Talk abstracts of the
2021 Workshop on Security Frameworks
“Cybersecurity needs abstract thinking”

Theory and practice, same old fellas. Can your skillset ferry you back and forth the fen between them? Why bother?! You’d better do, for the same reasons why a construction engineer ought to try out working as a builder, and a top notch builder ought to get to grips with some engineering principles. Understand the general intricacies then try ‘em out then go back to understanding them and continue the cycle indefinitely. This is the message arising form this year’s edition of the Workshop on Security Frameworks. Creating Digital Twins is fun and trendy, but the security and people’s privacy implications are only half apparent, so you need some abstraction away from the functional goal. Wherever (and that’s everywhere!) people liaise with technology, ceremonies are born whose security and privacy must be thoroughly understood. And while you practice with clever injections of code in a (web) form, abstracting the general language will deepen your eyesight once again. Even the automotive area stands at a difficult juncture, between safety and security, a very practical one indeed, and is facing it by representing relevant scenarios in an abstract language. So, rest assured: you need abstract thinking for mastering cybersecurity.

Vlado Stankovski, University of Ljubljana, Slovenia: *“Privacy and security issues in the context of Digital Twins”.*
Abstract. Digital Twins are growingly seen as a representation of context in real time. The DECENTER Fog Computing and Brokerage platform (www.decenter-project.eu) employs various Artificial Intelligence (AI) methods that run on video streams in order to generate a Knowledge Base that can be used to interpret the context in the real time. When AI models are used in order to generate information in real time, it may give rise to a number of real-world problems. The amount of the generated context can be vast, and it may contain privacy and security related information that must be handled according with existing regulations, such as the European GDPR. In this presentation, we shall pinpoint the issues in this context and provide some approaches for addressing them, such as the use of formal methods.

Diego Sempreboni, King's College London, United Kingdom: *“X-Men: A Mutation-Based Approach for the Formal Analysis of Security Ceremonies”.*
Abstract. There is an increasing number of cyber-systems (e.g., payment, transportation, voting, critical-infrastructure systems) whose security depends intrinsically on human users. A security ceremony expands a security protocol with everything that is considered out-of-band to it, including, in particular, the mistakes that human users might make when participating actively in the security ceremony. In this paper, we introduce a novel approach for the formal analysis of security ceremonies. Our approach defines mutation rules that model possible behaviors of a human user, and automatically generates mutations in the behavior of the other agents of the ceremony to match the human-induced mutations. This allows for the analysis of the original ceremony specification and its possible mutations, which may include the way in which the ceremony has actually been implemented. To automate our approach, we have developed the tool X-Men, which is a prototype that extends Tamarin, one of the most common tools for the automatic unbounded verification of security protocols. As a proof of concept, we have applied our approach to two real-life case studies, uncovering a number of concrete vulnerabilities.

Erik Poll, Radboud University Nijmegen, Netherlands: *“Some Security by Construction thanks to LangSec”.*
Abstract. Software plays a central role in cybersecurity: systems can be 'hacked' because they contain software. These security problems nearly always involve insecure input handling. This talk will present some of the insights and ideas from the LangSec paradigm to tackle the root causes in insecure input handling. These ideas revolve around input languages and the parsing of input languages. After

all, most security problems are caused by 1) the variety, complexity, and poor specification of many input languages, which e.g. includes file formats, data encodings, and network protocols, and 2) the buggy or unintended parsing of these languages and formats.

Fabrizio Tronci, Huawei, Italy: *“Functional Safety and Cyber Security synergy in complex automotive systems”*.
Abstract. Connected cars and related infrastructures are more and more complex and include safety related functionalities. Connectivity provides the opportunity for new and improved services but, at the same time, increases the risks of injuries caused by cyber security attacks. The talk addresses the main common points between cyber security and functional safety in the automotive environment and why it is important to create an integrated process for software product development. During the talk, the two main standards for functional safety and cyber security for automotive will be introduced: ISO 26262 and ISO 21434.