



Fraunhofer

ACADEMY



CYBERSECURITY TRAINING LAB

The Challenge: Growing Cybersecurity Risks, Few Specialists

Training and development in the field of IT security is an issue of national interest, given that cyber attacks on critical infrastructures or industrial complexes can result in significant financial losses, the disruption of vital supply networks, or the breakdown of public order. The growing trend toward connectivity and digitalization only accentuates the threat. Already in 2014, 61 percent of the companies cited expertise in IT security as one of their priorities when recruiting qualified staff. And yet in 2015 only five of the 64 major universities with computer science departments offered degree courses in IT and cybersecurity. Moreover, the shortage of trained specialists in the security industry will reach 1.5 million worldwide by 2020. Hence, professionally trained IT security specialists are a rare commodity in Germany.

The Solution: Cybersecurity Training Lab for Security Experts of Tomorrow

So as not to fall behind in the arms race with cyber criminals, IT teams and managers must constantly hone their skills and improve their expertise in order to stay at least one step ahead. Several Fraunhofer Institutes and universities of applied sciences are now offering a modular, part-time study program to alleviate the unmet demand for training opportunities. The Cybersecurity Training Lab created for this purpose will receive six million euros per year in funding from the German Federal Ministry of Education and Research (BMBF) during its first years of operation.

Fraunhofer Academy

Phone: +49 89 1205-1555
cybersicherheit@fraunhofer.de

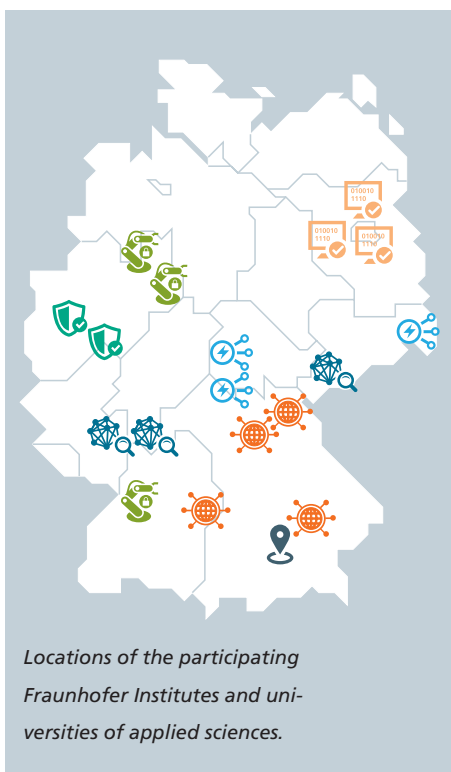
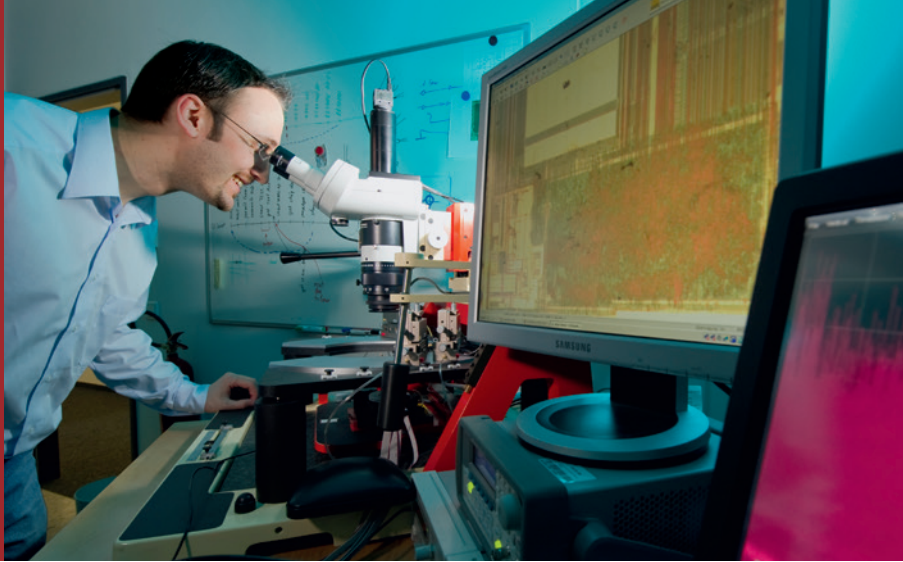
[www.academy.fraunhofer.de/
cybersecurity](http://www.academy.fraunhofer.de/cybersecurity)



```

import socket, sys, os
print "][ Attacking " +
print "injecting " + sys
def attack():
#pid = os.fork()
s = socket.socket(
s.connect((sys.argv[
print ">> GET /" + sys.
s.send("GET /" + sys.arg
s.send("Host: " + sys.ar

```



The Concept: Collaboration with Technical Colleges for Up-to-Date Research Knowledge

Fraunhofer and a select group of universities have developed a modular concept for cybersecurity training. This collaborative approach enables the latest theoretical or practical research findings to be immediately incorporated into the teaching program. Students will work in modern laboratories equipped with simulation tools allowing real threat scenarios to be tested. They can specialize in the following thematic areas:



Industrial manufacturing/
Industry 4.0



Critical infrastructures/Use cases for
energy and water infrastructures



High-security and emergency-
response facilities



Internet security and IT forensics



Software quality/certification



Embedded systems, mobile security
and the internet of things

The Recipe for Success: Accumulation of Competence Meeting the Needs

The teaching components are condensed into a compact format requiring only part-time attendance, and the modules can be combined in different ways to match the IT security requirements of various professional functions. The Fraunhofer Academy intends to develop new modules based on demand and provides end-to-end quality management. Industry supports this initiative, as confirmed by Thomas Tschersich, Senior Vice President Internal Security & Cyber Defense at Deutsche Telekom AG:

"We particularly appreciate the modular format that concentrates teaching content in short training units, enabling the transfer of knowledge in specific subject areas. This is ideal for part-time study and for specific training in the use of modern tools."

Your benefits at a glance



Practically presented **cutting-edge research knowledge**



Testing of customised solution strategies in high-value labs



Compact and transfer-oriented formats for integrated professional learning



Flexible combinable modules tailored for the specific needs of the business or institution