Der Tuya-Smart-Home-Hack

IoT-Komponenten von unsicherer Tuya-Firmware befreien

Mit einer Handvoll Skripten kann man Tausende Smart-Home-Geräte von der Cloud befreien. c't stellt den Hack in Zusammenarbeit mit seinem Entdecker im Detail vor.

Von Merlin Schumacher

Auf dem 35C3, dem Jahres-Kongress des CCC, demonstrierte Michael Steigerwald vom IT-Startup VTRUST die Sicherheitslücken des chinesischen IoT-Produzenten Tuya. Laut Angaben des Herstellers basieren über 11.000 unterschiedliche Gerätemodelle auf Tuya-Soft- und -Hardware. Das Unternehmen bietet für 1500 US-Dollar einen Service an, bei dem der Auftraggeber die Hardware und Software nach seinen Wünschen anpassen kann. Tuya produziert die Geräte dann nach diesen Vorgaben. Softwarebasis und Cloud-Infrastruktur kommen dabei immer von Tuya.

Die Details des Hacks der Smart-Home- und IoT-Plattform des chinesischen Herstellers Tuya hat c't in Zusammenarbeit mit Michael Steigerwald veröffentlicht. Die für den Vortrag entwickelten Skripte wurden überarbeitet und auf GitHub als Open Source bereitgestellt, sodass nun jeder seine Tuya-Geräte mit einer offenen Firmware betreiben kann. Dazu benötigt man lediglich einen Linux-PC mit WLAN-Adapter oder einen Raspberry Pi, der WLAN ab Version 3 integriert hat. Die genauen Details zum Flashen der Tuya-Geräte erklärt ein kostenloser Online-Artikel auf ct.de. Das Repository und den zugehörigen Artikel finden Sie über ct.de/yaev.

ESP8266 inside

Herzstück der Tuya-Produkte ist oft der WLAN-fähige Mikrocontroller ESP8266, der in der Smart-Home-Szene unter Bastlern extrem populär ist. Infolgedessen gibt es allerhand Open-Source-Projekte, die alternative Firmwares entwickeln, die keine Starthilfe aus der chinesischen Cloud benötigen. Tuya tarnt den Prozessor zwar als TYWE3S oder TYWE2S, die inneren Werte sind jedoch gleich.

Für den Hack hat Steigerwald den Provisionierungsprozess der Geräte belauscht und so herausbekommen, dass Tuya das Smartconfig-Verfahren nutzt, um das IoT-Gerät ins heimische WLAN einzubinden. Dabei sendet die Tuya-App Pakete per UDP-Broadcast über das WLAN, mit dem das benutzte Smartphone verbunden ist. Gleichzeitig lauscht das Smarthome-Gerät auf solche Pakete. Der Inhalt ist zwar verschlüsselt, deren Längen jedoch nicht. In diese Paketlängen kodiert die App dann SSID, Schlüssel und das Zugangs-Token für die Cloud. Dadurch kann aber jeder, der in Empfangsreichweite des WLANs ist, die Zugangsdaten mithören. Andere Systeme wie etwa Zigbee umgehen das Problem, indem sie die Sendeleistung bei der Anmeldung so stark reduzieren, dass man nur wenige Zentimeter vom Empfänger entfernt sein darf, um neue Geräte koppeln zu können.

War die Verbindung mit dem WLAN erfolgreich, meldet sich das Gerät mittels des erhaltenen Token per unverschlüsseltem HTTP bei der Tuya-Cloud an, um dort die Schlüssel für die Kommunikation mit Tuyas MQTT-Broker zu erhalten. Diese Schlüssel werden ebenfalls im Klartext über das Internet versandt. Anschließend verbindet sich das Gerät mit dem MQTT-Dienst. Auch hier kommt keine Verschlüsselung mittels TLS (Transport Layer Security) zum Einsatz, immerhin werden aber die MQTT-Nutzdaten per AES-128 verschlüsselt.

Angriffe möglich

Für potenzielle Angreifer bedeutet das Beschaffen der Zugangsdaten zwar etwas Mühe, denn Sie müssen zum richtigen Zeitpunkt am richtigen Ort sein, aber dann haben sie unbeschränkten Zugriff auf das Heimnetz des Opfers. Ein perfideres Szenario bestünde darin einige Tuya-Geräte bei einem Versandhändler zu erstehen, diese mit einer gehackten Firmware zu versehen und zurückzusenden. Da man am Gerät selbst keine äußerlichen Veränderungen vornehmen muss, fällt der Hack nicht sofort auf. Der nächste Kunde der das vom Angreifer retournierte Gerät erhält, hat dann eine Wanze im Haus. *(mls@ct.de)* c't

Kostenlose Anleitung zum Tuya-Hack: ct.de/yaev

Tuya-Provisionierung

Während der Provisionierung hört das Gerät auf Broadcast-Pakete, ohne selbst im WLAN zu sein. Anschließend kommuniziert es mit dem Tuya-Server unverschlüsselt. Hier ist es leicht, in den Verkehr einzugreifen.