Switch Tech – Recommendation for deployment in Apartment Environments

Date: 5/05/2023

Recap

Apartment buildings typically create a high density of users and cores. This density can lead to unintended outcomes when background mode is utilized with Switch™ Tech cores. Most current generation mobile devices have very strong Bluetooth antennas and in a multistory building that signal can reach to units above and below a given unit. This coupled with high density of users means there can be unintended signal clash degrading the user experience with background mode. **We recommend not using background mode in these environments.**

Switch™ Tech App Modes

The Switch™ Tech platform supports several different engagement types between the mobile application and the core. Many users default to using the direct method where they touch the core to awaken it and then touch the activate button to initiate the unlock command to the core.

Direct Mode:

Background Mode:

- If this feature is enabled for a site by the account owner / admin, a user can turn on 'background mode' in the app and the phone will automatically connect to an activated Switch™ Tech device to which the user has access. No need to get the phone out of pocket, open app, touch button, etc.
- Inherently, using background mode is a trade-off between security and convenience.

How does background mode work?

- Phone continually broadcasts LEGIC project ID
- When a core has been awakened within range of the phone, it connects to the phone automatically and initiates BLE channel / session keys
- If the mobile app has the necessary neon file / subfile for the specific core, it is delivered to the core
- The core makes the access decision and returns the access audit to the phone for delivery to the cloud / PACS.

With Apple devices, you can have background mode running but the Apple iOS will cancel the connection to Bluetooth after an extended period of time. A corrective action is as simple as opening the app and using the activate button to get the connection back, but it will require that user interaction. This is an inherent issue with iOS and not Switch.

For Android, the user can force close the app (shut it down) it will turn off and background mode will not be operational.

Security Levels within Switch™ Tech:

Switch™ Tech is an 'Offline' system. Therefore, it can never be as 'quickly secured' as an 'Online' system. Switch™ Tech has no way to guarantee revocation of a given credential other than by expiration date. In an online system, a credential can be revoked immediately during a direct wired communication with the online readers in the building. Switch™ Tech relies on wifi or cellular signal to revoke a given credential before the expiration date of the credential is reached.

All Switch™ Tech crypto keys are held in secure storage on the Switch™ Tech device using an EAL5+ secure element (Tamper-resistant physical security chip). Customer-specific Crypto keys are delivered when the Switch™ Core is configured by the site owner / installer.

Lowest level of security / highest level of convenience:

- Allow background mode at the facility, do not require PIN or biometric verification, No perimeter check in required at a hard-wired reader
- Susceptible to BLE relay attack / nefarious person waiting near a door that he wants to enter, waiting for someone to pass by with the phone in background mode.
- Susceptible to use of credential after revocation in the Access Control System (put phone in airplane mode to block revocation of the credential
- Susceptible to phone 'borrowing' even if phone screen is locked (due to background mode).
- Susceptible to use of credential after revocation in the Access Control System (put phone in airplane mode to block revocation of the credential)

- Not susceptible to Replay attacks due to session keys during BLE communication
- Mitigation: Disable background mode / Blocklist compromised / revoked credentials
- Mitigation: Can 'blocklist' a specific credential at specific high-risk doors. (requires visit to each door to be blocked)

Average level of security / medium level of convenience:

- No background mode allowed
- User must open the mobile app or use a fob to access the door. Requires active participation of the user
- Not susceptible to relay attack because the BLE communication is shut down when not in use.
- Not susceptible to phone cloning because hardware ID of the device must match the hardware ID stored in the file meta data.
- Not susceptible to Replay attacks due to session keys used during BLE communication
- Susceptible to phone 'borrowing' if phone screen is unlocked.
- Susceptible to use of credential after revocation in the Access Control System (put phone in airplane mode to block revocation of the credential)
- Mitigation: Can 'blocklist' a specific credential at specific high-risk doors. (requires visit to each door to be blocked)

We encourage users to evaluate their specific application of Switch™ Tech and how they chose to engage the devices. Switch™ Tech offers options that can streamline access to doors or elevate their access requirements far beyond that of a traditional mechanical key. When in doubt we always recommend defaulting to a higher level of security over convenience as a best practice. Contact your local dormakaba Sales Representative for demonstration of the different options or you can see our Knowledge Base at https://dhwsupport.dormakaba.com/hc/en-us for additional information.

Travis
Senior Product Manager – Switch Tech