Introduction to the ACSAC'19 Special Issue—Vol. 2

The Annual Computer Security Applications Conference (ACSAC) brings together cutting-edge researchers, with a broad cross-section of security professionals drawn from academia, industry, and government, gathered to present and discuss the latest security results and topics. ACSAC's core mission is to investigate practical solutions for computer and network security technology.

The 35th Annual Computer Security Applications Conference was held in Puerto Rico on December 9–13, 2019. ACSAC 2019 especially encouraged contributions in the area of *Deployable and Impactful Security*. Deployable and impactful security solutions aim to address key real-world challenges, which may include accuracy, runtime overhead, ground-truth labeling, human aspects, usability, and energy consumption. Having the deployability and impactfulness goals motivates one to focus on solving the most critical real-world challenges, which may otherwise be ignored by the fast-moving research community. In addition, ACSAC encourages authors of accepted papers to submit software and data artifacts and make them publicly available to the entire community. Releasing software and data artifacts represents an important step toward facilitating the reproducibility of research results and ultimately contributes to the real-world deployment of novel security solutions.

This special issue includes extended versions of papers that appeared at ACSAC 2019, focusing especially on research on computer security applications with a high potential for being deployed in real-world environments or that have already been deployed and used to implement practical defense systems.

This volume contains six articles on topics including DNS security and privacy, anti-virus and malicious software, and IoT and cyber-physical systems security.

In "PREMADOMA: An Operational Solution to Prevent Malicious Domain Name Registrations in the .eu TLD," Desmet et al. propose a system for detecting malicious domains at registration time, before they have an opportunity to be used. PREMADOMA has already been deployed to defend the `.eu` country-code top-level domain (ccTLD) registrar. The evaluation includes 11 months of real-world observations from the `.eu` ccTLD, showing that PREMADOMA is effective at blocking a significant number malicious domain registrations.

Nakatsuka et al. propose to enable end-to-end DNS privacy in an article titled "PDoT: Private DNS-over-TLS with TEE Support." The PDoT system is a DNS resolver that can run within a Trusted Execution Environment (TEE). Using remote attestation, clients can verify the TEE-based DNS resolver execution, providing a guarantee that the DNS operator running the resolver will not be able to monitor the clients' DNS requests. To provide strong privacy guarantees, PDoT relies on the fact that the confidentiality of client-to-resolver and resolver-to-name-servers DNS queries can be protected by DNS-over-TLS (DoT), a recently proposed protocol. The evaluation presents experimental results and measurements using a PDoT prototype, demonstrating that achieving strong DNS privacy is feasible.

In "Cut-and-Mouse and Ghost Control: Exploiting Antivirus Software with Synthesized Inputs," Genç et al. present two classes of attacks against popular antivirus (AV) software: *Ghost Control* and *Cut-and-Mouse*. The first attack allows malware to avoid detection by simulating mouse events to disable the AV protection. The latter attack allows malware to trigger whitelisted applications into performing malicious activities on their behalf.

ACM Reference format:
Roberto Perdisci, Martina Lindorfer, Adam Doupé, Andrea Lanzi, Alexandros Kapravelos, and Gianluca Stringhini. 2020. Introduction to the ACSAC'19 Special Issue—Vol. 2. *Digit. Threat.: Res. Pract.* 2, 1, Article 1 (January 2021), 2 pages.
https://doi.org/10.1145/3437253

2576-5337/2020/01-ART1
https://doi.org/10.1145/3437253

The authors evaluated their attacks against 29 AVs and found almost half of them vulnerable. The authors also show that sandboxing and CAPTCHAs do not necessarily prevent against these types of attacks, and ultimately fixes need to be employed on the OS level. Microsoft acknowledged the issues and is working on fixing them in Windows 10. The authors also disclosed their findings to the affected AV vendors and provide interesting insights into the (sometimes cumbersome) disclosure process.

In "Automatic Reverse Engineering of Script Engine Binaries for Building Script API Tracers," Toshinori et al. face the problem of the unbalanced cost due to script languages asymmetry in the malware analysis context. The diversity of choices in terms of script languages on the attacker's side unexpectedly imposes a significant cost on the development of analysis tools on the defense side. To solve this problem, the authors proposed a dynamic method for automatically generating script API tracers by automatically analyzing the binaries of script engines. Such a method consists of several steps: execution trace logging, hook point detection, tap point detection, hook and tap point verification, and script API tracer generation. The resulting system is able to generate the script API tracer for the most three popular script languages (VBA, VBScript, and PowerShell). The authors show the effectiveness of their approach by providing case studies that demonstrated that the generated script API tracers can analyze malicious scripts in the wild.

In "Aegis+: A Context-aware Platform Independent Security Framework for Smart Home Systems," Sikder et al. present a system for defending Smart Home Systems (SHSs) against possible malicious applications or devices. To this end, Aegis+ learns context-aware behavioral models that allow for detecting anomalous or malicious activities performed by devices in an SHS. The evaluation is performed in three different realistic home layouts, with real-world smart devices and users. The experimental results show that Aegis+ can accurately detect and report anomalous or malicious SHS behaviors to the user, for instance, via smartphone app notifications.

Finally, in "Stealthy Attacks Against Robotic Vehicles Protected by Control-based Intrusion Detection Techniques," Dash et al. show that control-based intrusion detection systems used in robotic vehicles (RVs) are vulnerable to attacks, and develop practical attacks able to disrupt RV missions. They then demonstrate their attacks on eight types of RVs, showing that their attacks are general. This article has the potential of influencing future designs of robotic vehicles, making them more resilient and able to carry out their missions more effectively.

As Associate Editors for this special issue, we are very pleased that the authors of the above articles have significantly extended and improved their ACSCA'19 publications, and that many of them have released their proof-of-concept software to the public to foster the reproducibility of their research results.

We thank the authors, reviewers, and ACSAC'19 program committee members who have contributed to selecting the articles that appear in this special issue. We would also like to thank the DTRAP Co-Editors-in-Chief and the ACM for the opportunity to work on this special issue.

Roberto Perdisci
Martina Lindorfer
Adam Doupé
Andrea Lanzi
Alexandros Kapravelos
Gianluca Stringhini
Guest Editors