

# **2021 IEEE Security and Privacy Workshops (SPW 2021)**

**Virtual Conference  
27 May 2021**



**IEEE Catalog Number: CFP21SPX-POD**  
**ISBN: 978-1-6654-3733-2**

**Copyright © 2021 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:	CFP21SPX-POD
ISBN (Print-On-Demand):	978-1-6654-3733-2
ISBN (Online):	978-1-6654-3732-5

**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](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

# 2021 IEEE Symposium on Security and Privacy Workshops **SPW 2021**

## Table of Contents

Message from the General Chair .xi.....  
Message from the Workshop Chair .xv.....  
Workshop Organizers .xvii.....

### **6th International Workshop on Traffic Measurements for Cybersecurity (WTMC 2021)**

Discovering and Measuring Malicious URL Redirection Campaigns from Fake News Domains .1.....  
*Zhouhan Chen (New York University, USA) and Freire Juliana (New York University, USA)*

Troubleshooting an Intrusion Detection Dataset: The CICIDS2017 Case Study .7.....  
*Gints Engelen (imec-DistriNet, KU Leuven, Belgium), Vera Rimmer (imec-DistriNet, KU Leuven, Belgium), and Wouter Joosen (imec-DistriNet, KU Leuven, Belgium)*

Training Regime Influences to Semi-Supervised Learning for Insider Threat Detection .13.....  
*Duc C. Le (Dalhousie University, Canada), Nur Zincir-Heywood (Dalhousie University, Canada), and Malcolm Heywood (Dalhousie University, Canada)*

Examining Traffic Microstructures to Improve Model Development .19.....  
*Henry Clausen (University of Edinburgh, UK) and David Aspinall (University of Edinburgh, UK)*

On the Feasibility of Short-Lived Dynamic Onion Services .25.....  
*Tobias Höller (Johannes Kepler University Linz), Thomas Raab (Johannes Kepler University Linz), Michael Roland (Johannes Kepler University Linz), and René Mayrhofer (Johannes Kepler University Linz)*

AMon: A Monitoring Multidimensional Feature Application to Secure Android Environments .31...  
*J. A. Gómez-Hernández (Dept. Languages and Computer Systems, Spain), P. García-Teodoro (Dept. Signal Theory, Telematics and Communications, Spain), J. A. Holgado-Terriza (Dept. Languages and Computer Systems, Spain), G. Maciá-Fernandez (Dept. Signal Theory, Telematics and Communications, Spain), J. Camacho-Páez (Dept. Signal Theory, Telematics and Communications, Spain), and M. Robles-Carrillo (Dept. International Law and International Relations, Spain)*

DPI Solutions in Practice: Benchmark and Comparison .37.....  
*Tommaso Rescio (Politecnico di Torino, Italy), Thomas Favale (Politecnico di Torino, Italy), Francesca Soro (Politecnico di Torino, Italy), Marco Mellia (Politecnico di Torino, Italy), and Idilio Drago (University of Turin, Italy)*

Revisiting the Pervasiveness of Weak Keys in Network Devices .43.....  
*Philippe Elbaz-Vincent (Univ. Grenoble Alpes, France) and Mohamed Traoré (Uni. Grenoble Alpes, France)*

## DLS 2021: 4th Deep Learning and Security Workshop

Innocent Until Proven Guilty (IUPG): Building Deep Learning Models with Embedded Robustness to Out-of-Distribution Content .49.....  
*Brody Kutt (Palo Alto Networks, California), William Hewlett (Palo Alto Networks, California), Oleksii Starov (Palo Alto Networks, California), and Yuchen Zhou (Palo Alto Networks, California)*

SAFELearn: Secure Aggregation for Private FEderated Learning .56.....  
*Hossein Fereidooni (Technical University of Darmstadt, Germany), Samuel Marchal (Aalto University and F-Secure Corporation, Finland), Markus Miettinen (Technical University of Darmstadt, Germany), Azalia Mirhoseini (Google, USA), Helen Möllering (Technical University of Darmstadt, Germany), Thien Duc Nguyen (Technical University of Darmstadt, Germany), Phillip Rieger (Technical University of Darmstadt, Germany), Ahmad-Reza Sadeghi (Technical University of Darmstadt, Germany), Thomas Schneider (Technical University of Darmstadt, Germany), Hossein Yalame (Technical University of Darmstadt, Germany), and Shaza Zeitouni (Technical University of Darmstadt, Germany)*

Applying Deep Learning to Combat Mass Robocalls .63.....  
*Sharbani Pandit (Georgia Institute of Technology, USA), Jienan Liu (University of Georgia, USA), Roberto Perdisci (Georgia Institute of Technology; University of Georgia, USA), and Mustaque Ahamad (Georgia Institute of Technology, USA)*

MMGuard: Automatically Protecting On-Device Deep Learning Models in Android Apps .71.....  
*Jiayi Hua (Beijing University of Posts and Telecommunications, China), Yuanchun Li (Microsoft Research Asia, China), and Haoyu Wang (Beijing University of Posts and Telecommunications, China)*

BODMAS: An Open Dataset for Learning based Temporal Analysis of PE Malware .78.....  
*Limin Yang (University of Illinois at Urbana-Champaign), Arridhana Ciptadi (Blue Hexagon), Ihar Laziuk (Blue Hexagon), Ali Ahmadzadeh (Blue Hexagon), and Gang Wang (University of Illinois at Urbana-Champaign)*

Binary Black-Box Attacks Against Static Malware Detectors with Reinforcement Learning in Discrete Action Spaces .85.....  
*Mohammadreza Ebrahimi (University of Arizona, USA), Jason Pacheco (University of Arizona, USA), Weifeng Li (University of Georgia, USA), James Lee Hu (University of Arizona, USA), and Hsinchun Chen (University of Arizona, USA)*

# LangSec 2021: Seventh Workshop on Language-Theoretic Security

## Research Papers

Verbatim: A Verified Lexer Generator .92.....	
<i>Derek Egolf (Tufts University, USA), Sam Lasser (Tufts University, USA), and Kathleen Fisher (Tufts University, USA)</i>	
Formal Language Theory for Practical Security: Extended Abstract .101.....	
<i>Andreas Jakoby (Bauhaus-Universität Weimar), Jannis Leuther (Bauhaus-Universität Weimar), and Stefan Lucks (Bauhaus-Universität Weimar)</i>	
Formal Synthesis of Filter Components for Use in Security-Enhancing Architectural Transformations .111.....	
<i>David S. Hardin (Collins Aerospace, USA) and Konrad L. Slind (Collins Aerospace, USA)</i>	
Research Report: Building a File Observatory for Secure Parser Development .121.....	
<i>Tim Allison (Jet Propulsion Laboratory, California Institute of Technology, USA), Wayne Burke (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), Philip Southam (Jet Propulsion Laboratory, California Institute of Technology, USA), and Ryan Stonebraker (Jet Propulsion Laboratory, California Institute of Technology, USA)</i>	
Research Report: Parsing PEGs with Length Fields in Software and Hardware .128.....	
<i>Zephyr S. Lucas (Dartmouth College, USA), Joanna Y. Liu (Dartmouth College, USA), Prashant Anantharaman (Dartmouth College, USA), and Sean W. Smith (Dartmouth College, USA)</i>	
Formal Languages, Deep Learning, Topology and Algebraic Word Problems .134.....	
<i>Joshua Ackerman (Dartmouth College, USA) and George Cybenko (Dartmouth College, USA)</i>	
Accessible Formal Methods for Verified Parser Development .142.....	
<i>Letitia W. Li (BAE Systems, USA), Greg Eakman (BAE Systems, USA), Elias J.M. Garcia (Special Circumstances, Belgium), and Sam Atman (Special Circumstances, Belgium)</i>	
Differential Analysis of x86-64 Instruction Decoders .152.....	
<i>William Woodruff (Trail of Bits, USA), Niki Carroll (George Mason University, USA), and Sebastiaan Peters (Eindhoven University of Technology, The Netherlands)</i>	
Bohemia — A Validator for Parser Frameworks .162.....	
<i>Anish Paranjpe (Pennsylvania State University) and Gang Tan (Pennsylvania State University)</i>	
RL-GRIT: Reinforcement Learning for Grammar Inference .171.....	
<i>Walt Woods (Galois, Inc.)</i>	

Looking for Non-Compliant Documents using Error Messages from Multiple Parsers .184.....	
	<i>Michael Robinson (American University, USA)</i>
Mechanized Type Safety for Gradual Information Flow .194.....	
	<i>Tianyu Chen (Indiana University, USA) and Jeremy G. Siek (Indiana University, USA)</i>

## SafeThings 2021: IEEE Workshop on the Internet of Safe Things

### Technical Papers - Session 1

Alexa in Phishingland: Empirical Assessment of Susceptibility to Phishing Pretexting in Voice Assistant Environments .207.....	
	<i>Filipo Sharevski (DePaul University, USA) and Peter Jachim (DePaul University, USA)</i>
BLEKeeper: Response Time Behavior Based Man-in-the-Middle Attack Detection .214.....	
	<i>Muhammed Ali Yurdagul (TOBB-ETU, Turkey) and Husrev Taha Sencar (Qatar Computing Research Institute, HBKU, Qatar)</i>
LIRA-V: Lightweight Remote Attestation for Constrained RISC-V Devices .221.....	
	<i>Carlton Shepherd (University of London, United Kingdom), Konstantinos Markantonakis (University of London, United Kingdom), and Georges-Axel Jaloyan (PSL University, France)</i>
HybriDiagnostics: Evaluating Security Issues in Hybrid SmartHome Companion Apps .228.....	
	<i>Abhinav Mohanty (University of North Carolina at Charlotte, USA) and Meera Sridhar (University of North Carolina at Charlotte, USA)</i>
On the Safety Implications of Misordered Events and Commands in IoT Systems .235.....	
	<i>Furkan Goksel (Middle East Technical University), Muslum Ozgur Ozmen (Purdue University), Michael Reeves (Purdue University), Basavesh Shivakumar (Purdue University), and Z. Berkay Celik (Purdue University)</i>

### Demo Session

Demo: Attacking Multi-sensor Fusion based Localization in High-Level Autonomous Driving .242	
	<i>Junjie Shen (University of California, Irvine), Jun Yeon Won (University of California, Irvine), Zeyuan Chen (University of California, Irvine), and Qi Alfred Chen (University of California, Irvine)</i>
Demo: Security of Camera-Based Perception for Autonomous Driving under Adversarial Attack .243	
	<i>Christopher DiPalma (University of California, Irvine), Ningfei Wang (University of California, Irvine), Takami Sato (University of California, Irvine), and Qi Alfred Chen (University of California, Irvine)</i>

- Demo: Security of Deep Learning Based Automated Lane Centering under Physical-World Attack.244  
*Takami Sato (University of California, Irvine), Junjie Shen (University of California, Irvine), Ningfei Wang (University of California, Irvine), Yunhan Jack Jia (ByteDance), Xue Lin (Northeastern University), and Qi Alfred Chen (University of California, Irvine)*
- Demo: ROI Attacks on Traffic Light Detection in High-Level Autonomous Driving .245.....  
*Kanglan Tang (University of California, Irvine), Junjie Shen (University of California, Irvine), and Qi Alfred Chen (University of California, Irvine)*

## Technical Papers - Session 2

- A Containerization-Based Backfit Approach for Industrial Control System Resiliency .246.....  
*James Schaffter (The Johns Hopkins University, USA), Aviel Rubin (The Johns Hopkins University, USA), and Lanier Watkins (The Johns Hopkins University, USA)*
- HIOA-CPS: Combining Hybrid Input-Output Automaton and Game Theory for Security Modeling of Cyber-Physical Systems .253.....  
*Mustafa Abdallah (Purdue University), Sayan Mitra (University of Illinois at Urbana-Champaign), Shreyas Sundaram (Purdue University), and Saurabh Bagchi (Purdue University)*
- Protecting IoT Devices through Localized Detection of BGP Hijacks for Individual Things .260.....  
*DongInn Kim (Indiana University), Vafa Andalibi (Indiana University), and Jean Camp (Indiana University)*
- Egocentric Abstractions for Modeling and Safety Verification of Distributed Cyber-Physical Systems .268.....  
*Sung Woo Jeon (University of Illinois at Urbana-Champaign, USA) and Sayan Mitra (University of Illinois at Urbana-Champaign, USA)*

# SADFE 2021: Systematic Approaches to Digital Forensic Engineering

## Paper Session 1

- DeepFake-o-Meter: An Open Platform for DeepFake Detection .277.....  
*Yuezun Li (Ocean University of China, China), Cong Zhang (University of Chinese Academy of Sciences, China), Pu Sun (University of Chinese Academy of Sciences, China), Lipeng Ke (University at Buffalo, State University of New York, USA), Yan Ju (University at Buffalo, State University of New York, USA), Honggang Qi (University of Chinese Academy of Sciences, China), and Siwei Lyu (University at Buffalo, State University of New York, USA)*
- User Identification in Dynamic Web Traffic via Deep Temporal Features .282.....  
*Jihye Kim (Korea Army Academy, Republic of Korea) and John V. Monaco (Naval Postgraduate School, USA)*

Nomen est Omen - The Role of Signatures in Ascribing Email Author Identity with Transformer Neural Networks .291.....  
*Sudarshan Srinivasan (Oak Ridge National Laboratory, USA), Edmon Begoli (Oak Ridge National Laboratory, USA), Maria Mahbub (Oak Ridge National Laboratory, USA), and Kathryn Knight (Oak Ridge National Laboratory, USA)*

## Paper Session 2

Protected Process Light is not Protected: MemoryRanger Fills the Gap Again .298.....  
*Igor Korkin (Independent Researcher, Russian Federation)*

Machine Learning Based Approach for the Automated Mapping of Discovered Vulnerabilities to Adversarial Tactics .309.....  
*Yosra Lakhdhar (University of Carthage, Tunisia) and Slim Rekhis (University of Carthage, Tunisia)*

Forensic Analysis of Fitbit Versa: Android vs iOS .318.....  
*Joseph Williams (Merseyside Police's Digital Forensics Unit), Áine MacDermott (Liverpool John Moores University, UK), Kellyann Stamp (Liverpool John Moores University, UK), and Farkhund Iqbal (Zayed University, United Arab Emirates)*

## WOOT 2021: 15th IEEE Workshop on Offensive Technologies

BadUSB-C: Revisiting BadUSB with Type-C .327.....  
*Hongyi Lu (Southern University of Science and Technology), Yechang Wu (Southern University of Science and Technology), Shuqing Li (Southern University of Science and Technology), You Lin (Southern University of Science and Technology), Chanzu Zhang (Southern University of Science and Technology), and Fengwei Zhang (Southern University of Science and Technology)*

BlueMirror: Reflections on Bluetooth Pairing and Provisioning Protocols .339.....  
*Tristan Claverie (ANSSI, France) and José Lopes Esteves (ANSSI, France)*

An In-Memory Embedding of CPython for Offensive Use .352.....  
*Ateeq Sharfuddin (SCYTHE), Brian Chapman (SCYTHE), and Chris Balles (SCYTHE)*

Evaluation of the Executional Power in Windows using Return Oriented Programming .361.....  
*Daniel Uroz (University of Zaragoza, Spain) and Ricardo J. Rodríguez (University of Zaragoza, Spain)*

Identifying Valuable Pointers in Heap Data .373.....  
*James Roney (Harvard University, Cambridge), Troy Appel (Harvard University, Cambridge), Prateek Piniseti (Harvard University, Cambridge), and James Mickens (Harvard University, Cambridge)*

Empirical Study of PLC Authentication Protocols in Industrial Control Systems .383.....  
*Adeen Ayub (Virginia Commonwealth University, USA), Hyungkook Yoo (The University of New Orleans, USA), and Irfan Ahmed (Virginia Commonwealth University, USA)*



Your Censor is My Censor: Weaponizing Censorship Infrastructure for Availability Attacks .398...	
<i>Kevin Bock (University of Maryland), Pranav Bharadwaj (University of Maryland), Jasraj Singh (University of Maryland), and Dave Levin (University of Maryland)</i>	
Zero Conf Protocols and their Numerous Man in the Middle (MITM) Attacks .410.....	
<i>Dhia Farrah (Digital Security Department, EURECOM, France) and Marc Dacier (Digital Security Department, EURECOM, France)</i>	
A Low-Cost Attack Against the hCaptcha System .422.....	
<i>Md Imran Hossen (University of Louisiana at Lafayette, USA) and Xiali Hei (University of Louisiana at Lafayette, USA)</i>	
The Remote on the Local: Exacerbating Web Attacks via Service Workers Caches .432.....	
<i>Marco Squarcina (TU Wien), Stefano Calzavara (Università Ca' Foscari Venezia &amp; OWASP), and Matteo Maffei (TU Wien)</i>	
SEVerity: Code Injection Attacks against Encrypted Virtual Machines .444.....	
<i>Mathias Morbitzer (Fraunhofer AISEC), Sergej Proskurin (Technical University of Munich), Martin Radev (Fraunhofer AISEC), Marko Dorfhuber (Technical University of Munich), and Erick Quintanar Salas (Fraunhofer AISEC)</i>	
undeSErVed Trust: Exploiting Permutation-Agnostic Remote Attestation .456.....	
<i>Luca Wilke (University of Lübeck, Germany), Jan Wichelmann (University of Lübeck, Germany), Florian Sieck (University of Lübeck, Germany), and Thomas Eisenbarth (University of Lübeck, Germany)</i>	
<b>Author Index</b> .467.....	