



December 9-13, 2019 | The Condado Plaza Hilton | San Juan, Puerto Rico, USA



**Welcome
to
ACSAC 35 !!**



<https://www.acsac.org/2019/proceedings/>



December 9-13, 2019 | The Condado Plaza Hilton | San Juan, Puerto Rico, USA

Welcome (Back) to The Condado Plaza Hilton



<http://www.condadoplaza.com/>, <https://www.booking.com/hotel/pr/plaza-de-armas-san-juan.html>



December 9-13, 2019 | The Condado Plaza Hilton | San Juan, Puerto Rico, USA

David Balenson, Conference Chair
Administrative Announcements

Guofei Gu, Program Co-Chair
Technical Program and Distinguished Paper Awards

Mary Ellen Zurko and Jeremy Epstein, ACSA
SWSIS Scholarship Presentations

Carrie Gates, Distinguished Practitioner Keynote
Can You Get That to Me Soon? Lessons Learned from Life
in Industry Research



December 9-13, 2019 | The Condado Plaza Hilton | San Juan, Puerto Rico, USA

Wi-Fi Access

- The hotel provides Wi-Fi access from the meeting rooms

SSID: HILTON MEETING ROOMS ONLY

Password: ACSAC2019

- There is a limited number of connections, so please restrict your Wi-Fi access in the meeting rooms to one device at a time (e.g., laptop, tablet, or smartphone).



<https://demgeeks.com/hack-get-free-wifi-on-paid-access-hotspots/>



December 9-13, 2019 | The Condado Plaza Hilton | San Juan, Puerto Rico, USA

Program At-a-Glance (Wednesday)

- Breakfast
- **Welcome**
- **Distinguished Practitioner Keynote**
- Break
- **Multi-track Sessions**
- Lunch
- **Multi-track Sessions**
- Break
- **Multi-track Sessions**
- Conference Dinner w/ Entertainment



December 9-13, 2019 | The Condado Plaza Hilton | San Juan, Puerto Rico, USA

Program At-a-Glance (Thursday)

- Breakfast
- **Test of Time Paper Awards**
- **Distinguished Practitioner Keynote**
- Break
- **Multi-track Sessions**
- Lunch
- **Multi-track Sessions**
- Break
- **Multi-track Sessions**
- **Works-in-Progress**
- **Poster Session w/ Light Refreshments**



December 9-13, 2019 | The Condado Plaza Hilton | San Juan, Puerto Rico, USA

Program At-a-Glance (Friday)

- Breakfast
- **Multi-track Sessions**
- Break
- **Multi-track Sessions**
- Closing with Prize Giveaway

- Optional Social Event
 - El Yunque National Forest (Rain Forest)



December 9-13, 2019 | The Condado Plaza Hilton | San Juan, Puerto Rico, USA

Panels & National Interest Track

Wednesday

- Panel: Disinformation and Other Harmful Messaging: Can Technology Tame the Beast It Created?
- NITRD Panel: Federal Cybersecurity R&D Strategic Plan

Thursday

- Panel: Framing the Ransomware Problem
- NITRD Panel: Making AI Forget You



December 9-13, 2019 | The Condado Plaza Hilton | San Juan, Puerto Rico, USA

Case Studies

Wednesday

- ~~Cybersecurity Test and Evaluation Lessons Learned~~
- Defeating the PCAP Problem: Making a Mountain into a Molehill
- “Operation CWAL”: The Dying Art of Product Penetration Testing

Thursday

- Hype or Hope? Machine Learning Based Security Analytics for Web Applications
- Applying the Guilt By Association Principle to Threat Detection with Sparsely Labeled Data
- JEX: A Straightforward, Portable and Scalable Framework for Automatic Exploit Generation for Java



December 9-13, 2019 | The Condado Plaza Hilton | San Juan, Puerto Rico, USA

Student Conferenceships – Thank You to our Sponsors!!



Student meet-and-greet and group photo in Royal Ballroom
during Wednesday afternoon break



December 9-13, 2019 | The Condado Plaza Hilton | San Juan, Puerto Rico, USA

Wednesday Evening Conference Dinner

- In Brisas del Mar overlooking the ocean
- Features a trio playing Latin and tropical instrumental music
- Plus, a live Carnival Parade after dinner – **DON'T LEAVE EARLY!!**
- Reminders:
 - Tell the waiter if you have dietary restrictions
 - Look for signs by the food for ingredients
 - Bring your drink tickets!





December 9-13, 2019 | The Condado Plaza Hilton | San Juan, Puerto Rico, USA

Test of Time Paper Awards

- Recognize and honor selected papers from the first 20 years (1985-2004) that have had a significant impact
 - Led to a major change in the field
 - Are used commercially
 - Have been well cited
 - Are well known as strong papers



<https://www.wabisabilearning.com/blog/13-educational-tools-test-time>



December 9-13, 2019 | The Condado Plaza Hilton | San Juan, Puerto Rico, USA

El Yunque National Forest

- A very limited number of spaces available!
- **SIGN UP AT REGISTRATION DESK BY 12:00 NOON ON THURSDAY**
- Cost: \$95
 - Bus transportation
 - Lunch
 - Admission to the forest
- Features a guided tour, with stops at the scenic Coco Falls, Yukaho tower (climb the 95 steps to the top for a scenic view of the ocean above the rainforest canopy). Walk down (steep steps and dirt trail) to La Mina Falls (bring your bathing suit for a swim if desired)
- **BUSES LEAVE THE HOTEL AT 12:30PM – DON'T BE LATE!!**

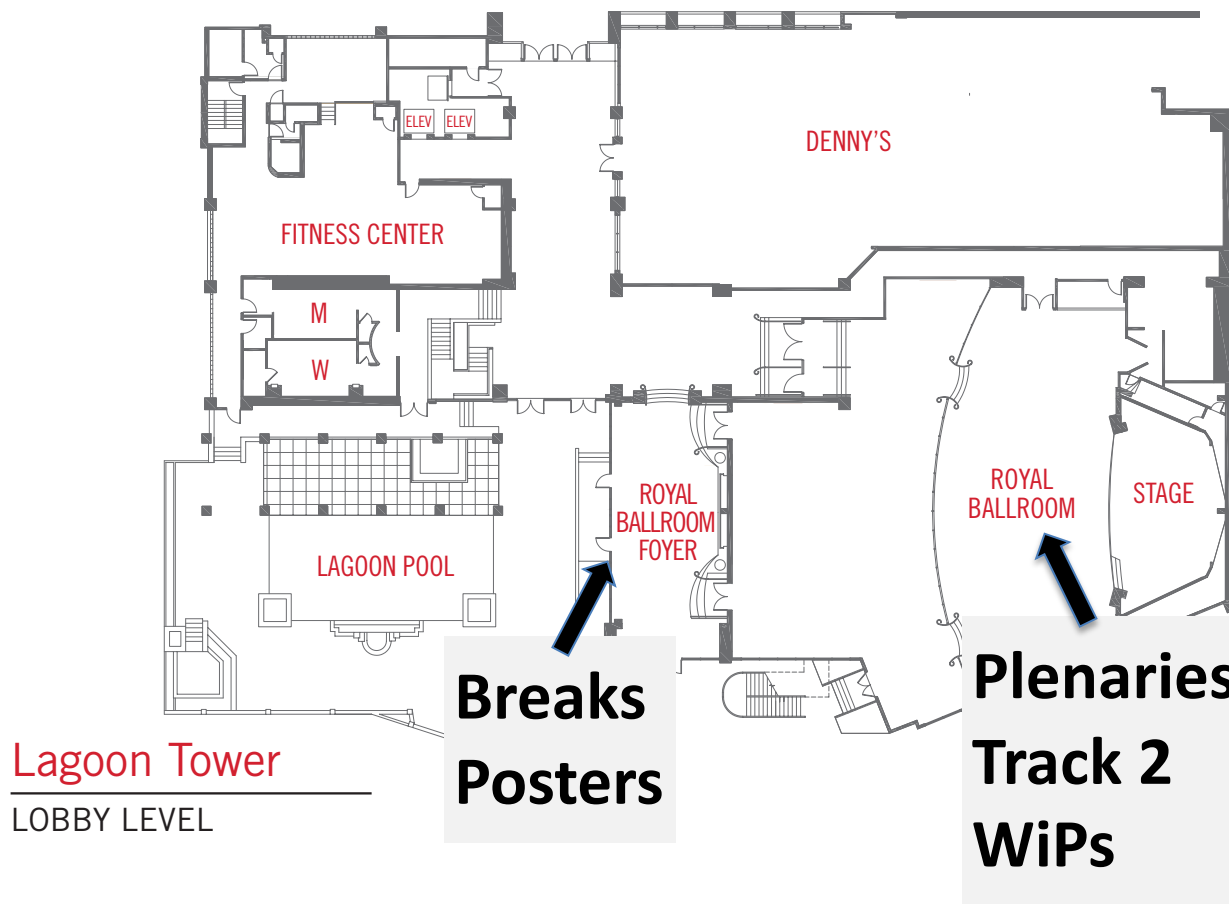


https://www.fs.usda.gov/Internet/FSE_MEDIA/fseprd615682.jpg



December 9-13, 2019 | The Condado Plaza Hilton | San Juan, Puerto Rico, USA

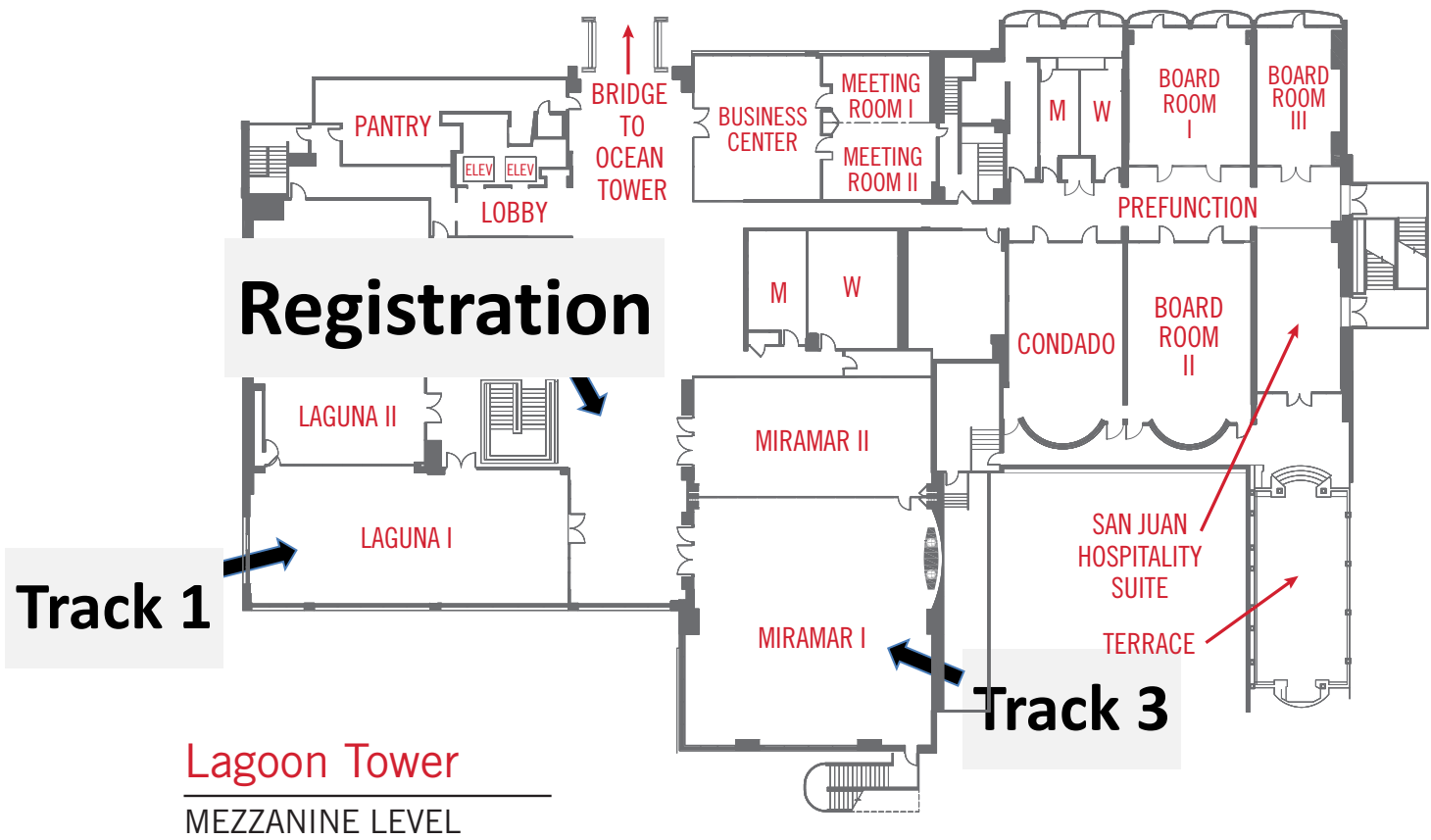
Conference Sessions (Lobby Level)





December 9-13, 2019 | The Condado Plaza Hilton | San Juan, Puerto Rico, USA

Conference Sessions (Mezzanine Level)



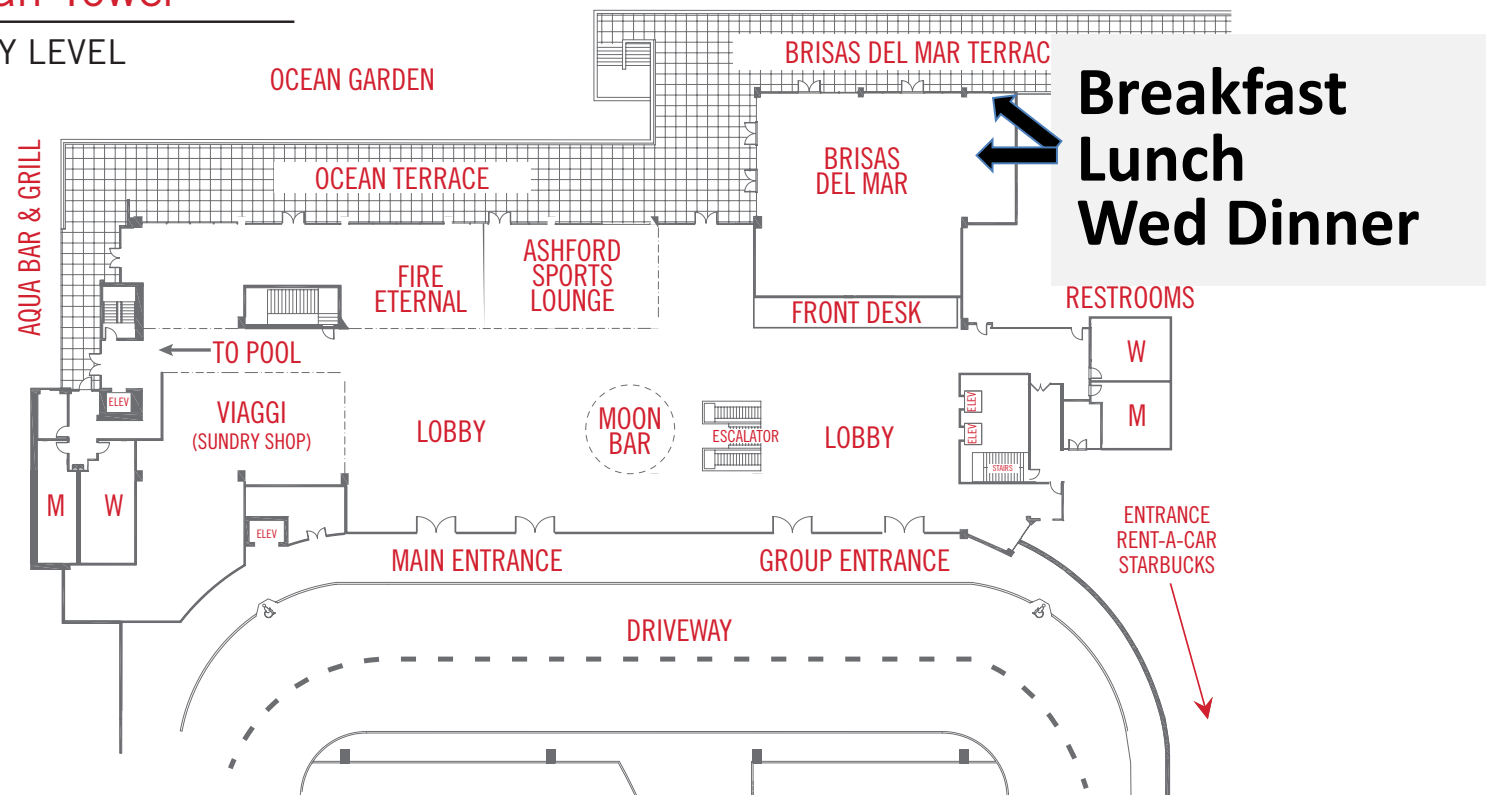


December 9-13, 2019 | The Condado Plaza Hilton | San Juan, Puerto Rico, USA

Meals

Ocean Tower

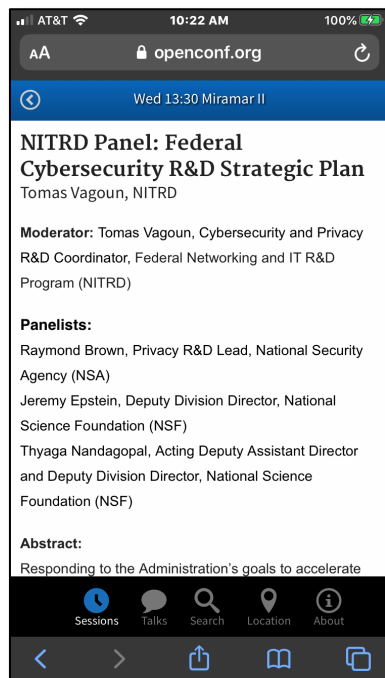
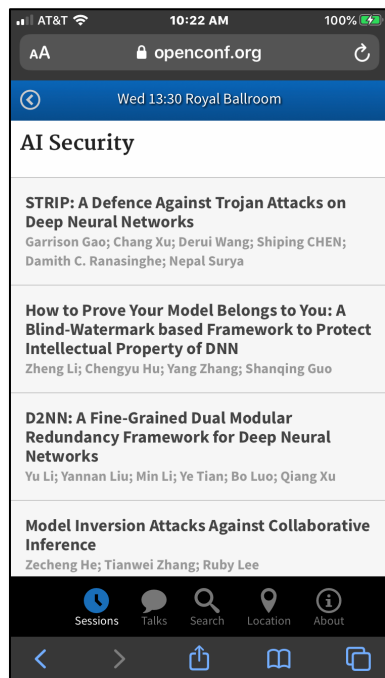
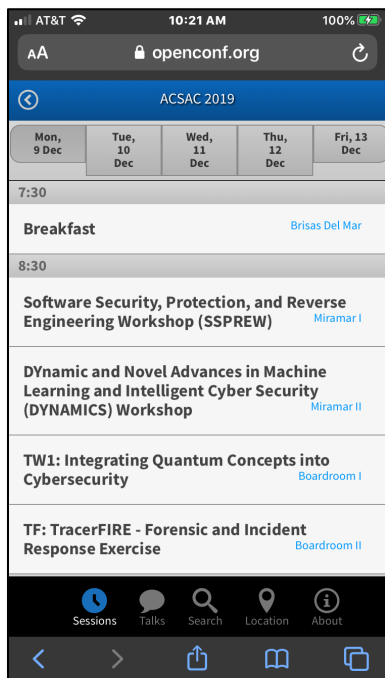
LOBBY LEVEL





December 9-13, 2019 | The Condado Plaza Hilton | San Juan, Puerto Rico, USA

Mobile Program

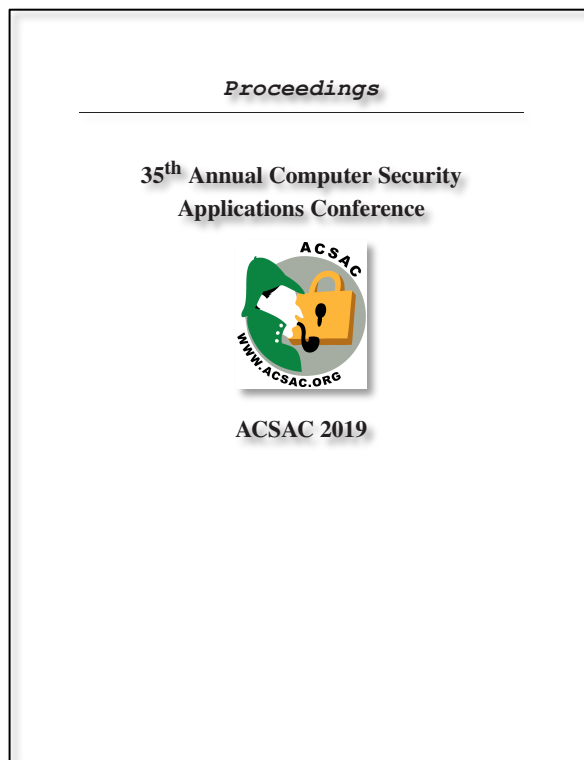


<https://www.openconf.org/acsac2019/mobile>



December 9-13, 2019 | The Condado Plaza Hilton | San Juan, Puerto Rico, USA

Conference Proceedings



Technical Program	
IOT Security	
Proof of Aliveness	1
<i>Chengta Jin, Zheng Yang, Marten van Dijk, Jianying Zhou</i>	
Co-Evaluation of Pattern Matching Algorithms on IoT Devices with Embedded GPUs	17
<i>Charalampos Stylianopoulos, Simon Kindstrom, Magnus Almgren, Olaf Landsiedel, Marina Papatriantafyllou</i>	
Aegis: A Context-aware Security Framework for Smart Home Systems	28
<i>Ami Kumar Sikder, Leonardo Babun, Hideoyuki Aka, A. Selcuk Uluoguz</i>	
Defeating Hidden Audio Channel Attacks on Voice Assistants via Audio-Induced Surface Vibrations ..	42
<i>Chen Wang, S Abhishek Anand, Jian Liu, Peyton Walker, Yingying Chen, Nitesh Saxena</i>	
Binary Analysis & Defense	
TF-BIV: Transparent and Fine-grained Binary Integrity Verification in the Cloud	57
<i>Fangjie Jiang, Quanwei Cai, Jingqiang Liu, Bo Luo, Le Guan, Ziqiang Ma</i>	
Nibbler: Debloating Binary Shared Libraries	70
<i>Ioannis Agadokos, Di Jin, David Williams-King, Vasileios P. Kemerlis, Georgios Portokalidis</i>	
Function Boundary Detection in Stripped Binaries	84
<i>Jim Alves-Foss, Jia Song</i>	
VPS: Excavating High-Level C++ Constructs from Low-Level Binaries to Protect Dynamic Dispatching	97
<i>Andre Pawlowski, Victor van der Veen, Dennis Andriese, Erik van der Kouwe, Thorsten Holt, Cristiano Giuffrida, Herbert Bos</i>	
AI Security	
STRIP: A Defence Against Trojan Attacks on Deep Neural Networks	113
<i>Yansong Gao, Chang Xu, Dersai Wang, Shiping Chen, Dumith C. Ranasinghe, Surya Nepal</i>	
How to Prove Your Model Belongs to You: A Blind-Watermark based Framework to Protect Intellectual Property of DNN	126
<i>Zheng Li, Chengwu Hu, Yang Zhang, Shangqing Gao</i>	
D2NN: A Fine-Grained Dual Modular Redundancy Framework for Deep Neural Networks	138
<i>Yu Li, Yunnan Liu, Min Li, Ye Tian, Bo Luo, Qiang Xu</i>	
Model Inversion Attacks Against Collaborative Inference	148
<i>Ze Cheng He, Tianwei Zhang, Ruby B. Lee</i>	
Software Security I	
Systematic Comparison of Symbolic Execution Systems: Intermediate Representation and its Generation	163
<i>Sebastian Poepplau, Aurelien Francillon</i>	
How to Kill Symbolic Deobfuscation for Free (or: Unleashing the Potential of Path-Oriented Protections)	177
<i>Mahlida Olivier, Sebastian Bardin, Richard Bonichon, Jean-Yves Marion</i>	
Sleak: Automating Address Space Layout Derandomization	190
<i>Christophe Hauser, Jayakrishna Menon, Yun Shoshitaishvili, Ruoyu Wang, Giovanni Vigna, Christopher Kruegel</i>	





December 9-13, 2019 | The Condado Plaza Hilton | San Juan, Puerto Rico, USA

Via ACM Digital Library (thru Friday)

The screenshot shows a web browser window with the URL <https://dl.acm.org/citation.cfm?id=3359789>. The page title is "Proceedings of the 35th Annual Computer Security Applications Conference". The conference chair is listed as David Balenson from SRI International. The publication information includes "ACSAC '19 2019 Annual Computer Security Applications Conference, San Juan, PR, USA — December 09 - 13, 2019". A "Bibliometrics" section shows: Citation Count: 0, Downloads (cumulative): 180, Downloads (12 Months): 180, and Downloads (6 Weeks): 180. The page also features a "Tools and Resources" sidebar with options for TOC Service, Save to Binder, and Export Formats.

<https://www.acsac.org/2019/proceedings>



<https://dl.acm.org/citation.cfm?id=3359789>



December 9-13, 2019 | The Condado Plaza Hilton | San Juan, Puerto Rico, USA

Via ACSAC List of Accepted Papers (Indefinitely)

The screenshot shows a web browser window with the URL <https://www.acsac.org/2019/program/papers/>. The page header includes the ACSAC 2019 logo, the dates "December 9-13, 2019 • San Juan", and navigation links for "Archive", "FAQs", and "Mailing List". A search bar is present with the placeholder text "search on duckduckgo". The main navigation menu includes "Submissions", "Workshops", "Committees", "Program" (which is underlined), "Venue", and "Registration". The main content area is titled "Accepted Papers" and contains the following text:

The following technical papers have been accepted for this year's program. ACM will enable access to the papers just prior to the event.

[STRIP: A Defence Against Trojan Attacks on Deep Neural Networks](#)
Yansong (Garrison) Gao (NJUST, China and Data61, Australia); Chang Xu (Data61, CSIRO, Sydney, Australia); Derui Wang (Swinburne University of Technology, Australia); Shiping Chen (Data61, CSIRO, Sydney, Australia); Damith C. Ranasinghe (Auto-ID Lab, The School of Computer Science, The University of Adelaide); Nepal Surya (Data61 CSIRO Australia)

[MalRank: A Measure of Maliciousness in SIEM-based Knowledge Graphs](#)
Pejman Najafi, Alexander Muehle, Wenzel Puenster, Feng Cheng, and Christoph Meinel (Hasso Plattner Institute)

[Survivor: A Fine-Grained Intrusion Response and Recovery Approach for Commodity Operating Systems](#)
Ronny Chevalier (HP Labs, CentraleSupélec / Inria / CNRS / IRISA); David Plaquin and Chris Dalton (HP Labs); Guillaume Hiet (CentraleSupélec / Inria / CNRS / IRISA)

[https://www.acsac.org/2019/
program/papers/](https://www.acsac.org/2019/program/papers/)



December 9-13, 2019 | The Condado Plaza Hilton | San Juan, Puerto Rico, USA

Compendium (Front Matter and Papers)

https://emailwsu-my.sharepoint.com/:f:/g/personal/a_hahn_wsu_edu/En4qE75UeEdPni68serU2esBxvs29De46plzR8VLiWvM6A?e=5FcNmo →

<https://bit.ly/2E41xj1>



December 9-13, 2019 | The Condado Plaza Hilton | San Juan, Puerto Rico, USA

Organizing Committee

- David Balenson, SRI International (Conference Chair)
 - Guofei Gu, Texas A&M University (Program Chair)
 - Danfeng (Daphne) Yao, Virginia Tech (Program Co-Chair)
 - Larry Wagoner, NSA (Case Studies Co-Chair)
 - Randy Smith, Boeing (Case Studies Co-Chair)
 - Charles Payne, Adventium (Panels Chair)
 - Tomas Vagoun, NITRD (National Interest Track Chair)
 - Adam Aviv, USNA (Posters & WiP Co-Chair)
 - Kevin Roundy, Symantec (Posters & WiP Co-Chair)
 - Harvey Rubinovitz, MITRE (Workshops Chair)
 - Daniel P. Faigin, Aerospace (Training Workshops Chair)
 - Dan Thomsen, SIFT (Knowledge Coordinator)
 - Jeremy Epstein, NSF (Local Arrangements)
 - Adam Hahn, WSU (Proceedings Co-Coordinator)
 - Ali Tamimi, WSU (Proceedings Co-Coordinator)
 - Daniel Zappala, Brigham Young (Publicity Coordinator)
 - Peter Mayer, Karlsruhe Institute of Technology
 - Karen Davis (Registration Coordinator)
 - Thomas Moyer, UNC Charlotte (Student Conferencships)
 - Romke de Haan, Guidepoint Security (Web Advisor)
 - Robert H'obbes' Zakon, Zakon Group LLC (Web Advisor)
 - Marshall Abrams, Retired (ACSAC Curmudgeon and Treasurer)
-
- Mike Moshell, Carole Mann, Sharri Hanacek, Registration Systems Lab (Registration)



December 9-13, 2019 | The Condado Plaza Hilton | San Juan, Puerto Rico, USA

Steering Committee

- Marshall Abrams, MITRE
- David Balenson, SRI International
- Davide Balzarotti, Eurecom
- Kevin Butler, Univ. of Florida
- Juan Caballero, IMDEA Software Institute
- Jeremy Epstein, National Science Foundation
- Daniel P. Faigin, The Aerospace Corporation
- Carrie Gates, Bank of America
- Guofei Gu, Texas A&M University
- Ann Marmor-Squires, The Sq Group
- Charles Payne, Adventium Labs
- Wil Robertson, Northeastern Univ.
- Harvey Rubinovitz, MITRE
- Steve Schwab, USC-ISI
- Cristina Serban, AT&T Security Research Center
- Dan Thomsen, SIFT
- Robert H'obbes' Zakon, Zakon Group LLC



December 9-13, 2019 | The Condado Plaza Hilton | San Juan, Puerto Rico, USA

Keep Up with ACSAC on Social Media



Twitter

– @ACSAC_Conf

– https://twitter.com/ACSAC_Conf



Facebook

– <https://www.facebook.com/acsaconf/>

– <https://www.facebook.com/groups/acsaconfattendeess/>



LinkedIn

– <https://www.linkedin.com/in/acsaconf-chair/>