



**HANDS-ON
SECURITY**

BREAKING MICROSOFT'S DEFAULT BITLOCKER SETUP

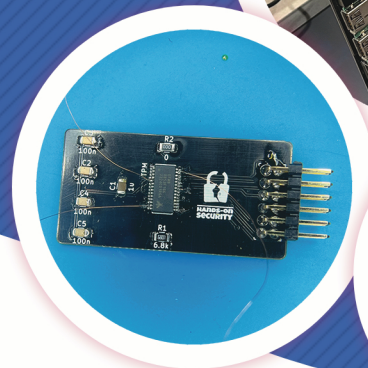
Start as a beginner and emerge as a hardware hacker: Dive into our BitLocker TPM training to learn micro soldering, hardware reversing, logic analyzer sniffing and decrypt your BitLocker TPM protected target device.

CONTENT

In our 2-day training, we'll guide you step-by-step, ensuring you not only learn but truly understand the magic behind BitLocker & TPM setups.

Never held a soldering iron? No worries! We'll start with the basics of micro soldering, and by the end of the first day, you'll be soldering your own attack adapters. You'll even get to take home a test notebook and all required hardware for successful hardware attacks!

For those of you who've never ventured into the realm of hardware, this is your golden ticket.



INCLUDING
ALL HARDWARE
3499.-
CHF



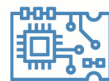
SOLDERING

You will solder your own attack adapters. After in-depth theory and a warmup with the soldering iron you will learn how to micro solder on target devices.



LOGIC ANALYZER

Understand the capabilities and limitations of logic analyzers and undertake common bus sniffing attacks.



REVERSING ELECTRONICS

Learn to identify components, find datasheets, read schematics and link all together to find weak spots.

HARDWARE KIT

- detailed slide set
- script to extract VMKs
- script to decrypt BitLocker recovery passwords
- extensive hardware kit including:
 - U3Pro16 logic analyzer
 - microsolder station
 - soldering set
 - custom TPM attack adapters
 - target device with TPM



UPCOMING TRAINING
30. – 31.01.2025



HWZ, Lagerstrasse 5,
8021 Zürich, Switzerland



training@hands-on-security.com
www.hands-on-security.com