Competence Centers for Excellent Technologies

Research – Update

SBA Research

Mai 2014

Research Impact

Viele unserer Forschungsergebnisse haben direkte und indirekte Auswirkungen auf mehrere Millionen Menschen. Einige Beispiele: die Daten von 10 Millionen Nutzerinnen und Nutzern des Cloud Speicherdienstes Dropbox[1] konnten unbemerkt von jedermann ausgelesen werden, wenn der Hashwert bekannt war[2]. Durch die von SBA Research aufgezeigten Sicherheitslücken hat Dropbox, mit mittlerweile **mehr als 275 Millionen Nutzerinnen und Nutzern**, neue **Schutzmaßnahmen implementiert, die heute noch im Einsatz sind**.

Facebook, mit im Moment mehr als **1,25 Milliarden Nutzerinnen und Nutzern**, hat auf unsere Ergebnisse aus dem Jahr 2013[3,4] reagiert und die **Berechtigungen von Facebook Apps eingeschränkt**. Unsere Ergebnisse führten weiters zu der **Behebung von Sicherheitsschwachstellen in Applikationen** von denen mehrere Millionen Nutzerinnen und Nutzer betroffen waren[5].

Tor, der im Moment **führende Anonymisierungsdienst** im Internet, ist ebenfalls nicht frei von schwarzen Schafen. Mit einem neuartigen Scanner und einer Laufzeit von mehreren Monaten konnten wir **40 bösartige Exitrelays identifizieren**, die aktiv unverschlüsselte Protokolle ausnutzten. Diese Arbeit wird zwar erst im Juli präsentiert, die betroffenen Tor Relays wurden aber schon kurz nach der Entdeckung vom Tor Projekt gesperrt.

MMulazzani@sba-research.org

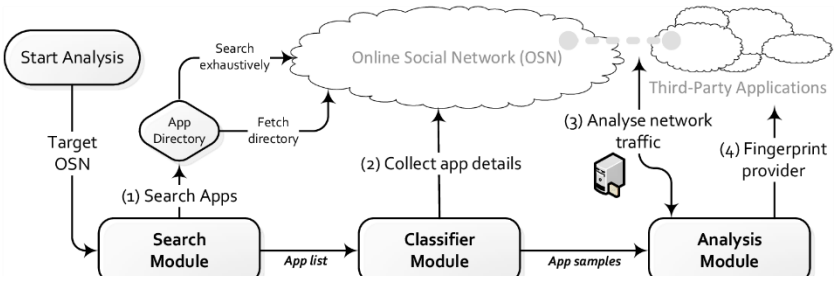

Abbildung 1: Analyse von Social Networking Apps mit AppInspect

[1] Stand: 2011; http://www.sba-research.org/wp-content/uploads/publications/dropboxUSENIX2011.pdf
[2] https://www.slideshare.net/SBAResearch/presentation-usenix
[3] http://ai.sba-research.org/
[4] http://www.sba-research.org/wp-content/uploads/publications/AppInspect_peprint.pdf
[5] http://www.slideshare.net/SBAResearch/appinspect-largescale-evaluation-of-social-networking-apps

Heartbleed

Im April 2014 wurde unter dem Namen "Heartbleed" eine der gravierendsten Sicherheitsschwachstellen der letzten Jahre bekannt. **Der Programmierfehler ermöglicht Angreiferinnen und Angreifern, vertrauliche Daten, wie zum Beispiel SSL Schlüssel oder Passwörter, von fremden Internetservern auszulesen.** SBA Research reagierte rasch auf diese Sicherheitslücke und führte aufgrund der akuten Bedrohungslage **automatisierte Heartbleed-Untersuchungen aller österreichischen IP-Adressen**[6] (ca. 12 Millionen) durch. Dabei wurden 121.420 IP-Adressen identifiziert, die potentiell von Heartbleed betroffen waren. Die Ergebnisse zeigten, dass von diesen knapp 120.000 Systemen zwei Tage nach der Veröffentlichung von Heartbleed noch rund 6% potentiell verwundbar waren (in absoluten Zahlen: 7.014). Die betroffenen Firmen wurden von SBA Research informiert. Unsere Untersuchungen trugen somit zu der Beseitigung der Heartbleed-Schwachstelle in Österreich bei. Zusätzlich wurde ein Whitepaper[7] mit Informationen zur Beseitigung der Heartbleed-Lücke veröffentlicht.

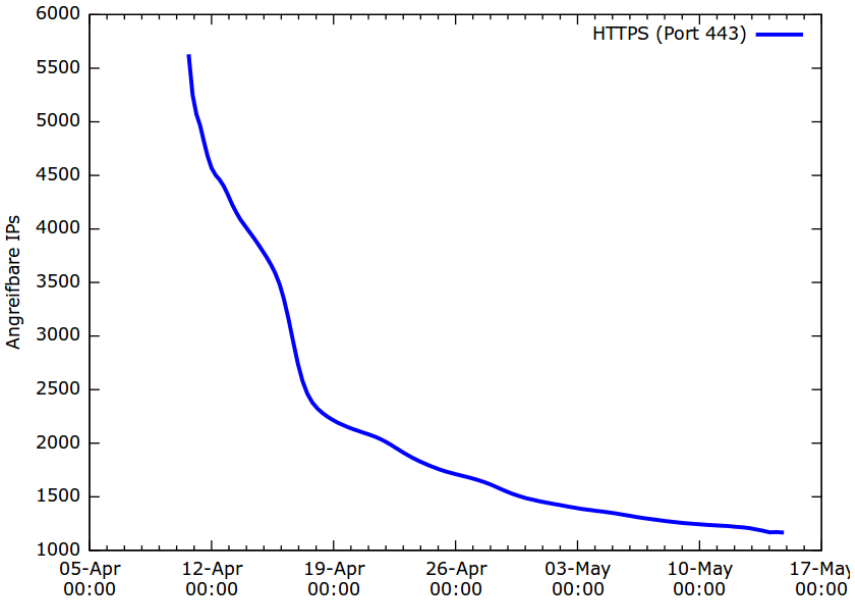

Abbildung 2: Analyse von SBA Research zur Heartbleed Bedrohungslage in Österreich, April/Mai 2014

MHuber@sba-research.org

Smartphone Messenger

Smartphone-Applikationen zum Versenden von kostenlosen Kurznachrichten erfreuen sich auch in Österreich großer Beliebtheit, allen voran WhatsApp, das auf mehreren hunderttausend Smartphones in Österreich installiert ist. Die einfache Konfiguration - das Anlegen eines Benutzerkontos ist nicht erforderlich - trägt einerseits zu dieser rasanten Verbreitung bei, andererseits sorgt dieses Konzept auch für gravierende Schwachstellen, wie Forschungsarbeiten[8] von SBA Research zeigen. Bei einer Studie[9] im Jahre 2012 konnte von neun getesteten Applikationen für iPhone und Android keine einzige restlos überzeugen und die teils gravierenden Sicherheitslücken[10], die die Privatsphäre der Nutzerinnen und Nutzer gefährdeten, überraschten

[6] http://www.sba-research.org/2014/04/15/heartbleed-bedrohungslage-in-osterreich/
[7] http://www.sba-research.org/wp-content/uploads/2014/04/HeartbleedWhitepaperv02.pdf
[8] http://www.sba-research.org/wp-content/uploads/2012/03/sebastian_s_20121.pdf
[9] http://www.sba-research.org/wp-content/uploads/publications/ndss2012_final.pdf
[10] http://www.slideshare.net/SBAResearch/schrittwieser-smartphone

selbst die Sicherheitsforscherinnen und Sicherheitsforscher von SBA Research. So konnten etwa Benutzerkonten mühelos übernommen werden und in weiterer Folge Nachrichten dieser Nutzerinnen und Nutzer empfangen und gesendet werden. Auch gelang es, die Status-Nachrichten aller WhatsApp-Nutzerinnen und -Nutzer von ganz Österreich auszulesen und sogar zu verändern. Eine **Vergleichsstudie**[11] **im Jahr 2014 ergab, dass die Herstellerinnen und Hersteller von WhatsApp und ähnlichen Applikationen einige der Sicherheitslücken geschlossen** haben, **andere Schwachstellen jedoch nach wie vor existieren**.

SSchrittwieser@sba-research.org

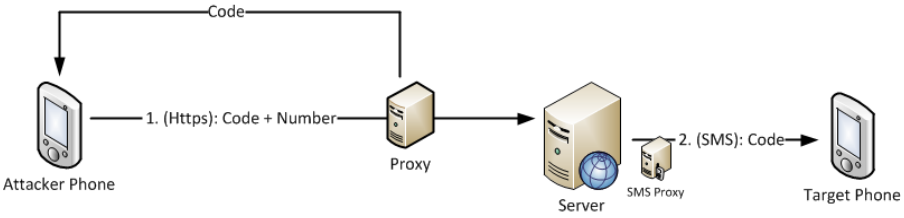

Abbildung 3: Accountübernahme in WhatsApp (Protokollversion 2011)

Hardware & Security

Embedded Systems, also Kleinstcomputer, sind inzwischen omnipräsent und trotzdem kaum sichtbar. Sie verbergen sich in Gegensprechanlagen, Schließsystemen, Telefonapparaten, Druckern, Waschmaschinen, Fahrzeugen und praktisch jedem elektronischen Gerät, das aus mehr als einem simplen Ein-/Ausschaltknopf besteht. Mit dem Einzug der Computer in diese Domäne brachten sie auch deren Sicherheits- und Komplexitätsprobleme mit. Produkte, die direkt Sicherheitsaspekte steuern, sind besonders exponiert. **Drahtlose Technologien vergrößern die Angriffsfläche**, da deren Signale nicht an Sichtbarkeit oder physischen Kontakt gebunden sind. Im Jahr 2012 betrachteten wir unterschiedliche drahtlose Transponder-Systeme (RFID) von Schließanlagen und elektronischen Geldbörsen[12,13,14]. Allgemein stellten wir bei vielen betrachteten Produkten ein niedriges Sicherheitsniveau fest. Seit 2005 wird der in vielen österreichischen Städten verwendete Post- und Behörden-Schlüssel für Mehrparteienhäuser (auch Z oder BG genannt) durch eine elektronische Alternative ersetzt.

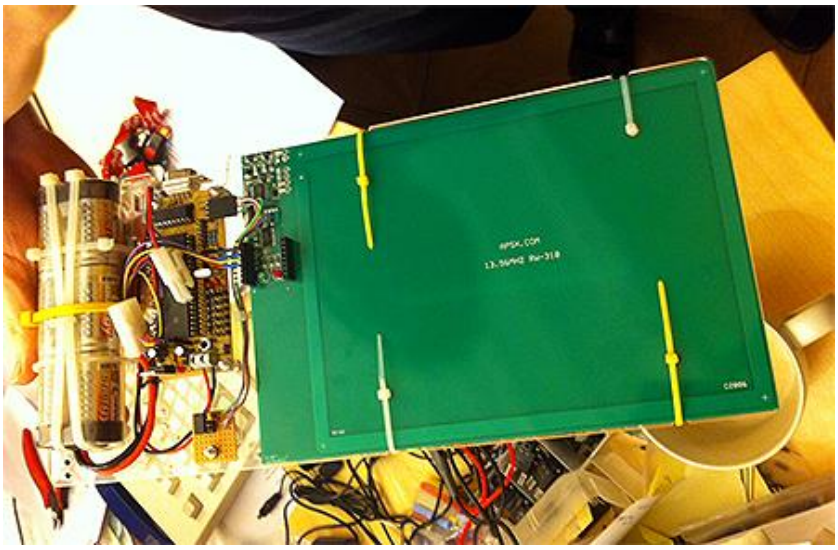

Abbildung 4: RFID Entwicklungsboard zur Analyse von Sicherheitslücken

[11] http://www.sba-research.org/pubs/reevaluating_smartphone_app_security.pdf
[12] http://events.ccc.de/congress/2013/Fahrplan/events/5334.html
[13] http://www.informatik.tuwien.ac.at/studium/studierende/epilog/poster_dabrowski.pdf
[14] https://www.youtube.com/watch?v=gTj5Ni7_zes

SBA Research konnte zeigen, dass diese Systeme bedenkliche Schwächen aufweisen: Manche Schlüsseltypen sind auf alte Schipässe übertragbar, andere lassen sich einfach und unauffällig kopieren. In einem Experiment verschickten wir einen aktiven RFID Reader[15] mit der Post und waren so in der Lage, die Schlüsseldaten der Postangestellten auszulesen. SBA Research hat die betroffenen Herstellerinnen und Hersteller informiert und konnte somit einen direkten Beitrag zur Sicherheit der österreichischen Bevölkerung leisten[16].

ADabrowski@sba-research.org

Impressum & Kontakt:

Edgar Weippl
eweippl@sba-research.org
SBA Research gGmbH
Favoritenstraße 16, 1040 Wien

[15] http://fm4.orf.at/v2static/storyimages/site/fm4/2014013/rfid_board.jpg

[16] Weitere Medienberichte:
http://www.faz.net/aktuell/politik/chaos-communication-congress-der-verstand-ist-ein-computerprogramm-12731286.html
http://www.wired.com/threatlevel/2013/12/citywide-rfid-master-house-key-already-broken/
http://www.heise.de/newsticker/meldung/30C3-RFID-Ueberwachung-in-China-Pannen-in-Oesterreich-2073043.html
http://futurezone.at/science/forscher-knackt-rfid-zutrittssystem-via-skipass/43.174.691
http://derstandard.at/1385172201331/30C3-RFID-Schliessanlagen-in-Wien-lassen-sich-leicht-ueberlisten
http://derstandard.at/1385172304649/RFID-Horror-Forscher-knackt-Wiener-Haustueren-mit-Skipass
http://www.golem.de/news/rfid-begehcard-ohne-sicherheit-mit-dem-skipass-in-wiens-wohnhaeuser-1312-103616.html
http://www.golem.de/news/rfid-sicherheitsluecke-begehcard-hersteller-wusste-von-kopierbarkeit-1401-103653.html