Media Information

asvin develops solution to secure AI data supply chains

Stuttgart, 03.02.2021. Due to the Solarwinds hack, attacks on IT supply chains have become the biggest real threat. Attacks on supply chains are a massive new threat, especially for artificial intelligence (AI). To prevent the next superhit of an attack on AI data supply chains, especially machine learning, Stuttgart-based startup asvin is working with top researchers at the Karlsruhe Institute of Technology (KIT) to develop new approaches to secure data supply chains against attacks.

The scenario is familiar from crime novels: Assassins hijack a party service, disguised as suppliers enter a building unnoticed by security, and wreak havoc among the party guests. Using a similar pattern, cybercriminals recently attacked the software company's customers worldwide in the Solarwinds hack: Attackers built a "backdoor" into an update of Solarwinds' "Orion" networking software without anyone noticing, through which they gained access to some 18,000 corporate and government networks.

Threat to data supply chains

"Since the software supply chain was compromised here at the cybersecurity supplier level, conventional cybersecurity measures such as anti-virus protection or the zero-trust principle can be overcome by attackers," explains asvin CEO Mirko Ross. "Rather, companies should urgently address the risk management of third-party software vendors. This means development, manufacturing, support and maintenance processes of software suppliers must be trustworthy and secure. To realize a secure digital infrastructure in this sense, all stakeholders should develop a cooperative attitude and work together globally."

Seamless protection of technology and data supply chains is essential, above all, to protect artificial intelligence from attacks. After all, if attackers manage to intervene in the data supply chain and corrupt data records, AI can be specifically steered toward false statements. This can have fatal consequences. For example, it is to be feared that an AI-based medical diagnostic procedure will deliver false diagnoses unnoticed due to manipulated training data. Manipulated data in production can lead to quality losses or downtimes. It is also conceivable that attackers could train the AI in a "smart" vehicle to negatively influence the vehicle's behavior.

Innovative chain-of-trust

asvin has developed a secure, robust solution to close security gaps in IoT devices via updates and keep them functional in the long term. The software platform and decentralized infrastructure provided by asvin distribute updates and patches for IoT endpoints. The process is documented and secures the delivery of updates from manipulation through the use of smart contracts. With the "Poison Ivy" research project funded by the Baden-Württemberg Ministry of Economics, asvin is developing a system for securing data supply chains together with top researchers from KIT and tsenso GmbH. In this process, data is linked with a traceable "certificate of trust" from the data source to processing in the cloud and is secured in an unalterable manner via a blockchain system in a traceable manner.
The goal of the innovative asvin Chain-of-Trust is to detect and close backdoors for data-based attacks in AI applications. The solution is intended to fill the gap between conventional offerings and high-end methods and aims to help enable chains of trust in complex distributed architectures of the IoT at moderate cost. The results of the research project are expected by the end of 2021.

asvin GmbH
Schulze-Delitzsch-Str. 16
70565 Stuttgart
T 0711 2204093 0
F 0711 2240493 44

contact@asvin.io
www.asvin.io

@asvin_io

IBAN: DE64 6117 0024 0043 2245 00
BIC: DEUTDEDB611

Sitz Stuttgart
HRB 76700, Amtsgericht Stuttgart

Reprint free of charge, please provide proof (print, scan, link).

About asvin GmbH
Founded in September 2018, the Stuttgart-based start-up company asvin develops a secure open source solution for the software lifecycle in the Internet of Things. The application allows to close security vulnerabilities in IoT and IIoT and thus to manage business processes without risk.

Further information: www.asvin.io

Image

The management of the Stuttgart cybersecurity start-up asvin: CEO Mirko Ross, COO Sven Rahlfs and CTO Rohit Bohara (from left to right), © asvin GmbH

Contact
seidel kommunikation
Brunnengasse 3
73650 Winterbach (Stuttgart)
T: 07181 / 26 29 376
E: medien@seidel-kommunikation.de