1500 - DOOMed Point of Sale Systems

Saturday at 15:00 in Track 3
45 minutes | Demo, Exploit
trixr4skids*Security Engineer*

In response to public security breaches many retailers have begun efforts to minimize or completely prevent the transmission of unencrypted credit card data through their store networks and point of sale systems. While this is definitely a great improvement over the previous state of affairs; it places the security of transactions squarely in the hands of credit card terminals purchased from third party vendors. These terminals have a security posture that is often not well understood by the retail chains purchasing them. To better understand if the trust placed in these devices is warranted, the attack surface and hardening of a commonly deployed credit card terminal series is reviewed and a discussion of reverse engineered security APIs is presented. Despite the reduced attack surface of the terminals and hardened configuration, attacks that allow recovery of magstripe track data and PIN codes are demonstrated to be possible.
trixr4skids
trixr4skids is a security engineer and a recovering consultant. He enjoys hardware hacking, reverse engineering, the occasional webapp RCE, robots, beer, and of course robots that bring him beer. As a child he enjoyed taking apart everything he could get his hands on in a quest to figure out how it worked (his parents did not always appreciate this). He could never figure out what the green rectangles with the black rectangles on them did and often resorted to smashing them with a hammer to see what was inside. Since then he has learned more effective ways to go about discovering the secrets those black things are hiding and even how to make them do different things than intended. His current research projects include attacking embedded devices based on the rabbit 2000/3000 CPUs, studying the security of payment card systems, and hacking anything interesting that he can buy off eBay.

@trixr4skids

#defcon25/by_track/track3/saturday #defcon25/By_Day/_saturday