KOMPETENZZENTRUM CyberProtect

EIN QUICK-CHECK DES KOMPETENZZENTRUMS CyberProtect

DRAG&BOT SECURITY CHECK

KONTAKT

Fraunhofer IOSB

Fraunhofer IOSB
Anne Borcherding
anne.borcherding@iosb.fraunhofer.de

FZI Forschungszentrum Informatik
Niklas Goerke
goerke@fzi.de

IN ZUSAMMENARBEIT MIT

drag and bot GmbH

Martin Naumann
martin.naumann@dragandbot.com

Ausgangssituation und Problem

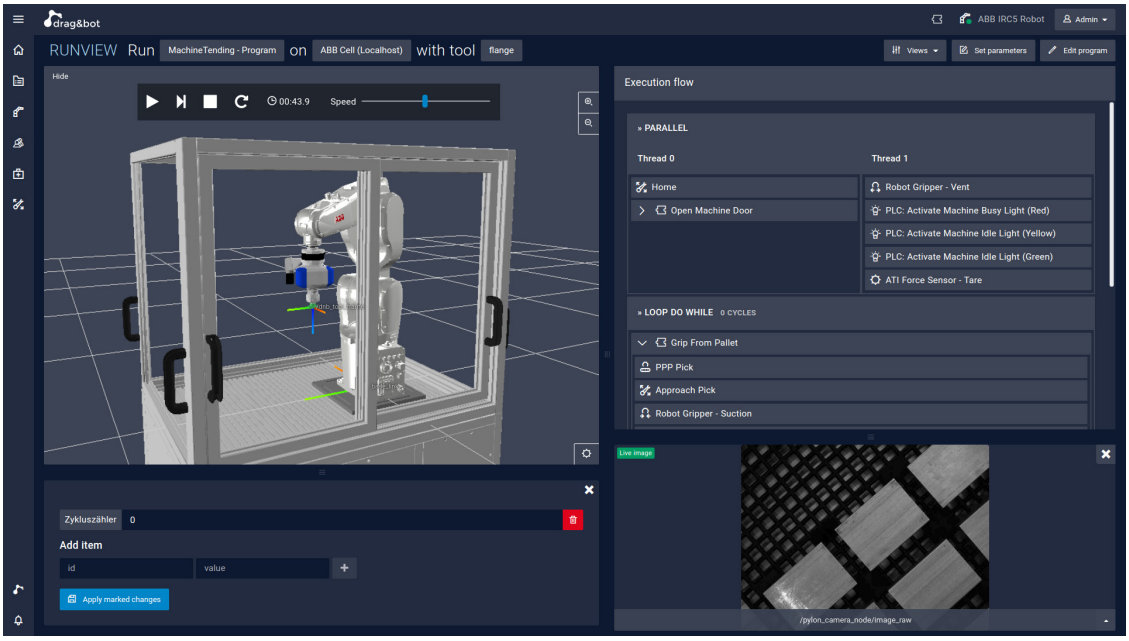
Die Software von drag&bot bietet eine grafische Programmieroberfläche für Industrieroboter. Um diese Funktionalität bereitstellen zu können, benötigt die Software diverse Schnittstellen. Diese Schnittstellen können von möglichen Angreifern potenziell als Einfallstore verwendet werden. Ein Angreifer könnte insbesondere die angebotene Weboberfläche ausnutzen. Um eine fundierte Einschätzung über den aktuellen Stand der Security der drag&bot-Software treffen zu können, werden in diesem Quick-Check Analysen auf zwei verschiedenen Ebenen durchgeführt. Zum einen erfolgt eine Sicherheitsanalyse der Architektur der drag&bot-Software. Zum anderen wird die Security der Webanwendung unter Zuhilfenahme verschiedener automatisierter Web-Security-Scanner untersucht. Die verwendeten Web-Security-Scanner wurden zuvor im Rahmen des Security-Testlabors am Fraunhofer IOSB bereits für die Untersuchung industrieller Kontroll- und Steuerungssysteme evaluiert und praktisch eingesetzt. In diesem Projekt können sie nun für eine Webanwendung im Kontext der Roboterprogrammierung evaluiert werden.

Lösungsansatz

Sowohl die Sicherheitsanalyse der Architektur als auch die Untersuchung der Webanwendung werden im Rahmen eines Workshops bei drag&bot durchgeführt. So kann ein direkter und persönlicher Austausch gewährleistet werden. Zunächst wird die Architektur der Software von drag&bot vorgestellt, um eine gemeinsame Ausgangslage für die Sicherheitsanalyse zu schaffen.
Die Sicherheitsanalyse der Architektur wird anschließend in mehreren Teilschritten durchgeführt. Zunächst werden die Assets von drag&bot bestimmt. Auf Basis dieser Informationen können die folgenden Schritte fokussierter durchgeführt werden.

DRAG&BOT SECURITY CHECK

EIN QUICK-CHECK DES KOMPETENZZENTRUMS CyberProtect



Auf Basis dieser Assets werden realistische Angreifermodelle definiert und für beide Angreifermodelle mögliche Angriffsvektoren bestimmt. Die Angriffsvektoren werden im Nachgang des Workshops in ihren Grundzügen analysiert und bewertet.

Für die automatisierte Untersuchung der Webanwendung werden drei Web-Security-Scanner verwendet, die sich im Security-Testlabor des Fraunhofer IOSB bereits bewährt haben. Die Untersuchungen werden während des Workshops durchgeführt und im Anschluss an den Workshop ausgewertet.

Nutzen

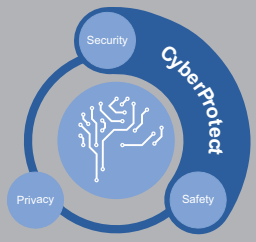
Der konkrete Nutzen des Quick-Checks lässt sich in zwei Bereiche aufteilen. Zum einen können durch die Sicherheitsanalyse der Architektur und durch die Verwendung der Web-Security-Scanner im Kontext einer Webseite für die Roboterprogrammierung neue Erfahrungen gesammelt werden. Diese Erfahrungen werden in den weiteren Aufbau des Security-Testlabors einfließen. Ebenso werden sie einen Einfluss auf die im Security-Testlabor durchgeführten Untersuchungen haben. Zum anderen kann drag&bot durch den Workshop und die anschließende Bewertung einen Überblick über den Zustand der Security der Architektur und der Webanwendung der drag&bot-Software erhalten. Diese Ergebnisse dienen nun als Grundlage für die Weiterentwicklung der drag&bot-Software und tragen so zu deren Security bei.

Projektergebnisse

Die Ergebnisse des Quick-Checks beziehen sich zum einen auf die Bewertung des Zustands der Security der drag&bot-Software und zum anderen auf die Evaluation der Web-Security-Scanner.

Bei der Sicherheitsanalyse der Architektur wurde zwischen einem internen und einem externen Angreifer unterschieden. Für beide Angreifermodelle wurden verschiedene Angriffsvektoren erarbeitet und bewertet. Teil der Bewertung waren auch konkrete Handlungsempfehlungen, um die Angriffsvektoren zu verringern.

Die Evaluation der Web-Security-Scanner zeigte, dass sie Probleme mit der Authentifizierung gegenüber der Webanwendung hatten. Aus diesem Grund konnten nur Teile der Webanwendung überprüft werden. Es hat sich gezeigt, dass diese Probleme nicht domänenspezifisch sind, sondern dass die Authentifizierung bei Web-Security-Scannern im Allgemeinen Optimierungspotenzial bietet.



KOMPETENZZENTRUM CyberProtect

EIN QUICK-CHECK DES KOMPETENZZENTRUMS CyberProtect

FZI
Forschungszentrum Informatik FZI

Fraunhofer IOSB
Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung

Fraunhofer IPA
Fraunhofer-Institut für Produktionstechnik und Automatisierung

Gefördert durch:

Baden-Württemberg
MINISTERIUM FÜR WIRTSCHAFT. ARBEIT UND WOHNUNGSBAU
Ministerium für Wirtschaft, Arbeit und Wohnungsbau

Ansprechpartner
Dr.-Ing. Arne Rönnau
Telefon 0721 9654-228
roennau@fzi.de

Dr.-Ing. Erik Krempel
Telefon 0721 6091-292
erik.krempel@iosb.fraunhofer.de

Dipl.-Wi.-Ing. Ramez Awad
Telefon 0711 970-1844
ramez.awad@ipa.fraunhofer.de

ÜBER DAS KOMPETENZZENTRUM CyberProtect

Das durch das Ministerium für Wirtschaft, Arbeit und Wohnungsbau Baden-Württemberg geförderte Projekt CyberProtect verfolgt im Sinne der Stärkung von Firmen in Baden-Württemberg das Ziel der besseren Absicherung von komplexen Softwaresystemen. Dabei werden alle drei Bereiche von Sicherheit (Security, Safety und Privacy) betrachtet, der Fokus liegt hierbei auf dem Teilgebiet der Security. Im Rahmen des Projektes werden hierfür Methoden entwickelt, um das Verhalten bzw. die Entscheidungen von komplexen Softwaresystemen z.B. von KI-Systemen sichtbar zu machen und somit Aussagen über den Sicherheitszustand der Systeme zu ermöglichen. Über ein weitreichendes Angebot wie Quick-Checks, Schulungen und Open Lab Days werden Firmen in das Projekt einbezogen, um ihnen die Möglichkeit zu bieten, ihre komplexe Software auf Sicherheit untersuchen und ggf. verbessern zu lassen.

Bereit für Ihre Anwendung

Quick-Checks sind ein kostenloses, individuelles Angebot hinsichtlich Sicherheit in der Produktion für Firmen aus Baden-Württemberg. In diesen Quick-Checks werden mit ausgewählten Unternehmen die Themen Safety, Security und Privacy bearbeitet.
Die Ergebnisse aller Quick-Checks werden als Steckbriefe im Webauftritt des Kompetenzzentrums CyberProtect (www.cyberprotect-bw.de) veröffentlicht.