

2022 IEEE Security and Privacy Workshops (SPW 2022)

**San Francisco, California, USA
22 – 26 May 2022**



**IEEE Catalog Number: CFP22SPX-POD
ISBN: 978-1-6654-9644-5**

**Copyright © 2022 by the Institute of Electrical and Electronics Engineers, Inc.
All Rights Reserved**

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

| | |
|-------------------------|-------------------|
| IEEE Catalog Number: | CFP22SPX-POD |
| ISBN (Print-On-Demand): | 978-1-6654-9644-5 |
| ISBN (Online): | 978-1-6654-9643-8 |
| ISSN: | 2639-7862 |

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

2022 IEEE Security and Privacy Workshops (SPW) SPW 2022

Table of Contents

SecWeb: Workshop on Designing Security for the Web

| | |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| To Hash or not to Hash: A Security Assessment of CSP's Unsafe-Hashes Expression | 1 |
| <i>Peter Stolz (Saarland University & Bitahoy GmbH), Sebastian Roth (CISPA Helmholtz Center for Information Security), and Ben Stock (CISPA Helmholtz Center for Information Security)</i> | |
| A Client-Side Seat to TLS Deployment | 13 |
| <i>Mortiz Birghan (Mozilla Corporation) and Thyla van der Merwe (ETH Zurich)</i> | |
| Towards Improving the Deprecation Process of Web Features Through Progressive Web Security... | 20 |
| <i>Tom Van Goethem (imec-DistriNet, KU Leuven) and Wouter Joosen (imec-DistriNet, KU Leuven)</i> | |
| Measuring Developers' Web Security Awareness from Attack and Defense Perspectives | 31 |
| <i>Merve Sahin (SAP Security Research, France), Tolga Ünlü (Abertay University, United Kingdom), Cédric Hébert (SAP Security Research, France), Lynsay A. Shepherd (Abertay University, United Kingdom), Natalie Coull (Abertay University, United Kingdom), and Colin McLean (Abertay University, United Kingdom)</i> | |
| "It Builds Trust with the Customers" - Exploring User Perceptions of the Padlock Icon in Browser UI | 44 |
| <i>Emanuel von Zezschwitz (Google Inc.), Serena Chen (Google Inc.), and Emily Stark (Google Inc.)</i> | |
| yoU aRe a Liar://A Unified Framework for Cross-Testing URL Parsers | 51 |
| <i>Dashmeet Kaur Ajmani (North Carolina State University), Igibek Koishybayev (North Carolina State University), and Alexandros Kapravelos (North Carolina State University)</i> | |

DLS: Deep Learning and Security Workshop

| | |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Misleading Deep-Fake Detection with GAN Fingerprints | 59 |
| <i>Vera Wesselkamp (Technische Universität Braunschweig, Germany), Konrad Rieck (Technische Universität Braunschweig, Germany), Daniel Arp (Technische Universität Berlin, Germany), and Erwin Quiring (Technische Universität Braunschweig, Germany)</i> | |
| Concept-Based Adversarial Attacks: Tricking Humans and Classifiers Alike | 66 |
| <i>Johannes Schneider (University of Liechtenstein) and Giovanni Apruzzese (University of Liechtenstein)</i> | |

| | |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Ares: A System-Oriented Wargame Framework for Adversarial ML | 73 |
| <i>Farhan Ahmed (Stony Brook University), Pratik Vaishnavi (Stony Brook University), Kevin Eykholt (IBM Research), and Amir Rahmati (Stony Brook University)</i> | |
| Parameterizing Activation Functions for Adversarial Robustness | 80 |
| <i>Sihui Dai (Princeton University, USA), Saeed Mahloujifar (Princeton University, USA), and Prateek Mittal (Princeton University, USA)</i> | |

LangSec: The 8th Workshop on Language-theoretic Security and Applications

| | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Anomaly Detection with Neural Parsers That Never Reject | 88 |
| <i>Alexander Grushin (Galois, Inc.) and Walt Woods (Galois, Inc.)</i> | |
| Statistical Detection of Format Dialects Using the Weighted Dowker Complex | 98 |
| <i>Michael Robinson (American University, USA), Cory Anderson (BAE Systems FAST Labs, USA), Letitia W. Li (BAE Systems FAST Labs, USA), and Steve Huntsman (Arlington, VA)</i> | |
| Certified Parsing of Dependent Regular Grammars | 113 |
| <i>John Sarracino (Cornell University), Gang Tan (The Pennsylvania State University), and Greg Morrisett (Cornell Tech)</i> | |
| A Secure Parser Generation Framework for IoT Protocols on Microcontrollers | 124 |
| <i>Sameed Ali (Dartmouth College, USA) and Sean Smith (Dartmouth College, USA)</i> | |
| A Format-Aware Reducer for Scriptable Rewriting of PDF Files | 136 |
| <i>Prashant Anantharaman (Dartmouth College, NH), Steven Cheung (SRI International, USA), Nicholas Boorman (SRI International, USA), and Michael E. Locasto (Narf Industries, USA)</i> | |
| Research Report: Strengthening Weak Links in the PDF Trust Chain | 152 |
| <i>Mark Tullsen (Galois, Inc.), William Harris (Galois, Inc.), and Peter Wyatt (PDF Association)</i> | |
| Research Report: Progress on Building a File Observatory for Secure Parser Development | 168 |
| <i>Tim Allison (Jet Propulsion Laboratory, California Institute of Technology, USA), Wayne Burke (Jet Propulsion Laboratory, California Institute of Technology, USA), Dustin Graf (Jet Propulsion Laboratory, California Institute of Technology, USA), Chris Mattmann (Jet Propulsion Laboratory, California Institute of Technology, USA), Anastasija Mensikova (Jet Propulsion Laboratory, California Institute of Technology, USA), Mike Milano (Jet Propulsion Laboratory, California Institute of Technology, USA), Philip Southam (Jet Propulsion Laboratory, California Institute of Technology, USA), and Ryan Stonebraker (Jet Propulsion Laboratory, California Institute of Technology, USA)</i> | |

| | |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Capturing the iccMAX Calculatorelement: A Case Study on Format Design | 176 |
| <i>Vijay H. Kothari (Dartmouth College, USA), Prashant Anantharaman (Dartmouth College, USA), Sean W. Smith (Dartmouth College, USA), Briland Hitaj (SRI International, USA), Prashanth Mundkur (SRI International, USA), Natarajan Shankar (SRI International, USA), Letitia W. Li (BAE Systems FAST Labs, USA), Iavor Diatchki (Galois Inc., USA), and William Harris (Galois Inc., USA)</i> | |
| Research Report: On the Feasibility of Retrofitting Operating Systems with Generated Protocol Parsers | 198 |
| <i>Wayne Wang (Middlebury College) and Peter C. Johnson (Middlebury College)</i> | |

SafeThings: Workshop on the Internet of Safe Things

| | |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| BLE-Doubt: Smartphone-Based Detection of Malicious Bluetooth Trackers | 208 |
| <i>Jimmy Briggs (Unaffiliated) and Christine Geeng (University of Washington)</i> | |
| Biometric Identification System Based on Object Interactions in Internet of Things Environments | 215 |
| <i>Klaudia Krawiecka (University of Oxford, United Kingdom), Simon Birnbach (University of Oxford, United Kingdom), Simon Eberz (University of Oxford, United Kingdom), and Ivan Martinovic (University of Oxford, United Kingdom)</i> | |
| Capabilities-Based Access Control for IoT Devices Using Verifiable Credentials | 222 |
| <i>Nikos Fotiou (Athens University of Economics and Business, Greece), Vasilios A. Siris (Athens University of Economics and Business, Greece), George C. Polyzos (Athens University of Economics and Business, Greece), Yki Kortensniemi (Aalto University, Finland), and Dmitrij Lagutin (Aalto University, Finland)</i> | |
| Using 3D Shadows to Detect Object Hiding Attacks on Autonomous Vehicle Perception | 229 |
| <i>Zhongyuan Hau (Imperial College London, UK), Soteris Demetriou (Imperial College London, UK), and Emil C. Lupu (Imperial College London, UK)</i> | |
| AutoCPS: Control Software Dataset Generation for Semantic Reverse Engineering | 236 |
| <i>Haoda Wang (University of Southern California, USA), Christohpe Hauser (University of Southern California, USA), and Luis Garcia (University of Southern California, USA)</i> | |
| You Can't Protect What You Don't Understand: Characterizing an Operational Gas SCADA Network | 243 |
| <i>Xi Qin (University of California, Santa Cruz, USA), Martin Rosso (Eindhoven University of Technology, The Netherlands), Alvaro A. Cardenas (University of California, Santa Cruz, USA), Sandro Etalle (Eindhoven University of Technology, The Netherlands), Jerry den Hartog (Eindhoven University of Technology, The Netherlands), and Emmanuele Zambon (Eindhoven University of Technology, The Netherlands)</i> | |

| | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Towards Wireless Spiking of Smart Locks | 251 |
| <i>Abdullah Z. Mohammed (Virginia Tech, USA), Alok Singh (Virginia Tech, USA), Gökçen Y Dayanıklı (Qualcomm, USA), Ryan Gerdes (Virginia Tech, USA), Mani Mina (Iowa State University, USA), and Ming Li (University of Arizona, USA)</i> | |
| Face Recognition Systems: Are you Sure they only Consider Your Face? | 258 |
| <i>Pavan Srihari Darbha (BITS-Pilani, India), Mauro Conti (University of Padova, Italy), Eleonora Losiouk (University of Padova, Italy), and Rajib Ranjan Maiti (BITS-Pilani, India)</i> | |

WOOT: Workshop on Offensive Technologies

| | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Abusing Trust: Mobile Kernel Subversion via TrustZone Rootkits | 265 |
| <i>Daniel Marth (RISE – Research Industrial Systems Engineering GmbH; Research group for Industrial Software, TU Wien), Clemens Hlauschek (RISE – Research Industrial Systems Engineering GmbH; Research group for Industrial Software, TU Wien), Christian Schanes (RISE – Research Industrial Systems Engineering GmbH; Research group for Industrial Software, TU Wien), and Thomas Grechenig (RISE – Research Industrial Systems Engineering GmbH; Research group for Industrial Software, TU Wien)</i> | |
| Exploring Widevine for Fun and Profit | 277 |
| <i>Gwendal Patat (Univ Rennes, France), Mohamed Sabt (Univ Rennes, France), and Pierre-Alain Fouque (Univ Rennes, France)</i> | |
| Hack the Heap: Heap Layout Manipulation Made Easy | 289 |
| <i>Jordy Gennissen (University of London) and Dan O’Keeffe (University of London)</i> | |
| AirTag of the Clones: Shenanigans with Liberated Item Finders | 301 |
| <i>Thomas Roth (Leveldown Security), Fabian Freyer (Independent Researcher), Matthias Hollick (SEEMOO, TU Darmstadt), and Jiska Classen (SEEMOO, TU Darmstadt)</i> | |
| Clairvoyance: Exploiting Far-Field EM Emanations of GPU to "See" Your DNN Models Through Obstacles at a Distance | 312 |
| <i>Sisheng Liang (Clemson University, USA), Zihao Zhan (University of Florida, USA), Fan Yao (University of Central Florida, USA), Long Cheng (Clemson University, USA), and Zhenkai Zhang (Clemson University, USA)</i> | |
| DABANGG: A Case for Noise Resilient Flush-Based Cache Attacks | 323 |
| <i>Anish Saxena (Georgia Institute of Technology) and Biswabandan Panda (Indian Institute of Technology Bombay)</i> | |
| Interactive History Sniffing with Dynamically-Generated QR Codes and CSS Difference Blending | 335 |
| <i>Keith O’Neal (University of St. Thomas, USA) and Scott Yilek (University of St. Thomas, USA)</i> | |
| On the Security of Parsing Security-Relevant HTTP Headers in Modern Browsers | 342 |
| <i>Hendrik Siewert (Paderborn University), Martin Kretschmer (IT.NRW), Marcus Niemietz (Niederrhein University of Applied Science), and Juraj Somorovsky (Paderborn University)</i> | |

| | |
|----------------------------------------------------------------------------------|------------|
| On the Insecurity of Vehicles Against Protocol-Level Bluetooth Threats | 353 |
| <i>Daniele Antonioli (EURECOM, France) and Mathias Payer (EPFL, Switzerland)</i> | |
| Author Index | 363 |