UNIVERSITÀ
DI PAVIA

Ph.D. Program in Electronics, Computer Science and Electrical Engineering

SEMINAR

Vulnerability Discovery: SAST and Fuzz Testing

Giacomo Benedetti

IMATI – CNR, Genova

October 15, 2025 - h. 14:30
EF2 Classroom
Department of Electrical, Computer and Biomedical Engineering

Abstract: Software bugs have been a security concern for a long time. In fact, threat actors can use them to subvert the expected flow of execution, resulting in economic, reputational, and social damages. Effective testing techniques have been developed to counter the emergence of bugs by enabling developers to promptly identify and resolve them. *Static Application Security Testing* (SAST) and *fuzz testing* have proven to be two of the most effective ways to discover weaknesses in software and potential vulnerabilities. The first makes use of well-established program analysis methodologies, such as taint analysis, while the second exploits the generation of inputs to trigger bugs at runtime in the program control flow. Nowadays, most of the vulnerabilities in software are found through *grey-box fuzz testing*, making this specific type of testing one of the "hot topics" in information security research.

This talk introduces SAST and fuzz testing approaches to discover security bugs or weaknesses. Emphasis will be placed on fuzz testing, its operation, and its applications. The talk also provides a real example of how to discover a bug in a real application via the AFL++ fuzzer.

Bio: Giacomo Benedetti is a postdoctoral researcher at the Institute for Applied Mathematics and Information Technology (IMATI) of the National Research Council of Italy (CNR) and a visiting researcher at the North Carolina State University. He holds a M. Sc. degree in Computer Science and a Ph.D. degree in Security, Risk, and Vulnerabilities, both from the University of Genoa. He is involved in several research projects on security of container ecosystems and the use of information hiding applied to Android applications. His research interests include CI/CD automation security, supply chain modeling, dependency management, and reproducible builds.

Organizer
Prof. M.C. Calzarossa

Ph.D. Coordinator
Prof. Ilaria Cristiani

For more information: mcc@unipv.it