

Bachelor-/Masterarbeit

LLM-gestützte Sicherheitsbewertung von OT-Anlagen

Ziel

Industrielle Anlagen (Operational Technology, OT) werden zunehmend mit der Unternehmens-IT und dem Internet vernetzt. Dabei treten immer wieder typische Schwachstellen auf: fehlende oder fehlerhafte Netzwerksegmentierung zwischen IT und OT, unverschlüsselte und nicht authentifizierte Industrieprotokolle, ungeschützte Fernwartungszugänge oder veraltete Firmware. Die Sicherheitsbewertung solcher Anlagen ist heute meist aufwendige Handarbeit von Fachleuten.

Ziel dieser Arbeit ist es, die Sicherheitsbewertung von OT-Anlagen zu **automatisieren**. Dazu werden verschiedene Datenquellen **zusammengeführt**: Ergebnisse **aktiver Scans**, **passiv** mitgeschnittene Netzwerkverkehrsdaten sowie weitere Informationen wie Netzwerkpläne oder Asset-Listen. **Large Language Models (LLMs)** sollen diese Daten auswerten, daraus Risiken ableiten und deren Kritikalität bewerten, z. B. angelehnt an das Zonen- und Conduit-Modell der IEC 62443. Das genaue Thema wird in Absprache gefunden. Mögliche Schwerpunkte:

- Erfassung von Assets und Kommunikation durch aktive Scans und passive Analyse
- Zusammenführung von Scan- und Verkehrsdaten mit Netzwerkplänen
- Automatisierte Prüfung der Netzwerksegmentierung gegen ein Zonenmodell
- LLM-gestützte Risikoidentifikation und Kritikalitätsbewertung
- Vergleich der automatisierten Bewertung mit Expertenbewertungen

Anforderungen und Voraussetzungen

- Einarbeitung in OT-Security, Industrieprotokolle und die IEC 62443
- Einordnung bestehender Werkzeuge (z. B. Zeek, Malcolm, Nmap) und Ansätze
- Konzeption und prototypische Implementierung einer LLM-gestützten Bewertung
- Evaluation an Testanlagen bzw. Netzwerkmitschnitten
- Programmierkenntnisse (z. B. Python), Netzwerkgrundlagen, Interesse an OT-Sicherheit

Ansprechpartner

Prof. Dr. Lothar Braun | ✉ lothar.braun@tha.de | ☎ +49 8215586-3378

THA_innos

Das Institut für innovative Sicherheit (THA_innos) bietet eine Vielzahl von Abschluss- und Projektarbeiten im Themenfeld der Cyber Security an. Unser Team unterstützt Studierende dabei mit Know-How und Praxiserfahrung und ist zudem offen für eigene Themenvorschläge. Durch die enge Zusammenarbeit mit der Forschungsgruppe vor Ort im MRM-Gebäude lernen Studierende sowohl das Institutsleben, als auch die aktuelle Forschung von THA_innos kennen.

Weitere Informationen auch unter <https://innos.tha.de>