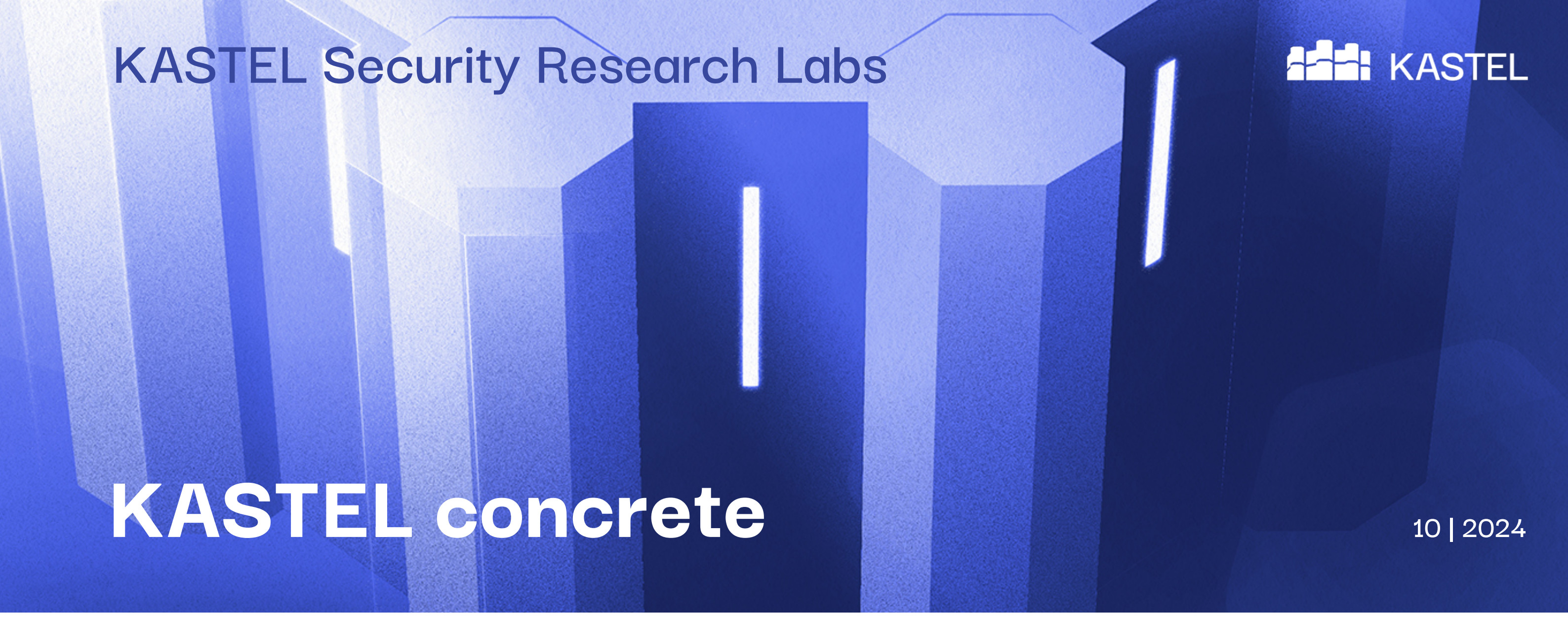


KASTEL Security Research Labs

KASTEL

KASTEL concrete

10 | 2024

Distributed Usage Control in Interactive Assembly Assistance Systems

Interactive assembly assistance systems offer production workers individual support when carrying out complicated work steps. However, video cameras and AI-based image processing software not only capture workpieces, tools and components, but also the workers themselves and their activities. This results in data privacy risks for production workers, which must be mitigated by effective technical measures.

Data Protection Through Distributed Usage Control

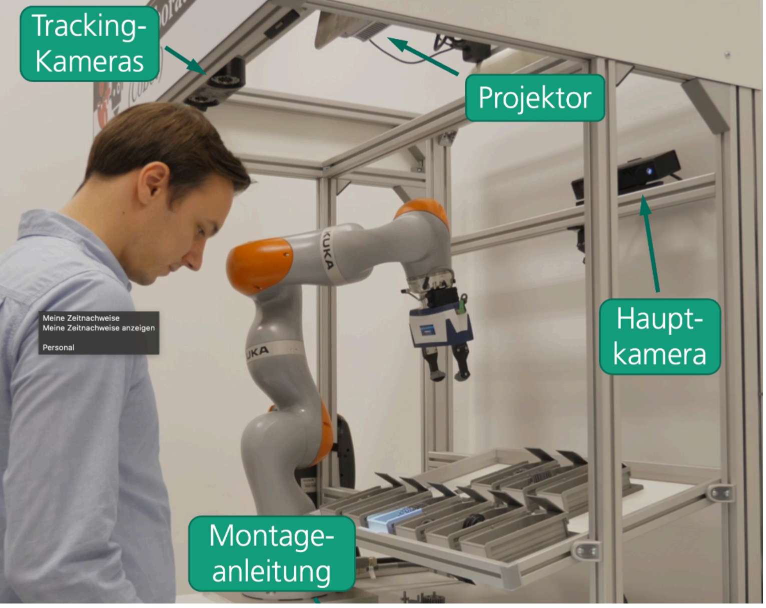
Applying distributed usage control technology in assembly assistance systems allows to restrict the processing of captured information based on previously approved security guidelines. In cases where data should be forwarded to external parties, for example as part of a quality assurance process, the usage rules are also transferred and enforced in the remote systems. This makes usage control an effective tool for the technical enforcement of data processing regulations, which for assembly assistance systems are often established as part of company agreements.

Challenge: Establishing Trust in Usage Control Infrastructures

A major challenge when operating distributed usage control infrastructures is to ensure system integrity. If the endpoints receiving sensitive data are not trustworthy, they may not enforce the transmitted usage rules correctly in the remote domain. Trusted computing technologies provide the solution for this issue. By using tamper-resistant hardware modules such as TPMs (Trusted Platform Modules), which leverage cryptographic methods to generate unique system fingerprints, the state of remote usage control systems can be verified even before sensitive data is disclosed. This effectively prevents malicious tampering of usage control components in the data receiving domains.

Our Research

In the Competence Center for Applied Security Technology, KASTEL Security Research Labs, KIT and Fraunhofer IOSB are jointly researching methods for the use of trustworthy usage control in interactive assembly assistance systems.



Besides classical TPMs, we also research solutions based on the Intel Software Guard Extensions (SGX) and ARM TrustZone to protect distributed usage control components against malicious tampering. Another research focus lies on achieving interoperability between different trusted computing technologies. This makes it possible to process the data collected in assistance systems in a tamper-proof and trustworthy manner according to their usage rules, even in heterogeneous infrastructures.

Paul Wagner

https://primo.bibliothek.kit.edu/permalink/f/4jne3t/KITSRCE1000172286