Fraunhofer
AISEC

Fraunhofer-Institut für Angewandte
und Integrierte Sicherheit AISEC

Philip Sperl

02. April 2025 – Artificial Intelligence in Bavaria and Northern Europe

Breakout Session II: AI & Service Sector

AI and Security – Hinder or Foster Each Other?

AI and Security – Hinder or Foster Each Other?

Overview

Risks and Challenges posed by AI

AI as a Tool for Enhancing Security

Balancing Risks and Benefits

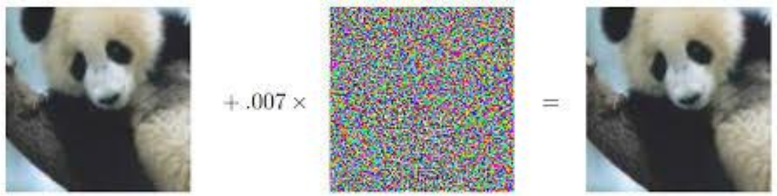
Risks and Challenges Posed by AI

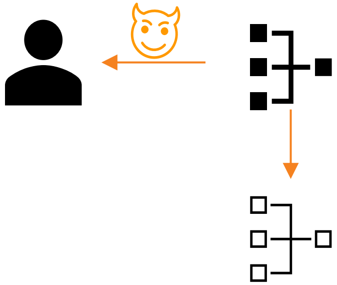
Three Perspectives

AI as an Attack Tool

Automated, large-scale attacks

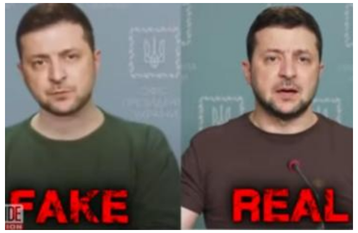
Tricking AI

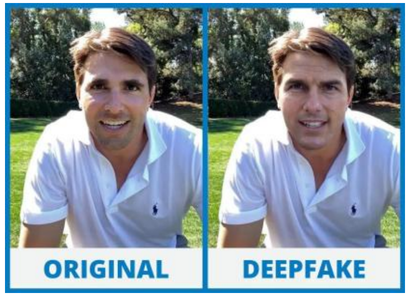




Change the output or extract information

Tricking Humans



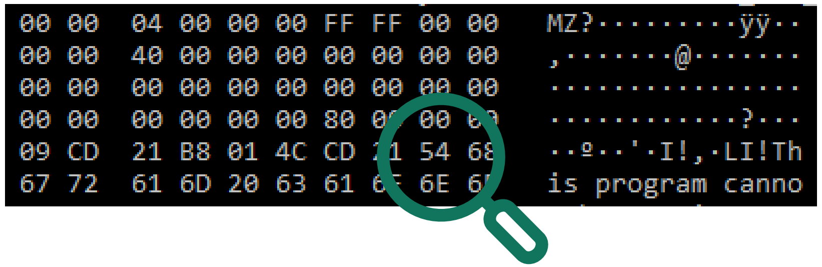


Deepfakes created by generative AI

AI as a Tool for Enhancing Security

Insights from Research

Software Analysis



```
00 00  04 00 00 00 FF FF 00 00   MZ?·········ÿÿ··
00 00  40 00 00 00 00 00 00 00   ,·······@·······
00 00  00 00 00 00 00 00 00 00   ················
00 00  00 00 00 00 80 00 00 00   ············?···
09 CD  21 B8 01 4C CD 21 54 68   ··º··'·I!,·LI!Th
67 72  61 6D 20 63 61 6E 6E 6F   is program canno
```

Helping human experts

Intrusion & Threat Detection

Large-scale data analysis

Compliance

§

Automatic checks and documentations

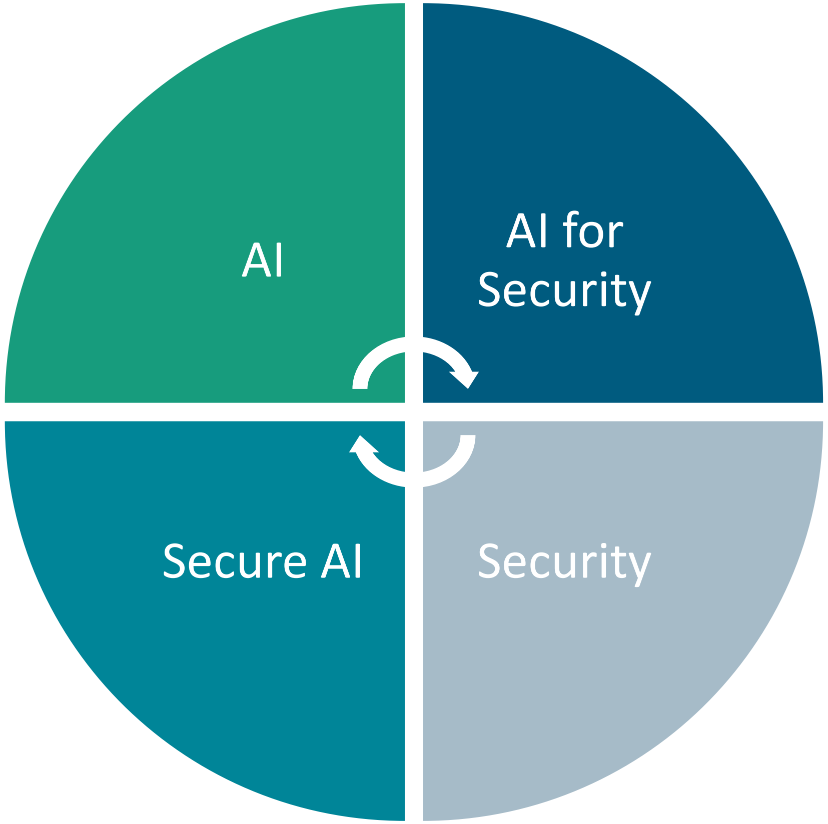
Balancing Risks and Benefits

New Dynamics in the Research Landscape

The areas of AI and IT security are no longer clearly separated.

Current research is developing more and more interfaces.

Regulations are needed – but with caution.



Contact

Fraunhofer AISEC

Fraunhofer-Institut für Angewandte
und Integrierte Sicherheit AISEC

Dr. Philip Sperl

Head of Department Cognitive Security Technologies
philip.sperl@aisec.fraunhofer.de