TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

Bluetooth Hacking: A Practical Introduction

Date of the training: **June 22nd – 23rd, 2026** in Heidelberg, Germany

Book now using the voucher code: **TR26_HMTRAINING** and save an additional 5% of the current valid rate of any package!

Overview

Bluetooth is ubiquitous across mobile devices, automotive systems, IoT devices, and really any device you can think of (including [Lego]!) Despite its widespread adoption, it is often overlooked as a possible attack vector and not properly assessed during the development phase of a product.
While the Bluetooth protocol specification has its own weaknesses, in practice security issues more often stem from specific design choices and stack configurations, making it essential to cover both aspects.

This hands-on workshop provides an introduction to Bluetooth hacking from a security researcher's perspective. Participants will gain an understanding of the Bluetooth protocol stack, including the physical layer, link management, and higher-level protocols such as L2CAP, RFCOMM, and GATT. The goal is to equip the participants with the necessary skills, knowledge, and tools to get started with their own Bluetooth security research.

The workshop covers device discovery and enumeration for both Bluetooth Classic and Low Energy, pairing and authentication mechanisms, and the exploitation of common vulnerabilities in the pairing process. Participants will learn traffic capture techniques, protocol testing methodologies for custom GATT and RFCOMM services, and address spoofing attacks. The workshop also contains practical exercises involving the analysis and exploitation of a real Bluetooth-enabled device.

No prior Bluetooth expertise is required. Participants should be comfortable with the Linux command line and ideally have some basic Python scripting skills. By the end of the workshop, attendees will have acquired skills for Bluetooth security assessments and practical experience with Bluetooth devices and tooling.

Who should attend this training?

The workshop is target towards:

- Security professionals
- Developers
- People interested in Bluetooth security

Requirements

The attendees should have:

- Linux CLI Skills
- Python skills (optional, but helpful)

About the Trainers:

Frieder Steinmetz earned his Master's degree on the security of embedded and cyber-physical devices from the Technical University of Hamburg. He has a background in cryptography, published work on the security of encrypted messaging protocols and malicious USB devices and Bluetooth security. He works as Senior Security Analyst at ERNW Enno Rey Netzwerke GmbH. His work focuses on pentesting mobile and embedded devices, as well as their back-end communication and infrastructure. He regularly gives Trainings on subjects such as IoT, RFID/NFC Hacking, web application pentesting and communications security.

Dennis Heinze is a Senior Security Researcher and Penetration Tester at ERNW Enno Rey Netzwerke GmbH. He holds a Master's degree in IT Security from TU Darmstadt, with a focus on network and system security. Dennis has published multiple research works on Bluetooth security, including analyses of Bluetooth protocol implementations within the Apple ecosystem and research into the security properties of Bluetooth Auracast. At ERNW, his work primarily focuses on penetration testing of mobile and embedded devices, as well as the security of their communication channels and backend systems.

Booking

Recommended online booking of trainings through:
https://troopers.de/tickets/

Voucher code: TR26_HMTRAINING
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 6221 480390 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@hm-ts.de
+49 6022 5089999 / https://hm-ts.de