2019 IEEE Security and Privacy Workshops (SPW 2019)

San Francisco, California, USA
23 May 2019

IEEE Catalog Number: CFP19SPX-POD
ISBN: 978-1-7281-3509-0

Copyright © 2019 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:	CFP19SPX-POD
ISBN (Print-On-Demand):	978-1-7281-3509-0
ISBN (Online):	978-1-7281-3508-3

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

2019 IEEE Security and Privacy Workshops (SPW)

SPW 2019

Table of Contents

Message from the Workshop General Chair ix
Message from the DLS Organizers xi
DLS 2019 Organization xii
Message from the IWPE 2019 Organizers xiv
IWPE 2019 Organization xv
Message from the SafeThings 2019 Organizers xvi
SafeThings 2019 Organization xvii
Message from the WTMC 2019 Organizers xviii
WTMC 2019 Organization xx

DLS 2019: 2nd IEEE Workshop on Deep Learning and Security

On the Robustness of Deep K-Nearest Neighbors 1
Chawin Sitawarin (University of California, Berkeley) and David Wagner (University of California, Berkeley)

Exploring Adversarial Examples in Malware Detection 8
Octavian Suciu (University of Maryland, College Park), Scott E. Coull (FireEye, Inc.), and Jeffrey Johns (FireEye, Inc.)

Targeted Adversarial Examples for Black Box Audio Systems 15
Rohan Taori (UC Berkeley), Amog Kamsetty (UC Berkeley), Brenton Chu (UC Berkeley), and Nikita Vemuri (UC Berkeley)

Activation Analysis of a Byte-Based Deep Neural Network for Malware Classification 21
Scott E. Coull (FireEye, Inc.) and Christopher Gardner (FireEye, Inc.)

MaxNet: Neural Network Architecture for Continuous Detection of Malicious Activity 28
Petr Gronát (Avast Software), Javier Alejandro Aldana-Iuit (Avast Software), and Martin Bálek (Avast Software)

Deep in the Dark - Deep Learning-Based Malware Traffic Detection Without Expert Knowledge 36
Gonzalo Marín (IIE-FING, Universidad de la República), Pedro Casas (AIT Austrian Institute of Technology), and Germán Capdehourat (IIE-FING, Universidad de la República)

Defending Against Neural Network Model Stealing Attacks Using Deceptive Perturbations 43
Taesung Lee (IBM Research AI), Benjamin Edwards (Independent), Ian Molloy (IBM Research AI), and Dong Su (Independent)

Membership Inference Attacks Against Adversarially Robust Deep Learning Models 50
Liwei Song (Princeton University), Reza Shokri (National University of Singapore), and Prateek Mittal (Princeton University)

Efficient Evaluation of Activation Functions over Encrypted Data 57
Patricia Thaine (University of Toronto), Sergey Gorbunov (University of Waterloo), and Gerald Penn (University of Toronto)

IWPE 2019: IEEE Workshop on Privacy Engineering

Privacy Risk Assessment for Data Subject-Aware Threat Modeling 64
Laurens Sion (imec-DistriNet, KU Leuven), Dimitri Van Landuyt (imec-DistriNet, KU Leuven), Kim Wuyts (imec-DistriNet, KU Leuven), and Wouter Joosen (imec-DistriNet, KU Leuven)

Differential Inference Testing: A Practical Approach to Evaluate Sanitizations of Datasets 72
Ali Kassem (INRIA), Gergely Ács (Crysys Lab, BME-HIT), Claude Castelluccia (Univ. Grenoble Alpes, INRIA), and Catuscia Palamidessi (INRIA, Ecole Polytechnique, Univ. of Paris Saclay)

Knowledge is Power: Systematic Reuse of Privacy Knowledge for Threat Elicitation 80
Kim Wuyts (imec-DistriNet, KU Leuven), Laurens Sion (imec-DistriNet, KU Leuven), Dimitri Van Landuyt (imec-DistriNet, KU Leuven), and Wouter Joosen (imec-DistriNet, KU Leuven)

You Talk Too Much: Limiting Privacy Exposure Via Voice Input 84
Tavish Vaidya (Georgetown University) and Micah Sherr (Georgetown University)

After GDPR, Still Tracking or Not? Understanding Opt-Out States for Online Behavioral Advertising 92
Takahito Sakamoto (Intelligent Systems Laboratory, SECOM Co., Ltd.) and Masahiro Matsunaga (Intelligent Systems Laboratory, SECOM Co., Ltd.)

A Privacy-Aware V-Model for Software Development 100
Ala'a Al-Momani (Ulm University), Frank Kargl (Ulm University), Robert Schmidt (Denso Automotive Deutschland GmbH), Antonio Kung (Trialog), and Christoph Bösch (Ulm University)

SwitchMan: An Easy-to-Use Approach to Secure User Input and Output 105
Shengbao Zheng (Duke University), Zhenyu Zhou (Duke University), Heyi Tang (Tsinghua University), and Xiaowei Yang (Duke University)

SafeThings 2019: IEEE Workshop on the Internet of Safe Things

ROS-Defender: SDN-Based Security Policy Enforcement for Robotic Applications 114
Sean Rivera (University of Luxembourg), Sofiane Lagraa (University of Luxembourg), Cristina Nita-Rotaru (Northeastern University), Sheila Becker (Defence Directorate, Luxembourg), and Radu State (University of Luxembourg)

Resilience of Multi-Robot Systems to Physical Masquerade Attacks 120
Kacper Wardega (Boston University), Roberto Tron (Boston University), and Wenchao Li (Boston University)

Ensuring the Safe and Secure Operation of Electronic Control Units in Road Vehicles 126
Florian Kohnhäuser (TU Darmstadt), Dominik Püllen (TU Darmstadt), and Stefan Katzenbeisser (TU Darmstadt)

Are Self-Driving Cars Secure? Evasion Attacks Against Deep Neural Networks for Steering Angle Prediction 132

Alesia Chernikova (Northeastern University), Alina Oprea (Northeastern University), Cristina Nita-Rotaru (Northeastern University), and BaekGyu Kim (Toyota ITC)

Analysis of the Susceptibility of Smart Home Programming Interfaces to End User Error 138

Mitali Palekar (University of Washington), Earlence Fernandes (University of Washington), and Franziska Roesner (University of Washington)

Smart Speaker Privacy Control - Acoustic Tagging for Personal Voice Assistants 144

Peng Cheng (Lancaster University), Ibrahim Ethem Bagci (Lancaster University), Jeff Yan (Linköping University), and Utz Roedig (University College Cork)

When Smart Devices Are Stupid: Negative Experiences Using Home Smart Devices 150

Weijia He (University of Chicago), Jesse Martinez (University of Chicago), Roshni Padhi (University of Chicago), Lefan Zhang (University of Chicago), and Blase Ur (University of Chicago)

Side Channel Attacks in Computation Offloading Systems with GPU Virtualization 156

Sihang Liu (University of Virginia), Yizhou Wei (University of Virginia), Jianfeng Chi (University of Virginia), Faysal Hossain Shezan (University of Virginia), and Yuan Tian (University of Virginia)

Demo: An Emulator-Based Active Protection System Against IoT Malware 162

Shin-Ming Cheng (National Taiwan University of Science and Technology) and Sheng-Hao Ma (National Taiwan University of Science and Technology)

SpyCon: Adaptation Based Spyware in Human-in-the-Loop IoT 163

Salma Elmalaki (University of California, Los Angeles), Bo-Jhang Ho (University of California, Los Angeles), Moustafa Alzantot (University of California, Los Angeles), Yasser Shoukry (University of Maryland, College Park), and Mani Srivastava (University of California, Los Angeles)

Devil in the Detail: Attack Scenarios in Industrial Applications 169

Simon D. Duque Anton (German Research Center for Artificial Intelligence), Alexander Hafner (German Research Center for Artificial Intelligence), and Hans Dieter Schotten (German Research Center for Artificial Intelligence)

IOTFLA : A Secured and Privacy-Preserving Smart Home Architecture Implementing Federated Learning 175

Ulrich Matchi Aïvodji (Université du Québec à Montréal (UQAM)), Sébastien Gambs (Université du Québec à Montréal (UQAM)), and Alexandre Martin (Université du Québec à Montréal (UQAM))

A Study of Vulnerability Analysis of Popular Smart Devices Through Their Companion Apps 181

Davino Mauro Junior (CIn-UFPE), Luis Melo (CIn-UFPE), Hao Lu (UMICH), Marcelo d'Amorim (CIn-UFPE), and Atul Prakash (UMICH)

WTMC 2019: 4th IEEE Workshop on Traffic Measurements for Cybersecurity

A Smörgåsbord of Typos: Exploring International Keyboard Layout Typosquatting 187
Victor Le Pochat (imec-DistriNet, KU Leuven), Tom Van Goethem (imec-DistriNet, KU Leuven), and Wouter Joosen (imec-DistriNet, KU Leuven)

Characterizing Vulnerability of DNS AXFR Transfers with Global-Scale Scanning 193
Marcin Skwarek (Warsaw University of Technology), Maciej Korczynski (Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG), Wojciech Mazurczyk (Warsaw University of Technology), and Andrzej Duda (Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG)

Assessing the Effectiveness of Domain Blacklisting Against Malicious DNS Registrations 199
Thomas Vissers (imec-DistriNet, KU Leuven), Peter Janssen (EURid VZW), Wouter Joosen (imec-DistriNet, KU Leuven), and Lieven Desmet (imec-DistriNet, KU Leuven)

Analysing Censorship Circumvention with VPNs Via DNS Cache Snooping 205
Oliver Farnan (University of Oxford), Joss Wright (Oxford Internet Institute), and Alexander Darer (University of Oxford)

Feasibility of a Keystroke Timing Attack on Search Engines with Autocomplete 212
John V. Monaco (Naval Postgraduate School)

Detecting Malicious Campaigns in Obfuscated JavaScript with Scalable Behavioral Analysis 218
Oleksii Starov (Palo Alto Networks, Inc.), Yuchen Zhou (Palo Alto Networks, Inc.), and Jun Wang (Palo Alto Networks, Inc.)

Counting Outdated Honeypots: Legal and Useful 224
Alexander Vetterl (University of Cambridge), Richard Clayton (University of Cambridge), and Ian Walden (Queen Mary University of London)

MLSEC - Benchmarking Shallow and Deep Machine Learning Models for Network Security 230
Pedro Casas (AIT Austrian Institute of Technology), Gonzalo Marín (IIE-FING, Universidad de la República), Germán Capdehourat (IIE-FING, Universidad de la República), and Maciej Korczynski (University Grenoble Alpes, CNRS, Grenoble INP, LIG)

IEC 60870-5-104 Network Characterization of a Large-Scale Operational Power Grid 236
Kelvin Mai (The University of Texas at Dallas), Xi Qin (University of California Santa Cruz), Neil Ortiz Silva (University of California Santa Cruz), and Alvaro A. Cardenas (University of California Santa Cruz)

Victim Routine Influences the Number of DDoS Attacks: Evidence from Dutch Educational Network 242
Abhishta Abhishta (University of Twente), Marianne Junger (University of Twente), Reinoud Joosten (University of Twente), and Lambert J.M. Nieuwenhuis (University of Twente)

Author Index 249