ACSAC 2020: Furthering the Quest to Tackle Hard Problems and Find Practical Solutions

Danfeng (Daphne) Yao | Virginia Tech
Terry Benzel | University of Southern California Information Sciences Institutes

The Annual Computer Security Applications Conference (ACSAC) 2020 marked the 36th edition of ACSAC. The vision of Marshall Abrams, a beloved founder and tireless organizer of ACSAC, is to take hard problems and find practical solutions. In September 2020, Marshall died of heart failure at the age of 79. Prior to his passing, he was actively working on signing a virtual meeting vendor for the conference. As Charles Payne, ACSAC local arrangements chair, said during the tribute, Marshall asked us to focus on solving hard problems, hard problems that require the combined effort of government, industry, and academia to address; and Marshall insisted on practical solutions. With rampaging ransomware and zero-day supply-chain attacks tearing through critical national and computing infrastructures, Marshall's longtime vision seems more relevant today than ever.

The vision of tackling hard problems and finding practical solutions is also reflected in the multiyear ACSAC hard topic theme, "Deployable and Impactful Security." Deployable and impactful security generally involves the development of defensive solutions rather than simply exposing weaknesses and vulnerabilities. While ACSAC has always prioritized work on applied security, by explicitly setting it as a hard topic theme we put a greater emphasis on deployability.

Artifact evaluation, a proud and successful ACSAC tradition, continues to flourish. In 2020, the dedicated ACSAC artifact evaluation team, led by Roberto Perdisci, consisted of 50 students and 27 mentors. Sixteen ACSAC 2020 papers are awarded with Association of Computing Machinery (ACM) Functional Badges and 10 with ACM Reusable Badges. This special issue includes two badged papers.

The 302 submissions in 2020, a new ACSAC record, covered a broad spectrum of applied security topics. Most submissions went through two rounds of review and discussion by members of a large international program committee, which consisted of 89 experts from government, industry, and academia across 17 countries. Seventy outstanding papers were accepted, which gives an acceptance rate of 23.2%, comparable to 2019's 22.6%.

For this special issue, we invited the authors of selected papers to submit a longer version that targets a broader magazine audience. Some papers received special ACSAC recognitions. For example, the work evaluating privacy policies of voice assistant applications by Liao et al. was selected as one of the two Distinguished Papers at ACSAC 2020 as well as receiving an ACM Functional Artifact Badge. The other Distinguished Paper Award–winning work is also included in this

Digital Object Identifier 10.1109/MSEC.2021.3106595
Date of current version: 28 October 2021

special issue, which is on the security and privacy risks of parental control solutions by Ali et al. The work that models the open stock markets security by Yagemann et al. also received an ACM Functional Artifact Badge. We appreciate all authors' contributions to this special issue.

In This Issue

A main roadblock to dynamically analyzing Internet of Things firmware security is the diverse hardware platforms. State-of-the-art emulation environments can only execute less than one-fifth of the thousands of firmware images tested by Dongkwan Kim, Eunsoo Kim, Mingeun Kim, Yeongjin Jang, and Yongdae Kim. In "Enabling the Large-Scale Emulation of Internet of Things Firmware With Heuristic Workarounds," the authors present a technique called *arbitrated emulation* and achieve a nearly five-times execution rate.

In "Parental Controls: Safer Internet Solutions or New Pitfalls?" Suzan Ali, Mounir Elgharabawy, Quentin Duchaussoy, Mohammad Mannan, and Amr Youssef provide the first comprehensive study of parental control tools. Using their experimental framework, they comprehensively evaluate security and privacy issues on multiple platforms, including network devices, Windows applications, Chrome extensions, and Android apps. They point out how these vulnerabilities may be exploited by cyber predators.

Stephan Wiefling, Markus Dürmuth, and Luigi Lo Iacono compared multiple authentication schemes, including a risk-based authentication, in terms of their usability and security perceptions. Risk-based authentication, a relatively new approach, utilizes additional features at login, e.g., network or device information. The article "Verify It's You: How Users Perceive Risk-Based Authentication" shares many insights obtained from their user study.

In "Modeling Large-Scale Manipulation in Open Stock Markets," Carter Yagemann, Pak Ho Chung, Erkam Uzun, Sai Ragam, Brendan Saltaformaggio, and Wenke Lee studied U.S. Securities and Exchange Commission case files on stock market fraud. They identify multiple types of criminal trading activities that manipulate stock prices. The authors then show in a simulated environment how such attacks can be performed automatically.

Privacy guarantees of voice assistants, such as Amazon Alexa and Google Assistant, are the center of focus in the article by Song Liao, Christin Wilson, Cheng Long, Hongxin Hu, and Huixing Deng. Their work, "Problematic Privacy Policies of Voice Assistant Applications," analyzed tens of thousands of voice assistant extensions written by voice-app developers. The team developed a natural language processing based method to automatically identify inconsistencies between privacy policies and descriptions of voice apps.

Seemingly distinct malwares are oftentimes just variants exploiting the same weakness. If the most significant weakness types are identified, then defenders can focus on preventing them. That is the vision of the Assane Gueye, Carlos E.C. Galhardo, Irena Bojanova, and Peter Mell in the article "A Decade of Reoccurring Software Weaknesses." Based on the Common Weakness Enumeration and other public repositories, the team shows how to quantitatively identify the most dangerous software errors.

In "Authentication of Voice Commands by Leveraging Vibrations in Wearables," Cong Shi, Yan Wang, Yingying (Jennifer) Chen, and Nitesh Saxena present an innovative voice authentication system aiming to prevent acoustic-based attacks (e.g., impersonation and reply) in voice assistants. The authors utilize motion sensors and vibration data obtained from the user's wearable device to verify the audio commands received by the microphone.

We hope that by bringing a subset of the ACSAC program to you, this *IEEE Security & Privacy* special issue will enhance the connection between the conference and the magazine communities. Both platforms are highly impactful in our cybersecurity profession. We encourage you to attend ACSAC 2021, to be held virtually again. We also look forward to continuing to exchange ideas with you through the magazine pages. ■

Danfeng (Daphne) Yao is a professor of computer science at Virginia Tech, Blacksburg, Virgina, 24061, USA. Her research interests include building cyber defenses and machine learning for digital health, with a shared focus on accuracy and deployment. Yao received her Ph.D. in computer science from Brown University. She served as the lead program chair of ACSAC 2020 with cochair Heng Yin of the University of California, Riverside and Artifact Evaluation Chair Roberto Perdisci of the University of Georgia. Contact her at danfeng@vt.edu.

Terry Benzel is the director of the networking and cybersecurity at the Information Sciences Institute of the University of Southern California, Los Angeles, California, 90292, USA. Benzel received an M.A. from Boston University and an executive M.B.A. from the University of California, Los Angeles. She is a senior member of the IEEE Computer Society, an associate editor in chief of *IEEE Security & Privacy*, and a member of the Board of Governors of the IEEE Computer Society. Contact her at tbenzel@isi.edu.