Security-focused Networks of the Future

Sandra Scott-Hayward
Centre for Security Information Technologies
Queen's University Belfast, Belfast, N. Ireland
s.scott-hayward@qub.ac.uk

ABSTRACT

Network attack and data breach statistics are abundant; from the 2020 Cisco Annual Internet Report citing an anticipated increase in Distributed Denial-of-Service (DDoS) attacks from 7.9 million in 2018 to 15.4 million by 2023, to almost daily reports of data breaches, hackers targeting network device vulnerabilities, attacks on network services etc. This is, of course, unsurprising. Our lives are increasingly reliant on communication networks. In 2020, because of the COVID-19 pandemic, we have seen the accelerated provision of health services in the home and an increased prevalence of home schooling and working. This has placed a significant burden on our home networks, one which cyber-criminals have been only too eager to exploit. The challenge to protect network users extends from there.

So, what does cyber security look like in the networks of the future? The emergence of technologies such as Software-Defined Networking (SDN), Network Functions Virtualization (NFV), and Multi-Access Edge Computing (MEC) enable innovation in network security, but these technologies create additional attack surfaces. Dramatic advances in Machine Learning (ML) and Artificial Intelligence (AI) techniques are influencing security services and design for security, but they can also be exploited to produce sophisticated attacks. How can we leverage these technologies while managing the challenge of the attacker to better protect, secure and maintain resilient networks? Can we deliver scalable, analytics-based, security-focused network orchestration and management?

This talk will introduce our latest research addressing these challenging questions, present developments in the field, and discuss future research directions.

CCS Concepts/ACM Classifiers

• Networks -> Network security; Programmable networks; • Security and privacy -> Network security;

Author Keywords: Software-Defined Networking; Network Functions Virtualization; Multi-Access Edge Computing; Network Security, Machine Learning

SDN-NFV Sec '21, April 28, 2021, Virtual Event, USA.

ACM ISBN 978-1-4503-8143-7/21/04.
https://doi.org/10.1145/3445968.3456870

BIOGRAPHY

Sandra Scott-Hayward is a Lecturer (Assistant Professor) with the School of Electronics, Electrical Engineering and Computer Science, and a Member of the Centre for Secure Information Technologies at Queen's University Belfast (QUB). She began her career in industry and became a Chartered Engineer in 2006 having worked as a Systems Engineer and Engineering Group Leader with Airbus. Since joining academia, she has published a series of IEEE/ACM papers on security designs and solutions for softwarized networks based on her research on the development of network security architectures and security functions for emerging networks. She received Outstanding Technical Contributor and Outstanding Leadership awards from the Open Networking Foundation in 2015 and 2016, respectively, having been elected and serving as the Vice-Chair of the ONF Security Working Group from 2015 to 2017. Amongst many other service memberships, she was the TPC Co-Chair for IEEE NFV-SDN 2020 and is an Associate Editor of IEEE Transactions on Network and Service Management. She is Director of the QUB Academic Centre of Excellence in Cyber Security Education (ACE-CSE), one of the first universities to be awarded this recognition by the U.K. National Cyber Security Centre.