Verteilte Nutzungskontrolle in interaktiven Montageassistenzsystemen

Interaktive Montageassistenzsysteme bieten Arbeitenden in der Produktion individuelle Unterstützung bei der Durchführung komplizierter Arbeitsschritte. Mittels Kameras und KI-gestützter Bildverarbeitung werden dabei jedoch nicht nur Werkstücke, Werkzeuge und Bauteile, sondern auch die Arbeitenden selbst und ihre Tätigkeiten erfasst. Hierdurch können erhebliche Datenschutzrisiken für die Arbeitenden entstehen, welche durch technische Maßnahmen minimiert werden müssen.

Datenschutz durch verteilte Nutzungskontrolle

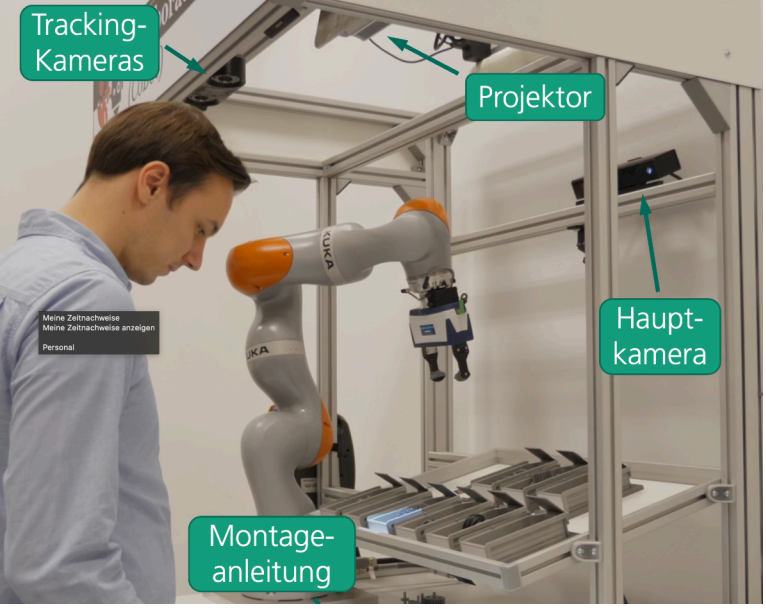
Der Einsatz von Nutzungskontrolltechnologie in Montageassistenzsystemen ermöglicht es, die Verarbeitung der erhobenen Daten auf Basis zuvor beschlossener Sicherheitsrichtlinien einzuschränken. Werden die Daten an externe Stellen weitergeleitet, etwa zur weiteren Auswertung im Rahmen der Qualitätssicherung. So werden auch die Nutzungsregeln mit übertragen und in den fremden Systemen durchgesetzt. Somit bietet verteilte Nutzungskontrolle ein effektives Werkzeug zur technischen Durchsetzung von Datenverarbeitungsrichtlinien, wie sie etwa in Betriebsvereinbarungen festgelegt werden können.

Herausforderung: Etablierung von Vertrauen in Nutzungskontrollinfrastrukturen

Eine zentrale Herausforderung beim Betrieb von verteilter Nutzungskontrolle ist die Sicherstellung der Systemintegrität. Sind die datenempfangenden Systeme nicht vertrauenswürdig, so besteht die Gefahr, dass die übertragenen Nutzungsregeln dort nicht korrekt durchgesetzt werden können. Abhilfe schaffen hier Techniken des Trusted Computing. Durch manipulationsresistente Hardwarebausteine wie etwa TPMs (Trusted Platform Modules), welche die Erzeugung eindeutiger Fingerabdrücke eines Systems ermöglichen, kann der Zustand von fremden Nutzungskontrollsystemen noch vor der Datenweiterleitung verifiziert werden. Bösartige Manipulationen an den empfangenden Nutzungskontrollkomponenten können so ausgeschlossen werden.

Unsere Forschung

Im Kompetenzzentrum für angewandte Sicherheitstechnologie, KASTEL Security Research Labs, forscht das KIT gemeinsam mit dem Fraunhofer IOSB an Methoden zum Einsatz vertrauenswürdiger Nutzungskontrolle in interaktiven Montageassistenzsystemen. Zur Ab-



sicherung der verteilten Nutzungskontrollkomponenten untersuchen wir neben klassischen TPMs auch Lösungen basierend auf den Intel Software Guard Extensions (SGX) sowie ARM TrustZone. Ein weiterer Forschungsschwerpunkt liegt auf der Herstellung von Interoperabilität zwischen unterschiedlichen Trusted-Computing-Technologien. Dies ermöglicht es, die in den Assistenzsystemen erhobenen und mit Nutzungsregeln versehenen Daten auch in heterogenen Infrastrukturen manipulationssicher und vertrauenswürdig gemäß den Sicherheitsrichtlinien zu verarbeiten.

Paul Wagner

https://primo.bibliothek.kit.edu/permalink/f/4jne3t/KITSRCE1000172286l-labs.de