Talk abstracts of the

2023 Workshop on Security Frameworks

“Intelligence rests on Knowledge”

Intelligence. Its artificial version (if that makes sense) has been pivotal to laymen’s pub chit-chatting throughout this year, leaving its own inventors bewildered. Its human, elder version ought to be best understood but, when we look at the number of wars worldwide, we may wonder if it is so common after all – no offence intended! Knowledge. This forms the foundational core of intelligence, hence may turn out to be the fundamental deficiency every time intelligence seems to falter, be it human or artificial. If you bake a cake that turns out to be rubbish, maybe the reason is not that you are not sufficiently intelligent but, rather, that you did not know a good recipe or how to follow one. Likewise, if your favourite GPT appears to make mistakes, perhaps it was not trained with the relevant information. This duality is this year’s workshop’s workbench. We must acknowledge that data tenancy is an issue even within the intelligence of the semantic web, pretty much as we need to be aware that stateful fuzzing can be made much cleverer than it has long been. Similarly, digital forensics must be scrutinized with the same care typically devoted to cryptographic protocols, in order to pinpoint security as well as privacy properties from the perspectives of both defendants and claimants. Moreover, understanding the entire kill chain is essential to attacking and defending the increasingly popular voice personal assistants, as well as sharpening the tools to predict vulnerabilities and how to exploit them in general. First comes knowledge, I must say. Intelligence follows on top, and with all that, we shall be able to work wonders!

Daniele Francesco Santamaria, Assistant Professor, University of Catania, Italy: *“Securing data in the Semantic Web: the tenancy matter”*

The Semantic Web was conceived with security in mind by defining with three stack layers, namely, Cryptography, Signature and Trust. Even though Semantic Web technologies are nowadays present in industrial realities, security on the Semantic Web just exists on paper. For instance, data tenancy, a family of mechanisms that aim at isolating data and enabling data compliance with requirements, is underrated in such a context. The importance of data tenancy is well-known: just consider a web platform hosting governance data of users. It includes medical data together with car assurance, income, estates, and tax information. One desire is that medical information is accessible only by medical services, car assurance by assurance companies, and so on. In this talk we explore the matter of data tenancy in the Semantic Web, analyzing strategies and future perspectives to deal with it and, in a broader sense, with security in the Semantic Web.

Gianpietro Castiglione, PhD student at University of Catania, Italy: “*Leveraging Compliance Verification towards Vulnerability Prediction.*”

The rapid-expanding landscape of cyber threats have obliged governments and worldwide organisations to respond with legislation aimed at bolstering digital defences for their citizens and critical infrastructures. This has implicated them in the intricate process of compliance verification. Concurrently, critical infrastructures face the potential impact of vulnerabilities that may result in dangerous exploits.

Findings from compliance verification step can guide the identification of particular vulnerabilities tailored to the missing security measures.

Cristian Daniele, PhD student at Radboud University, Nijmegen, Netherlands*: "AFL*: a simple and effective stateful fuzzer"*

Fuzzing is a widely used testing technique that aims to find vulnerabilities in the code. Although (stateless) fuzzing has been widely explored, stateless fuzzing is still relatively new and thus gives room for further research and investigation. In this talk, we will introduce the simple (but effective) idea behind fuzzing, and then dive into the challenges of stateful fuzzing. Finally, we will introduce AFL*, a novel stateful fuzzer that outperforms the state-of-the-art fuzzer performance by 3 orders of magnitude while still achieving better state and code coverage.

Mario Raciti, Scuola IMT Alti Studi Lucca - Università di Catania, Italy: *"Behind the Screens: An MSC-Model of Digital Forensics in Crime Investigation"*.

Criminal investigations are inherently complex as they typically involve interactions among various actors like investigators, prosecutors, and defendants. The pervasive integration of technology in daily life adds an extra layer of complexity, especially in crimes that involve a digital element. The establishment of digital forensics as a foundational discipline for extracting digital evidence further exacerbates the complex nature of criminal investigations, leading to the proliferation of multiple scenarios. Recognising the need to structure standard operating procedures for the handling of digital evidence, the representation of digital forensics as a protocol emerges as a valuable opportunity to identify security and privacy threats. In this presentation, we delineate the protocols that compose digital forensics within a criminal case, formalise them as message sequence charts (MSC) and identify their salient cybersecurity and privacy properties.

Sergio Esposito, Doctor of Philosophy, Royal Holloway University of London, UK: *"The VOCODES Kill Chain for Voice Controllable Devices"*

We introduce a formalisation of attacks on Voice Controllable Devices (VCDs), focusing specifically on attacks leveraging the voice command self-issue. The presentation starts from the seminal Lockheed Martin kill chain, which is used to derive a tailored kill chain with the necessary steps to perform self-activation attacks. Our new kill chain, termed the VOice COntrollable DEvice Self-issue (VOCODES) kill chain, is relevant to assess both ongoing and past attacks, enhancing analysis activities of both ethical adversaries and of defenders. To demonstrate VOCODES in practice, we use it to analyse a popular self-issue attack against Amazon Echo devices, that is, the AvA attack. We show that the VOCODES kill chain succeeds in the full description of the attack and all its nuances. Moreover, it is effective to quickly map out the attacker's malicious activities over specific attack steps, thereby favouring their interpretation. Finally, we show that, even if VOCODES is derived from the Lockheed Martin kill chain, VOCODES addresses some of the drawbacks of the seminal kill chain which have been pointed out over the years.