[TT.-Prof. Christian Wressnegger // **Intelligente Systemsicherheit**]

Christian Wressnegger ist Leiter des Lehrstuhls für Intelligente Systemsicherheit am KASTEL-Institut. Er und sein Team forschen an der Schnittstelle des maschinellen Lernens und der IT-Sicherheit. Dabei beschäftigten sie sich mit dem Einsatz von KI zum Schutz von Computersystemen aber auch mit der Sicherheit und Erklärbarkeit von KI selbst.

Bereits in seinem Masterstudium an der TU Graz hat er IT-Sicherheit und KI als Studienschwerpunkte verfolgt. Nach mehreren Jahren in der IT-Sicherheitsindustrie in Wien und Berlin, wechselte er zur Promotion in die akademische Welt.

Im Jahr 2018 promovierte Christian Wressnegger an der TU Braunschweig zum Thema „Effizientes Maschinelles Lernen für die Angriffserkennung" ehe er dem Ruf ans KIT folgte. Dort ist er seit 2019 als Junior-Professor tätig und baut das Forschungsprofil des KIT in Richtung Cybersicherheit von KI aus.

Er ist PI der „KASTEL Security Research Labs" und Co-Sprecher des Produktionslabors des HGF-Topics „Engineering Secure Systems". Des Weiteren engagiert er sich als Sprecher der „KIT Graduate School Cyber Security" in der Förderung des wissenschaftlichen Nachwuchs. International ist er als Gutachter für höchstrangige Konferenzen und Journale tätig.

Für seine Arbeit erhielt er ua. den Distinguished Paper Award des „USENIX Security Symposiums" und stand im Finale des CAST/GI Dissertationspreises für IT-Sicherheit. In der Lehre wurde er sowohl am KIT als auch an der TU Braunschweig für die beste Vorlesung ausgezeichnet.

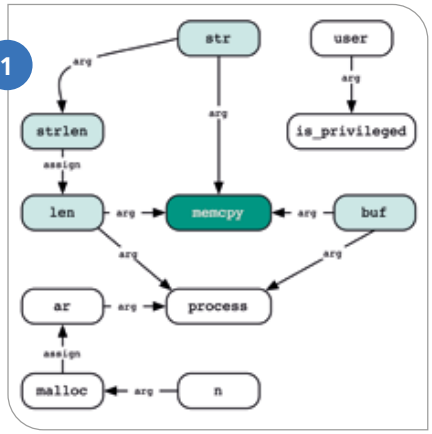
// Überblick und Allgemeines

Die Forschung der Gruppe „Intelligente Systemsicherheit" am KASTEL-Institut für Informationssicherheit und Verlässlichkeit unterteilt sich in drei Bereiche:

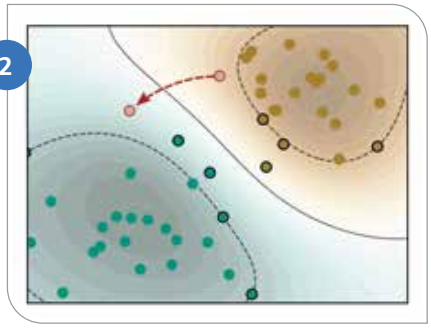
1. MLSEC
Zum einen beschäftigen wir uns mit dem Einsatz von maschinellem Lernen in der Computersicherheit. Hier untersuchen wir wie man mit Hilfe von lernenden Systemen, zum Beispiel, Schwachstellen in Software findet oder Schadcode (Malware) identifiziert und analysiert. Auch die selbst-lernende Angriffserkennung auf Netzwerkebene ist ein zentrales Thema. (Abb. 1)

2. SECML
Zum anderen forschen wir an der Sicherheit von maschinellem Lernen. Also wie lernende Systeme über Manipulationen der Eingabedaten oder des KI-Modells angegriffen und wie diese Angriffe abgewehrt werden können. Solche Angriffe sind sowohl für klassische Anwendungen wie das autonome Fahren oder die Robotik relevant, als auch für das Umgehen von lernenden Angriffserkennungssystemen wie sie oben erwähnt wurden. (Abb. 2)

3. SEC
Zusätzlich setzen wir uns auch leidenschaftlich gerne mit praktischer IT-Sicherheit auseinander die ohne maschinelles



1



2

Lernen auskommt (SEC). Zum Beispiel, führen wir Internet-weite Messungen zu web-basierter Sicherheit durch, untersuchen die Effektivität von Aimbots für Onlinespiele oder nutzen Laser zur verstecken Kommunikation mit Schadcode über die Grenzen von abgeschotteten Computersystemen hinweg. (Abb. 3)

// Projekte und Erfolge

Aktuell sind wir in unterschiedlichen Forschungsprojekten zu IT-Sicherheit und der Sicherheit von lernenden Systemen beteiligt. Zum Beispiel forschen wir zur Robustheit von maschinellem Lernen in IoT-Systemen oder wie Datenlieferketten von KI-basierten Anwendungen effektiv abgesichert werden können. Hier leistet die IntelliSec Forschungsgruppe wichtige Beiträge zur Forschung für die sie regelmäßig ausgezeichnet wird.

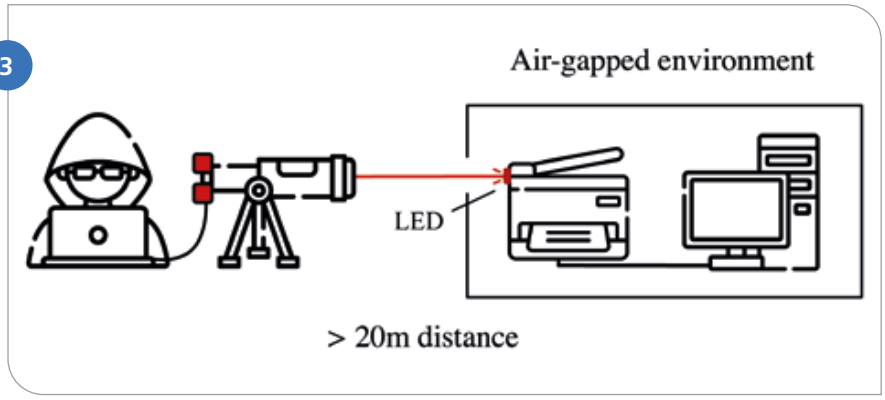
// Ausgewählte Publikationen

D. Arp et al. „Dos and Don'ts of Machine Learning in Computer Security"
USENIX Security Symposium 2022
Distinguished Paper Award

Q. Zhao et al. „Non-Uniform Adversarially Robust Pruning"
International Conference on Automated Machine Learning (AutoML) 2022

N. Demir et al., „Reproducibility and Replicability of Web Measurement Studies"
ACM Web Conference (WWW) 2022
Best Paper Award Runner-Up

N. Kühnapfel et al. „LaserShark: Establishing Fast, Bidirectional Communication into Air-Gapped Systems"
Annual Computer Security Applications Conference (ACSAC) 2021



3

// Mitarbeiterinnen und Mitarbeiter

Verwaltungspersonal
Hildegard Sauer
Dr. Philipp Scherzer

Wissenschaftliches Personal
Nurullah Demir
Achyut Hegde
Yilin Ji
Daniel Kaestner
Qi Lei
Max Noppel
Gustavo Sánchez
Qi Zhao

// Website

intellisec.de