12. Dezember 2018 Studie · Privatsphäre & Krypto · Mobile Sicherheit

Sichere Push-Benachrichtigungen

Der Volltext liegt derzeit nur in der Fassung „English“ vor. Die Übersetzung folgt.

Archiviert. Dieser Inhalt wird nicht mehr aktualisiert. Er bleibt zur Information verfügbar.

Quelle https://technology2.a-sit.at/veroeffentlichungen/sichere-push-benachrichtigungen/

Push-Benachrichtigungen sind Schlüsselkomponenten für Entwickler von mobilen Anwendungen, mit denen sie ihre Benutzer auf wichtige Neuerungen aufmerksam machen und an die Anwendung binden können. Diese Nachrichten werden im Allgemeinen über Push-Messaging-Dienste von Drittanbietern über eine TLS-Verbindung gesendet. Dabei fehlt jedoch eine Ende-zu-Ende-Verschlüsselung zwischen dem Entwicklerserver und den Nutzern. Deshalb demonstriert das Secure Push Notifications-Projekt die Implementierung von Ende-zu-Ende-verschlüsselten Push-Benachrichtigungen zwischen dem Entwicklerserver und den Android-Geräten der Nutzer. Hierbei werden auf dem Smartphone des Nutzers generierte und auf dem Entwickleranwendungsserver registrierte Schlüssel verwendet, um Push-Benachrichtigungen Ende-zu-Ende zu verschlüsseln. Das Projekt demonstriert auch die Funktionalität zum Senden vertraulicher Push-Benachrichtigungen, die verschlüsselt bleiben, bis der Benutzer das Gerät entsperrt hat.