Chair of Security in Information Technology
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Forschungspraxis

# Glitching Attacks on FPGA SoCs (AISEC)

Moderne SoC werden üblicherweise mittels einem "Secure Boot" Prozess geschützt. Dieser soll sicherstellen, dass nur autorisierte Firmware ausgeführt wird und dass diese geheim bleibt.
Ziel dieser Arbeit ist es zu untersuchen, ob der Secure Boot Prozess eines bestimmten SoC mittels Glitching kompromittiert werden kann, sodass z.B. die Firmware extrahiert werden kann, nicht autorisierte Firmware geladen wird, oder aber Debug-Schnittstellen aktiviert werden.
Glitching-Angriffe versuchen externe Eingänge wie Takt oder Versorgungsspannung gezielt so zu manipulieren, dass Fehler im regulären Programmablauf entstehen. Hierfür wird der Systemtakt kurzzeitig auf Werte außerhalb der Spezifikation erhöht oder die Versorgungsspannung kurzzeitig auf GND gezogen.

## Prerequisites

- Gute Kenntnisse in der Programmiersprache C, dem Umgang mit Mikrocontrollern und VHDL
- Grundlegende Kenntnisse in IT-Sicherheit
- Eigenständiges Arbeiten und Motivation zum Entwickeln eigener Lösungen

## Contact

Bodo Selmke
Telefon: +49 89 3229986-132
E-Mail: bodo.selmke@aisec.fraunhofer.de

Nisha Jacob Kabakci
Telefon: +49 89 3229986-116
E-Mail: nisha.jacob@aisec.fraunhofer.de

## Advisors

Georg Sigl
Bodo Selmke, Nisha Jacob Kabakci (Fraunhofer AISEC)