Security Verification and testing

A.Y. 2024/25

Special Projects Proposals (Prof. Sisto)

1) Development of a Proof of Concept to exploit a potential vulnerability found by Proverif

Proverif has been used to model and analyze some Over-The-Air (OTA) update protocols. In some cases, Proverif found that the analyzed protocol may be subject to an attack. The purpose of the project is to a) study one of such protocols with its documentation, and the already performed Proverif analysis, confirming the validity of the analysis and of the found attack (or adjusting the analysis as necessary); b) based on the attack reconstructed by Proverif, develop a proof-of-concept exploit of the protocol that showcases the attack on one of the available implementations of the protocol.

2) Development of a Proverif Challenge

The work consists of developing a Proverif Challenge like the one proposed this year. The work involves:

a) identifying a real (but simple) protocol with an existing implementation which is subject to a flaw like the ones Proverif can detect (e.g., replay or MITM attacks). It can even be a non-flawed protocol that is modified to introduce a flaw.

b) Create a Proverif model of the protocol, with its properties. One of the properties should not hold when verified by Proverif.

c) Build the challenge, including an introductory text, and the protocol implementation modified with the introduction of the flag.

3) Exploitability analysis for eBPF C code

eBPF is a technology that enables the extension of OS kernel functionality without requiring kernel recompilation, by allowing the integration of user-written code (generally written in C) into the kernel, while providing security properties such as isolation and protection through its built-in bytecode verifier (https://ebpf.io/). A previous study, based on injecting C code weaknesses into eBPF code, identified some instances of eBPF C programs that are potentially affected by security vulnerabilities not detected by the bytecode verifier. The proposed work consists of studying such programs to discern whether their weaknesses are real security vulnerabilities or not. This will be done by trying to develop a proof-of-concept exploit based on the C instance code.

A similar work is also proposed with reference to some eBPF-related CVEs for which no exploit is publicly known. In this case, the goal is to develop working exploits for such vulnerabilities, using the technical expertise acquired during this course and the concrete information and techniques extracted from existing public exploits.

How to apply

Send an email to riccardo.sisto@polito.it specifying the projects you would like to do, sorted by preference, and attach your CV, which must include the exams you passed with their marks, and any other useful information (e.g., previous involvement in challenges).