

Saal: Project 12:00 00:30 Day: 2 Track: Security & Hacking nA  
2501

Title: **Keys? Where were going we dont need keys.**

Subtitle:

Speaker: **Damien Cauquil**

**Short:** *Smartlocks are the new way of securing doors by replacing the old mechanical locks by new high-tech and connected locks, able to communicate with other smart devices such as smartphones and computers.*

**Long:** Vendors argue that key dematerialization is the future of keys, where anybody would be able to give, control and revoke keys for one or multiple locks by using his smartphone. No more physical keys needed for a better control, or not. Well go through the challenges of key dematerialization in the actual world, from technical challenges to real world implementations ... and failures. Widespread smartlocks are not so smart, and developers often fail at correctly implementing cryptographic algorithms (especially when the smartlock is advertised as using a strong AES-256 implementation), and of course security by obscurity is still used and broken when dealing with critical embedded systems. During this talk, were going to demonstrate some real world attacks on one of these smartlocks, from information leaks to wireless lockpicking through fuzzing.