Vulnerability Report TTLock State Consistency Attack

Arvid Viderberg

June 2019

1 Evade the revocation from a time limited account

To test the guest account of the TTLock Smart Lock, a time limited guest user was created and invited to share the lock. The guest user first tried locking the lock with network enabled and while the timeframe of the users access was valid. The guest user then disabled network, leaving only Bluetooth activated. The guest user then waited for the valid timeframe to expired, and then tried to unlock the lock. When time expired, it was not possible to unlock the lock. The app would display an error message of *Operation failed*. When looking into the settings of the lock, there seems to be a clock installed on the lock itself, see figure 1. The clock in the lock keeps track if the timed key has passed its time limit. It is possible to adjust the time on the clock, however the time is fetched from the cloud API, and not the smartphones current time. Therefore, it was not possible to spoof the time at this stage.

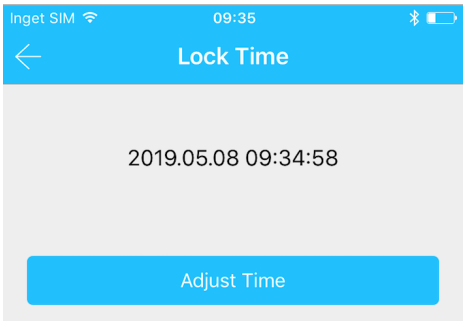

Figure 1: The time of the lock

2 Evade the revocation from a non-time limited account

A guest user was created and invited to share the lock. The guest user first tried locking the lock with network enabled. The guest user then disabled network, leaving only Bluetooth activated. The owner of the lock revoked the access of the guest user. When the guest user had no network, he/she could still control the lock via Bluetooth, even though access should have been revoked. The TTLock Smart Lock app showed the access key as *"Deleting..."* in the owners app when the guest user had turned off network and it had been revoked. The next time the guest user connected to network, it was marked as deleted. Hence, the TTLock Smart Lock app showed an indication that the access hadn't been completely removed when the guest user had turned of its network. This approach worked regardless if the lock was paired with the hub or not.