-welt-verbinden-1409-109174.html

http://www.scip.ch/?labs.20140716

https://nest.com/thermostat/life-with-nest-thermostat

http://www.design.philips.com/about/design/designportfolio/design_futures/design_probes/projects/microbial_home/apothecary.page

http://www.bankinfosecurity.com/interviews/shellshock-bug-how-to-respond-i-2463

Zum Stöbern: spannende Präsentationen, Artikel und Videos

Die neuen Toplevel-Domains wie .support werden vermehrt auch von Kriminellen genutzt, beispielsweise um Phishing-Mails möglichst echt aussehen zu lassen:

http://www.csoonline.com/article/2687132/social-engineering/recently-introduced-tlds-create-new-opportunities-for-criminals.html

Adam Caudill und Brandon Wilson haben auf der Sicherheitskonferenz DerbyCon in Louisville, Kentucky einen Talk zu «BadUSB» gehalten und ihre Hacks veröffentlicht. Caudill sagte gegenüber dem Technikmagazin «Wired»: «Die Leute sehen in USB-Sticks nicht mehr als ein Speichergerät. Dabei handelt es sich um reprogrammierbare Computer. »

http://www.irongeek.com/i.php?page=videos/derbycon4/t510-making-badusb-work-for-you-adam-caudill-brandon-wilson

http://www.wired.com/2014/10/code-published-for-unfixable-usb-attack/

Umweltfreundliches Bitcoin-Mining: Ken Shirriff zeigt, wie man die im Miningprozess verwendete Hashfunktion SHA-256 mit Bleistift und Papier ausrechnen kann:

http://www.righto.com/2014/09/mining-bitcoin-with-pencil-and-paper.html

http://www.youtube.com/watch?v=y3dqhixzGVo

Dieser SWITCH-CERT Security Report wurde von Dieter Brecheis und Frank Herberg verfasst.