Schwachstellen bei Online-Diensten

Einleitung

Online-Dienste wie Storage-Services (z.B. Dropbox) und Kommunikationsapplikationen für Smartphones (z.B. WhatsApp) haben seit ihrer Markteinführung zunehmend an Beliebtheit gewonnen und können Millionen an Benutzern verzeichnen.
Die Angebote sind niedrigschwellig: Die Installation, Registrierung und Anwendung gestalten sich höchst unkompliziert und rasch, die Services sind meist kostenlos bzw. können gegen geringe Entgelte erweitert werden (z.B. zusätzlicher Speicherplatz bei Dropbox). In genau diesen Vorteilen verbergen sich allerdings signifikante Sicherheitslücken – so ist es für einen versierten Angreifer leicht, sich in den WhatsApp-Anmeldeprozess einzuklinken oder unberechtigt Dateien bei Dropbox abzuspeichern bzw. herunterzuladen.
Forscher der SBA Research gGmbH widmen sich in ihren Projekten solchen Sicherheitsrisiken sowie der Entwicklung von Gegenmaßnahmen.

Guess Who's Texting You? – Evaluierung der Sicherheit von Nachrichtenapplikationen für Smartphones

WhatsApp ist eine von zahlreichen jüngeren Entwicklungen für den wachsenden Markt an Smartphone-Anwendern. Diese und ähnliche Applikationen ermöglichen das Versenden von Kurznachrichten bzw. Telefonie via VoIP – und das kostenlos. Installation und Aktivierung der Applikationen sind äußerst einfach, zusätzlich können bestehende Kontakte meist ohne weiteren Aufwand importiert werden. All das sorgt für eine Niedrigschwelligkeit des Produkts und zieht potenzielle Anwender an, deren Anzahl im Millionenbereich liegen dürfte.
Zur Aktivierung von WhatsApp und ähnlichen Services genügt in der Regel die Bekanntgabe der eigenen Telefonnummer, zu der in Folge ein PIN gesendet wird, welche in der Benutzermaske einzugeben ist – und schon ist man registriert. Das hat einerseits – neben der raschen Abwicklung – den Vorteil, dass auch andere Endgeräte (z.B. ein WiFi-Tablet) auf diese Art für WhatsApp aktiviert werden können; gleichzeitig bringt dies erhebliche Sicherheitsrisiken mit sich. Forscher der SBA Research gGmbH konnten diese und vier weitere Angriffsarten identifizieren, für welche die Nachrichtenapplikationen Angriffsfläche bieten:

- Authentifizierungsmechanismus und feindliche Übernahme eines Benutzerkontos
- Manipulation der Sender-Identität/Manipulation der Nachrichten
- unerwünschte SMS/Anrufe
- Enumeration
- Modifikation von Statusnachrichten

Insgesamt wurden neun Applikationen getestet – neben WhatsApp u.a. Viber und Tango – mit dem Ergebnis, dass die Anwendungen zahlreiche Schwachstellen aufweisen: von einer möglichen Übernahme eines fremden Benutzerkontos im Zuge der Registrierung über das Versenden von Nachrichten unter einem „falschen Namen" bis hin zum Eruieren aktiver Telefonnummern, indem ein simuliertes Adressbuch z.B. in WhatsApp importiert wird (Enumeration).

Diese Schwachstellen beruhen auf bekannten Fehlern in Design und Implementierung der Software und können nachhaltige Auswirkungen auf die Privatsphäre der Benutzer haben.

Cloud-Speicherdienste als Angriffsvektoren

Die Vorteile von *Dropbox* umfassen die Minimierung von Datentransfer und nahezu unbegrenzte Speicherkapazität. Da Datentransfer und Speicherplatzbelegung für den Betreiber signifikante Kostenfaktoren darstellen, wurde eine Methode basierend auf Prüfsummen („hash values“) entwickelt, um Daten nicht doppelt zu speichern sowie ihren Transfer zu beschleunigen – letzteres kommt den Nutzern insbesondere im Hinblick auf eine rasche Synchronisation zwischen Server und lokalem Gerät zugute. Da der Client-Software bei diesem Verfahren ungeprüft Vertrauen entgegengebracht wird, ergeben sich zahlreiche Angriffsmöglichkeiten, die von den Forschern der SBA Research gGmbH untersucht wurden. Drei Angriffsszenarien auf *Dropbox*, die einzig das Wissen um die Hashwerte (Prüfsummen) der anvisierten Dateien voraussetzen, wurden analysiert:

- „Hash Value Manipulation“-Angriff: Via der Manipulation von Prüfsummen erlangt der Angreifer direkten Zugriff auf die gewünschten Dateien, ohne dass der Anwender oder *Dropbox* den Angriff als solchen identifizieren.
- „Stolen Host ID“-Angriff: *Dropbox* verlangt lediglich eine einmalige Registrierung des Nutzers bei Erstinstallation der Software; ist dies erfolgt, ist keine neuerliche Anmeldung mehr nötig; sobald ein Angreifer in Besitz der Host-ID ist, hat er Zugriff auf alle Daten des Opfers.
- „Direkter Download“-Angriff: *Dropbox* überprüft nicht, ob der mit der Host-ID verlinkte Account bzw. dessen Nutzer tatsächlich im Besitz von mittels Hashwerten angeforderten Dateien ist.
- „Online Slack Space“: Hierbei handelt es sich um eine Sicherheitslücke, die ein unbemerktes Hochladen unbeschränkt großer Dateien möglich macht.

Es konnten gezeigt werden, dass Dropbox zum Speichern von teilweise urheberrechtlich geschützten Dateien aus Filesharing-Netzwerken verwendet wird. Dabei wurde nachgewiesen, dass es relativ einfach ist, Daten versteckt auf Dropbox zu lagern, ohne strafrechtliche Konsequenzen befürchten zu müssen.
Als Gegenmaßnahme ist allen voran zu überprüfen, ob ein Nutzer wirklich im Besitz einer angeforderten Datei ist – hierzu wird die Implementierung eines einfachen Challenge-Response-Mechanismus empfohlen. Regelmäßiges Löschen von Daten, die nicht mit einer speziellen Datei verknüpft sind, sowie die Kontrolle der Host-ID-Aktivitäten sollten ebenfalls Teil der Schutzmaßnahmen sein.

Weiterführende Informationen

Sebastian Schrittwieser and Peter Fruehwirt and Peter Kieseberg and Manuel Leithner and Martin Mulazzani and Markus Huber and Edgar R. Weippl, "Guess Who Is Texting You? Evaluating the Security of Smartphone Messaging Applications," in*Network and Distributed System Security Symposium (NDSS 2012)*, 2012.
Martin Mulazzani and Sebastian Schrittwieser and Manuel Leithner and Markus Huber and Edgar R. Weippl, "Dark Clouds on the Horizon: Using Cloud Storage as Attack Vector and Online Slack Space," in *USENIX Security*, 2011.

Kontakt:

Privatdoz. Dipl.-Ing. Mag.rer.soc.oec.
Dr.techn. Edgar Weippl
E188 - Institut für Softwaretechnik und Interaktive Systeme
Technische Universität Wien
SBA Research, www.sba-research.org
edgar.weippl@tuwien.ac.at