Secure Supply Chains for Critical Systems

The aim of the SSCCS project is to ensure the resilience and security of supply chains to cyber attacks. This is done in a structured, interdisciplinary approach based on real use cases and takes into account both highly integrated SCs and such low organizational levels.

Coordinated and lean production processes in the supply chain (SC) require the seamless integration of suppliers and customers on an industrial level - i.e. the production facilities require fast action, not only along the supply chain, but also with regard to order placement, changes in the supply system and the reaction to disruptions in the supply chain. There are different degrees of integration in such supply chains, depending on the size and structure of the partners involved: among equal partners or very open structures with many different customers, the SC often has to be very flexible and no dedicated platforms can be created.

This can lead to very low levels of organisation, which are correspondingly susceptible to social engineering techniques, but also to a proliferation of different communication and management platforms, which are difficult to maintain in terms of technical security. Large companies with high market power, on the other hand, have deeply integrated their component suppliers into their backbone systems. In terms of cyber security, the problem is that small suppliers with low budgets can be used to attack these integrated platforms of the large organisations.

Within the framework of SSCCS, we will therefore investigate the issues of cyber security in SCs and develop appropriate resilience-building measures. In our analyses, we focus on use cases from the real world in order to solve real problems away from purely academic laboratory environments. This concerns both the analysis and modelling of SC systems, as well as security analyses and attacker models.

From the analysis results, we will develop security patterns and templates that can be used in real SCs and directly contribute to improving resilience. In particular, this also includes the preventive establishment of situation images for the detection of attacks and threat potentials specifically for supply chains.

A key feature of the project is the shift away from a purely technical perspective towards the integration of social engineering and the central use of real use cases. The findings of this project are considered to be highly relevant for the economy due to their practical relevance and should also provide important input for existing courses of study as well as those currently being established.

contact details of the project manager:
Mag. Michael Herburger, BA MA
+43 5 0804 33255, michael.herburger@fh-steyr.at

funding programme with financial support from the Austrian research promotion authorities (FFG)

duration (start and end) 01.07.2021 – 30.06.2025

fh/// st.pölten | fh OBERÖSTERREICH | UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA