

1500 - Real-time RFID Cloning in the Field


Thursday at 15:00 in 101 Track 2

20 minutes | Demo, Tool, Audience Participation

Dennis Maldonado*Adversarial Engineer - LARES Consulting*

Ever been on a job that required you to clone live RFID credentials? There are many different solutions to cloning RFID in the field and they all work fine, but the process can be slow, tedious, and error prone. What if there was a new way of cloning badges that solved these problems? In this presentation, we will discuss a smarter way for cloning RFID in the field that is vastly more efficient, useful, and just plane cool. We will go over the current tools and methods for long-range RFID cloning, than discuss and demonstrate a new method that will allow you to clone RFID credentials in the field in just seconds, changing the way you perform red team engagements forever.

Dennis Maldonado

Dennis Maldonado is a Security Consultant at LARES Consulting. His current work includes penetration testing, red teaming, and security research. Dennis' focus is encompassing all forms information security into an assessment in order to better simulate a real world attack against systems and infrastructure. As a security researcher and evangelist, Dennis spends his time sharing what he knows about Information Security with anyone willing to learn. Dennis co-founded Houston Locksport in  Houston, Texas where he shares his love for lock-picking and physical security as well as Houston Area Hackers Anonymous (HAHA), a meet-up for hackers and InfoSec professionals in the Houston area. Dennis is also a returning speaker to DEF CON having spoken at DEF CON 23 and DEF CON 24.

@DennisMald

[#defcon25/by_track/101-Track2/Thursday](#)

[#defcon25/By_Day/_thursday](#)