The July 2020 Issue

This July 2020 issue contains four technical papers, the second paper of our education series, as well as two editorial notes.

The first technical paper, *Tracking the deployment of TLS 1.3 on the Web: A story of experimentation and centralization*, by Ralph Holz and his colleagues, deals with Transport Layer Security (TLS) 1.3, a redesign of the Web's most important security protocol. TLS 1.3 was standardized in August 2018 after a four year-long, unprecedented design process involving many cryptographers and industry stakeholders. In their work, the authors track deployment, uptake, and use of TLS 1.3 from the early design phase until well over a year after standardization.

The second technical paper, *Does Domain Name Encryption Increase Users' Privacy?*, by Martino Trevisan and colleagues, is on a topic related to the first technical paper. This work shows that DNS over HTTP (DoH) does not offer the privacy protection that many assume. For the purposes of reproducibility, the authors provide the data used under NDA with the institution owning the data. The authors also share config files and ML environment details in the interest of promoting replicability in other environments.

Our third paper, *Using Application Layer Banner Data to Automatically Identify IoT Devices*, by Talha Javed and his colleagues, is of the "repeatable technical papers" type, which are technical contributions that provide their artefacts, e.g., software, datasets. This paper attempts to replicate a Usenix Security 2018 paper. It describes the efforts of the authors at re-implementing the solution described in the Usenix Security paper, especially the challenges encountered when authors of the original paper are unwilling to respond to requests for artefacts. We hope it will encourage additional reproducibility studies.

The fourth paper, *Towards Declarative Self-Adapting Buffer Management*, by Pavel Chuprikov and his colleagues, introduces a novel machine learning based approach to buffer management. The idea is to provide a queue management infrastructure that automatically adapts to traffic changes and identifies the policy that is hypothetically best suited for current traffic patterns. The authors adopt a multi-armed bandits model, and given that different objectives and assumptions lead to different bandit algorithms, they discuss and explore the design space while providing an experimental evaluation that validates their recommendations. The authors provide a GitHub repository that allows for the reproducibility of their result through the NS-2 simulator.

The fifth paper, also our second paper in the new education series, *Open Educational Resources for Computer Networking*, by Olivier Bonaventure and his colleagues, describes an effort to create an online, interactive textbook for computer networking. What distinguishes this textbook from traditional ones is that it not only is it free and available for anyone in the world to use, but also, it is also interactive. Therefore, this goes way beyond what a textbook usually offers: it is an interactive learning platform for computer networking. The authors here report on about ten years of experience with it, that led to some interesting experiences and lessons learned.

Then, we have two editorial notes. The first, *Lessons Learned Organizing the PAM 2020 Virtual Conference*, by Chris Misa and his colleagues, reports on the experience from the organizing committee of the 2020 edition of the Passive and Active Measurement (PAM) conference, that took place as a virtual event. It provides important lessons learned for future conferences that decide to go for an virtual event. The second editorial note, *Update on ACM SIGCOMM CCR*

reviewing process: making the review process more open, by the whole CCR editorial board, aims to inform the SIGCOMM community on the reviewing process in place currently at CCR, and to share our plans to make CCR a more open and welcoming venue, adding more value to the SIGCOMM community.

Steve Uhlig
CCR Editor