Talk abstracts of the
2022 Workshop on Security Frameworks
"Security Testing"

Go around and sell the ultimate, comprehensive yet readily-applicable, Security Testing methodology and you'll see your bank account leaven to heaven (what a rhyme!) as well as some Turing Award descend on you, for good measure. The need to test that cybersecurity is practically working couldn't be more pervasive this minute. For sure, you will want to protect your modern car from any form of intrusion and will want to protect your Alexa from someone else's issuance of voice commands in your stead. Protection benefits from an ontological representation of the applicable measures and improves if it is made somewhat intelligent (yes, Machine Learning yet again!). Here applies OWASP's Web Security Testing Guide v4.2 page 40, which prescribes testing each and every phase of your software development effort. Testing calls for fuzzing (not a rhyme this time 'round!) more and more often today, mimicking that sort of juvenile attitude at thrusting a Hot Wheels car bullet-fast to the wall to see if the die cast holds together. Funny, eh?! But valid too, to spot software vulnerabilities especially, and itself challenging. We shall see that a challenge is to fuzz systems that make state, and another one is to fuzz systems that fork over child processes, open challenges in fact, so that the hunt for the golden approach continues. Still, we know from kindergarten that cybersecurity threats retain some likelihood, yet subjectivity hinders the understanding of that likelihood. Get your own flavour of all the above by attending this year's event – yes, again in person.

Ivan Mercanti, Università di Perugia, Italy: *"Can blockchain satisfy all e-voting system properties?"*.

Abstract. An E-voting system must respect many properties to be safe and usable. We present all these properties and discuss when and why they should be respected. In particular, we analyze these properties in three different e-voting solutions based on blockchain. The first one uses the Bitcoin blockchain and Kerberos authentication. The second one is based on a permissioned blockchain called Multichain. The last one uses Ethereum and tornado cash, a protocol to anonymize crypto.

Gianpietro Castiglione, Università di Catania, Italy: *"Towards ontology-inspired offensive security"*.

Abstract. This research aims to automatize the compliance verification activity with security directives on ICT systems, in order to consolidate compliance as a high-level instrument to regulate defence against cyber-criminal activities. Security directives and security standards are promulgated by national and international institutions that want to stabilize and, sometimes, impose some best-practice to follow. Thanks to the ontological approach, measures (both of directives and of systems) can be modelled and subjected to logical derivations together. The research argues that the outcome can be used by additional instruments, such as machine learning, towards exploitability prediction as well as exploit generation, which are crucial through security testing by offensive activities.

Mario Raciti, Scuola IMT Alti Studi Lucca, Italy: *"Risk assessement with AILA: Automated and Intelligent Likelihood Assignment"*.

Abstract. The Automated and Intelligent Likelihood Assignment (AILA) methodology recognises the widespread application of risk assessment in ICT and aims at reducing the influence of human subjectivity and distraction. AILA facilitates the identification of entities from a given policy and then the assignment of likelihood values to threats for assets. It adopts Natural Language Processing for summarisation and entity recognition, it tailors fully-supervised Machine Learning over policy documents and then leverages an existing tool supporting risk assessment towards a more objective likelihood assignment. Demonstration comes over three real-world case studies from the automotive domain, culminating with risk assessment exercises over the privacy policies of Toyota, Mercedes and

Tesla. In comparison with a risk assessment tool by ENISA, AILA is dramatically more automated. The executable components of AILA, the AILA Entity Extractor and the AILA Classifier are open source.

Sergio Esposito, Royal Holloway University of London, UK: *"Protecting against Self-Issued Voice Commands"*.

Abstract. Self-issued voice commands leverage a voice-controllable device's internal speaker to issue a malicious voice command to the device itself. We propose a practical countermeasure against this kind of attack by training a Siamese Neural Network to recognise the differences between what is being played and what is being recorded by the voice-controllable device. In fact, these audios are similar in case of voice command self-issue attacks and different in case of legitimate commands. Our solution correctly classifies commands in the benign (real-user) and malign (self-issued) categories 97% of the times on average.

Marcello Maugeri, Università di Catania, Italy: *"Fork-Awareness property of Coverage-Guided Fuzzers"*.

Abstract. Fuzz testing (or fuzzing) is an effective technique used to find security vulnerabilities. It consists of feeding a System-Under-Test (SUT) with malformed inputs, waiting for weird system behaviours. One of the most popular approaches is coverage-based. It relies on the instrumentation of the system to generate inputs able to cover as much code as possible. The success of this technique is due to its usability since research aims at approaches that do not require (or only partially require) human interactions. Despite the efforts, devising a fully-automated fuzzer still seems to be a challenging task. Target systems may be very complex; they may integrate cryptographic primitives, compute and verify check-sums and employ forks to enhance the system security, achieve better performances or manage different connections at the same time. This talk introduces the fork-awareness property to express the fuzzer ability to manage systems using forks. This property highlights how current fuzzers are ineffective against systems using forks.

Davide Micale, Università di Catania, Italy: *"CAHOOT: a Context-Aware veHicular intrusiOn detectiOn sysTem"*.

Abstract. Software in modern vehicles is becoming increasingly complex and subject to vulnerabilities that an intruder can exploit to alter the functionality of vehicles. To this purpose, we introduce CAHOOT, a novel context-aware Intrusion Detection System (IDS) capable of detecting potential intrusions in both human and autonomous driving modes. In CAHOOT, context information consists of data collected at run-time by vehicle's sensors and engine. Such information is used to determine drivers' habits and information related to the environment, like traffic conditions. We create and use a dataset by using a customised version of the MetaDrive simulator capable of collecting both human and AI driving data. Then we simulate several types of intrusions while driving: denial of service, spoofing and replay attacks. As a final step, we use the generated dataset to evaluate the CAHOOT algorithm by using several machine learning methods. The results show that CAHOOT is extremely reliable in detecting intrusions.