Verschlüsselung bei vielen Android-Apps mangelhaft

19. Oktober 2012

Bei einer Analyse von Android-Apps, die Verschlüsselung einsetzen, fanden Informatiker der Uni Hannover und Marburg katastrophale Zustände vor: Mehr als 1000 der 13.500 populärsten Apps zeigten Anzeichen für eine fehlerhafte und unsichere Implementierung der SSL/TLS-Verschlüsselung. Tests mit 100 ausgewählten Apps bestätigten, dass davon immerhin 41 anfällig für konkrete Angriffe waren. Dabei fielen ausser Bank- und Kreditkartendaten auch Zugangs-Tokens für Facebook, E-Mail-Konten und Messaging-Services an.

In einem besonders plakativen Test schoben die Forscher Zoner AntiVirus für Android eine gefälschte Signatur unter, die auf die App selbst passte. Daraufhin stufte die sich auch prompt selbst als Bedrohung ein und bot die eigene Löschung an.

Der Code der Apps wurde zunächst statisch nach typischen Anzeichen für unzureichende Überprüfung der Zertifikate, die die Identität des Kommunikationspartners bestätigen müssen, untersucht. Da nicht eindeutig klar ist, ob der dabei gefundene Code tatsächlich zum Einsatz kommt, wurden danach explizit Man-In-The-Middle-Attacken durchgeführt, um die verschlüsselte Verbindung aufzubrechen.

Die dabei gefundenen Anfälligkeiten lassen sich in zwei Kategorien einteilen: 20 Apps akzeptierten einfach jedes Zertifikat. 21 weitere kontrollierten zwar, ob das Zertifikat eine gültige Unterschrift trägt, nicht jedoch, ob es auf den richtigen Namen ausgestellt ist. So konnten die Sicherheitsexperten mit einem gültigen Zertifikat für einen eigenen Server die Antiviren-Software narren.

Die Forscher von der Leibniz Universität in Hannover und der Phillips Universität Marburg fassen ihre Erkenntnisse in dem Paper Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security zusammen. Das für die Code-Analyse entwickelte Tool MallaDroid wollen sie demnächst veröffentlichen. Welche Apps konkret betroffen sind, verraten sie jedoch nicht. Aber anscheinend handelt es sich dabei nicht um Exoten: Immerhin 40 bis 185 Millionen Installation weist Google Play für die von den Lücken konkret betroffenen Apps aus.

Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security