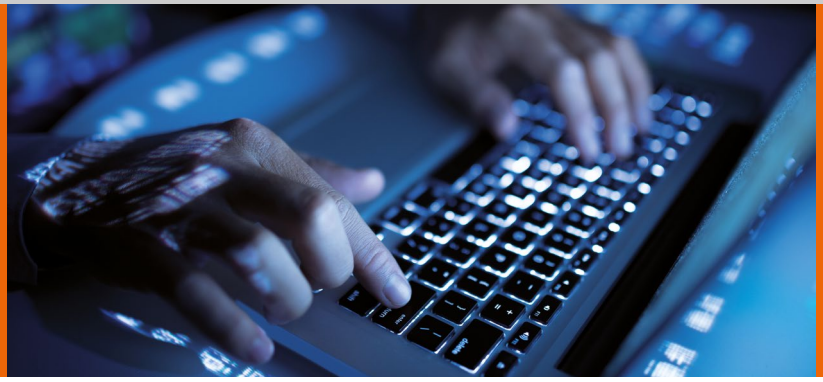
Fraunhofer
ACADEMY



HOW YOU CAN BENEFIT: AT A GLANCE

After the seminar, you will be able to ...

... understand the actions of a hacker and develop exploits to expose their weaknesses.

... understand typical programming errors in C code, and the limitations of protection mechanisms.

... assess the applicability of protection mechanisms for your own development.

This seminar will provide you with ...

... a profound overview of select techniques of binary exploitation.

… knowledge of practical implementation methods for circumventing protection mechanisms and developing your own exploits.

HACKING: BINARY EXPLOITATION

Buffer overflows and their consequences

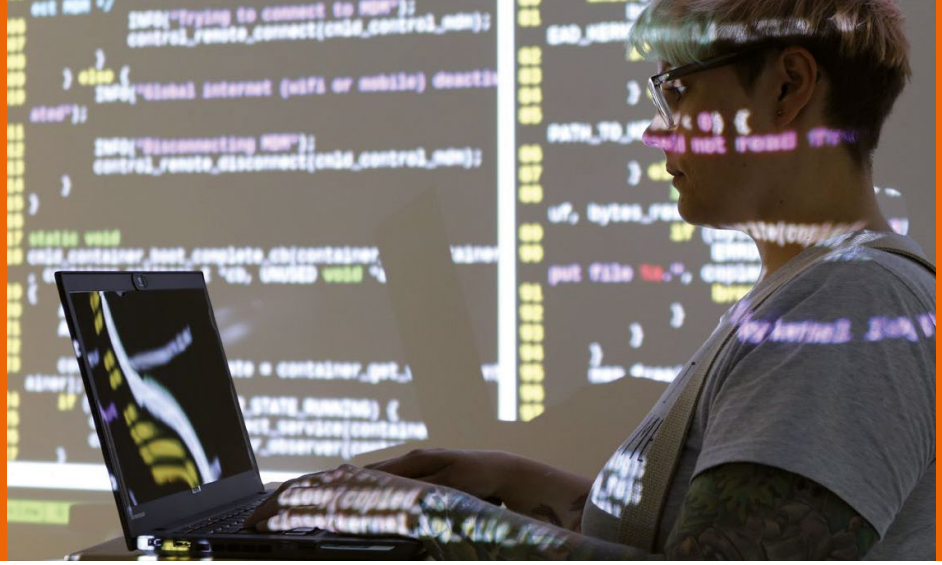
The challenge:
New attack scenarios as part of growing connectivity

More and more devices and systems can now be reached through the Internet and other networks, exposing them to direct attacks. This creates challenges for many companies to appropriately secure their systems and protect themselves against possible hacker attacks. Despite the protection mechanisms currently available (e.g. non-executable storage regions, ran-domization of addresses or stack cookies inserted by the compiler), weaknesses in applications are still being successfully exploited. This poses the question of how these protection mechanisms can be circumvented by the attackers.

The solution:
Understanding and predicting binary exploitation from the viewpoint of hackers

As part of this seminar, participants will discover the approaches used by hackers in order to be better prepared for such attacks.

The main focus of this seminar is the field of binary exploitation: for example, how programming errors in C code can be exploited to inject and execute external code. As part of this, the question of how effective the system and compiler protection mechanisms are, and how and in what circumstances attackers can circumvent such protection, is answered.



INFORMATION OVERVIEW

Course: Hacking: Binary Exploitation

Prerequisites:
- Linux basics: Routine operations with the Bourne-Again Shell (BASH) and the GNU Debugger (GDB)
- Programming knowledge: Fluent reading and understanding of code in C, pro-gramming experience in C or Python
- Assembler: Reading and understanding of x86_64 assembler, programming in assembler is not required

Duration: 3 days in class

Cost: 1.800 €

Organized by:

Fraunhofer AISEC

OUR SPEAKER

Tilo Fischer
Research specialists for safe sensor systems at Fraunhofer AISEC

Contents: Exploitation in theory and practice

- Basics of buffer overflow, debugging, disassembler
- Practical training: Debugging and reverse engineering
- Introduction to stacks
- Practical training: First exploit without protective measures

- Protective measures through compilers
- Practical training: Exploit with compiler protective measures
- Protective measures through the system
- Practical training: Exploit with system protective measures

- Introduction to heaps
- Practical training: Exploit without protective measures
- Practical training: Exploit with protective measures (optional)

Learning objectives: Successful identification of weaknesses

- Identification of typical programming errors in the C language
- Recognition of the limits of the protection mechanisms available
- Profound knowledge of storage device architectures
- Learning methods for circumventing protection mechanisms
- Development of exploits for using weaknesses in applications

Target group: Developers, testers, operators and users

Developers, testers, operators and users who would like to learn the approaches used by hackers to improve the security of their systems with this knowledge.

The Cyber-Security Training Lab: Advanced Training for the IT security experts of tomorrow

The Cyber-Security Training Lab is the result of a collaborative effort between Fraunhofer and a number of select technical colleges, transferring up-to-date knowledge of cyber-security as part of advanced training courses offered to companies. All over Germany, specialists and managers in industry and public administration receive compact qualifications in top labs with the latest IT infrastructure.

DO YOU STILL HAVE QUESTIONS ABOUT ...

... binary exploitation and secure operating systems?
Tilo Fischer
Fraunhofer AISEC
Phone +49 89 3229986-201
tilo.fischer@aisec.fraunhofer.de

... registration, organization or information about other courses offered?
Adem Salgin | Fraunhofer Academy
Phone +49 89 1205-1555
cybersicherheit@fraunhofer.de