

Training:

RFID/NFC: Rise of Proxmark3 - directors' cut

Date of the training: **March 16-17, 2020** in Heidelberg, Germany

Book now using the voucher code: **TR20_HMTS** and save an additional 5% of the current valid rate of any package!

Overview

You will enjoy hacking with RFID/NFC cards and devices by means of open source. Several tools will be presented such as the SCL3711, RFIDler, HydraNFC, Chameleon Rev E rebooted, brand new Chameleon Rev G rebooted, but the primarily tool being used in this training is the **Proxmark3 RDV4**, the latest and most featured of the Proxmark3 generations (additional onboard storage, SIM interface, swappable antennas, etc.). You will have plenty of time to get familiar with the Proxmark3 RDV4 and operate it by yourself in various conditions and challenges.

During both days you will deal with different types of the most common transponders that can be found in the wild guided by **Doegox** and **Iceman** themselves, who will make sure you have a pleasant and instructive time.

The workshop covers RFID from the Low Frequency band (mainly used for individual physical access to buildings, garages, hotels, etc.) to the High Frequency band, where credit cards, passports, but also NFC come into play. You will understand which type of access cards can be emulated or even cloned.

We will discuss some case studies, practical hacks and lessons learned from working systems that can be found in the wild, including ePassports, RFID Toys, Credit Cards, Entry systems (PACS), transport ticket systems and Host-based Card Emulation. To setup your development environment, there are guides on the Proxmark3 RDV4 Github repo which are essential to follow. If everyone comes prepared, we can have better focus during the workshop on using / compiling / flashing / jtagging the proxmark3 device.

If you already have a Proxmark3 device, bring it with you and we show you how to use it with new firmware as well. We will also have a JTAG tool with us in order to demonstrate the easiness of recover a “bricked” device.

Prerequisites

Be at ease with C code, read documentation on Github.

Requirements

Bring your laptop with a configured development environment already installed:

- If you are under Linux (preferred), please follow these instructions¹ and make sure Modem Manager is removed;
- If you are under Windows, please follow these instructions² (we recommend WSL or Proxspace v3.2);
- If you are under OS X / Homebrew users, please follow these instructions³.

1

https://github.com/RfidResearchGroup/proxmark3/blob/master/doc/md/Installation_Instructions/Linux-Installation-Instructions.md

2

https://github.com/RfidResearchGroup/proxmark3/blob/master/doc/md/Installation_Instructions/Windows-Installation-Instructions.md

3

https://github.com/RfidResearchGroup/proxmark3/blob/master/doc/md/Installation_Instructions/Mac-OS-X-Homebrew-Installation-Instructions.md

About the Trainers

Philippe Teuwen (@doegox) is Security Researcher at Quarkslab. He's one of the LibNFC and Proxmark3 RDV4 maintainers and gave about 20+ workshops on RFID & NFC security and privacy issues at Troopers, Hack.lu, Brucon, RFIDsec, Hackito Ergo Sum, RMLL, etc. along with talks on other security topics such as Wi-Fi Protected Setup, eBanking, eVoting, reverse-engineering, Side-channel and fault injection, White-Box cryptanalysis etc.

He's in the editorial team of the International Journal of PoC/GTFO and makes hardware oriented CTFs.

Christian Herrmann (@Iceman) is administrator for the Proxmark3 forum, maintainer of Github Proxmark3 repo, iceman fork of chameleon mini and Proxmark3.

- Been giving talks at Black Alps, NullCon, Pass-The-Salt, Wireless village DEFCON,
- Some people might even say that I know one or two things about Proxmark3.
- Usually looking into all kind of RFID based systems.

Booking

Recommended online booking of trainings through:

<https://troopers.de/tickets/>

Voucher code: TR20_HMTS

Using this voucher code automatically gives you an additional 5% off the current valid price! You can register with this code until seats have run out.

Contact

Need assistance? Don't hesitate to call us. We are fluent in English and German.

+49 151 16228365 or info@troopers.de

Booking is also possible offline through your trusted partner:

HM Training Solutions, Falkenstrasse 6, 63820 Elsenfeld, Germany

+49 6022 508200 / info@hmtrainingsolutions.com

+49 6022 5089999 / www.hmtrainingsolutions.com