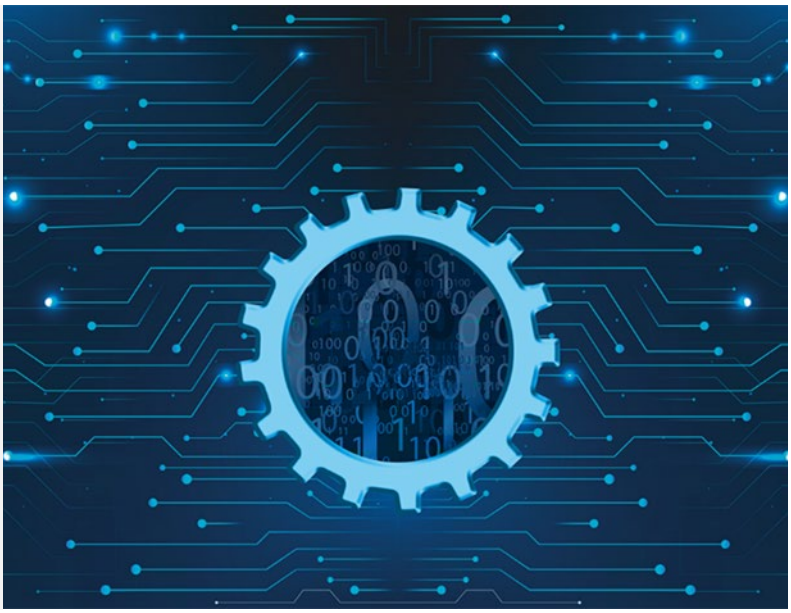
DEPS - https://deps.scch.at
Dependable Production Environments with Software Security

Host: SCCH, www.scch.at

Programme: COMET – Competence Centers for Excellent Technologies

Programme line: COMET-Module



R^2C: REFLECTIVE AND REACTIVE CAMOUFLAGE

MITIGATING ADDRESS-OBLIVIOUS CODE REUSE ATTACKS

Address-Oblivious Code Reuse Attacks (AOCR Attacks, for short), discovered in 2017, are among the most dangerous code reuse attacks, since no mitigation without prohibitive performance penalties was known.

In the realm of DEPS, we could successfully demonstrate a novel defense, which – surprisingly – leveraged principles underlying software diversity. This surprise was primarily due to the original AOCR authors claiming that their attack demonstrates fundamental limits to software diversity. Our research on

R^2C shows that AOCR does not identify fundamental limitations to diversification, but shows that exclusive focus on code diversification is a *dead end*.

By exploring novel, efficient data diversification techniques, and combining them with highly efficient code diversification techniques, R^2C invalidates core assumptions underlying the AOCR attack. In addition, R^2C's code diversification technique, called booby-trapped return addresses (BTRAs), renders another high-profile attack, called Position-Independent Return-Oriented Programming (PIROP) impotent in many cases.

The resulting paper was accepted for publication in one of Europe's top tier computer science conferences, namely the 18th European Conference on Com-

Federal Ministry
Republic of Austria
Climate Action, Environment, Energy, Mobility, Innovation and Technology

Federal Ministry
Republic of Austria
Labour and Economy

FFG
Promoting Innovation.
Austrian Research Promotion Agency
Sensengasse 1, A-1090 Vienna
P +43 (0) 5 77 55 - 0
office@ffg.at
www.ffg.at

puter Systems (EuroSys), which took place in Rome in May of 2023.

Reference

Felix Berlakovich and Stefan Brunthaler. $\boldsymbol{R^2C}$*: AOCR-Resilient Diversity with Reactive and Reflective Camouflage*. In Proceedings of the Eighteenth European Conference on Computer Systems, EuroSys, May 8th – 12th 2023, Rome, Italy. Pages 488 – 504.

Contact:
Juliana Küster Filipe Bowles, DEPS Coordinator, SCCH, T +43 50 343 900, juliana.bowles@scch.at

Consortium: