

UEFI offensive security

Overview

- modern x86 architecture
- boot flow from power on to system take off
- understanding Intel security features
- attacking Intel security features
- overview most popular Uefi forensics tools
- firmware weakness analysis
- SMM known attacks – theory and practice
- TPM
- Intel TXT and SGX
- Uefi variables and S3 attacks
- Update mechanism exploitation
- Non Uefi attack vectors WiFi/BT/3G/4G and USB
- DMA as an attack vector
- recent Lenovo and Dell vulnerabilities

Audience

People familiar with computer architecture on intermediate level.
Computer Science or similar Master of Science degree. Minimal knowledge of Python is required.

Materials

All training materials presentations and source code will be available for customer internal usage..



Duration

5 days

40 hours (8h/day)

70% lectures

30% hands-on workshop

Language

English.