Digital Deception: Cyber Fraud and Online Misinformation

George Loukas
University of Greenwich

Charalampos Z. Patrikakis
University of West Attica, Computer Networks and Services Research Lab

Linda R. Wilbanks
Towson University

Phishing, user account takeovers, and other computing-related threats have made it easy for criminals to deceive people for financial and other gain. It is now considered standard practice for an advanced cyberattack, even a highly technical one, to start in a nontechnical manner: a spearphishing email deceiving an organization's employees into providing their credentials, a watering hole website infecting their computer, and so on. It is the human that is the initial target, as well as the first line of defense.

At the same time, social media has become a dominant, direct, and highly effective form of news generation and sharing at a global scale, in a manner that influences and enhances, but also challenges and often antagonizes, traditional media corporations. News passes through the hands of actors whose credibility and goals are unknown. Even less is known about the credibility and quality of the information cascades they trigger. High-profile misinformation campaigns are now focused on social media because of the exceptional speed they can provide. By the time a piece of misinformation on the Coronavirus has been fact-checked and debunked, it has already achieved its aim: It has deceived people into forming an opinion, making a decision, or causing damage to an organization or group of people.

As there is an exceptional diversity in the types of deception that are currently employed and in the platforms that are exploited in the process, suitably, this special issue hosts articles addressing the topic of digital deception and threats from a diverse range of points of view. Both the problem of deception through fake information aiming at disinforming, threatening or deceive users, as well as countermeasures and technologies that can be deployed are discussed. Starting with the article on "Attacking key management in ransomware," the authors highlight the criticality of key management in ransomware's cryptosystem in order to facilitate the provision of effective solutions against this threat. Moving from attacks that are targeting individuals to threats at community or government level, the authors of "Encryption-then-compression based copyright protection scheme for e-governance" discuss a joint encryption-then-compression based watermarking scheme for copyright protection and content verification that can be applied in a variety of applications.

The rest of the articles in this Special Issue, focusing on the topic of digital deception, address the same problem, which is considered as one of the most significant threats in information over the Internet and social networks: content deception,

which can take the form of fake news or fake videos. The articles hosted in the special issue report not only on the status of the problem, proposing methodologies for classifying the different forms in which it appears, but also solutions and state-of-the-art approaches on how to fight it. In particular, in "Detecting online content deception," the authors, starting from the identification of main types of content deception, propose a classification scheme for deception attacks and discuss defense measures, highlighting some outstanding challenges. Focusing more on the topic of fake news, the authors of "Food for thought: Fighting fake news and online disinformation" try to explain why people are susceptible to fake news and present the impact fake news, using examples from agri-food and other sectors, while they discuss how advances in machine learning and semantic technologies can be utilized to detect fake news and mitigate online disinformation. In the same course, in "Fake news, disinformation, and deepfakes: Leveraging Distributed ledger technologies and blockchain to combat digital deception and counterfeit reality," the authors discuss the potential of distributed ledger technologies to combat digital deception, describing the most relevant applications and identifying their main open challenges, while they provide recommendations to researchers on research toward strengthening the resilience against cyber-threats on today's online media.

One interesting conclusion that can be drawn from the articles in this Special Issue is the attention given both by the research and professional communities on understanding and fighting content deception. This can also be seen in large-scale research grants. The case of European Union funding is characteristic, with the H2020 program running several projects on deception across the secure societies, ICT, and other themes. Specifically addressing deception through social media, H2020 is producing a digital observatory for disinformation analysis (Project SOMA), an ecosystem for access to information verification services (SocialTruth), a new participatory verification approach (WeVerify), analytics for the verification of multimedia (PROVENANCE), and project EUNOMIA's novel methods for assisting the user in determining the original source of a piece of information, how it has been modified in an information cascade and how likely it is to be trustworthy. As artificial intelligence is also now becoming a key component in deception, with deepfake images and videos, automatically generated opinion articles, and cyberattacks based on adversarial machine learning, all indications are toward a future where deception continues to be a primary facilitator of malicious activity. So, it is important to see that appropriate research focus is placed on defense against deception, not only limited to technical and automated defenses, but also on equipping the users with the knowledge and tools to be able to defend themselves.

George Loukas is an Associate Professor and the Head of the Internet of Things and Security Research Group, University of Greenwich, London, U.K. He is currently the Project Coordinator of the H2020 project EUNOMIA on assisting the user in assessing the trustworthiness of information posted in social media, Project Coordinator of the EPSRC project CHAI on cyber hygiene in AI-enabled domestic life, and Principal Investigator in several other projects related to cyber security and the Internet of Things. His book defining cyber-physical attacks was shortlisted by ACM in the top 10 most notable books and articles in the 2015 Computing Milieux category.

Charalampos Z. Patrikakis is currently a Professor with the Department of Electrical and Electronics Engineering, University of West Attica, Athens, Greece, and the Director of the Computer Networks and Services Research Lab (CONSERT), Athens, Greece. He has more than 20 years of experience in international research projects, having participated in more than 32 national, European, and international programs. In 16 of these programs, he has been involved as a Technical/Scientific Coordinator or Principal Researcher. He has authored or coauthored more than 200 publications in book chapters, international journals, and conferences and has two contributions to national legislation. He is a Senior Member of IEEE and an IEEE student counselor with the University of West Attica. Contact him at bpatr@uniwa.gr.

Linda R. Wilbanks is currently a Lecturer with the Department of Computer and Information Sciences, Towson University, Towson, MD, USA. She recently retired from Federal Service, where she was the Senior Advisory for Cyber Risk Management, and previously held the position of Chief Information Officer for the Naval Criminal Investigative Service (NCIS), National Nuclear Security Administration (NNSA), and Goddard Space Flight Center, NASA (GSFC). She has authored more than 100 publications for international journals and conferences on software metrics and cyber security. She is a Senior Member of the IEEE.