DOI: 10.1049/ise2.12084

The Institution of Engineering and Technology WILEY

GUEST EDITORIAL

COVID-19 and cybersecurity

The COVID19 pandemic is having a worldwide impact on the way business is conducted, people interact, work is organised, and more. In a line, it is changing our way of life. In this Special Issue: COVID-19 and Cybersecurity, we focus on the many ramifications of COVID-19 into the Cybersecurity realm. In particular, the collected scientific contributions, subject to a thorough review process, touch on the following topics:

1. COVID19: digitalization, AI-enabled bot and social media tools, techniques, and platforms for the arms race

   The impact of AI-enabled bot is a subject of discussion in academic venues, while the general public is not much aware of it. However, the topic is affecting the lives of hundreds of millions, if not billions, of people. In particular, the cited pandemic has also shown the main shortcomings of our interconnectedness, especially related to the OSNs. It has further highlighted that information is a weapon, and that it can be a deadly weapon: the uncertain, unverified, contradictory, and sometimes outright false information on the vaccine, has generated in the general public a certain degree of diffidence that has slowed down the vaccination process. As a result, lives have been lost.

   To shed light on the introduced topic, we requested the following types of contributions:
   - Highlighting the interplay between the trustworthiness of information on the Covid-19 vaccine, the propagation of information and, especially, fake news.
   - Quantification of the misinformation on the topic that has been developed through bot.
   - OSNs countermeasures (implemented and forecasted) to limit bots spreading misinformation on the COVID19.
2. COVID19 and contact tracing: security, privacy, and future architectures

   A plethora of contact tracing apps have been developed and deployed in several countries around the world in the battle against COVID-19. However, people are rightfully concerned about the security and privacy risks of such applications. To this end, we requested the following types of contributions:
   - An in-depth analysis of the security and privacy characteristics of the most prominent contact tracing protocols, under both passive and active adversaries.
   - The design and implementation of novel contact tracing protocol that can defend against most passive and active attacks, thus providing strong (provable) security and privacy guarantees that are necessary for such a sensitive application.
   - The design of future architecture that can help to improve the preparedness against COVID19 and future pandemics.
3. COVID-19 E-health digital certificates: security and privacy

   As a response to the COVID-19 crisis, the EU designed and implemented digital Covid certificates to ease the movements of EU citizens across Europe.

   This poses new potential security and privacy issues: people can be traced by apps that potentially expose their personal data.

   To this end, we requested the following types of contributions:
   - Analysis of the security, legal and privacy issues posed by the so-called DGC apps and infrastructure and their EU interoperability.
   - Design and implementation of alternative architectures or improvements to the DGC model.
   - Human aspect of security–Indeed, 60% of over 65 do not have a smartphone.

   We are glad to share with you that the above expectations have been fully met by the selected papers. Details on the three papers on the above-referred topics that this Special Issue is composed of are reported in the sequel.

1 | COVID19: DIGITALISATION, AI-ENABLED BOT AND SOCIAL MEDIA TOOLS, TECHNIQUES, AND PLATFORMS FOR THE ARMS RACE

The paper, 'The COVID-19 Scamdemic: A Survey of Phishing Attacks and their Countermeasures during COVID-19' by Ali Al-Qathani and Stefano Cresci, brings some unity and categorisation to a not so well investigated phenomenon: COVID-19 scamdemics. Where scamdemic refers to the global epidemic of scams and frauds triggered or enabled by COVID-19. Indeed, the unprecedented cybersecurity concerns that emerged during the pandemic sparked a torrent of

research to investigate cyber-attacks and to propose solutions and countermeasures. Within the scamdemic, phishing was by far the most frequent type of attack. This survey paper reviews, summarises, compares and critically discusses 54 scientific studies and many reports by governmental bodies, security firms and the grey literature that investigated phishing attacks during COVID-19, or that proposed countermeasures against them. The provided analysis identifies the main characteristics of the attacks and the main scientific trends for defending against them, thus highlighting current scientific challenges and promising avenues for future research and experimentation.

2 | COVID19 AND CONTACT TRACING

The paper, 'A Secure Contact Tracing Platform from Simplest PSI-Cardinality', by Jiahui Gao, Chetan Surana, and Ni Trieu, is inspired by the fact that contact tracing is an essential tool for controlling the spread of disease through human populations. However, existing contact tracing applications are either vulnerable to privacy and security attacks or have heavy bandwidth/computational requirements on the client's devices. In this work, the authors introduce SecureCT, a Secure Contact Tracing platform with strong privacy protection and lightweight cost. SecureCT prevents linkage attacks, eliminates replay and relay attacks, and allows the phone's holder to delegate their contact tracing computation to untrusted servers while maintaining the user's privacy. The technical core of the proposed scheme is an ingenious, efficient Private Set Intersection Cardinality (PSI-CA) protocol that only relies on symmetric-key primitives. A thorough assessment of the proposed solution shows its full feasibility for real deployment.

3 | COVID-19 E-HEALTH DIGITAL CERTIFICATES: SECURITY AND PRIVACY

The paper, 'AI BOT to detect fake COVID19 Vaccine certificates' by Muhammad Arif, Shermin Shamsudheen, Ajesh F, Guojun Wang, and Jianer Chen, intends to thwart the plague related to fake COVID-19 vaccination certificates. In particular, forged vaccine certificates are created using advanced software and digital tools which create artefacts that are difficult to distinguish from real vaccine certificates. This illegal behaviour also generates immense pressure on the governments as well as healthcare workers, not to mention that people who have fake vaccine certificates roam around, possibly contributing to the spreading of the infection. So, to address this safety and security problem, in this paper the authors focus on detecting fake vaccine certificates using a bot powered by Artificial Intelligence. The results are striking, achieving an accuracy of 94%, and hence providing a viable solution to the exposed safety and security threat.

4 | SUMMARY/CONCLUSION

All the papers selected for this Special Issue enjoy a unique set of features: applicability to the real world—to contribute to the fight against the ongoing pandemic; being rooted on sound theory and analysis; enjoying a strong formalism; and, being supported by experimental results that complement the theoretical findings. What is more, the results herein reported, other than being directly applicable to thwart the COVID-19 pandemic, also transcend it, enjoying a more general applicability as well as having a relevant potential to foster further research.

ACKNOWLEDGEMENTS

We would like to express our gratitude and congratulations to all the authors of the selected papers in this Special Issue of COVID-19 and Cybersecurity for their valuable contributions. We would like to thank also all the reviewers for their contributions to the selection and improvement process of the publications in this Special Issue. Our hope is that this Special Issue will stimulate researchers in both industry and academia to undertake further research in this challenging field, where lives are at stake. We are also grateful to the IET Editor-in-Chief, Yvo Desmedt, and the Editorial Office for their support throughout the editorial process.

PERMISSION TO REPRODUCE MATERIALS FROM OTHER SOURCES

We did not use any material from any other source for this Guest Editorial.

Roberto Di Pietro[1]
Ni Trieu[2]
Vincenzo Iovino[3,4]

[1]*ICT Department, College of Science and Engineering, Hamad Bin Khalifa University, Doha, Qatar*
[2]*School of Computing and Augmented Intelligence, Arizona State University, Phoenix, Arizona, USA*
[3]*DIEM, University of Salerno, Salerno, Italy*
[4]*Aragon Association, Zug, Switzerland*

Correspondence
Roberto Di Pietro, ICT Department, College of Science and Engineering, Hamad Bin Khalifa University, Education City, 34110, Doha, Qatar.
Email: rdipietro@hbku.edu.qa

DATA AVAILABILITY STATEMENT

There is no data associated with this Guest Editorial.

AUTHOR BIOGRAPHIES

Roberto Di Pietro, ACM Distinguished Scientist, is a Full Professor in Cybersecurity at HBKU-CSE. Previously, he was in the capacity of Global Head Security Research at Nokia Bell Labs, and Associate Professor (with tenure) of Computer Science at the University of Padova, Italy. He also served 10+ years as a senior military technical officer. Overall, he has been working in the cybersecurity field for 25+ years, leading both technology-oriented and research-focussed teams in the private sector, government, and academia (MoD, United Nations HQ, EUROJUST, IAEA, WIPO). His main research interests include security and privacy for wired and wireless distributed systems (e.g. Blockchain technology, Cloud, IoT, On-line Social Networks), virtualization security, applied cryptography, computer forensics, and data science. Other than being involved in M and A of start-up—and having founded one (exited)—, he has been producing 250+ scientific papers and 16 patents over the cited topics, has co-authored three books, edited one, and contributed to a few others. He is serving as the EiC for Security and Communication Networks (Wiley-Hindawi), and as AE for IET Security, ComCom, ComNet, PerCom, Journal of Computer Security, as well as serving in the advisory board of FGCS. In 2011–2012 he was awarded a Chair of Excellence from University Carlos III, Madrid. In 2020 he received the Jean-Claude Laprie Award for having significantly influenced the theory and practice of Dependable Computing.

Ni Trieu is an Assistant Professor of computer science at Arizona State University. Her research interests are in the area of cryptography and security, with a specific focus on secure computation and its applications such as private set intersection, secure bio-computing, and privacy-preserving machine learning. She received her Ph. D. degree from Oregon State University. Before joining ASU, she was a postdoctoral researcher at UC Berkeley.

Vincenzo Iovino received his PhD from the University of Salerno in 2012. His research interests are in cryptography and security, in particular functional encryption and e-voting. He is currently an Assistant Professor at the University of Salerno and Cryptography Researcher at Aragon Association. Previously, he was Research Associate at the University of Luxembourg and postdoctoral Researcher at Warsaw University.