Vulnerability Report Glue Smart Lock State Consistency Attack

Arvid Viderberg

June 2019

1 Evade the revocation from a time limited account

To test the guest account of the Glue 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. The lock was successfully unlocked, meaning that it was possible for the guest user to evade the time limits of its account. This approach only worked when the lock was not paired with the hub. If the lock was paired with the hub, the guest would get an error message when trying to unlock the lock without network, see figure 1.

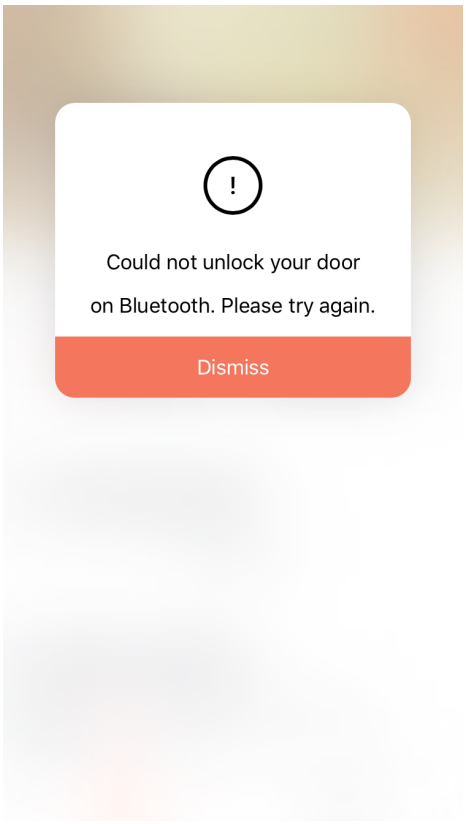

Figure 1: Error message when trying to control the lock without network.

2 Evade the revocation from a non-time limited account

To test the guest account of the Glue Smart Lock, 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 When the guest user had no network, he/she could still control the lock via Bluetooth, even though access should have been revoked. As soon as the guest user enabled network, the access was revoked. This approach only worked when the lock was not paired with the hub. If the lock was paired with the hub and trying to unlock the lock without network, the guest would get the same error message as with the time limited account, see figure 1.