EPFL-Inria
INTERNATIONAL LAB

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Inria
INVENTEURS DU MONDE NUMÉRIQUE

Workshop EPFL-Inria
January 30 and 31, 2019, Lausanne

***Mathias Payer*, EPFL**

Title: « Memory Corruption: Exploit-guided Software Testing »

Abstract:
Memory corruption plagues systems since the dawn of computing. Attacks have evolved alongside the development of ever stronger defenses resulting in an eternal war in memory. With the rise of mitigations like stack cookies, ASLR, and DEP, exploits now rely on code reuse. Control-Flow Integrity (CFI), an upcoming mitigation, further restricts the control flow of the application, limiting the power of attacks to whatever code is reachable by the original application. Unfortunately, even the strongest form of CFI leaves some opportunity to the attacker that can be exploited.
We tackle the security problem of over-privileged applications along two dimensions: attack surface reduction and adversarial program testing. First, we reduce the reachable code to the minimal required functionality. Pruning unused functionality reduces the attack surface, limiting the attacker to the required functionality (and program paths that are likely better tested), increases the precision for CFI by minimizing the target sets, and potentially improving the performance through novel opportunities for inlining and optimization. Second, we develop fuzzing techniques that follow an adversarial approach, focusing on the exposed attack surface and exploring reachable vulnerabilities before an attacker. Through transformational fuzzing we extract underexplored program components and fine-tune the program under test to particular use cases. Due to rigid performance constraints, mitigations will never be complete. This situation calls for program testing techniques that discover reachable vulnerabilities before the attacker. Developers are at an inherent advantage: they have access to the source code, know the environment, and have specialized knowledge about the functionality constraints.

Bio:
Mathias Payer is a security researcher and an assistant professor at the EPFL school of computer and communication sciences (IC), leading the HexHive group.
His research focuses on protecting applications in the presence of vulnerabilities, with a focus on memory corruption and type violations. He is interested in software security, system security, binary exploitation, effective mitigations, fault isolation/privilege separation, strong sanitization, and software testing (fuzzing) using a combination of binary analysis and compiler-based techniques.
After 4 years at Purdue university, he joined EPFL in 2018. Before joining Purdue in 2014 he spent two years as PostDoc in Dawn Song's BitBlaze group at UC Berkeley. He graduated from ETH Zurich with a Dr. sc. ETH in 2012, focusing on low-level binary translation and security. He analyzed different exploit techniques and wondered how we can enforce integrity for a subset of data (e.g., code pointers). All prototype implementations are open-source. In 2018, he co-founded the EPFL polygl0t CTF team and in 2014, he founded the Purdue b01lers CTF team.