TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

RFID/NFC fully reloaded and even dirtier: Interaction, Cloning, Emulation, Replaying & Relaying

Date of the training: **March 18–19, 2019** in Heidelberg, Germany

Book Now using the voucher code: **TR19_HMTS** and save an additional 5% of the current valid rate of any package!

Overview

You will learn by example how to play with RFID/NFC cards and equipment. SCL3711, ACR122U, Proxmark3, Mifare Ultralight, Ultralight C, Classic, Plus, DesFire, iClass, HID Proximity, EM, credit cards, passports and more.

During the first day you will deal with different types of the most common transponders that can be found in the wild (aka tags, tokens, etc.). More tinkering, hacking and hands-on than ever, starting right away from the first day. Not a ton of theory. You can read the papers later, right? During the second day, you will interact with real digital payment systems such as “Samsung Pay”, “Visa PayWave”, “Apple Pay”, etc. and their possible exploitation (e.g. Relay & Replay attacks).

The first day of this unique 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. We will provide you with all the tools, materials and references for further study and research, with a strong emphasis on free software & free hardware.

You will understand which type of access cards can be emulated or even cloned; then, we are going to use traditional NFC USB readers, we will compile and execute the famous LibNFC, and play with some special hardware like the Proxmark3 and Chameleon Mini. Arduino examples will be shown to deal with both Low and High frequency cards and tokens. You will learn how to deal with the most common LF and HF transponders.

HID iClass vulnerabilities will be discussed as well as the NXP MIFARE Classic (and Plus) technology along with its public hacks.

We will also discuss some case studies, practical hacks and lessons learned from working systems the can be found in the wild, including ePassports, RFID Toys, Credit Cards, etc.

The second day will focus on digital payments and RFID/NFC attacks on them. You will understand the risk of the real threats that can be faced by all types of institutions that handle digital and physical payments (using NFC as well as Magnetic Secure Transmission -MST-). Demonstrations and real practices will be presented with real digital payments and their possible exploitation (eg. Relay and Replay attacks). Furthermore, we will discuss new type of attacks or data extraction that is not documented ;-).

So, yes, two days for getting very dirty playing with RFID and NFC devices!

Requirements

- The attendees are encouraged to bring their laptops with preferably a Linux setup (natively or in a VM, e.g. a Kali) and a compilation environment (git, gcc and gcc-arm <5) to play with the equipment.
- It is desirable to have a minimum knowledge of C language – debugging, compiling, and running. You may succeed using other OSes but you're on your own…
- An Android phone (also optional) with 4.4 KitKat system or higher, with NFC technology.
- Any RFID/NFC transponder or device is very welcome to share experiences and try some hacks on with it.

About the Speaker: Salvador Mendoza

Salvador Mendoza is a security researcher focusing in tokenization processes, mag-stripe information, payment systems and embedded prototypes. He has presented on tokenization flaws and payment methods at Black Hat USA, DEF CON 24/25, DerbyCon, Ekoparty, HITB, Troopers, 8dot8 and many other conferences.

He designed different tools to pentest mag-stripe and tokenization processes. In his designed toolset includes MagSpoofPI, JamSpay, TokenGet, SamyKam, BlueSpoof and lately NFCopy.

He has discovered vulnerabilities in different digital payment systems such as Samsung Pay, Google Wallet, Wells Fargo Wallet exploiting their NFC and MST protocols.

About the Speaker: Philippe Teuwen

Philippe Teuwen (@doegox) is a software & hardware security researcher / engineer at Quarkslab after having spent about 15 years in the industry. He organized numerous trainings, workshops & CTFs about RFID & NFC, microsoldering, cryptography as well as various talks and publications.

About the Speaker: Nahuel Grisolía

Nahuel Grisolía is the Founder and CEO of Cinta Infinita, an Information Security company based in Buenos Aires, Argentina. He is specialized in (Web) Application Penetration Testing and Hardware Hacking. He loves playing with Arduino's, IOT devices, ARM based hardware devices, Tamagotchis, Quadcopters, Lasers, etc. He has delivered trainings and talks in conferences and events around the world: BugCON (Mexico), H2HC (Brazil), Ekoparty (Argentina), OWASP events (Argentina), TROOPERS (Germany), PHDays (Russia), Ground Zero Summit (India), etc. He has discovered vulnerabilities in software from McAfee, VMWare, Manage Engine, Oracle, Websense, Google, Twitter, Auth0 and also in free software projects like Achievo, Cacti, OSSIM, Dolibarr and osTicket.

More Info at: http://cintainfinita.com
http://www.linkedin.com/in/nahuelgrisolia
http://www.exploit-db.com/author/?a=2008
http://www.proxmark.org/forum/profile.php?id=3000

TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Booking

Recommended Online Booking of Trainings Through:

Sign-Up Form https://troopers.de/tickets/

Voucher code: **TR19_HMTS**

Using this voucher code automatically gives you an additional 5% off the current valid price! You can register with this code up until March 11th, 2019 or until seats have run out.

Contact

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

Zögern Sie nicht uns zu kontaktieren. Wir sprechen fließend Englisch und Deutsch.

Troopers Organization Team

+49 151 16228365 or info@troopers.de

Booking is also possible offline through your trusted partner from:

HMTS HM Training Solutions

HM Training Solutions, Falkenstrasse 6, 63820 Elsenfeld, Germany

+49 6022 508200 / info@hmtrainingsolutions.com

+49 6022 5089999 / www.hmtrainingsolutions.com