2020 IEEE Security and Privacy Workshops (SPW 2020)

San Francisco, California, USA
21 May 2020

IEEE Catalog Number: CFP20SPX-POD
ISBN: 978-1-7281-9347-2

Copyright © 2020 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:	CFP20SPX-POD
ISBN (Print-On-Demand):	978-1-7281-9347-2
ISBN (Online):	978-1-7281-9346-5

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
Web: www.proceedings.com

2020 Symposium on Security and Privacy Workshops (SPW)

SPW 2020

Table of Contents

Message from the Security and Privacy General Chair xi
Message from the Security and Privacy Workshops General Chair xiv
Workshop Organizers xvi
Message from the DLS 2020 Chairs xvii
DLS 2020 Organization xviii
Message from the SafeThings 2020 Chairs xx
SafeThings 2020 Organization xxi
Message from the CReSCT 2020 Chairs xxiii
CReSCT 2020 Program Committee xxiv
Message from the WAAS 2020 Chairs xxv
WAAS 2020 Organization xxvi
Message from the LangSec 2020 Chairs xxviii
LangSec 2020 Organization xxix

DLS 2020: 3rd Deep Learning and Security Workshop

Learning from Context: A Multi-view Deep Learning Architecture for Malware Detection 1
Adarsh Kyadige (Sophos), Ethan Rudd (FireEye Inc.), and Konstantin Berlin (Sophos)

Attributing and Detecting Fake Images Generated by Known GANs 8
Matthew Joslin (University of Texas at Dallas, USA) and Shuang Hao (University of Texas at Dallas, USA)

Adversarial Attacks against LipNet: End-to-End Sentence Level Lipreading 15
Mahir Jethanandani (University of California, Berkeley) and Derek Tang (University of California, Berkeley)

Detecting Cyber Threats in Non-English Hacker Forums: An Adversarial Cross-Lingual Knowledge Transfer Approach 20
Mohammadreza Ebrahimi (University of Arizona, USA), Sagar Samtani (Indiana Univeristy, USA), Yidong Chai (Tsinghua University, China), and Hsinchun Chen (University of Arizona, USA)

RTA3: A Real Time Adversarial Attack on Recurrent Neural Networks 27
Christopher Serrano (HRL Laboratories, USA), Pape Sylla (HRL Laboratories, USA), Sicun Gao (University of California San Diego, USA), and Michael Warren (HRL Laboratories, USA)

Minimum-Norm Adversarial Examples onKNN and KNN-Based Models 34
Chawin Sitawarin (UC Berkeley) and David Wagner (UC Berkeley)

Backdooring and Poisoning Neural Networks with Image-Scaling Attacks .41
Erwin Quiring (TU Braunschweig, Germany) and Konrad Rieck (TU Braunschweig, Germany)

SentiNet: Detecting Localized Universal Attacks against Deep Learning Systems .48
Edward Chou (Carnegie Mellon University), Florian Tramèr (Stanford University), and Giancarlo Pellegrino (CISPA Helmholtz Center for Information Security)

Clipped BagNet: Defending against Sticker Attacks with Clipped Bag-of-Features .55
Zhanyuan Zhang (University of California, Berkeley), Benson Yuan (University of California, Berkeley), Michael McCoyd (University of California, Berkeley), and David Wagner (University of California, Berkeley)

On the Robustness of Cooperative Multi-agent Reinforcement Learning .62
Jieyu Lin (University of Toronto), Kristina Dzeparoska (University of Toronto), Sai Qian Zhang (Harvard University), Alberto Leon-Garcia (University of Toronto), and Nicolas Papernot (University of Toronto and Vector Institute)

Adversarial Machine Learning - Industry Perspectives .69
Ram Shankar Siva Kumar (Microsoft, USA), Magnus Nyström (Microsoft, USA), John Lambert (Microsoft, USA), Andrew Marshall (Microsoft, USA), Andi Comissoneru (Microsoft, USA), Matt Swann (Microsoft, USA), Sharon Xia (Microsoft, USA), and Mario Goertzel (Microsoft, USA)

SafeThings 2020: IEEE Workshop on the Internet of Safe Things

A Case Study of the Security Vetting Process of Smart-Home Assistant Applications .76
Hang Hu (Virginia Tech), Limin Yang (University of Illinois at Urbana-Champaign), Shihan Lin (Fudan University), and Gang Wang (University of Illinois at Urbana-Champaign)

Privacy-Preserving Continuous Tumour Relapse Monitoring Using In-Body Radio Signals .82
Sam Hylamia (Uppsala University), Wenqing Yan (Uppsala University), Andre Teixeira (Uppsala University), Noor Badariah Asan (Uppsala University), Mauricio Perez (Uppsala University), Robin Augustine (Uppsala University), and Thiemo Voigt (Uppsala University)

On the Feasibility of Acoustic Attacks Using Commodity Smart Devices .88
Matthew Wixey (University College London, UK), Emiliano De Cristofaro (University College London, UK), and Shane D Johnson (University College London, UK)

Electromagnetic Sensor and Actuator Attacks on Power Converters for Electric Vehicles .98
Gokcen Yilmaz Dayanikli (Virginia Tech, USA), Rees R. Hatch (Utah State University, USA), Ryan M. Gerdes (Virginia Tech, USA), Hongjie Wang (Utah State University, USA), and Regan Zane (Utah State University, USA)

Never Ending Story: Authentication and Access Control Design Flaws in Shared IoT Devices .104
Blake Janes (Florida Institute of Technology), Heather Crawford (Florida Institute of Technology), and TJ O'Connor (Florida Institute of Technology)

On Using Camera-Based Visible Light Communication for Security Protocols 110
Wen-Yi Chu (National Taiwan University, Taiwan), Ting-Guang Yu (National Taiwan University, Taiwan), Yu-Kai Lin (National Taiwan University, Taiwan), Shao-Chuan Lee (National Taiwan University, Taiwan), and Hsu-Chun Hsiao (National Taiwan University, Taiwan)

Security Analysis of Networked 3D Printers 118
Matthew McCormack (Carnegie Mellon University, USA), Sanjay Chandrasekaran (University of California, Santa Barbara, USA), Guyue Liu (Carnegie Mellon University, USA), Tianlong Yu (Carnegie Mellon University, USA), Sandra DeVincent Wolf (Carnegie Mellon University, USA), and Vyas Sekar (Carnegie Mellon University, USA)

ELF Analyzer Demo: Online Identification for IoT Malwares with Multiple Hardware Architectures 126
Shin-Ming Cheng (National Taiwan University of Science and Technology), Tao Ban (National Institute of Information and Communications Technology), Jr-Wei Huang (National Taiwan University of Science and Technology), Bing-Kai Hong (National Taiwan University of Science and Technology), and Daisuke Inoue (National Institute of Information and Communications Technology)

Poster: Radiometric Signatures for Wireless Device Identification over Dynamic Channels 127
Wenqing Yan (Uppsala University), Thiemo Voigt (SICS, Swedish ICT), and Christian Rohner (Uppsala University)

CReSCT 2020: Cyber Resilient Supply Chain Technologies

Assessment of Cyber Security Implications of New Technology Integrations into Military Supply Chains 128
Theresa May Sobb (University of New South Wales) and Benjamin Turnbull (University of New South Wales)

Toward a Trustable, Self-Hosting Computer System 136
Gabriel Somlo (CERT - SEI, Carnegie Mellon University)

EM Fingerprints: Towards Identifying Unauthorized Hardware Substitutions in the Supply Chain Jungle 144
Constantinos Kolias (University of Idaho), Daniel Barbara (George Mason University), Craig Rieger (Idaho National Laboratory), and Jacob Ulrich (Idaho National Laboratory)

Binary Analysis with Architecture and Code Section Detection Using Supervised Machine Learning 152
Bryan Beckman (Idaho National Laboratory) and Jed Haile (Idaho National Laboratory)

Identifying Ubiquitious Third-Party Libraries in Compiled Executables Using Annotated and Translated Disassembled Code with Supervised Machine Learning 157
Jedediah Haile (Idaho National Laboratory, USA) and Sage Havens (Idaho National Laboratory, USA)

Modeling and Assessment of IoT Supply Chain Security Risks: The Role of Structural and Parametric Uncertainties .163
Timothy Kieras (New York University Tandon School of Engineering, USA), Muhammad Junaid Farooq (New York University Tandon School of Engineering, USA), and Quanyan Zhu (New York University Tandon School of Engineering, USA)

On-Chip Randomization for Memory Protection against Hardware Supply Chain Attacks to DRAM ... 171
H. Brett Meadows (University of Colorado Colorado Springs), Nathan Edwards (Resilience and Systems Security Engineering, The MITRE Corporation), and Sang-Yoon Chang (University of Colorado Colorado Springs)

WAAS 2020: Workshop on Assured Autonomous Systems

Using Taint Analysis and Reinforcement Learning (TARL) to Repair Autonomous Robot Software .181
Damian Lyons (Fordham University) and Saba Zara (Fordham University)

Partially Observable Games for Secure Autonomy .185
Mohamadreza Ahmadi (California Institute of Technology), Arun Viswanathan (NASA Jet Propulsion Laboratory), Michel D. Ingham (NASA Jet Propulsion Laboratory), Kymie Tan (NASA Jet Propulsion Laboratory), and Aaron D. Ames (California Institute of Technology)

Case Study: Safety Verification of an Unmanned Underwater Vehicle .189
Diego Manzanas Lopez (Vanderbilt University), Patrick Musau (Vanderbilt University), Nathaniel Hamilton (Vanderbilt University), Hoang-Dung Tran (Vanderbilt University), and Taylor Johnson (Vanderbilt University)

Automated Decision Systems for Cybersecurity and Infrastructure Security .196
Luanne Burns Chamberlain (The Johns Hopkins University Applied Physics Laboratory, USA), Lauren Eisenberg Davis (The Johns Hopkins University Applied Physics Laboratory, USA), Martin Stanley (Cybersecurity and Infrastructure Security Agency, USA), and Brian R. Gattoni (Cybersecurity and Infrastructure Security Agency, USA)

A Non-Cooperative Game Based Model for the Cybersecurity of Autonomous Systems .202
Farha Jahan (The University of Toledo), Weiqing Sun (The University of Toledo), and Quamar Niyaz (Purdue University Northwest)

Detecting Adversarial Examples in Learning-Enabled Cyber-Physical Systems using Variational Autoencoder for Regression .208
Feiyang Cai (Vanderbilt University, USA), Jiani Li (Vanderbilt University, USA), and Xenofon Koutsoukos (Vanderbilt University, USA)

A Smart City Internet for Autonomous Systems .215
Gregory Falco (Stanford University)

Fooling a Deep-Learning Based Gait Behavioral Biometric System 221
Honghao Guo (Johns Hopkins University Information Security Institute, USA), Zuo Wang (Johns Hopkins University Information Security Institute, USA), Benfang Wang (Johns Hopkins University Information Security Institute, USA), Xiangyang Li (Johns Hopkins University Information Security Institute, USA), and Devu Shila (Unknot.ID Inc. USA)

Trusted Confidence Bounds for Learning Enabled Cyber-Physical Systems 228
Dimitrios Boursinos (Vanderbilt University) and Xenofon Koutsoukos (Vanderbilt University)

A Framework for the Analysis of Deep Neural Networks in Autonomous Aerospace Applications using Bayesian Statistics 234
Yuning He (NASA Ames Research Center, USA) and Johann Schumann (SGT, Inc/KBR NASA Ames, USA)

Towards an AI-Based After-Collision Forensic Analysis Protocol for Autonomous Vehicles 240
Prinkle Sharma (University of Massachusetts Dartmouth), Umesh Siddanagaiah (University of Massachusetts Dartmouth), and Gökhan Kul (University of Massachusetts Dartmouth)

Mission Assurance for Autonomous Undersea Vehicles 244
Karl Siil (JHU Applied Physics Laboratory, USA), Aviel Rubin (Johns Hopkins University, USA), Matthew Elder (JHU Applied Physics Laboratory, USA), Anton Dahbura (Johns Hopkins University, USA), Matthew Green (Johns Hopkins University, USA), and Lanier Watkins (Johns Hopkins University, USA)

Out-of-Distribution Detection in Multi-label Datasets using Latent Space of β-VAE 250
Vijaya Kumar Sundar (Nanyang Technological University), Shreyas Ramakrishna (Vanderbilt University), Zahra Rahiminasab (Nanyang Technological University), Arvind Easwaran (Nanyang Technological University), and Abhishek Dubey (Vanderbilt University)

A Capability for Autonomous IoT System Security: Pushing IoT Assurance to the Edge 256
Jeffrey Chavis (The Johns Hopkins University Applied Physics Laboratory), Aaron Kunz (The Johns Hopkins University Applied Physics Laboratory), Lanier Watkins (The Johns Hopkins University Applied Physics Laboratory), Anna Buczak (The Johns Hopkins University Applied Physics Laboratory), and Aviel Rubin (The Johns Hopkins University Whiting School of Engineering)

A Privacy Filter Framework for Internet of Robotic Things Applications 262
Zahir Alsulaimawi Alsulaimawi (Oregon State University)

LangSec 2020: The Sixth Workshop on Language-Theoretic Security

Language-Agnostic Injection Detection 268
Lars Hermerschmidt (AXA Konzern AG), Andreas Straub (RWTH Aachen University), and Goran Piskachev (Fraunhofer IEM)

Toward Automated Grammar Extraction via Semantic Labeling of Parser Implementations 276
Carson Harmon (Trail of Bits), Bradford Larsen (Trail of Bits), and Evan Sultanik (Trail of Bits)

The Geometry of Syntax and Semantics for Directed File Transformations 284
Steve Huntsman (BAE Systems FAST Labs) and Michael Robinson (American University)

Armor Within: Defending against Vulnerabilities in Third-Party Libraries 291
Sameed Ali (Dartmouth College, USA), Prashant Anantharaman (Dartmouth College, USA), and Sean Smith (Dartmouth College, USA)

Research Report: The Parsley Data Format Definition Language 300
Prashanth Mundkur (SRI International), Prashant Anantharaman (Dartmouth College), Sameed Ali (Dartmouth College), Zephyr Lucas (Dartmouth College), Linda Briesemeister (SRI International), Natarajan Shankar (SRI International), and Sean Smith (Dartmouth College)

Research Report: Formally-Verified ASN.1 Protocol C-Language Stack 308
Nika Pona (Digamma.ai) and Vadim Zaliva (Carnegie Mellon University)

Research Report: Building a Wide Reach Corpus for Secure Parser Development 318
Tim Allison (Jet Propulsion Laboratory, California Institute of Technology, USA), Wayne Burke (Jet Propulsion Laboratory, California Institute of Technology, USA), Valentino Constantinou (Jet Propulsion Laboratory, California Institute of Technology, USA), Edwin Goh (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), Ryan Stonebraker (Jet Propulsion Laboratory, California Institute of Technology, USA), and Virisha Timmaraju (Jet Propulsion Laboratory, California Institute of Technology, USA)

Research Report: ICARUS: Understanding De Facto Formats by Way of Feathers and Wax 327
Sam Cowger (Galois, Inc), Yerim Lee (Galois, Inc), Nichole Schimanski (Galois, Inc), Mark Tullsen (Galois, Inc), Walt Woods (Galois, Inc.), Richard Jones (Galois, Inc), EW Davis (Galois, Inc), William Harris (Galois, Inc), Trent Brunson (Trail of Bits), Carson Harmon (Trail of Bits), Bradford Larsen (Trail of Bits), and Evan Sultanik (Trail of Bits)

Author Index 335