PREFACE

DAMOCLES: First International Workshop on Detection And Mitigation Of Cyber attacks that exploit human vuLnerabilitiES

The pervasive nature of technology in our daily lives has significantly enhanced our world, yet it has also left us vulnerable to cyber threats. By 2025, global cybercrime costs are projected to soar to $10.5 trillion annually from $3 trillion in 2015. In this landscape, cyber attacks are increasingly recognized as stemming not only from technological shortcomings but also from human factors overlooked in the design of interactive systems. Reports from cybersecurity leaders like IBM and Verizon reveal that as much as 95% of cyber attacks are attributable to human errors, such as inadvertently opening phishing websites, downloading malware-infected attachments, failing to update software, and using weak passwords. The challenges were exacerbated during the pandemic, which exploited users' fear, stress, and distraction while working remotely. Italian public administrations (PAs) are particularly targeted by cyber criminals, facing a digitalization deficit underscored by the European Union's Digital Economy and Society Index (DESI). This disparity is especially notable in cybersecurity, where Italian PAs invest a mere 3% of their budgets significantly less than the private sector's 15% to 20% allocation. Small and mid-sized government agencies, including schools, municipalities, and agencies, struggle daily with limited financial and human resources that hinder their ability to address cybersecurity concerns internally or through external consultation.

The imminent intensification of Italy's PA digitalization program, as promoted by the National Recovery and Resilience Plan (PNRR), foresees an exponential increase in cyber threats. The PNRR aims to leverage digital channels like websites and apps to enhance citizen access to information and services. However, without a comprehensive cybersecurity strategy centered on users, the sensitive data and services managed by PAs remain at considerable risk.

The DAMOCLES project enhances the digital defense of Italian public administrations (PAs) against human error-related security incidents. It uses a framework with two components: Human Vulnerability Assessment (HVA) and Human Vulnerability Mitigation (HVM). HVA identifies risky behaviors through prevention (questionnaires), detection (simulated cyber-attacks), and simulation (Digital Twins). HVM then uses these insights to create customized training programs using various methods like podcasts and role-playing games. DAMOCLES will be tailored to specific PAs through user-friendly approaches, ensuring easy adoption and effectiveness in diverse environments.

To shed light on these critical issues, we organized the first edition of the DAMOCLES workshop in conjunction with the 17th International Conference on Advanced Visual Interfaces (AVI 2024), with the aim of opening the discussion to all interested researchers and practitioners.

Twelve papers were originally submitted to the workshop. Eight of them, published in these proceedings, were presented, in presence, and led to a fruitful discussion which involved the authors and other attendees as well.
Several topics were addressed.

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

The workshop showcased a wide range of topics and research inquiries within the cybersecurity field, exemplified by the 8 quality submissions from esteemed universities across Italy, featuring the participation of more than 26 researchers. Discussions explored diverse aspects of cybersecurity, tackling significant challenges and presenting innovative methodologies. Areas of focus included strategies to reduce human errors and cognitive biases to enhance human-AI collaboration in cybersecurity, the utilization of white-box techniques such as statistical model checking and process mining for validating threat models, and the development of effective incident reporting systems to unlock insights from security incidents. Additionally, submissions examined the influence of human factors on simulated phishing campaigns and the application of machine learning techniques to benchmark fake account datasets. Other topics investigated methods to combat vishing attacks through real-time user guidance employing large language models, the role of human factors and perception in cybersecurity education, and the creation of dynamic knowledge assessment techniques for tailoring network traffic visual platform interfaces. These discussions collectively highlighted the interdisciplinary nature of research on human factors in cybersecurity and proposed innovative strategies to tackle intricate cybersecurity issues.

We are planning to have new editions of the international DAMOCLES workshop in the near future, so as to foster the exploration of novel solutions, perspectives and challenges.

The workshop organizers
Bernardo Breve, University of Salerno
Giuseppe Desolda, University of Bari “Aldo Moro”
Vincenzo Deufemia, University of Salerno
Lucio Davide Spano, University of Cagliari