Title: From App to Cloud --- Private cloud API forensics for IoT android apps

Authors: Johannes Olegård, Stefan Axelsson

Note: This is the abstract of a submitted paper that I could present at swits as a **normal presentation** (not poster).

Abstract: Digital forensic practitioners are facing many challenges investigating Internet of Things (IoT) systems, e.g. recovery of deleted data, the need to reverse engineer an evermore growing plethora of devices and the volatility of data on physical devices. In this paper, we address these challenges by investigating the feasibility of extracting evidence from the cloud in IoT systems, via the same Application Programming Interfaces (APIs) used by the Android mobile apps in those systems. Six IoT-related Android apps (and IoT devices) were chosen and investigated: Mydlink, Kasa, Imou, Suunto, Huawei Health and Home Connect. The investigation consisted of dynamically instrumenting the apps (but not the IoT devices) on a pre-rooted Android device to collect and decrypt Transport Layer Security (TLS) traffic. Forensically useful cloud API endpoints were then easily identified from the decrypted data. Requests to these endpoints were imitated, using credentials extracted from the mobile device, to download forensic artifacts. Using cloud APIs, we could in some cases obtain slightly more data than what is necessarily stored in the apps. Some forensically useful artifacts were seen being uploaded with no visible way to be downloaded again, but this information could put practitioners in a better position when requesting forensic data from companies. Future work therefore includes improving API forensics by developing non-intrusive methods of uncovering additional API endpoints, so that more evidence can be recovered. In conclusion, we believe that automated API forensics could potentially help make IoT forensics more realistic in practice.