Talk abstracts of the
2020 Workshop on Security Frameworks
“Cybersecuritytians exceed nerds”

Isabella Corradini, Themis, Italy: *“Building an effective Cybersecurity Culture: the role of human factors”.*
Abstract. Over the last few years, cybersecurity has become one of the most important issues for organizations across all sectors. Institutions and companies are working to improve their capabilities to strengthen their cyber resilience, but results are far from being effective. Building a strong Cybersecurity Culture, first and foremost investing in awareness and education, is the best response to face the issue. In fact, many cyberattacks successfully exploit human weaknesses, such as in the case of social engineering attacks. Focusing on the human factor means understanding people’s vulnerabilities but also their strengths, going beyond the stereotype according to which human beings are the weakest link in the security chain. Given the scenario, it is clear that a multidisciplinary approach is needed to better manage cybersecurity.

Tom Chothia, University of Birmingham, UK: *“EMV bank card relay attacks and distance bounding protocols”.*
Abstract. Relay attackers can forward messages between a contactless Europay, Mastercard, and Visa (EMV) card and a shop reader, making it possible to wirelessly pickpocket money. In this talk I'll discuss how EMV cards can be protected using distance-bounding protocols, in which ther eader will measure round trip times of message-exchanges, and reject replies that take longer than expected (which suggests they have been relayed). I'll show how these protocols can be formally modelled and verified, and discuss a solution that has been added to the Mastercard EMV specification. As with most protocols in this area, Mastercard's protocol requires the reader to enforce the distance bounding checks,however it is exactly the reader that stands to benefit from relayed payments, so this creates a conflict of interest. I will propose a novel proximity-checking protocol that uses a trusted platform module (TPM) that ensures that the reader performs the time measurements correctly, in a way that can be verified by the bank.

Francesco Capparelli, ICT Cyber Consulting, Italy: *“Do we trust in an artificialised ICT?”.*
Abstract. With the recent outburst in the development of artificial intelligence technologies, the legal tools to safeguard individuals’ personal data and, more in general, increase peoples' confidence in the use of Information and Communication Technologies, struggle to cope. In particular, the novel concept of Digital Twin Machine Learning makes it very complex to understand the legitimacy of data processing through the ecosystems that will govern our lives in the coming decades, especially due to the ever increasing capillarity of the Internet of Everything. It is therefore necessary to begin a structured assessment on how our legal tools complement and intertwine with the technical ones and on how we should start twisting them to increase the assistance they may offer to tomorrow’s end users.

Stefania Catacchio, General Electrics, France: *“Discover your strengths through the colours of your personality and the beauty of diversity”.*
Abstract. It is well understood that protecting a company from cyber-attacks is crucial. Putting cyber security measures in place and maintaining them requires partitipation from many different actors, including sysadmins, nerds and employees at all levels. However, the inherent differences between those individuals may well have a negative impact on cybersecurity. This raises a number of general and fundamental questions such as the following ones. How impactful could be the role of the different personalities forming a company, a team or a project on the achievement of a strategic common goal? Can personalities work together successfully only if they are similar? This talk will draw from practical

experience to illustrate how large companies leverage the DISC personality and behavioral assessment approach to increase efficient interaction and success rate in a team.

Sasa Radomirovic, Heriot-Watt University, UK: *“Secure Communication with Humans”*.
Abstract. Many security protocols involve humans, not machines, as endpoints. The differences are critical: humans are not only computationally weaker than machines, they are naive, gullible, and stressed. I will present a formal theory accounting for human errors in security protocols. The theory allows to model untrained or trained humans. Untrained humans have no knowledge about the protocol and may deviate arbitrarily from its specification. Trained humans generally follow rules or follow the protocol, but may make mistakes such as omitting a critical security check. The model allows to derive what general rules have to be known by a human such that desired security properties are provided by a protocol. Joint work with David Basin and Lara Schmid.