# 2021 IEEE European Symposium on Security and Privacy (EuroS&P 2021)

## Virtual Conference
## 6 – 10 September 2021

IEEE Catalog Number: CFP21C75-POD
ISBN: 978-1-6654-3048-7

**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: | CFP21C75-POD |
| ISBN (Print-On-Demand): | 978-1-6654-3048-7 |
| ISBN (Online): | 978-1-6654-1491-3 |

**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

# 2021 IEEE European Symposium on Security and Privacy (EuroS&P)

# EuroSP 2021

## Table of Contents

**Message from the General Chairs** ........ xi
**Message from the Program Chairs** ........ xii
**Message from the Poster Chairs** ........ xiv
**Organizing Committee** ........ xv
**Program Committee** ........ xvi
**Posters Program Committee** ........ xviii
**Steering Committee** ........ xix

## Session: Human aspects of security and privacy

An Investigation of Online Reverse Engineering Community Discussions in the Context of Ghidra ........ 1
*Daniel Votipka (Tufts University), Mary Nicole Punzalan (University of Maryland), Seth M. Rabin (University of Maryland), Yla Tausczik (University of Maryland), and Michelle L. Mazurek (University of Maryland)*

Countering Concurrent Login Attacks in "Just Tap" Push-Based Authentication: A Redesign and Usability Evaluations ........ 21
*Jay Prakash (Silence Laboratories, Singapore; Singapore University of Technology and Design, Singapore), Clarice Chua Qing Yu (Silence Laboratories, Singapore; Singapore University of Technology and Design, Singapore), Tanvi Ravindra Thombre (Singapore University of Technology and Design, Singapore), Andrei Bytes (Singapore University of Technology and Design, Singapore), Mohammed Jubur (University of Alabama at Birmingham, USA), Nitesh Saxena (University of Alabama at Birmingham, USA), Lucienne Blessing (Singapore University of Technology and Design, Singapore), Jianying Zhou (Singapore University of Technology and Design, Singapore), and Tony Q. S Quek (Singapore University of Technology and Design, Singapore)*

SoK: Context Sensing for Access Control in the Adversarial Home IoT ........ 37
*Weijia He (University of Chicago), Valerie Zhao (University of Chicago), Olivia Morkved (University of Chicago), Sabeeka Siddiqui (University of Chicago), Earlence Fernandes (University of Wisconsin–Madison), Josiah Hester (Northwestern University), and Blase Ur (University of Chicago)*

Secure Messaging Authentication Against Active Man-in-the-Middle Attacks ........ 54
*Benjamin Dowling (ETH Zürich, Switzerland) and Britta Hale (Naval Postgraduate School (NPS), USA)*

Press @$@$ to Login: Strong Wearable Second Factor Authentication via Short Memorywise Effortless Typing Gestures 71
*Prakash Shrestha (Equifax Inc.), Nitesh Saxena (University of Alabama at Birmingham), Diksha Shukla (University of Wyoming), and Vir V. Phoha (Syracuse University)*

## Session: Blockchain & cryptocurrencies

Fully Distributed Verifiable Random Functions and Their Application to Decentralised Random Beacons 88
*David Galindo (Fetch.ai, UK; University of Birmingham, UK), Jia Liu (Fetch.ai, UK), Mihai Ordean (University of Birmingham, UK), and Jin-Mann Wong (British Antarctic Survey, UK)*

ConFuzzius: A Data Dependency-Aware Hybrid Fuzzer for Smart Contracts 103
*Christof Ferreira Torres (University of Luxembourg), Antonio Ken Iannillo (University of Luxembourg), Arthur Gervais (Imperial College London), and Radu State (University of Luxembourg)*

SoK: Cryptojacking Malware 120
*Ege Tekiner (Florida International University), Abbas Acar (Florida International University), A. Selcuk Uluagac (Florida International University), Engin Kirda (Northeastern University), and Ali Aydin Selcuk (TOBB University of Economics and Technology)*

Cryptocurrencies with Security Policies and Two-Factor Authentication 140
*Florian Breuer (KIT), Vipul Goyal (CMU and NTT), and Giulio Malavolta (MPI-SP)*

## Session: Security of AI

Bullseye Polytope: A Scalable Clean-Label Poisoning Attack with Improved Transferability 159
*Hojjat Aghakhani (University of California, Santa Barbara), Dongyu Meng (University of California, Santa Barbara), Yu-Xiang Wang (University of California, Santa Barbara), Christopher Kruegel (University of California, Santa Barbara), and Giovanni Vigna (University of California, Santa Barbara)*

Trojaning Language Models for Fun and Profit 179
*Xinyang Zhang (Pennsylvania State University), Zheng Zhang (Pennsylvania State University), Shouling Ji (Zhejiang University), and Ting Wang (Pennsylvania State University)*

Fall of Giants: How Popular Text-Based MLaaS Fall Against a Simple Evasion Attack 198
*Luca Pajola (University of Padua, Italy) and Mauro Conti (University of Padua, Italy)*

Sponge Examples: Energy-Latency Attacks on Neural Networks 212
*Ilia Shumailov (University of Cambridge), Yiren Zhao (University of Cambridge), Daniel Bates (University of Cambridge), Nicolas Papernot (University of Toronto and Vector Institute), Robert Mullins (University of Cambridge), and Ross Anderson (University of Cambridge)*

On the (In) Feasibility of Attribute Inference Attacks on Machine Learning Models .232..........
*Benjamin Zi Hao Zhao (University of New South Wales, Australia; Data61-CSIRO, Australia), Aviral Agrawal (BITS Pilani K.K.Birla Goa campus, India; Macquarie University, Australia; Data61-CSIRO, Australia), Catisha Coburn (Defence Science and Technology Group, Australia), Hassan Jameel Asghar (Macquarie University, Australia; Data61-CSIRO, Australia), Raghav Bhaskar (Data61-CSIRO, Australia), Mohamed Ali Kaafar (Macquarie University, Australia; Data61-CSIRO, Australia), Darren Webb (Defence Science and Technology Group, Australia), and Peter Dickinson (Defence Science and Technology Group, Australia)*

## Session: Privacy

Privacy of DNS-over-HTTPS: Requiem for a Dream? .252....................................................
*Levente Csikor (National University of Singapore), Himanshu Singh (IIIT, Naya Raipur), Min Suk Kang (KAIST), and Dinil Mon Divakaran (Trustwave)*

Epoque: Practical End-to-End Verifiable Post-Quantum-Secure E-Voting .272.........................
*Xavier Boyen (Queensland University of Technology, Australia), Thomas Haines (NTNU Trondheim, Norway), and Johannes Mueller (SnT/University of Luxembourg, Luxembourg)*

On the Privacy Risks of Algorithmic Fairness .292..............................................................
*Hongyan Chang (National University of Singapore, Singapore) and Reza Shokri (National University of Singapore, Singapore)*

Compression Boosts Differentially Private Federated Learning .304......................................
*Raouf Kerkouche (Privatics team, Univ. Grenoble Alpes, Inria, France), Gergely Ács (Crysys Lab, BME-HIT, Hungary), Claude Castelluccia (Privatics team, Univ. Grenoble Alpes, Inria, France), and Pierre Genevès (Tyrex team, Univ. Grenoble Alpes, CNRS, Inria, Grenoble INP, LIG, France)*

We Built This Circuit: Exploring Threat Vectors in Circuit Establishment in Tor .319................
*Theodor Schnitzler (Ruhr-Universität Bochum, Germany), Christina Pöpper (New York University Abu Dhabi, United Arab Emirates), Markus Dürmuth (Ruhr-Universität Bochum, Germany), and Katharina Kohls (Radboud University, Netherlands)*

## Session: Malware defenses and industrial IoT security

Can ISPs Help Mitigate IoT Malware? A Longitudinal Study of Broadband ISP Security Efforts 337
*Arman Noroozian (TU-Delft, Netherlands), Elsa Turcios Rodriguez (TU-Delft, Netherlands), Elmer Lastdrager (SIDN Labs, Netherlands), Takahiro Kasama (NICT, Japan), Michel van Eeten (TU-Delft, Netherlands), and Carlos H. Ganan (TU-Delft, Netherlands)*

Prognosis Negative: Evaluating Real-Time Behavioral Ransomware Detectors .353.................
*Abhinav Gupta (University of Colorado Boulder), Aditi Prakash (University of Colorado Boulder), and Nolen Scaife (University of Colorado Boulder)*

Remote Non-Intrusive Malware Detection for PLCs Based on Chain of Trust Rooted in Hardware .. 369
*Prashant Hari Narayan Rajput (NYU Tandon School of Engineering, USA), Esha Sarkar (NYU Tandon School of Engineering, USA), Dimitrios Tychalas (NYU Tandon School of Engineering, USA), and Michail Maniatakos (New York University Abu Dhabi, United Arab Emirates)*

SoK: Attacks on Industrial Control Logic and Formal Verification-Based Defenses .385............
*Ruimin Sun (Northeastern University), Alejandro Mera (Northeastern University), Long Lu (Northeastern University), and David Choffnes (Northeastern University)*

## Session: Web, network, and mobile security

Ephemeral Astroturfing Attacks: The Case of Fake Twitter Trends .403.................................
*Tuğrulcan Elmas (EPFL, Switzerland), Rebekah Overdorf (EPFL, Switzerland), Ahmed Furkan Özkalay (EPFL, Switzerland), and Karl Aberer (EPFL, Switzerland)*

BGPeek-a-Boo: Active BGP-Based Traceback for Amplification DDoS Attacks .423..................
*Johannes Krupp (CISPA Helmholtz Center for Information Security, Germany) and Christian Rossow (CISPA Helmholtz Center for Information Security, Germany)*

SoK: A Framework for Asset Discovery: Systematizing Advances in Network Measurements for Protecting Organizations .440...................................................................................
*Mathew Vermeer (Delft University of Technology), Jonathan West (University of Tulsa), Alejandro Cuevas (Carnegie Mellon University), Shuonan Niu (University of Tulsa), Nicolas Christin (Carnegie Mellon University), Michel van Eeten (Delft University of Technology), Tobias Fiebig (Delft University of Technology), Carlos Gañán (Delft University of Technology), and Tyler Moore (University of Tulsa)*

AppJitsu: Investigating the Resiliency of Android Applications .457.....................................
*Onur Zungur (Boston University, USA), Antonio Bianchi (Purdue University, USA), Gianluca Stringhini (Boston University, USA), and Manuel Egele (Boston University, USA)*

SoK: In Search of Lost Time: A Review of JavaScript Timers in Browsers .472.........................
*Thomas Rokicki (Univ Rennes, CNRS, IRISA, France), Clémentine Maurice (Univ Lille, CNRS, Inria, France), and Pierre Laperdrix (Univ Lille, CNRS, Inria, France)*

## Session: Hardware security and formal methods for security

SoK: Secure FPGA Multi-Tenancy in the Cloud: Challenges and Opportunities .487.................
*Ghada Dessouky (Technische Universität Darmstadt, Germany), Ahmad-Reza Sadeghi (Technische Universität Darmstadt, Germany), and Shaza Zeitouni (Technische Universität Darmstadt, Germany)*

Nonce@Once: A Single-Trace EM Side Channel Attack on Several Constant-Time Elliptic Curve Implementations in Mobile Platforms .507.......................................................................
*Monjur Alam (Georgia Tech, USA), Baki Yilmaz (Georgia Tech, USA), Frank Werner (Georgia Tech, USA), Niels Samwel (Radboud University, Netherlands), Alenka Zajic (Georgia tech, USA), Daniel Genkin (University of Michigan), Yuval Yarom (University of Adelaide, Australia), and Milos Prvulovic (Georgia Tech, USA)*

DY: A Modular Symbolic Verification Framework for Executable Cryptographic Protocol Code .... 523
*Karthikeyan Bhargavan (INRIA, France), Abhishek Bichhawat (Carnegie Mellon University, USA and IIT Gandhinagar, India), Quoc Huy Do (University of Stuttgart, Germany), Pedram Hosseyni (University of Stuttgart, Germany), Ralf Küsters (University of Stuttgart, Germany), Guido Schmitz (University of Stuttgart, Germany), and Tim Würtele (University of Stuttgart, Germany)*

Nontransitive Policies Transpiled 543..................................................................................
*Mohammad M. Ahmadpanah (Chalmers University of Technology), Aslan Askarov (Aarhus University), and Andrei Sabelfeld (Chalmers University of Technology)*

## Session: AI-based security and privacy tools

ANDRUSPEX: Leveraging Graph Representation Learning to Predict Harmful App Installations on Mobile Devices 562..................................................................................
*Yun Shen (NortonLifeLock Research Group) and Gianluca Stringhini (Boston University)*

D-Fence: A Flexible, Efficient, and Comprehensive Phishing Email Detection System 578........
*Jehyun Lee (Trustwave), Farren Tang (Trustwave), Pingxiao Ye (Trustwave), Fahim Abbasi (Trustwave), Phil Hay (Trustwave), and Dinil Mon Divakaran (Trustwave)*

Extractor: Extracting Attack Behavior from Threat Reports 598............................................
*Kiavash Satvat (University of Illinois at Chicago), Rigel Gjomemo (University of Illinois at Chicago), and V.N. Venkatakrishnan (University of Illinois at Chicago)*

FastSpec: Scalable Generation and Detection of Spectre Gadgets using Neural Embeddings 616
*M. Caner Tol (Worcester Polytechnic Institute), Berk Gulmezoglu (Iowa State University), Koray Yurtseven (Worcester Polytechnic Institute), and Berk Sunar (Worcester Polytechnic Institute)*

## Session: System security

Bypassing Memory Safety Mechanisms Through Speculative Control flow Hijacks 633...........
*Andrea Mambretti (IBM Research - Zurich, Switzerland; Northeastern University, USA), Alexandra Sandulescu (IBM Research - Zurich, Switzerland), Alessandro Sorniotti (IBM Research - Zurich, Switzerland), William Robertson (Northeastern University, USA), Engin Kirda (Northeastern University, USA), and Anil Kurmus (IBM Research - Zurich, Switzerland)*

NoVT: Eliminating C++ Virtual Calls to Mitigate Vtable Hijacking 650.................................
*Bauer Markus (CISPA – Helmholtz Center for Information Security, Germany) and Rossow Christian (CISPA – Helmholtz Center for Information Security, Germany)*

Compiler-Assisted Hardening of Embedded Software Against Interrupt Latency Side-Channel Attacks 667..................................................................................................
*Hans Winderix (KU Leuven, Belgium), Jan Tobias Mühlberg (KU Leuven, Belgium), and Frank Piessens (KU Leuven, Belgium)*

Aim, Wait, Shoot: How the CACHESNIPER Technique Improves Unprivileged Cache Attacks 683
*Samira Briongos (NEC Laboratories Europe), Ida Bruhns (Universität zu Lübeck), Pedro Malagón (Universidad Politécnica de Madrid), Thomas Eisenbarth (Universität zu Lübeck), and José Moya (Universidad Politécnica de Madrid)*

## Posters

Poster: Angry Birding: Evaluating Application Exceptions as Attack Canaries 701
*Tolga Ünlü (Abertay University, United Kingdom), Lynsay A. Shepherd (Abertay University, United Kingdom), Natalie Coull (Abertay University, United Kingdom), and Colin McLean (Abertay University, United Kingdom)*

Poster: DyPolDroid: User-Centered Counter-Policies Against Android Permission-Abuse Attacks 704
*Matthew Hill (Texas A&M University - Corpus Christi, USA), Carlos E. Rubio-Medrano (Texas A&M University - Corpus Christi, USA), Luis M. Claramunt (Arizona State University, USA), Jaejong Baek (Arizona State University, USA), and Gail-Joon Ahn (Arizona State University, USA)*

Poster: FLATEE: Federated Learning Across Trusted Execution Environments 707
*Arup Mondal (Ashoka University), Yash More (Ashoka University), Ruthu Hulikal Rooparaghunath (Ashoka University), and Debayan Gupta (Ashoka University)*

Poster: Obfuscation Revealed - Using Electromagnetic Emanation to Identify and Classify Malware 710
*Duy-Phuc Pham (Univ Rennes, CNRS, IRISA, France), Damien Marion (Univ Rennes, CNRS, IRISA, France), and Annelie Heuser (Univ Rennes, CNRS, IRISA, France)*

Poster: Preventing Spatial and Privacy Attacks in Mobile Augmented Reality Technologies 713
*Larissa Pokam Epse (Arizona State University, USA), Carlos Rubio-Medrano (Texas A&M University - Corpus Christi, USA), Jaejong Baek (Arizona State University, USA), and Gail-Joon Ahn (Arizona State University & Samsung Research, USA)*

Poster: Reducing Data Leakage on Personal Data Management Systems 716
*Robin Carpentier (Univ. Versailles St-Q.-en-Yvelines, France), Iulian Sandu Popa (Univ. Versailles St-Q.-en-Yvelines, France), and Nicolas Anciaux (Inria Saclay, France)*

Poster: The Need for a Collaborative Approach to Cyber Security Education 719
*Gregor Langner (AIT Austrian Institute of Technology, Austria), Jerry Andriessen (Wise & Munro Learning Research, Netherlands), Gerald Quirchmayr (University of Vienna, Austria), Steven Furnell (University of Nottingham, United Kingdom), Vittorio Scarano (Universit`a degli Studi di Salerno, Italy), and Teemu Johannes Tokola (University of Oulu, Finland)*

Poster: Towards Verifiable Mutability for Blockchains 722
*Erik Daniel (Technische Universität Berlin) and Florian Tschorsch (Technische Universität Berlin)*

**Author Index 725**