

Curriculum Vitae

Christopher Kruegel

1 Personal Information

Name:	Christopher Kruegel	
Address (Work):	Department of Computer Science 2117 Harold Frank Hall University of California, Santa Barbara Santa Barbara, CA 93106, USA	VMware, Inc. 3425 Hillview Ave Palo Alto, CA 94304, USA
Email:	chris@cs.ucsb.edu	chris@vmware.com
Web:	http://www.cs.ucsb.edu/~chris/	

2 Work Experience

since 07/2013

Professor in Computer Science at the Department of Computer Science, University of California at Santa Barbara, USA

since 07/2020

VP Security Services at VMware, Inc.

10/2018 - 06/2020

Chief Product Officer at Lastline, Inc.

05/2016 - 09/2018

Chief Executive Officer (CEO) at Lastline, Inc.

02/2012 - 04/2016

Chief Scientist at Lastline, Inc.

07/2009 - 06/2013

Associate Professor and *Eugene Aas Chair* in Computer Science at the Department of Computer Science, University of California at Santa Barbara, USA

10/2007 - 06/2009

Assistant Professor and *Eugene Aas Chair* in Computer Science at the Department of Computer Science, University of California at Santa Barbara, USA

01/2004 - 09/2007

Assistant Professor in Computer Science at the Automation Systems Group, Technical University Vienna, Austria

10/2002 - 12/2003

Post-doctoral Researcher at the Reliable Software Group, University of California at Santa Barbara, USA

07/2000 - 09/2002

Research Assistant at the Distributed Systems Group, Technical University Vienna, Austria

3 Education

09/2006

Habilitation (comparable to tenure in the US) from Technical University Vienna

07/2000 - 06/2002

Dr.techn. (Ph.D.) in Computer Science (with highest distinction) from Technical University Vienna. Advisor: Prof. Dr. Mehdi Jazayeri

09/1995 - 06/2000

Dipl.-Ing. (M.Sc.) in Computer Science (with highest distinction) from Technical University Vienna. Advisor: Prof. Dr. Gerhard H. Schildt

4 Awards

2022

Distinguished Artifact Award of the Usenix Security Symposium for the paper “Fuzzware: Using Precise MMIO Modeling for Effective Firmware Fuzzing.”

2021

Test of Time Award of the Annual Computer Security Applications Conference (ACSAC) for the 2004 paper “Detecting Kernel-Level Rootkits Through Binary Analysis.”

2019

Distinguished Service Award from the Technical Committee on Security and Privacy of the IEEE Computer Society.

2018

Winner of the 6th Annual **Best Scientific Cybersecurity Paper** Competition, organized by the National Security Agency, for the paper “How Shall We Play a Game: A Game-Theoretical Model for Cyber-warfare Games.”

2017

Distinguished Paper Award of the Network and Distributed System Security Symposium (NDSS) for the paper “Ramblr: Making Reassembly Great Again.”

2015

Honorary appointment as **Distinguished YNU Professor** of the Yokohama National University in Japan (until 2018, reappointed until 2021).

2015

Best Paper Award of the Mobile Security Technologies Workshop (MoST 2015) for the paper “A Large-Scale Study of Mobile Web App Security.”

2011

IBM Faculty Award to “foster collaboration between researchers at leading universities worldwide and those in IBM research, development and services organizations.”

2011

Distinguished Paper Award of the Network and Distributed System Security Symposium (NDSS) for the paper “PiOS: Detecting Privacy Leaks in iOS Applications.”

2010

MIT TR35 Award - 2010 Young Innovator Award presented by MIT Technology Review.

2010

Best Student Paper Award of the Annual Computer Security Applications Conference (ACSAC) for the paper “Detecting Spammers On Social Networks.”

2010

Business Star Award: Innovation, awarded by the Santa Barbara Chamber of Commerce for “a significant innovative contribution to positively impacting our world.”

2009

National Science Foundation **CAREER Award**.

2009

Outstanding Faculty Member in the Department of Computer Science, UC Santa Barbara.

2007

Best Project Award of 1. FIT-IT Call: Trust in IT-Systems for the project “PathFinder - Malicious Code Analysis and Detection.”

2007

Distinguished Paper Award of the 6th Joint Meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE) for the paper “Mining Specifications of Malicious Behavior.”

2007

Best Student Paper Award of the 10th Information Security Conference (ISC) for the paper “Detecting System Emulators.”

2006

Best Paper Award of the 15th Annual Conference of the European Institute for Computer Antivirus Research (EICAR) for the paper “TtAnalyze: A Tool for Analyzing Malware”.

2005

Best Paper Award of the Information Technology Security Conference (AusCERT) for the paper “Reverse Engineering of Network Signatures”.

2005

Award of the Austrian Federal Economic Chamber (Wirtschaftskammerpreis) for the project “Malware Detection”.

2000

EIB Scientific Award for “an excelling student project in the field of Home and Building Electronic Systems based on the European Installation Bus EIB,” received for Master Thesis.

5 Publications

Publications at a Glance

Number of Peer-reviewed Publications

Total	263
Conference/Symposium	222
Journal	16
Workshop	25

Publications in Top-4 (Systems) Security Venues

Total	94
IEEE Symposium on Security and Privacy	22
Usenix Security Symposium	30
ACM CCS	18
NDSS	24

Impact (according to Google Scholar)

Number of Citations	47,466
H-Index	111

Full List of Publications

Conference and Workshop Publications

- [1] A Large Scale Study of the Ethereum Arbitrage Ecosystem. Robert McLaughlin, Christopher Kruegel, and Giovanni Vigna. In **32nd Usenix Security Symposium**, USA, August 2023.
- [2] Actor: Action-Guided Kernel Fuzzing. Marius Fleischer, Dipanjan Das, Priyanka Bose, Weiheng Bai, Kangjie Lu, Mathias Payer, Christopher Kruegel, and Giovanni Vigna. In **32nd Usenix Security Symposium**, USA, August 2023.
- [3] Confusum Contractum: Confused Deputy Vulnerabilities in Ethereum Smart Contracts. Fabio Gritti, Nicola Ruaro, Robert McLaughlin, Priyanka Bose, Dipanjan Das, Ilya Grishchenko, Christopher Kruegel, and Giovanni Vigna. In **32nd Usenix Security Symposium**, USA, August 2023.
- [4] Certifiably Vulnerable: Using Certificate Transparency Logs for Target Reconnaissance. Stijn Plet-inckx, Thanh-Dat Nguyen, Tobias Fiebig, Christopher Kruegel, and Giovanni Vigna. In *IEEE European Symposium on Security and Privacy (Euro S&P)*, Netherlands, July 2021.
- [5] TEEzz: Fuzzing Trusted Applications on COTS Android Devices. Marcel Busch, Aravind Machiry, Chad Spensky, Giovanni Vigna, Christopher Kruegel, and Mathias Payer. In **IEEE Symposium on Security and Privacy**, IEEE Computer Society Press, USA, May 2023.
- [6] Toss a Fault to Your Witcher: Applying Grey-box Coverage-Guided Mutational Fuzzing to Detect SQL and Command Injection Vulnerabilities. Erik Trickett, Fabio Pagani, Chang Zhu, Lukas Dresel, Giovanni Vigna, Christopher Kruegel, Ruoyu Wang, Tiffany Bao, Yan Shoshitaishvili, and Adam Doupe. In **IEEE Symposium on Security and Privacy**, IEEE Computer Society Press, USA, May 2023.

- [7] Columbus: Android App Testing Through Systematic Callback Exploration. Priyanka Bose, Dipanjan Das, Saastha Vasam, Sebastiano Mariani, Ilya Grishchenko, Andrea Continella, Antonio Bianchi, Christopher Kruegel, and Giovanni Vigna. In *International Conference on Software Engineering (ICSE)*, Australia, May 2023.
- [8] Venomave: Targeted Poisoning Against Speech Recognition. Hojjat Aghakhani, Lea Schoenherr, Thorsten Eisenhofer, Dorothea Kolossa, Thorsten Holz, Christopher Kruegel, and Giovanni Vigna. In *IEEE Conference on Secure and Trustworthy Machine Learning (SaTML)*, USA, February 2023.
- [9] Popkorn: Popping Windows Kernel Drivers At Scale. Rajat Gupta, Lukas Dresel, Noah Spahn, Giovanni Vigna, Christopher Kruegel, and Taesoo Kim. In *Annual Computer Security Applications Conference (ACSAC)*, USA, December 2022.
- [10] Understanding Security Issues in the NFT Ecosystem. Dipanjan Das, Priyanka Bose, Nicola Ruaro, Christopher Kruegel, and Giovanni Vigna. In **29th ACM Conference on Computer and Communications Security (CCS)**, USA, November 2022.
- [11] Fuzzware: Using Precise MMIO Modeling for Effective Firmware Fuzzing. Tobias Scharnowski, Nils Bars, Moritz Schloegel, Eric Gustafson, Marius Muench, Giovanni Vigna, Christopher Kruegel, Thorsten Holz, and Ali Abbas. In **31st Usenix Security Symposium**, USA, August 2022.
- [12] Regulator: Dynamic Analysis to Detect ReDoS. Robert McLaughlin, Fabio Pagani, Noah Spahn, Christopher Kruegel, and Giovanni Vigna. In **31st Usenix Security Symposium**, USA, August 2022.
- [13] Decomperson: How Humans Decompile and What We Can Learn From It. Kevin Burk, Fabio Pagani, Christopher Kruegel, and Giovanni Vigna. In **31st Usenix Security Symposium**, USA, August 2022.
- [14] Hybrid Pruning: Towards Precise Pointer and Taint Analysis. Dipanjan Das, Priyanka Bose, Aravind Machiry, Sebastiano Mariani, Yan Shoshitaishvili, Christopher Kruegel, and Giovanni Vigna. In *Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA)*, Italy, June 2022.
- [15] DeepCase: Semi-Supervised Contextual Analysis of Security Events. Thijs van Ede, Hojjat Aghakhani, Noah Spahn, Riccardo Bortolameotti, Marco Cova, Andrea Continella, Maarten Steen, Andreas Peter, Christopher Kruegel, and Giovanni Vigna. In **IEEE Symposium on Security and Privacy**, IEEE Computer Society Press, USA, May 2022.
- [16] Heapster: Analyzing the Security of Dynamic Allocators for Monolithic Firmware Images. Fabio Gritti, Fabio Pagani, Ilya Grishchenko, Lukas Dresel, Nilo Redini, Christopher Kruegel, and Giovanni Vigna. In **IEEE Symposium on Security and Privacy**, IEEE Computer Society Press, USA, May 2022.
- [17] SymbExcel: Automated Analysis and Understanding of Malicious Excel 4.0 Macros. Nicola Ruaro, Fabio Pagani, Stefano Ortolani, Christopher Kruegel, and Giovanni Vigna. In **IEEE Symposium on Security and Privacy**, IEEE Computer Society Press, USA, May 2022.
- [18] Sailfish: Vetting Smart Contract State-Inconsistency Bugs in Seconds. Priyanka Bose, Dipanjan Das, Yanju Chen, Yu Feng, Christopher Kruegel, and Giovanni Vigna. In **IEEE Symposium on Security and Privacy**, IEEE Computer Society Press, USA, May 2022.
- [19] Tarnhelm: Isolated, Transparent and Confidential Execution of Arbitrary Code in ARM’s Trust-Zone. Davide Quarta, Michele Ianni, Aravind Machiry, Yanick Fratantonio, Eric Gustafson, Davide Balzarotti, Martina Lindorfer, Christopher Kruegel, and Giovanni Vigna. In *ACM Workshop on Research on Offensive and Defensive Techniques in the Context of Man At The End Attacks (Check-MATE)*, South Korea, November 2021.

- [20] SyML: Guiding Symbolic Execution Toward Vulnerable States Through Pattern Learning. Nicola Ruaro, Lukas Dresel, Kyle Zeng, Tiffany Bao, Mario Polino, Andrea Continella, Stefano Zanero, Christopher Kruegel, and Giovanni Vigna. In *24th Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, Spain, October 2021.
- [21] Bullseye Polytope: A Scalable Clean-Label Poisoning Attack with Improved Transferability. Hojjat Aghakhani, Dongyu Meng, Yu-Xiang Wang, Christopher Kruegel, and Giovanni Vigna. In *IEEE European Symposium on Security and Privacy (Euro S&P)*, Austria, September 2021.
- [22] Token-Level Fuzzing. Christopher Salls, Chani Jindal, Jake Corina, Christopher Kruegel, and Giovanni Vigna. In **30th Usenix Security Symposium**, USA, August 2021.
- [23] Toward a Secure Crowdsourced Location Tracking System. Chinmay Garg, Aravind Machiry, Andrea Continella, Christopher Kruegel, and Giovanni Vigna. In *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, Abu Dhabi, July 21.
- [24] Glitching Demystified: Analyzing Control-flow-based Glitching Attacks and Defenses. Chad Spensky, Aravind Machiry, Nathan Burow, Hamed Okhravi, Rick Housley, Zhongshu Gu, Hani Jamjoom, Christopher Kruegel, and Giovanni Vigna. In *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Taiwan, June 2021.
- [25] Bran: Reduce Vulnerability Search Space in Large Open-Source Repositories by Learning Bug Symptoms. Dongyu Meng, Michele Guerriero, Aravind Machiry, Hojjat Aghakhani, Priyanka Bose, Andrea Continella, Christopher Kruegel, and Giovanni Vigna. In *ACM Asia Conference on Computer and Communications Security (AsiaCCS)*, China, June 2021.
- [26] Conware: Automated Modeling of Hardware Peripherals. Chad Spensky, Aravind Machiry, Nilo Redini, Colin Unger, Graham Foster, Evan Blasband, Hamed Okhravi, Christopher Kruegel, and Giovanni Vigna. In *ACM Asia Conference on Computer and Communications Security (AsiaCCS)*, China, June 2021.
- [27] Diane: Identifying Fuzzing Triggers in Apps to Generate Under-constrained Inputs for IoT Devices. Nilo Redini, Andrea Continella, Dipanjan Das, Giulio Pasquale, Noah Spahn, Aravind Machiry, Antonio Bianchi, Christopher Kruegel, and Giovanni Vigna. In **IEEE Symposium on Security and Privacy**, IEEE Computer Society Press, USA, May 2021.
- [28] Tracing and Analyzing Web Access Paths Based on User-Side Data Collection: How Do Users Reach Malicious URLs? Takeshi Takahashi, Christopher Kruegel, Giovanni Vigna, Katsunari Yoshioka, and Daisuke Inoue. In *23rd Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, Spain, October 2020.
- [29] HALucinator: Firmware Re-hosting through Abstraction Layer Emulation. Abraham Clements, Eric Gustafson, Tobias Scharnowski, Paul Grosen, David Fritz, Christopher Kruegel, Giovanni Vigna, Saurabh Bagchi, and Mathias Payer. In **29th Usenix Security Symposium**, USA, August 2020.
- [30] On the Security of Application Installers and Online Software Repositories. Marcus Botacin, Giovanni Bertao, Paulo de Geus, Andre Gregio, Christopher Kruegel, and Giovanni Vigna. In *Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA)*, Portugal, June 2020.
- [31] Exploring Abstraction Functions in Fuzzing. Christopher Salls, Aravind Machiry, Adam Doupe, Yan Shoshitaishvili, Christopher Kruegel, and Giovanni Vigna. In *IEEE Conference on Communications and Network Security (CNS)*, France, June 2020.
- [32] Trust.IO: Protecting Physical Interfaces on Cyber-physical Systems. Chad Spensky, Aravind Machiry, Marcel Busch, Kevin Leach, Rick Housley, Christopher Kruegel, and Giovanni Vigna. In *IEEE Conference on Communications and Network Security (CNS)*, France, June 2020.

- [33] Symbion: Interleaving Symbolic with Concrete Execution Fabio Gritti, Lorenzo Fontana, Eric Gustafson, Fabio Pagani, Andrea Continella, Christopher Kruegel, and Giovanni Vigna. In *IEEE Conference on Communications and Network Security (CNS)*, France, June 2020.
- [34] Spider: Enabling Fast Patch Propagation in Related Software Repositories. Aravind Machiry, Nilo Camellini, Christopher Kruegel, and Giovanni Vigna. In **IEEE Symposium on Security and Privacy**, IEEE Computer Society Press, USA, May 2020.
- [35] Karonte: Detecting Insecure Multi-binary Interactions in Embedded Firmware. Nilo Redini, Aravind Machiry, Ruoyu Wang, Chad Spensky, Andrea Continella, Yan Shoshitaishvili, Christopher Kruegel, Giovanni Vigna. In **IEEE Symposium on Security and Privacy**, IEEE Computer Society Press, USA, May 2020.
- [36] Dirty Clicks: A Study of the Usability and Security Implications of Click-related Behaviors on the Web. Iskander Sanchez-Rola, Davide Balzarotti, Christopher Kruegel, Giovanni Vigna, and Igor Santos. In *The Web Conference*, Taiwan, April 2020.
- [37] When Malware is Packin’ Heat; Limits of Machine Learning Classifiers Based on Static Analysis Features. Hojjat Aghakhani, Fabio Gritti, Francesco Mecca, Martina Lindorfer, Stefano Ortolani, Davide Balzarotti, Giovanni Vigna, and Christopher Kruegel. In **Network and Distributed System Security Symposium (NDSS)**, USA, February 2020.
- [38] Neurlux: Dynamic Malware Analysis Without Feature Engineering. Chani Jindal, Christopher Salls, Hojjat Aghakhani, Keith Long, Christopher Kruegel, and Giovanni Vigna. In *Annual Computer Security Applications Conference (ACSAC)*, Puerto Rico, December 2019.
- [39] Sleak: Automating Address Space Layout Derandomization. Christophe Hauser, Jayakrishna Menon, Yan Shoshitaishvili, Ruoyu Wang, Giovanni Vigna, and Christopher Kruegel. In *Annual Computer Security Applications Conference (ACSAC)*, Puerto Rico, December 2019.
- [40] Toward the Analysis of Embedded Firmware through Automated Re-hosting. Eric Gustafson, Marius Muench, Chad Spensky, Nilo Redini, Aravind Machiry, Davide Balzarotti, Yanick Fratantonio, Aurelien Francillon, Yung Ryn Choe, Christopher Kruegel, and Giovanni Vigna. In *22nd Symposium on Research in Attacks, Intrusions and Defenses (RAID), Lecture Notes in Computer Science, Springer Verlag*, China, September 2019.
- [41] BinTrimmer: Towards Static Binary Debloating Through Abstract Interpretation. Nilo Redini, Ruoyu Wang, Aravind Machiry, Yan Shoshitaishvili, Giovanni Vigna, and Christopher Kruegel. In *Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA)*, Sweden, June 2019.
- [42] Think Outside the Dataset: Finding Fraudulent Reviews using Cross-Dataset Analysis. Shirin Nilizadeh, Hojjat Aghakhani, Eric Gustafson, Christopher Kruegel, and Giovanni Vigna. In *International World Wide Web Conference (WWW)*, USA, May 2019.
- [43] BootKeeper: Validating Software Integrity Properties on Boot Firmware Images. Ronny Chevalier, Stefano Cristalli, Christophe Hauser, Yan Shoshitaishvili, Ruoyu Wang, Christopher Kruegel, Giovanni Vigna, Danilo Bruschi, and Andrea LANZI. In *ACM Conference on Data and Application Security and Privacy (CODASPY)*, USA, March 2019.
- [44] Towards Automatically Generating a Sound and Complete Dataset for Evaluating Static Analysis Tools. Aravind Machiry, Nilo Redini, Eric Gustafson, Hojjat Aghakhani, Christopher Kruegel, and Giovanni Vigna. In *Workshop on Binary Analysis Research (BAR)*, USA, February 2019.
- [45] PeriScope: An Effective Probing and Fuzzing Framework for the Hardware-OS Boundary. Dokyung Song, Felicitas Hetzelt, Dipanjan Das, Chad Spensky, Yeoul Na, Stijn Volckaert, Giovanni Vigna, Christopher Kruegel, Jean-Pierre Seifert, and Michael Franz. In **Network and Distributed System Security Symposium (NDSS)**, Internet Society, USA, February 2019.

- [46] Using Loops For Malware Classification Resilient to Feature-unaware Perturbations. Aravind Machiry, Nilo Redini, Eric Gustafson, Yanick Fratantonio, Yung Ryn Choe, Christopher Kruegel, and Giovanni Vigna. In *Annual Computer Security Application Conference (ACSAC)*, USA, December 2018.
- [47] MineSweeper: An In-depth Look into Drive-by Cryptocurrency Mining and Its Defense. Radhesh Konoth, Emanuele Vineti, Veelasha Moonsamy, Martina Lindorfer, Christopher Kruegel, Herbert Bos, and Giovanni Vigna. In **25th ACM Conference on Computer and Communications Security (CCS)**, Canada, October 2018.
- [48] HeapHopper: Bringing Bounded Model Checking to Heap Implementation Security. Moritz Eckert, Antonio Bianchi, Ruoyu Wang, Yan Shoshitaishvili, Christopher Kruegel, and Giovanni Vigna. In **27th Usenix Security Symposium**, USA, August 2018.
- [49] Rampart: Protecting Web Applications from CPU-Exhaustion Denial-of-Service Attacks. Wei Meng, Chenxiong Qian, Shuang Hao, Kevin Borgolte, Giovanni Vigna, Christopher Kruegel, and Wenke Lee. In **27th Usenix Security Symposium**, USA, August 2018.
- [50] GuardION: Practical Mitigation of DMA-based Rowhammer Attacks on ARM. Victor van der Veen, Martina Lindorfer, Yanick Fratantonio, Harikrishnan Padmanabha Pillai, Giovanni Vigna, Christopher Kruegel, Herbert Bos, and Kaveh Razavi. In *Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA)*, France, June 2018.
- [51] Detecting Deceptive Reviews using Generative Adversarial Networks. Hojjat Aghakhani, Aravind Machiry, Shirin Nilizadeh, Christopher Kruegel, and Giovanni Vigna. In *Deep Learning and Security Workshop*, USA, May 2018.
- [52] Measuring E-Mail Header Injections on the World Wide Web. Sai Chandramouli, Pierre-Marie Bajan, Christopher Kruegel, Giovanni Vigna, Ziming Zhao, Adam Doupe, and Gail-Joon Ahn. In *ACM Symposium on Applied Computing (SAC)*, France, April 2018.
- [53] In rDNS We Trust: Revisiting a Common Data-Source’s Reliability. Tobias Fiebig, Kevin Borgolte, Shuang Hao, Christopher Kruegel, Giovanni Vigna, and Anja Feldmann. In *Passive and Active Measurement Conference (PAM)*, Germany, March 2018.
- [54] Broken Fingers: On the Usage of the Fingerprint API in Android. Antonio Bianchi, Yanick Fratantonio, Aravind Machiry, Christopher Kruegel, Giovanni Vigna, Pak Chung, and Wenke Lee. In **Network and Distributed System Security Symposium (NDSS)**, Internet Society, USA, February 2018.
- [55] Cloud Strife: Mitigating the Security Risks of Domain-Validated Certificate. Kevin Borgolte, Tobias Fiebig, Shuang Hao, Christopher Kruegel, and Giovanni Vigna. In **Network and Distributed System Security Symposium (NDSS)**, Internet Society, USA, February 2018.
- [56] Exploitation and Mitigation of Authentication Schemes Based on Device-Public Information. Antonio Bianchi, Eric Gustafson, Yanick Fratantonio, Christopher Kruegel, and Giovanni Vigna. In *Annual Computer Security Application Conference (ACSAC)*, USA, December 2017.
- [57] Piston: Uncooperative Remote Runtime Patching. Christopher Salls, Yan Shoshitaishvili, Nick Stephens, Christopher Kruegel, and Giovanni Vigna. In *Annual Computer Security Applications Conference (ACSAC)*, USA, December 2017.
- [58] Rise of the HaCRS: Augmenting Autonomous Cyber Reasoning Systems with Human Assistance. Yan Shoshitaishvili, Michael Weissbacher, Lukas Dresel, Christopher Salls, Ruoyu Wang, Christopher Kruegel, and Giovanni Vigna. In **24th ACM Conference on Computer and Communications Security (CCS)**, ACM Press, USA, October 2017.

- [59] Poised: Spotting Twitter Spam Off the Beaten Paths. Shirin Nilizadeh, Francois Labreche, Alireza Sadighian, Ali Zand, Jose Fernandez, Christopher Kruegel, Gianluca Stringhini, and Giovanni Vigna. In **24th ACM Conference on Computer and Communications Security (CCS)**, ACM Press, USA, October 2017.
- [60] Difuze: Interface Aware Fuzzing for Kernel Drivers. Jake Corina, Aravind Machiry, Christopher Salls, Yan Shoshitaishvili, Shuang Hao, Christopher Kruegel, and Giovanni Vigna. In **24th ACM Conference on Computer and Communications Security (CCS)**, ACM Press, USA, October 2017.
- [61] How Shall We Play a Game: A Game-Theoretical Model for Cyber-warfare Games. Tiffany Bao, Yan Shoshitaishvili, Ruoyu Wang, Christopher Kruegel, Giovanni Vigna, and David Brumley. In *IEEE Computer Security Foundations Symposium (CSF)*, USA, August 2017.
- [62] Dr. Checker: A Soundy Analysis for Linux Kernel Drivers Aravind Machiry, Chad Spensky, Jake Corina, Nick Stephens, Christopher Kruegel, and Giovanni Vigna. In **26th Usenix Security Symposium**, Canada, August 2017.
- [63] BootStomp: On the Security of Bootloaders in Mobile Devices. Nilo Redini, Aravind Machiry, Dipanjan Das, Yanick Fratantonio, Antonio Bianchi, Eric Gustafson, Yan Shoshitaishvili, Christopher Kruegel, and Giovanni Vigna. In **26th Usenix Security Symposium**, Canada, August 2017.
- [64] On the Privacy and Security of the Ultrasound Ecosystem. Vasilios Mavroudis, Shuang Hao, Yanick Fratantonio, Federico Maggi, Christopher Kruegel, and Giovanni Vigna. In *Privacy Enhancing Technologies Symposium (PETS)*, USA, July 2017.
- [65] Gossip: Automatically Identifying Malicious Domains from Mailing List Discussions. Cheng Huang, Shuang Hao, Luca Invernizzi, Jiayong Liu, Yong Fang, Christopher Kruegel, and Giovanni Vigna. In *ACM Asia Conference on Computer and Communications Security (AsiaCCS)*, UAE, April 2017.
- [66] Something From Nothing (There): Collecting Global IPv6 Datasets From DNS. Tobias Fiebig, Kevin Borgolte, Shuang Hao, Christopher Kruegel, and Giovanni Vigna. In *Passive Active Measurement Conference (PAM)*, Australia, March 2017.
- [67] Obfuscation-Resilient Privacy Leak Detection for Mobile Apps Through Differential Analysis. Andrea Continella, Yanick Fratantonio, Martina Lindorfer, Alessandro Puccetti, Ali Zand, Christopher Kruegel, and Giovanni Vigna. In **Network and Distributed System Security Symposium (NDSS)**, Internet Society, USA, February 2017.
- [68] Boomerang: Exploiting the Semantic Gap in Trusted Execution Environments. Aravind Machiry, Eric Gustafson, Chad Spensky, Christopher Salls, Nick Stephens, Ruoyu Wang, Antonio Bianchi, Yung Choe, Christopher Kruegel, and Giovanni Vigna. In **Network and Distributed System Security Symposium (NDSS)**, Internet Society, USA, February 2017.
- [69] Ramblr: Making Reassembly Great Again. Ruoyu Wang, Yan Shoshitaishvili, Antonio Bianchi, Aravind Machiry, John Grosen, Paul Grosen, Christopher Kruegel, and Giovanni Vigna. In **Network and Distributed System Security Symposium (NDSS)**, Internet Society, USA, February 2017.
- [70] Taming Transactions: Towards Hardware-Assisted Control Flow Integrity using Transactional Memory. Marius Muench, Fabio Pagani, Yan Shoshitaishvili, Christopher Kruegel, Giovanni Vigna, and Davide Balzarotti. In *19th Symposium on Research in Attacks, Intrusions and Defenses (RAID), Lecture Notes in Computer Science, Springer Verlag*, France, September 2016.
- [71] TriggerScope: Towards Detecting Logic Bombs in Android Applications. Yanick Fratantonio, Antonio Bianchi, William Robertson, Engin Kirda, Christopher Kruegel, and Giovanni Vigna. In **IEEE Symposium on Security and Privacy**, IEEE Computer Society Press, USA, May 2016.

- [72] SoK: (State of) The Art of War: Offensive Techniques in Binary Analysis. Yan Shoshitaishvili, Ruoyu Wang, Christopher Salls, Nick Stephens, Mario Polino, Audrey Dutcher, John Grosen, Siji Feng, Christophe Hauser, Christopher Kruegel, and Giovanni Vigna. In **IEEE Symposium on Security and Privacy**, IEEE Computer Society Press, USA, May 2016.
- [73] Going Native: Using a Large-Scale Analysis of Android Apps to Create a Practical Native-Code Sandboxing Policy. Vitor Afonso, Paulo de Geus, Antonio Bianchi, Yanick Fratantonio, Christopher Kruegel, Giovanni Vigna, Adam Doupe, and Mario Polino. In **Network and Distributed System Security Symposium (NDSS)**, Internet Society, USA, February 2016.
- [74] Driller: Augmenting Fuzzing Through Selective Symbolic Execution. Nick Stephens, John Grosen, Christopher Salls, Audrey Dutcher, Ruoyu Wang, Jacopo Corbetta, Yan Shoshitaishvili, Christopher Kruegel, and Giovanni Vigna. In **Network and Distributed System Security Symposium (NDSS)**, Internet Society, USA, February 2016.
- [75] Grab 'n Run: Secure and Practical Dynamic Code Loading for Android Applications. Luca Falsina, Yanick Fratantonio, Stefano Zanero, Christopher Kruegel, Giovanni Vigna, and Federico Maggi. In *31st Annual Computer Security Applications Conference (ACSAC)*, IEEE Computer Society Press, USA, December 2015.
- [76] BareDroid: Large-Scale Analysis of Android Apps on Real Devices. Simone Mutti, Yanick Fratantonio, Antonio Bianchi, Luca Invernizzi, Jacopo Corbetta, Dhilung Kirat, Christopher Kruegel, and Giovanni Vigna. In *31st Annual Computer Security Applications Conference (ACSAC)*, IEEE Computer Society Press, USA, December 2015.
- [77] Know Your Achilles' Heel: Automatic Detection of Network Critical Services. Ali Zand, Amir Houmansadr, Giovanni Vigna, Richard Kemmerer, and Christopher Kruegel. In *31st Annual Computer Security Applications Conference (ACSAC)*, IEEE Computer Society Press, USA, December 2015.
- [78] NJAS: Sandboxing Unmodified Applications in Non-rooted Devices Running Stock Android. Antonio Bianchi, Yanick Fratantonio, Christopher Kruegel, and Giovanni Vigna. In *5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*, USA, October 2015.
- [79] Prison: Tracking Process Interactions to Contain Malware. Benjamin Caillat, Bob Gilbert, Dick Kemmerer, Christopher Kruegel, and Giovanni Vigna. In *International Symposium on CyberSpace Safety and Security*, USA, August 2015.
- [80] CLAPP: Characterizing Loops in Android Applications. Yanick Fratantonio, Aravind Machiry, Antonio Bianchi, Christopher Kruegel, and Giovanni Vigna. In *10th Joint Meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE)*, ACM Press, Italy, August 2015.
- [81] ZigZag: Automatically Hardening Web Applications Against Client-side Validation Vulnerabilities. Michael Weissbacher, William Robertson, Engin Kirda, Christopher Kruegel, and Giovanni Vigna. In **24th Usenix Security Symposium**, USA, August 2015.
- [82] How the ELF Ruined Christmas. Alessandro Di Federico, Amat Cama, Yan Shoshitaishvili, Christopher Kruegel, and Giovanni Vigna. In **24th Usenix Security Symposium**, USA, August 2015.
- [83] Meerkat: Detecting Website Defacements through Image-based Object Recognition. Kevin Borgolte, Christopher Kruegel, and Giovanni Vigna. In **24th Usenix Security Symposium**, USA, August 2015.
- [84] EvilCohort: Detecting Communities of Malicious Accounts on Online Services. Gianluca Stringhini, Pierre Mourlante, Gregoire Jacob, Manuel Egele, Christopher Kruegel, and Giovanni Vigna. In **24th Usenix Security Symposium**, USA, August 2015.

- [85] On the Security and Engineering Implications of Finer-Grained Access Controls for Android Developers and Users. Yanick Fratantonio, Antonio Bianchi, William Robertson, Manuel Egele, Christopher Kruegel, Engin Kirda, and Giovanni Vigna. In *Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), Lecture Notes in Computer Science, Springer Verlag*, Italy, July 2015.
- [86] Portrait of a Privacy Invasion - Detecting Relationships Through Large-scale Photo Analysis. Yan Shoshitaishvili, Christopher Kruegel, and Giovanni Vigna. In *15th Privacy Enhancing Technologies Symposium (PETS), De Gruyter Open*, USA, June 2015.
- [87] Framing Dependencies Introduced by Underground Commoditization. Kurt Thomas, Danny Yuxing Huang, David Wang, Elie Bursztein, Chris Grier, Tom Holt, Christopher Kruegel, Damon McCoy, Stefan Savage, and Giovanni Vigna. In *Workshop on the Economics of Information Security (WEIS)*, Netherlands, June 2015.
- [88] A Large-Scale Study of Mobile Web App Security. Patrick Mutchler, Adam Doupe, John Mitchell, Christopher Kruegel, and Giovanni Vigna. In *Mobile Security Technologies Workshop (MoST)*, USA, May 2015.
- [89] What the App is That? Deception and Countermeasures in the Android User Interface. Antonio Bianchi, Jacopo Corbetta, Luca Invernizzi, Yanick Fratantonio, Christopher Kruegel, and Giovanni Vigna. In **IEEE Symposium on Security and Privacy**, IEEE Computer Society Press, USA, May 2015.
- [90] Firmalice - Automatic Detection of Authentication Bypass Vulnerabilities in Binary Firmware. Yan Shoshitaishvili, Ruoyu Wang, Christophe Hauser, Christopher Kruegel, and Giovanni Vigna. In **Network and Distributed System Security Symposium (NDSS)**, Internet Society, USA, February 2015.
- [91] EdgeMiner: Automatically Detecting Implicit Control Flow Transitions through the Android Framework. Yinzhi Cao, Yanick Fratantonio, Antonio Bianchi, Manuel Egele, Christopher Kruegel, Giovanni Vigna, and Yan Chen. In **Network and Distributed System Security Symposium (NDSS)**, Internet Society, USA, February 2015.
- [92] The Dark Alleys of Madison Avenue: Understanding Malicious Advertisements. Apostolis Zarras, Alexandros Kapravelos, Gianluca Stringhini, Thorsten Holz, Christopher Kruegel, and Giovanni Vigna. In *Internet Measurement Conference (IMC), ACM Press*, Canada, November 2014.
- [93] Eyes of a Human, Eyes of a Program: Leveraging different views of the web for analysis and detection. Jacopo Corbetta, Luca Invernizzi, Christopher Kruegel, and Giovanni Vigna. In *17th Symposium on Research in Attacks, Intrusions and Defenses (RAID), Lecture Notes in Computer Science, Springer Verlag*, Sweden, September 2014.
- [94] Protecting Web Single Sign-on against Relying party Impersonation Attacks through a Bi-directional Secure Channel with Authentication. Yinzhi Cao, Yan Shoshitaishvili, Kevin Borgolte, Christopher Kruegel, Giovanni Vigna, and Yan Chen. In *17th Symposium on Research in Attacks, Intrusions and Defenses (RAID), Lecture Notes in Computer Science, Springer Verlag*, Sweden, September 2014.
- [95] Hulk: Eliciting Malicious Behavior in Browser Extensions. Alexandros Kapravelos, Chris Grier, Neha Chachra, Christopher Kruegel, Giovanni Vigna, and Vern Paxson. In **23rd Usenix Security Symposium**, USA, August 2014.
- [96] BareCloud: Bare-metal Analysis-based Evasive Malware Detection. Dhilung Kirat, Giovanni Vigna, and Christopher Kruegel. In **23rd Usenix Security Symposium**, USA, August 2014.
- [97] PExy: The other side of Exploit Kits. Giancarlo De Maio, Alexandros Kapravelos, Yan Shoshitaishvili, Christopher Kruegel, and Giovanni Vigna. In *Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), Lecture Notes in Computer Science, Springer Verlag*, United Kingdom, July 2014.

- [98] The Harvester, the Botmaster, and the Spammer: On the Relations Between the Different Actors in the Spam Landscape. Gianluca Stringhini, Oliver Hohlfeld, Christopher Kruegel, and Giovanni Vigna. In *ACM Symposium on InformAtion, Computer and Communications Security (ASIACCS)*, ACM Press, Japan, June 2014.
- [99] The Tricks of the Trade: What Makes Spam Campaigns Successful?. Jane Iedemska, Gianluca Stringhini, Richard Kemmerer, Christopher Kruegel, and Giovanni Vigna. In *International Workshop on Cyber Crime (IWCC)*, IEEE Press, USA, May 2014.
- [100] Rippler: Delay Injection for Service Dependency Detection. Ali Zand, Giovanni Vigna, Richard Kemmerer, Christopher Kruegel. In *IEEE International Conference on Computer Communications (INFOCOM)*, IEEE Computer Society Press, Canada, April 2014.
- [101] Stranger Danger: Exploring the Ecosystem of Ad-based URL Shortening Services. Nick Nikiforakis, Federico Maggi, Gianluca Stringhini, M. Zubair Rafique, Wouter Joosen, Christopher Kruegel, Frank Piessens, Giovanni Vigna, and Stefano Zanero. In *International World Wide Web Conference (WWW)*, South Korea, April 2014.
- [102] Extracting Probable Command and Control Signatures for Detecting Botnets. Ali Zand, Giovanni Vigna, Xifeng Yan, and Christopher Kruegel. In *ACM Symposium on Applied Computing (SAC)*, ACM Press, South Korea, March 2014.
- [103] Execute This! Analyzing Unsafe and Malicious Dynamic Code Loading in Android Applications. Sebastian Poeplau, Yanick Fratantonio, Antonio Bianchi, Christopher Kruegel, and Giovanni Vigna. In **Network and Distributed System Security Symposium (NDSS)**, USA, February 2014.
- [104] Nazca: Detecting Malware Distribution in Large-Scale Networks. Luca Invernizzi, Stanislav Miskovic, Ruben Torres, Sabyasachi Saha, Sung-Ju Lee, Marco Mellia, Christopher Kruegel, and Giovanni Vigna. In **Network and Distributed System Security Symposium (NDSS)**, USA, February 2014.
- [105] Message In A Bottle: Sailing Past Censorship. Luca Invernizzi, Christopher Kruegel, and Giovanni Vigna. In *29th Annual Computer Security Applications Conference (ACSAC)*, IEEE Computer Society Press, USA, December 2013.
- [106] Shady Paths: Leveraging Surfing Crowds to Detect Malicious Web Pages. Gianluca Stringhini, Christopher Kruegel, and Giovanni Vigna. In **20th ACM Conference on Computer and Communications Security (CCS)**, ACM Press, Germany, November 2013.
- [107] deDacota: Toward Preventing Server-Side XSS via Automatic Code and Data Separation. Adam Doupe, Weidong Cui, Mariusz Jakubowski, Marcus Peinado, Christopher Kruegel, and Giovanni Vigna. In **20th ACM Conference on Computer and Communications Security (CCS)**, ACM Press, Germany, November 2013.
- [108] Delta: Automatic Identification of Unknown Web-based Infection Campaigns. Kevin Borgolte, Christopher Kruegel, and Giovanni Vigna. In **20th ACM Conference on Computer and Communications Security (CCS)**, ACM Press, Germany, November 2013.
- [109] An Empirical Study of Cryptographic Misuse in Android Applications. Manuel Egele, David Brumley, Yanick Fratantonio, and Christopher Kruegel. In **20th ACM Conference on Computer and Communications Security (CCS)**, ACM Press, Germany, November 2013.
- [110] Practical Attacks Against The I2P Network. Christoph Egger, Johannes Schlumberger, Christopher Kruegel, and Giovanni Vigna. In *16th Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, Lecture Notes in Computer Science, Springer Verlag, St. Lucia, October 2013.
- [111] Follow the Green: Growth and Dynamics in Twitter Follower Markets. Gianluca Stringhini, Gang Wang, Manuel Egele, Christopher Kruegel, Giovanni Vigna, Haitao Zheng, Ben Zhao. In *Internet Measurement Conference (IMC)*, ACM Press, Spain, October 2013.

- [112] Revolver: An Automated Approach to the Detection of Evasive Web-based Malware. Alexandros Kapravelos, Yan Shoshitaishvili, Marco Cova, Christopher Kruegel, and Giovanni Vigna. In **22nd Usenix Security Symposium**, USA, August 2013.
- [113] Steal This Movie - Automatically Bypassing DRM Protection in Streaming Media Services. Ryuou Wang, Yan Shoshitaishvili, Christopher Kruegel, and Giovanni Vigna. In **22nd Usenix Security Symposium**, USA, August 2013.
- [114] Cookieless Monster: Exploring the Ecosystem of Web-based Device Fingerprinting. Nick Nikiforakis, Alexandros Kapravelos, Wouter Joosen, Christopher Kruegel, Frank Piessens, Giovanni Vigna. In **IEEE Symposium on Security and Privacy**, USA, May 2013.
- [115] Two Years of Short URLs Internet Measurement: Security Threats and Countermeasures. Federico Maggi, Alessandro Frossi, Stefano Zanero, Gianluca Stringhini, Brett Stone-Gross, Christopher Kruegel, and Giovanni Vigna. In *International World Wide Web Conference (WWW)*, Brazil, April 2013.
- [116] EARs in the Wild: Large-Scale Analysis of Execution After Redirect Vulnerabilities. Pierre Payet, Adam Doupe, Christopher Kruegel, and Giovanni Vigna. In *ACM Symposium on Applied Computing (SAC)*, ACM Press, Portugal, March 2013.
- [117] Clickonomics: Determining the Effect of Anti-Piracy Measures for One-Click Hosting. Tobias Lauinger, Martin Szydłowski, Kaan Onarlioglu, Gilbert Wondracek, Engin Kirda and Christopher Kruegel. In **Network and Distributed System Security Symposium (NDSS)**, USA, February 2013.
- [118] COMPA: Detecting Compromised Accounts on Social Networks. Manuel Egele, Gianluca Stringhini, Christopher Kruegel, and Giovanni Vigna. In **Network and Distributed System Security Symposium (NDSS)**, USA, February 2013.
- [119] Jarhead: Analysis and Detection of Malicious Java Applets. Johannes Schlumberger, Christopher Kruegel, and Giovanni Vigna. In *28th Annual Computer Security Applications Conference (ACSAC)*, IEEE Computer Society Press, USA, December 2012.
- [120] Disclosure: Detecting Botnet Command and Control Servers Through Large-Scale NetFlow Analysis. Leyla Bilge, Davide Balzarotti, William Robertson, Engin Kirda, and Christopher Kruegel. In *28th Annual Computer Security Applications Conference (ACSAC)*, IEEE Computer Society Press, USA, December 2012.
- [121] BotFinder: Finding Bots in Network Traffic Without Deep Packet Inspection. Florian Tegeler, Xiaoming Fu, Giovanni Vigna, and Christopher Kruegel. In *ACM Conference on emerging Networking Experiments and Technologies (CoNEXT)*, ACM Press, USA, October 2012.
- [122] Blacksheep: Detecting Compromised Hosts in Homogeneous Crowds. Antonio Bianchi, Yan Shoshitaishvili, Christopher Kruegel, and Giovanni Vigna. In **19th ACM Conference on Computer and Communications Security (CCS)**, ACM Press, USA, October 2012.
- [123] PeerPress: Utilizing Enemies' P2P Strength Against Them. Zhaoyan Xu, Lingfeng Chen, Guofei Gu, and Christopher Kruegel. In **19th ACM Conference on Computer and Communications Security (CCS)**, ACM Press, USA, October 2012.
- [124] You Are What You Include: Large-scale Evaluation of Remote JavaScript Inclusions. Nick Nikiforakis, Luca Invernizzi, Alexandros Kapravelos, Steven Van Acker, Wouter Joosen, Christopher Kruegel, Frank Piessens, and Giovanni Vigna. In **19th ACM Conference on Computer and Communications Security (CCS)**, ACM Press, USA, October 2012.
- [125] FlashDetect: ActionScript 3 Malware Detection. Timon Van Overveldt, Christopher Kruegel, and Giovanni Vigna. In *Symposium on Recent Advances in Intrusion Detection (RAID)*, Lecture Notes in Computer Science, Springer Verlag, Netherlands, September 2012.

- [126] PUBCRAWL: Protecting Users and Businesses from CRAWLers. Gregoire Jacob, Engin Kirda, Christopher Kruegel, and Giovanni Vigna. In **21th Usenix Security Symposium**, USA, August 2012.
- [127] Enemy of the State: A State-Aware Black-Box Web Vulnerability Scanner. Adam Doupe, Ludovico Cavedon, Christopher Kruegel, and Giovanni Vigna. In **21th Usenix Security Symposium**, USA, August 2012.
- [128] B@bel: Leveraging Email Delivery for Spam Mitigation. Gianluca Stringhini, Manuel Egele, Apostolis Zarras, Thorsten Holz, Christopher Kruegel, and Giovanni Vigna. In **21th Usenix Security Symposium**, USA, August 2012.
- [129] Poultry Markets: On the Underground Economy of Twitter Followers. Gianluca Stringhini, Manuel Egele, Christopher Kruegel, and Giovanni Vigna. In *Workshop on Online Social Networks (WOSN)*, ACM Press, Finland, August 2012.
- [130] A Quantitative Study of Accuracy in System Call-Based Malware Detection. Davide Canali, Andrea Lanzi, Davide Balzarotti, Christopher Kruegel, Mihai Christodorescu, and Engin Kirda. In *International Symposium on Software Testing and Analysis (ISSTA)*, ACM Press, USA, July 2012.
- [131] ViewPoints: Differential String Analysis for Discovering Client- and Server-Side Input Validation Inconsistencies. Muath Alkhalaf, Shauvik Roy Choudhary, Mattia Fazzini, Tevfik Bultan, Alessandro Orso, and Christopher Kruegel. In *International Symposium on Software Testing and Analysis (ISSTA)*, ACM Press, USA, July 2012.
- [132] A static, packer-agnostic filter to detect similar malware samples. Gregoire Jacob, Paolo Milani Comparetti, Matthias Neugschwandtner, Christopher Kruegel, and Giovanni Vigna. In *Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA)*, Lecture Notes in Computer Science, Springer Verlag, Greece, July 2012.
- [133] Tracking Memory Writes for Malware Classification and Code Reuse Identification (Short Paper). Andre Gregio, Paulo Licio de Geus, Christopher Kruegel, and Giovanni Vigna. In *Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA)*, Lecture Notes in Computer Science, Springer Verlag, Greece, July 2012.
- [134] Enforcing Dynamic Spectrum Access with Spectrum Permits. Lei Yang, Zengbin Zhang, Ben Zhao, Christopher Kruegel, and Haitao Zheng. In *13th International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, ACM Press, USA, June 2012.
- [135] EvilSeed: A Guided Approach to Finding Malicious Web Pages. Luca Invernizzi, Stefano Benvenuti, Marco Cova, Paolo Milani Comparetti, Christopher Kruegel, and Giovanni Vigna. In **IEEE Symposium on Security and Privacy**, USA, May 2012.
- [136] Detecting social cliques for automated privacy control in online social networks. Hakan Yildiz and Christopher Kruegel. In *IEEE International Workshop on Security and SOcial Networking (SESOC)*, IEEE Press, Switzerland, March 2012.
- [137] ForeCast - Skimming off the Malware Cream. Matthias Neugschwandtner, Paolo Milani Comparetti, Gregoire Jacob, and Christopher Kruegel. In *27th Annual Computer Security Applications Conference (ACSAC)*, IEEE Computer Society Press, USA, December 2011.
- [138] BareBox: Efficient Malware Analysis on Bare-Metal. Dhilung Kirat, Giovanni Vigna, and Christopher Kruegel. In *27th Annual Computer Security Applications Conference (ACSAC)*, IEEE Computer Society Press, USA, December 2011.
- [139] Nexat: A history-based approach to predict attacker actions. Casey Cipriano, Ali Zand, Amir Houmansadr, Christopher Kruegel, and Giovanni Vigna. In *27th Annual Computer Security Applications Conference (ACSAC)*, IEEE Computer Society Press, USA, December 2011.

- [140] Understanding Fraudulent Activities in Online Ad Exchanges. Brett Stone-Gross, Ryan Stevens, Richard Kemmerer, Christopher Kruegel, Giovanni Vigna, and Apostolis Zarras. In *Internet Measurement Conference (IMC)*, ACM Press, Germany, November 2011.
- [141] The Power of Procrastination: Detection and Mitigation of Execution-Stalling Malicious Code. Clemens Kolbitsch, Engin Kirda, and Christopher Kruegel. In **18th ACM Conference on Computer and Communications Security (CCS)**, USA, October 2011.
- [142] Fear the EAR: Discovering and Mitigating Execution After Redirect Vulnerabilities. Adam Doupe, Bryce Boe, Christopher Kruegel, and Giovanni Vigna. In **18th ACM Conference on Computer and Communications Security (CCS)**, USA, October 2011.
- [143] Silverline: Toward Data Confidentiality in Storage-Intensive Cloud Applications. Krishna Puttaswamy, Christopher Kruegel, and Ben Zhao. In *ACM Symposium on Cloud Computing (SoCC)*, ACM Press, USA, October 2011.
- [144] Dymo: Tracking Dynamic Code Identity. Bob Gilbert, Richard Kemmerer, Christopher Kruegel, and Giovanni Vigna. In *Symposium on Recent Advances in Intrusion Detection (RAID)*, Lecture Notes in Computer Science, Springer Verlag, USA, September 2011.
- [145] Shellzer: A tool for the dynamic analysis of malicious shellcode. Yanick Fratantonio, Christopher Kruegel, and Giovanni Vigna. In *Symposium on Recent Advances in Intrusion Detection (RAID)*, Lecture Notes in Computer Science, Springer Verlag, USA, September 2011.
- [146] Jackstraws: Picking Command and Control Connections from Bot Traffic. Gregoire Jacob, Ralf Hund, Christopher Kruegel, and Thorsten Holz. In **20th Usenix Security Symposium**, USA, August 2011.
- [147] BotMagnifier: Locating Spambots on the Internet. Gianluca Stringhini, Thorsten Holz, Brett Stone-Gross, Christopher Kruegel, and Giovanni Vigna. In **20th Usenix Security Symposium**, USA, August 2011.
- [148] BTLab: A System-Centric, Data-Driven Analysis and Measurement Platform for BitTorrent Clients. Martin Szydlowski, Ben Zhao, Engin Kirda, and Christopher Kruegel. In *IEEE Workshop on Grid and P2P Systems and Applications (GridPeer)*, IEEE Computer Society Press, USA, August 2011.
- [149] Escape from Monkey Island: Evading High-Interaction Honeyclients. Alexandros Kapravelos, Marco Cova, Christopher Kruegel, and Giovanni Vigna. In *Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA)*, Lecture Notes in Computer Science, Springer Verlag, Netherlands, July 2011.
- [150] MISHIMA: Multilateration of Internet hosts hidden using malicious fast-flux agents (Short Paper). Greg Banks, Aristide Fattori, Richard Kemmerer, Christopher Kruegel, and Giovanni Vigna. In *Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA)*, Lecture Notes in Computer Science, Springer Verlag, Netherlands, July 2011.
- [151] The Underground Economy of Fake Antivirus Software. Brett Stone-Gross, Ryan Abman, Richard Kemmerer, Christopher Kruegel, Douglas Steigerwald, and Giovanni Vigna. In *10th Workshop on the Economics of Information Security (WEIS)*, USA, June 2011.
- [152] Peering Through the iFrame. Brett Stone-Gross, Marco Cova, Christopher Kruegel, and Giovanni Vigna. In *30th IEEE International Conference on Computer Communications (IEEE INFOCOM) Mini-Conference*, China, April 2011.
- [153] Prophiler: A Fast Filter for the Large-Scale Detection of Malicious Web Pages. Davide Canali, Marco Cova, Christopher Kruegel, and Giovanni Vigna. In *International World Wide Web Conference (WWW)*, India, March 2011.

- [154] PoX: Protecting Users from Malicious Facebook Applications. Manuel Egele, Andreas Moser, Christopher Kruegel, and Engin Kirda. In *3rd IEEE International Workshop on Security in Social Networks*, USA, March 2011.
- [155] Exposure: Finding Malicious Domains Using Passive DNS Analysis. Leyla Bilge, Engin Kirda, Christopher Kruegel, and Marco Balduzzi. In **Network and Distributed System Security Symposium (NDSS)**, USA, February 2011.
- [156] PiOS: Detecting Privacy Leaks in iOS Applications Manuel Egele, Christopher Kruegel, Engin Kirda, and Giovanni Vigna. In **Network and Distributed System Security Symposium (NDSS)**, USA, February 2011.
- [157] Detecting Spammers On Social Networks. Gianluca Stringhini, Christopher Kruegel, and Giovanni Vigna. In *26th Annual Computer Security Applications Conference (ACSAC)*, *IEEE Computer Society Press*, USA, December 2010.
- [158] AccessMiner: Using System-Centric Models for Malware Protection. Andrea Lanzi, Davide Balzarotti, Christopher Kruegel, Mihai Christoderescu, and Engin Kirda. In **17th ACM Conference on Computer and Communications Security (CCS)**, USA, October 2010.
- [159] Abusing Social Networks for Automated User Profiling. Marco Balduzzi, Christian Platzer, Thorsten Holz, Engin Kirda, Davide Balzarotti, and Christopher Kruegel. In *Symposium on Recent Advances in Intrusion Detection (RAID)*, *Lecture Notes in Computer Science*, Springer Verlag, Canada, September 2010.
- [160] Toward Automated Detection of Logic Vulnerabilities in Web Applications. Viktoria Felmetsger, Ludovico Cavedon, Christopher Kruegel, and Giovanni Vigna. In **19th Usenix Security Symposium**, USA, August 2010.
- [161] Is the Internet for Porn? An Insight Into the Online Adult Industry. Gilbert Wondracek, Thorsten Holz, Christian Platzer, Engin Kirda, and Christopher Kruegel. In *9th Workshop on the Economics of Information Security (WEIS)*, USA, June 2010.
- [162] Inspector Gadget: Automated Extraction of Proprietary Gadgets from Malware Binaries. Clemens Kolbitsch, Thorsten Holz, Christopher Kruegel, and Engin Kirda. In **IEEE Symposium on Security and Privacy**, IEEE Computer Society Press, USA, May 2010.
- [163] Identifying Dormant Functionality in Malware Programs. Paolo Milani Comparetti, Guido Salvaneschi, Engin Kirda, Clemens Kolbitsch, Christopher Kruegel, and Stefano Zanero. In **IEEE Symposium on Security and Privacy**, IEEE Computer Society Press, USA, May 2010.
- [164] A Practical Attack to De-Anonymize Social Network Users. Gilbert Wondracek, Thorsten Holz, Engin Kirda, and Christopher Kruegel. In **IEEE Symposium on Security and Privacy**, IEEE Computer Society Press, USA, May 2010.
- [165] Detection and Analysis of Drive-by-Download Attacks and Malicious JavaScript Code. Marco Cova, Christopher Kruegel, and Giovanni Vigna. In *International World Wide Web Conference (WWW)*, USA, April 2010.
- [166] A Solution for the Automated Detection of Clickjacking Attacks. Marco Balduzzi, Manuel Egele, Engin Kirda, Davide Balzarotti, and Christopher Kruegel. In *ACM Symposium on InformAtion, Computer and Communications Security (ASIACCS)*, *ACM Press*, China, April 2010.
- [167] Improving the Efficiency of Dynamic Malware Analysis. Ulrich Bayer, Engin Kirda, and Christopher Kruegel. In *ACM Symposium on Applied Computing (SAC)*, *ACM Press*, Switzerland, March 2010.
- [168] CAPTCHA Smuggling: Hijacking Web Browsing Sessions to Create CAPTCHA Farms. Manuel Egele, Leyla Bilge, Engin Kirda, and Christopher Kruegel. In *ACM Symposium on Applied Computing (SAC)*, *ACM Press*, Switzerland, March 2010.

- [169] Efficient Detection of Split Personalities in Malware. Davide Balzarotti, Marco Cova, Christoph Karlberger, Christopher Kruegel, Engin Kirda, and Giovanni Vigna. In **Network and Distributed System Security Symposium (NDSS)**, USA, February 2010.
- [170] Effective Anomaly Detection with Scarce Training Data. William Robertson, Federico Maggi, Christopher Kruegel, and Giovanni Vigna. In **Network and Distributed System Security Symposium (NDSS)**, USA, February 2010.
- [171] FIRE: FInding Rogue nETworks. Brett Stone-Gross, Andreas Moser, Kevin Almeroth, Christopher Kruegel, and Engin Kirda. In *25th Annual Computer Security Applications Conference (ACSAC)*, IEEE Computer Society Press, USA, December 2009.
- [172] Analyzing and Detecting Malicious Flash Advertisements. Sean Ford, Marco Cova, Christopher Kruegel, and Giovanni Vigna. In *25th Annual Computer Security Applications Conference (ACSAC)*, IEEE Computer Society Press, USA, December 2009.
- [173] Your Botnet is My Botnet: Analysis of a Botnet Takeover. Brett Stone-Gross, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski, Richard Kemmerer, Christopher Kruegel, and Giovanni Vigna. In **16th ACM Conference on Computer and Communications Security (CCS)**, USA, November 2009.
- [174] Automatically Generating Models for Botnet Detection. Peter Wurzinger, Leyla Bilge, Thorsten Holz, Jan Goebel, Christopher Kruegel, and Engin Kirda. In *14th European Symposium on Research in Computer Security (ESORICS)*, Lecture Notes in Computer Science, Springer Verlag, France, September 2009.
- [175] Protecting a Moving Target: Addressing Web Application Concept Drift. Federico Maggi, William Robertson, Christopher Kruegel, and Giovanni Vigna. In *Symposium on Recent Advances in Intrusion Detection (RAID)*, Lecture Notes in Computer Science, Springer Verlag, France, September 2009.
- [176] Automated Spyware Collection and Analysis. Andreas Stamminger, Christopher Kruegel, Giovanni Vigna, and Engin Kirda. In *12th Information Security Conference (ISC)*, Lecture Notes in Computer Science, Springer Verlag, Italy, September 2009.
- [177] Effective and Efficient Malware Detection at the End Host. Clemens Kolbitsch, Paolo Milani Comparetti, Christopher Kruegel, Engin Kirda, Xiaoyong Zhou, and XiaoFeng Wang. In **18th Usenix Security Symposium**, Canada, August 2009.
- [178] Defending Browsers against Drive-by Downloads: Mitigating Heap-spraying Code Injection Attacks. Manuel Egele, Peter Wurzinger, Christopher Kruegel, and Engin Kirda. In *Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA)*, Lecture Notes in Computer Science, Springer Verlag, Italy, July 2009.
- [179] Prospec: Protocol Specification Extraction. Paolo Milani Comparetti, Gilbert Wondracek, Christopher Kruegel, and Engin Kirda. In **IEEE Symposium on Security and Privacy**, IEEE Computer Society Press, USA, May 2009.
- [180] Removing Web Spam Links from Search Engine Results. Manuel Egele, Christopher Kruegel, and Engin Kirda. In *Annual Conference of the European Institute for Computer Antivirus Research (EICAR)*, Germany, May 2009.
- [181] SWAP: Mitigating XSS Attacks using a Reverse Proxy. Peter Wurzinger, Christian Platzer, Christian Ludl, Engin Kirda, and Christopher Kruegel. In *ICSE Workshop on Software Engineering for Secure Systems (SESS)*, IEEE Computer Society Press, Canada, May 2009.
- [182] A View on Current Malware Behaviors. Ulrich Bayer, Imam Habibi, Davide Balzarotti, Engin Kirda, and Christopher Kruegel. In *Usenix Workshop on Large-scale Exploits and Emergent Threats (LEET)*, April 2009.

- [183] Scalable, Behavior-Based Malware Clustering. Ulrich Bayer, Paolo Milani Comparetti, Clemens Hlauschek, Christopher Kruegel, and Engin Kirda. In **Network and Distributed System Security Symposium (NDSS)**, USA, February 2009.
- [184] A Parallel Architecture for Stateful, High-Speed Intrusion Detection. Luca Foschini, Ashish Thapliyal, Lorenzo Cavallaro, Christopher Kruegel, and Giovanni Vigna. In *International Conference on Information Systems Security (ICISS)*, *Lecture Notes in Computer Science*, Springer Verlag, India, December 2008.
- [185] Overbot - A botnet protocol based on Kademia. Guenther Starnberger, Christopher Kruegel, and Engin Kirda. In *IEEE International Conference on Security and Privacy for Emerging Areas in Communication Networks (Securecomm)*, *IEEE Computer Society Press*, Turkey, September 2008.
- [186] Visual Similarity-Based Phishing Detection. Eric Medvet, Engin Kirda, and Christopher Kruegel. In *IEEE International Conference on Security and Privacy for Emerging Areas in Communication Networks (Securecomm)*, *IEEE Computer Society Press*, Turkey, September 2008.
- [187] Leveraging User Interactions for In-Depth Testing of Web Applications. Sean McAllister, Christopher Kruegel, and Engin Kirda. In *Symposium on Recent Advances in Intrusion Detection (RAID)*, *Lecture Notes in Computer Science*, Springer Verlag, USA, September 2008.
- [188] VeriKey: A Dynamic Certificate Verification System for Public Key Exchanges. Brett Stone-Gross, David Sigal, Rob Cohn, John Morse, Kevin Almeroth, and Christopher Kruegel. In *Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA)*, *Lecture Notes in Computer Science*, Springer Verlag, France, July 2008.
- [189] There Is No Free Phish: An Analysis of “Free” and Live Phishing Kits. Marco Cova, Christopher Kruegel, and Giovanni Vigna. In *Usenix Workshop on Offensive Technologies (WOOT)*, USA, July 2008.
- [190] Davide Balzarotti, Marco Cova, Vika Felmetsger, Nenad Jovanovic, Engin Kirda, Christopher Kruegel, and Giovanni Vigna. Saner: Composing Static and Dynamic Analysis to Validate Sanitization in Web Applications. In **IEEE Symposium on Security and Privacy**, IEEE Computer Society Press, USA, May 2008.
- [191] Automatic Network Protocol Analysis. Gilbert Wondracek, Paulo Milani, Christopher Kruegel, and Engin Kirda. In **Network and Distributed System Security Symposium (NDSS)**, USA, February 2008.
- [192] Limits of Static Analysis for Malware Detection. Andreas Moser, Christopher Kruegel, and Engin Kirda. In *23rd Annual Computer Security Applications Conference (ACSAC)*, *IEEE Computer Society Press*, USA, December 2007.
- [193] Improving Signature Testing Through Dynamic Data Flow Analysis. Davide Balzarotti, William Robertson, Christopher Kruegel, and Giovanni Vigna. In *23rd Annual Computer Security Applications Conference (ACSAC)*, *IEEE Computer Society Press*, USA, December 2007.
- [194] Secure Input for Web Applications. Martin Szydlowski, Christopher Kruegel, and Engin Kirda. In *23rd Annual Computer Security Applications Conference (ACSAC)*, *IEEE Computer Society Press*, USA, December 2007.
- [195] Panorama: Capturing System-wide Information Flow for Malware Detection and Analysis. Heng Yin, Dawn Song, Manuel Egele, Christopher Kruegel, and Engin Kirda. In **14th ACM Conference on Computer and Communications Security (CCS)**, USA, October 2007.
- [196] Detecting System Emulators. Thomas Raffetseder, Christopher Kruegel, and Engin Kirda. In *10th Information Security Conference (ISC)*, *Lecture Notes in Computer Science*, Springer Verlag, Chile, October 2007.

- [197] Mining Specifications of Malicious Behavior. Mihai Christodorescu, Somesh Jha, and Christopher Kruegel. In *6th Joint Meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE)*, ACM Press, Croatia, September 2007.
- [198] A Layout-Similarity-Based Approach for Detecting Phishing Pages. Angelo Rosiello, Engin Kirda, Christopher Kruegel, and Fabrizio Ferrandi, In *IEEE International Conference on Security and Privacy for Emerging Areas in Communication Networks (Securecomm)*, IEEE Computer Society Press, France, September 2007.
- [199] On the Effectiveness of Techniques to Detect Phishing Sites. Christian Ludl, Sean McAllister, Engin Kirda, and Christopher Kruegel. In *Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), Lecture Notes in Computer Science, Springer Verlag*, Switzerland, July 2007.
- [200] Exploiting Redundancy in Natural Language to Penetrate Bayesian Spam Filters. Christoph Karlsruher, Guenter Bayler, Christopher Kruegel, and Engin Kirda. In *Usenix Workshop on Offensive Technologies (WOOT)*, USA, August 2007.
- [201] Dynamic Spyware Analysis. Manuel Egele, Christopher Kruegel, Engin Kirda, Heng Yin, and Dawn Song. In *Usenix Annual Technical Conference*, USA, June 2007.
- [202] Building Anti-Phishing Browser Plug-Ins: An Experience Report. Thomas Raffetseder, Engin Kirda, and Christopher Kruegel. In *ICSE Workshop on Software Engineering for Secure Systems (SESS)*, IEEE Computer Society Press, USA, May 2007.
- [203] Exploring Multiple Execution Paths for Malware Analysis. Andreas Moser, Christopher Kruegel, and Engin Kirda. In **IEEE Symposium on Security and Privacy**, IEEE Computer Society Press, USA, May 2007.
- [204] Philipp Vogt, Florian Nentwich, Nenad Jovanovic, Engin Kirda, Christopher Kruegel, and Giovanni Vigna. Cross Site Scripting Prevention with Dynamic Data Tainting and Static Analysis. In **Network and Distributed System Security Symposium (NDSS)**, USA, February 2007.
- [205] Patrick Klinkoff, Christopher Kruegel, and Engin Kirda. Extending .NET Security to Unmanaged Code. In *Information Security Conference (ISC), Lecture Notes in Computer Science, Springer Verlag*, Greece, September 2006.
- [206] Nenad Jovanovic, Engin Kirda, and Christopher Kruegel. Preventing Cross Site Request Forgery Attacks. In *IEEE International Conference on Security and Privacy for Emerging Areas in Communication Networks (Securecomm)*, USA, August 2006.
- [207] Engin Kirda, Christopher Kruegel, Greg Banks, Giovanni Vigna, and Richard Kemmerer. Behavior-based Spyware Detection. In **15th Usenix Security Symposium**, Canada, August 2006.
- [208] Manuel Egele, Martin Szydlowski, Engin Kirda, and Christopher Kruegel. Using Static Program Analysis to Aid Intrusion Detection. In *Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), Lecture Notes in Computer Science, Springer Verlag*, Germany, July 2006.
- [209] Nenad Jovanovic, Christopher Kruegel, and Engin Kirda. Precise Alias Analysis for Static Detection of Web Application Vulnerabilities. In *ACM Workshop on Programming Languages and Analysis for Security (PLAS)*, ACM Press, Canada, June 2006.
- [210] Stefan Kals, Engin Kirda, and Christopher Kruegel. SecuBat: A Web Vulnerability Scanner. In *15th International World Wide Web Conference*, United Kingdom, May 2006.

- [211] Nenad Jovanovic, Christopher Kruegel, and Engin Kirda. Pixy: A Static Analysis Tool for Detecting Web Application Vulnerabilities (Short Paper). In **IEEE Symposium on Security and Privacy**, IEEE Computer Society Press, USA, May 2006.
- [212] Ulrich Bayer, Christopher Kruegel, and Engin Kirda. TTAalyze: A Tool for Analyzing Malware. In *15th Annual Conference of the European Institute for Computer Antivirus Research (EICAR)*, Germany, May 2006.
- [213] Engin Kirda, Christopher Kruegel, Giovanni Vigna, and Nenad Jovanovic. Noxes: A Client-Side Solution for Mitigating Cross Site Scripting Attacks. In *21st ACM Symposium on Applied Computing (SAC)*, ACM Press, France, April 2006.
- [214] Fredrik Valeur, Giovanni Vigna, Christopher Kruegel, and Engin Kirda. An Anomaly-driven Reverse Proxy for Web Applications. In *21st ACM Symposium on Applied Computing (SAC)*, ACM Press, France, April 2006.
- [215] William Robertson, Giovanni Vigna, Christopher Kruegel and Richard Kemmerer. Using Generalization and Characterization Techniques in the Anomaly-based Detection of Web Attacks. In **Network and Distributed System Security Symposium (NDSS)**, USA, February 2006.
- [216] Christopher Kruegel, Engin Kirda, Darren Mutz, William Robertson, and Giovanni Vigna. Polymorphic Worm Detection Using Structural Information of Executables. In *8th International Symposium on Recent Advances in Intrusion Detection (RAID)*, USA, September 2005.
- [217] Christopher Kruegel, Engin Kirda, Darren Mutz, William Robertson, and Giovanni Vigna. Automating Mimicry Attacks Using Static Binary Analysis. In **14th Usenix Security Symposium**, USA, August 2005.
- [218] Engin Kirda and Christopher Kruegel. Protecting Users Against Phishing Attacks with AntiPhish. In *29th Annual International Computer Software and Applications Conference (COMPSAC)*, IEEE Computer Society Press, United Kingdom, July 2005.
- [219] Darren Mutz, Christopher Kruegel, William Robertson, Giovanni Vigna, and Richard Kemmerer. Reverse Engineering of Network Signatures. In *Information Technology Security Conference (AusCERT)*, Australia, May 2005.
- [220] Christopher Kruegel, William Robertson, and Giovanni Vigna. Detecting Kernel-Level Rootkits Through Binary Analysis. In *20th Annual Computer Security Applications Conference (ACSAC)*, IEEE Computer Society Press, USA, December 2004.
- [221] Christopher Kruegel, William Robertson, Fredrik Valeur, and Giovanni Vigna. Static Analysis of Obfuscated Binaries. In **13th Usenix Security Symposium**, USA, August 2004.
- [222] Christopher Kruegel and William Robertson. Alert Verification - Determining the Success of Intrusion Attempts. In *Workshop on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA), Lecture Notes in Informatics (LNI)*, Germany, July 2004.
- [223] Christopher Kruegel, Darren Mutz, William Robertson and Fredrik Valeur. Bayesian Event Classification for Intrusion Detection. In *19th Annual Computer Security Applications Conference (ACSAC)*, IEEE Computer Society Press, USA, December 2003.
- [224] Christopher Kruegel and Giovanni Vigna. Anomaly Detection of Web-based Attacks. In **10th ACM Conference on Computer and Communications Security (CCS)**, USA, October 2003.
- [225] William Robertson, Christopher Kruegel, Darren Mutz and Fredrik Valeur. Run-time Detection of Heap-based Overflows. In *17th Large Installation Systems Administration Conference (LISA), Usenix*, USA, October 2003.

- [226] Christopher Kruegel, Darren Mutz, Fredrik Valeur and Giovanni Vigna. On the Detection of Anomalous System Call Arguments. In *8th European Symposium on Research in Computer Security (ESORICS), Lecture Notes in Computer Science, Springer Verlag, Norway*, October 2003.
- [227] Christopher Kruegel, Darren Mutz, William Robertson and Fredrik Valeur. Topology-based Detection of Anomalous BGP Messages. In *6th Symposium on Recent Advances in Intrusion Detection (RAID), Lecture Notes in Computer Science, Springer Verlag, USA*, September 2003.
- [228] Christopher Kruegel and Thomas Toth. Using Decision Trees to Improve Signature-based Intrusion Detection. In *6th Symposium on Recent Advances in Intrusion Detection (RAID), Lecture Notes in Computer Science, Springer Verlag, USA*, September 2003.
- [229] Engin Kirda, Clemens Kerer, Christopher Kruegel and Roman Kurmanowytsh. Web Service Engineering with DIWE. In *29th Euromicro, IEEE Computer Society Press, Turkey*, September 2003.
- [230] Thomas Toth and Christopher Kruegel. Evaluating the Impact of Automated Intrusion Response Mechanisms. In *18th Annual Computer Security Applications Conference (ACSAC), IEEE Computer Society Press, USA*, December 2002.
- [231] Thomas Toth and Christopher Kruegel. Accurate Buffer Overflow Detection via Abstract Payload Execution. In *5th Symposium on Recent Advances in Intrusion Detection (RAID), Lecture Notes in Computer Science, Springer Verlag, Switzerland*, October 2002.
- [232] Pascal Fenkam, Harald Gall, Mehdi Jazayeri and Christopher Kruegel. DPS - An Architectural Style for Development of Secure Software. In *Infrastructure Security Conference (InfraSec), Lecture Notes in Computer Science, Springer Verlag, United Kingdom*, October 2002.
- [233] Thomas Toth and Christopher Kruegel. Connection-history based anomaly detection. In *3rd IEEE Information Assurance Workshop, IEEE Computer Society Press, USA*, June 2002.
- [234] Christopher Kruegel, Fredrik Valeur, Giovanni Vigna and Richard Kemmerer. Stateful Intrusion Detection for High-Speed Networks. In **IEEE Symposium on Security and Privacy**, IEEE Computer Society Press, USA, May 2002.
- [235] Engin Kirda, Clemens Kerer and Christopher Kruegel. XGuide - A Practical Guide to XML-based Web Engineering. In *International Workshop on Web Engineering, Lecture Notes in Computer Science, Springer Verlag, Italy*, May 2002.
- [236] Christopher Kruegel, Thomas Toth and Engin Kirda. Service Specific Anomaly Detection for Network Intrusion Detection. In *ACM Symposium on Applied Computing (SAC), ACM Press, Spain*, March 2002.
- [237] Christopher Kruegel and Thomas Toth. Distributed Pattern Detection for Intrusion Detection. In **Network and Distributed System Security Symposium (NDSS)**, USA, February 2002.
- [238] Christopher Kruegel and Thomas Toth. Flexible, Mobile Agent based Intrusion Detection for Dynamic Networks. In *European Wireless, Italy*, February 2002.
- [239] Christopher Kruegel, Thomas Toth and Clemens Kerer. Decentralized Event Correlation for Intrusion Detection. In *International Conference on Information Security and Cryptology (ICISC), Lecture Notes in Computer Science, Springer Verlag, Korea*, December 2001.
- [240] Christopher Kruegel and Thomas Toth. Sparta - A Mobile Agent based Intrusion Detection System. In *IFIP Conference on Network Security (I-NetSec), Kluwer Academic Publishers, Belgium*, November 2001.
- [241] Christopher Kruegel and Thomas Toth. An efficient, IP based solution to the “Logical Timestamp Wrapping” problem. In *6th International Conference on Telecommunications (ConTEL), Croatia*, June 2001.

- [242] Engin Kirda, Clemens Kerer, Mehdi Jazayeri and Christopher Kruegel. Supporting multi-device enabled services: Challenges and open problems. In *10th IEEE Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises*, IEEE Computer Society Press, USA, June 2001.
- [243] Christopher Kruegel and Thomas Toth. Applying Mobile Agent Technology to Intrusion Detection. In *ICSE Workshop on Software Engineering and Mobility*, Canada, May 2001.
- [244] Wolfgang Kastner and Christopher Kruegel. Improved fieldbus control via middleware technology. In *4th Conference on Automatic Control (Controlo)*, Portugal, October 2000.
- [245] Wolfgang Kastner and Christopher Kruegel. A new approach for Java in embedded networks. In *3rd IEEE Workshop on Factory Communication Systems*, IEEE Computer Society Press, Portugal, September 2000.
- [246] Wolfgang Kastner and Christopher Kruegel. Jini connectivity for EIB home and building networks - from design to implementation. In *EIB Scientific Conference*, Germany, October 1999.
- [247] Wolfgang Kastner, Christopher Kruegel and Heinrich Reiter. Jini: Ein guter Geist fuer die Gebaeudesystemtechnik (In German). In *Java Informations Tage (JIT)*, Germany, September 1999.

Journal Publications

- [248] One Size Does Not Fit All: A Longitudinal Analysis of Brazilian Financial Malware. Marcus Botacin, Hojjat Aghakhani, Stefano Ortolani, Christopher Kruegel, Giovanni Vigna, Daniela Oliveira, Paulo Geus, and Andre Gregio. In *ACM Transactions on Privacy and Security, Volume 24, Number 2*, January 2021.
- [249] Towards Detecting Compromised Accounts on Social Networks. Manuel Egele, Gianluca Stringhini, Christopher Kruegel, and Giovanni Vigna. In *IEEE Transactions on Dependable and Secure Computing, Volume 14, Number 4*, July/August 2017.
- [250] Exposure: A Passive DNS Analysis Service to Detect and Report Malicious Domains. Leyla Bilge, Sevil Sen, Davide Balzarotti, Engin Kirda, and Christopher Kruegel. In *ACM Transactions on Information and System Security (TISSEC), Volume 16, Number 4*, ACM Press, April 2014.
- [251] A Survey on Automated Dynamic Malware-Analysis Techniques and Tools. Manuel Egele, Theodoor Scholte, Engin Kirda, and Christopher Kruegel. In *ACM Computing Surveys, Volume 44, Number 2*, ACM Press, 2012.
- [252] Brett Stone-Gross, Marco Cova, Bob Gilbert, Richard Kemmerer, Christopher Kruegel, and Giovanni Vigna. Analysis of a Botnet Takeover. In *IEEE Security and Privacy Magazine, Volume 9, Number 1*, 2011.
- [253] Nenad Jovanovic, Christopher Kruegel, and Engin Kirda. Static Analysis for Detecting Taint-Style Vulnerabilities in Web Applications. In *Journal of Computer Security (JCS), Volume 18, Number 5*, IOS Press, 2010.
- [254] Engin Kirda, Nenad Jovanovic, Christopher Kruegel, and Giovanni Vigna. Client-side cross-site scripting protection. In *Computers and Security, Volume 28, Number 7*, Elsevier, 2009.
- [255] Giovanni Vigna, Fredrik Valeur, Davide Balzarotti, William Robertson, Christopher Kruegel, and Engin Kirda. Reducing errors in the anomaly-based detection of web-based attacks through the combined analysis of web requests and SQL queries. In *Journal of Computer Security, Volume 17, Number 3*, IOS Press, 2009.
- [256] Stefan Mitterhofer, Christian Platzer, Christopher Kruegel, and Engin Kirda. Server-side Bot Detection in Massive Multiplayer Online Games. In *IEEE Security and Privacy (Special Issue: Online Gaming Security), Volume 7, Number 3*, IEEE Computer Society, 2009.

- [257] Patrick Klinkoff, Christopher Kruegel, Engin Kirda, and Giovanni Vigna. Extending .NET Security to Unmanaged Code. In *International Journal of Information Security, Volume 6, Number 6, Springer Computer Science Journal*, 2007.
- [258] Ulrich Bayer, Andreas Moser, Christopher Kruegel, and Engin Kirda. Dynamic Analysis of Malicious Code. In *Journal in Computer Virology, Volume 2, Number 1, Springer Computer Science Journal*, 2006.
- [259] Darren Mutz, Fredrik Valuer, Christopher Kruegel, and Giovanni Vigna. Anomalous System Call Detection. In *ACM Transactions on Information and System Security, Vol. 9, No. 1, ACM Press*, 2006.
- [260] Engin Kirda and Christopher Kruegel. Protecting Users Against Phishing Attacks with AntiPhish. In *The Computer Journal, Volume 49, Number 5, Oxford University Press*, 2006.
- [261] Christopher Kruegel, William Robertson, and Giovanni Vigna. A Multi-model Approach to the Detection of Web-based Attacks. In *Computer Networks Journal, Vol. 48, No. 5, Elsevier*, 2005.
- [262] Fredrik Valeur, Giovanni Vigna, Christopher Kruegel, and Richard Kemmerer. A Comprehensive Approach to Intrusion Detection Alert Correlation. In *IEEE Transactions on Dependable and Secure Computing. Vol. 1, No. 3, IEEE Computer Society Press*, 2004.
- [263] Christopher Kruegel, William Robertson, and Giovanni Vigna. Using Alert Verification to Identify Successful Intrusion Attempts. In *Praxis der Informationsverarbeitung und Kommunikation (PIK), Sauer Verlag*, 2004.

Books and Book Chapters

- [264] Gerhard-Helge Schildt, Daniela Kahn, Christopher Kruegel, and Christian Moerz. Einfuehrung in die Technische Informatik (Introduction to Technical Computer Science), German Language. Springers Lehrbuecher der Informatik (Textbooks on Computer Science), Springer Verlag, ISBN 3-211-24346-1. April 2005.
- [265] Christopher Kruegel, Fredrik Valeur and Giovanni Vigna. Intrusion Detection and Correlation: Challenges and Solutions. In *Advances in Information Security, Vol. 14, ISBN 0-387-23398-9, Springer Verlag*. November 2004.
- [266] Christopher Kruegel. Characterizing the Behavior and Structure of Malicious Executables. In *Advances in Information Security, Vol. 27, ISBN 0-387-32720-7, Springer Verlag*, December 2006.
- [267] Giovanni Vigna and Christopher Kruegel. Host-Based Intrusion Detection. In *Handbook of Information Security, John Wiley and Sons, ISBN 0-471-64833-7*. December 2005.
- [268] Christopher Kruegel. Internet Security. In *The Industrial Communication Technology Handbook, CRC Press, ISBN 0-8493-3077-7*. February 2005.
- [269] Christopher Kruegel. Network Security and Secure Applications. In *The Industrial Information Technology Handbook, ISBN 0-849-31985-4, CRC Press*. May 2004.

Habilitation and Ph.D. Thesis

- [270] Christopher Kruegel. Malicious Code Analysis. Habilitation Thesis, Technical University Vienna, 2006.
- [271] Christopher Kruegel. Network Alertness - Towards an adaptive, collaborating Intrusion Detection System. PhD Thesis, Technical University Vienna, 2002.

Edited Volumes

- [272] Diego Zamboni and Christopher Kruegel. Proceedings of the 9th International Symposium on Recent Advances in Intrusion Detection. *Lecture Notes in Computer Science (LNCS)*, Vol. 4219, Springer Verlag, ISBN 3-540-39723-X. September 2006.
- [273] Klaus Julisch and Christopher Kruegel. Proceedings of the 2nd International Conference on Intrusion and Malware Detection and Vulnerability Assessment. *Lecture Notes in Computer Science (LNCS)*, Vol. 3548, Springer Verlag, ISBN 3-540-26613-5. July 2005.
- [274] Giovanni Vigna, Erland Jonsson and Christopher Kruegel. Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection. *Lecture Notes in Computer Science (LNCS)*, Vol. 2820, Springer Verlag, ISBN 3-540-40878-9. September 2003.

6 Teaching and Mentoring

Course Instructor

Time	Institution	Title	Enroll	Score (1-5) 1=best
S04	TU Vienna	Introduction to Technical Computer Science	~600	- (see note)
S04	TU Vienna	Advanced Internet Security	23	-
W05	TU Vienna	Internet Security	195	-
S05	TU Vienna	Introduction to Technical Computer Science	~600	-
S05	TU Vienna	Advanced Internet Security	46	-
W06	TU Vienna	Internet Security	170	1.2
S06	TU Vienna	Introduction to Technical Computer Science	~600	-
S06	TU Vienna	Advanced Internet Security	69	-
W07	TU Vienna	Internet Security	163	1.3
S07	TU Vienna	Introduction to Technical Computer Science	~600	-
S07	TU Vienna	Advanced Internet Security	51	-
W08	UC Santa Barbara	Operating Systems	21	1.2
F08	UC Santa Barbara	Translation of Programming Languages	28	1.7
W09	UC Santa Barbara	Host-based Security and Malicious Code	17	1.1
S09	UC Santa Barbara	Operating Systems	40	1.7
F09	UC Santa Barbara	Operating Systems	23	1.6
W10	UC Santa Barbara	Translation of Programming Languages	27	1.9
S10	UC Santa Barbara	Host-based Security and Malicious Code	17	1.4
W11	UC Santa Barbara	Software Engineering / Capstone	30	1.4
S11	UC Santa Barbara	Host-based Security and Malicious Code	10	1.3
S12	UC Santa Barbara	Operating Systems	79	1.4
W16	UC Santa Barbara	Translation of Programming Languages	37	1.6
F16	UC Santa Barbara	Translation of Programming Languages	77	1.4
W18	UC Santa Barbara	Software Engineering / Capstone	54	1.3
S19	UC Santa Barbara	Operating Systems	80	1.4
S20	UC Santa Barbara	Computer Security	71	1.3
F22	UC Santa Barbara	Computer Security	39	1.6
S23	UC Santa Barbara	Computer Security	29	1.4

Note: The Technical University (TU) Vienna introduced teaching evaluations only in 2006. Even then, evaluations were not done for all courses but only for selected lectures.

Additional Teaching

In addition to the courses listed above, I have organized various seminars both at UC Santa Barbara and TU Vienna. In these seminars, students have to read several research papers per week that are related to a specific, advanced topic. In class, students would then discuss these papers and give short, oral presentations.

Graduated Students (as Main Advisor / Co-Advisor)

Student Name	PhD/MS	Institution	Year of Degree
Nenad Jovanovic	PhD	TU Vienna	2007
Ulrich Bayer	PhD	TU Vienna	2010
Andreas Moser	PhD	TU Vienna	2010
Gilbert Wondracek	PhD	TU Vienna	2010
Manuel Egele	PhD	TU Vienna	2011
Clemens Kolbitsch	PhD	TU Vienna	2011
Brett Stone-Gross	PhD	UC Santa Barbara	2011
Gianluca Stringhini	PhD	UC Santa Barbara	2014
Adam Doupe	PhD	UC Santa Barbara	2014
Ali Zand	PhD	UC Santa Barbara	2015
Alexandros Kapravelos	PhD	UC Santa Barbara	2015
Luca Invernizzi	PhD	UC Santa Barbara	2015
Dhilung Kirat	PhD	UC Santa Barbara	2015
Yan Shoshitaishvili	PhD	UC Santa Barbara	2017
Yanick Fratantonio	PhD	UC Santa Barbara	2017
Antonio Bianchi	PhD	UC Santa Barbara	2018
Kevin Borgolte	PhD	UC Santa Barbara	2018
Ruoyu Wang	PhD	UC Santa Barbara	2018
Eric Gustafson	PhD	UC Santa Barbara	2020
Aravind Machiry	PhD	UC Santa Barbara	2020
Nilo Redini	PhD	UC Santa Barbara	2020
Christopher Salls	PhD	UC Santa Barbara	2020
Chad Spensky	PhD	UC Santa Barbara	2020
Hojjat Aghakhani	PhD	UC Santa Barbara	2023
Pryanka Bose	PhD	UC Santa Barbara	2023
Dipanjan Das	PhD	UC Santa Barbara	2023
Patrick Klinkoff	MS	TU Vienna	2005
Ulrich Bayer	MS	TU Vienna	2005
Stefan Kals	MS	TU Vienna	2006
Philipp Vogt	MS	TU Vienna	2006
David Tischler	MS	TU Vienna	2006
Manuel Egele	MS	TU Vienna	2006
Helmut Petritsch	MS	TU Vienna	2007
Martin Szydowski	MS	TU Vienna	2007
Guenther Bayler	MS	TU Vienna	2007
Florian Nentwich	MS	TU Vienna	2007
Andreas Stamminger	MS	TU Vienna	2007
Clemens Kolbitsch	MS	TU Vienna	2008
Sean McAllister	MS	TU Vienna	2008
Christian Ludl	MS	TU Vienna	2008
Stefan Mitterhofer	MS	TU Vienna	2009
Shriram Rajagopalan	MS	UC Santa Barbara	2009
Thomas Raffetseder	MS	TU Vienna	2010
Hans Nielsen	MS	UC Santa Barbara	2011
Jeffrey Tyson	MS	UC Santa Barbara	2011
Gorkem Yakin	MS	UC Santa Barbara	2012
Johannes Schlumberger	MS	UC Santa Barbara	2013
Vivek Goswami	MS	UC Santa Barbara	2014
Kyle MacNamara	MS	UC Santa Barbara	2014
Jonathan Brown	MS	UC Santa Barbara	2014

Student Name	PhD/MS	Institution	Year of Degree
Jason Berry	MS	UC Santa Barbara	2015
Jacopo Corbetta	MS	UC Santa Barbara	2016
Jacob Corina	MS	UC Santa Barbara	2017
Keith Long	MS	UC Santa Barbara	2019
Chani Jindal	MS	UC Santa Barbara	2019
Sebastiano Mariani	MS	UC Santa Barbara	2020
Chinmay Garg	MS	UC Santa Barbara	2020
Sid Senthilkumar	MS	UC Santa Barbara	2020
Kevin Burk	MS	UC Santa Barbara	2021
Alan Roddick	MS	UC Santa Barbara	2022

Graduated Students (as Committee Member)

Student Name	PhD/MS	Institution	Year of Degree
Andre Arnes	PhD	NTNU Norway	2006
Davide Balzarotti	PhD	Politecnico di Milano, Italy	2006
Yohann Thomas	PhD	ENST Bretagne, France	2007
Lorenzo Cavallaro	PhD	University of Milan, Italy	2008
William Robertson	PhD	UC Santa Barbara	2009
Gregoire Jacob	PhD	ESIEA, France	2009
Andrea Lanzi	PhD	University of Milan, Italy	2009
Lorenzo Martignoni	PhD	University of Milan, Italy	2009
Thorsten Holz	PhD	Univ. Mannheim, Germany	2009
Marco Cova	PhD	UC Santa Barbara	2010
Vika Felmetzger	PhD	UC Santa Barbara	2010
Bob Gilbert	PhD	UC Santa Barbara	2011
Krishna Puttaswamy	PhD	UC Santa Barbara	2011
Leyla Bilge	PhD	Eurecom, France	2011
Marco Balduzzi	PhD	Eurecom, France	2011
Jan Goebel	PhD	Univ. Mannheim, Germany	2011
Florian Tegeler	PhD	Univ. Goettingen, Germany	2012
Georges Bossert	PhD	SUPELEC, France	2014
Lakshmanan Nataraj	PhD	UC Santa Barbara	2015
Gang Wang	PhD	UC Santa Barbara	2016
Seemanta Saha	PhD	UC Santa Barbara	2023
Nicholas Childers	MS	UC Santa Barbara	2010
Ludovico Cavedon	MS	UC Santa Barbara	2011

Current Students

Lukas Dresel (PhD), Dongyu Meng (PhD), Fabio Gritti (PhD), Robert McLaughlin (PhD), Nicola Ruaro (PhD), Marius Fleischer (PhD), Eljon Harlicaj (PhD), Saastha Vasan (PhD), Stijn Pletinckx (PhD), Zihao (Jerry) Su (PhD).

Summer Undergraduate Research Program

In 2009, I started a summer research internship program at UC Santa Barbara. For this program, we invite every year a number of undergraduate students (typically, before their final senior year) to spend a three-month, paid internship in our lab. We select these students from top universities around the world

(although, so far, most students have come from European universities). Each intern works on a research project under the direct guidance of one of our graduate students. The goal is to get students engaged in and excited about academic research, and to create a pool from which we can recruit top PhD students. This program has been very successful.

7 Funding and Grants

Year	Source	Title	Amount
2005	OeNB	Solaris and Linux Baseline Security	€ 13K
2005-2007	FWF	Omnis - An Open Framework for Pervasive Services	€ 123K
2005-2008	FWF	Software Security through Binary Analysis	€ 127K
2006-2009	FWF	Web-Defense: Client-side Protection against Web Attacks	€ 231K
2007-2009	FIT-IT	Pathfinder: Malicious Code Analysis and Detection	€ 218K
2008-2009	EU-FP7	FORWARD: Managing Emerging Threats in ICT Infrastructures	€ 254K
2008-2010	FIT-IT	SECoverer: Finding Security Vulnerabilities in Web Applications	€ 199K
2008-2010	EU-FP7	WOMBAT: Worldwide Observatory of Malicious Behaviors and Attack Threats	€ 380K
2008-2009	NSF	Understanding the Underground Economy	\$ 200K
2009-2014	NSF	CAREER: Toward eliminating malicious code	\$ 405K
2009-2014	ONR	Botnet Attribution and Removal: from Axioms to Theories to Practice	\$ 1.8M
2009-2014	ARO	A Cyber-awareness Framework for Attack Analysis, Prediction and Visualization	\$ 6.3M
2009-2012	NSF	Automata Based String Analysis for Detecting Vulnerabilities in Web Applications	\$ 350K
2009-2012	NSF	Analyzing the Underground Economy	\$ 1.2M
2010-2011	Google	Automated Verification of the Native Client	\$ 50K
2011-2013	NSF	Viewpoints: Discovering Client- and Server-side Input Validation Inconsistencies	\$ 300K
2011	Narus	AppScout: Semantic Parser Module	\$ 45K
2011-2012	IBM	MalModels: Models for Capturing Malicious Program Activity	\$ 20K
2012-2015	ONR	ZigZag: Secure Execution of Client-Side Web Application Components	\$ 760K
2012-2015	DARPA	DarkDroid: Exposing the Dark Side of Android Marketplaces	\$ 2.3M
2012	Narus	Findig Malware Downloads in Network Traffic	\$ 45K
2013-2014	NSF	Attacking (and Defending) Information	\$ 200K
2013-2015	DHS	Malware on Smartphones: Collection, Analyses and Defense Measures	\$ 246K
2013-2017	DARPA	Modeling and Identifying Malice in Firmware	\$ 3.9M
2014	Narus	Combatting Application-level Denial of Service Attacks	\$ 45K
2014-2018	NSF	Identifying and Mitigating Trust Violations in the Smartphone Ecosystem	\$ 1.1M
2015-2018	ONR	Plasticity: Protection and Crash Forensics for Embedded Devices	\$ 1.1M
2015-2019	DARPA	Continuum: Finding Space and Time Vulnerabilities in Java Programs	\$ 1.6M
2017-2019	ONR	Defending Cyber Physical Systems	\$ 902K
2017-2020	NAVSEA	CobbleStone	\$ 1.1M
2017-2021	NSF	Augmenting Automated Vulnerability Analysis with Human Activity	\$ 1.1M
2017-2022	ONR	Binary Trimming for Improved Security	\$ 1.3M
2018	SANDIA	Symbion: A Symbiotic Program Analysis Environment	\$ 400K
2018-2020	Intel	Machine Learning for Vulnerability Analysis	\$ 400K
2018-2021	UCRI	Securing Smart Campuses	\$ 359K
2018-2022	DHS	Timely and ROBust Patching of Industrial Control Systems	\$ 250K
2018-2022	DARPA	Puppeteer - Achieving Remote Control Over Complex Remote Systems	\$ 2.5M
2019-2022	DARPA	Cognitive Human Enhancements for Cyber Reasoning Systems	\$ 2.2M
2020-2022	ONR	Shimware: Security Retrofitting of Monolithic Embedded Firmware	\$ 398K
2020-2024	DARPA	DICER: Directed Compilation for Assured Patching	\$ 1.3M
2021-2024	NSF	Detroit - A New End-to-end System for Practical and Accessible IoT	\$ 588K
2022-2025	DARPA	EMERGENCY: A Unified Framework for Discovering, Modeling, Analyzing & Mitigating Adversarial Emergent Computations	\$ 758K
Total			\$ 37M

8 Professional Activities

Conference/Program Chair

1. IEEE Symposium on Security and Privacy (Oakland), 2019
2. IEEE Symposium on Security and Privacy (Oakland), 2018
3. ACM Conference on Computer and Communications Security (CCS), 2016
4. ACM Conference on Computer and Communications Security (CCS), 2015
5. 4th Usenix Workshop on Large-Scale Exploits and Emergent Threats (LEET), 2011
6. 5th ACM CCS Workshop on Recurring Malcode (WORM), 2007
7. 10th International Symposium on Recent Advances in Intrusion Detection (RAID), 2007
8. Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), 2005

Journal Editorial Board

1. Associate Editor, ACM Transactions on Information and System Security (TISSEC), 2010-2014
2. Associate Editor, IEEE Transactions on Dependable and Secure Computing (TDSC), 2010-2014
3. Associate Editor, Journal of Computer Security, 2009-2013
4. Associate Editor, Springer International Journal of Information Security, 2007-2011

Program Committee Memberships

1. 33rd Usenix Security Symposium, 2024
2. ISOC Network and Distributed Systems Security Symposium (NDSS), 2024
3. ACM Conference on Computer and Communications Security (CCS), 2023
4. Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), 2023
5. ACM Conference on Computer and Communications Security (CCS), 2022
6. 31st Usenix Security Symposium, 2022
7. IEEE Symposium on Security and Privacy, 2022
8. 27th European Symposium on Research in Computer Security (ESORICS), 2022
9. Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), 2022
10. ACM Conference on Computer and Communications Security (CCS), 2021
11. 30th Usenix Security Symposium, 2021
12. 26th European Symposium on Research in Computer Security (ESORICS), 2021
13. Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), 2021
14. Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), 2017
15. ISOC Network and Distributed Systems Security Symposium (NDSS), 2016
16. IEEE European Symposium on Security and Privacy (Euro S&P), 2016
17. Symposium on Electronic Crime Research (eCrime), 2016
18. ISOC Network and Distributed Systems Security Symposium (NDSS), 2015
19. 18th International Symposium on Recent Advances in Intrusion Detection (RAID), 2015
20. International World Wide Web Conference (WWW), Security and Privacy Abuse Track, 2015

21. International Conference on Distributed Computing Systems (ICDCS), Security and Privacy, 2014
22. 23rd International World Wide Web Conference (WWW), Security, Privacy, Trust, and Abuse Track, 2014
23. 16th Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2013
24. International Conference on Availability, Reliability and Security (ARES)
25. Usenix Workshop on Large-Scale Exploits and Emergent Threats (LEET), 2013
26. Usenix Workshop on Offensive Technologies (WOOT), 2013
27. 22nd International World Wide Web Conference (WWW), Security, Privacy, Trust, and Abuse Track, 2013
28. IEEE Symposium on Security and Privacy, 2013
29. ACM Program Protection and Reverse Engineering Workshop (PPREW), 2013
30. 15th International Symposium on Recent Advances in Intrusion Detection (RAID), 2012
31. IEEE Symposium on Security and Privacy, 2012
32. ACM Conference on Computer and Communications Security (CCS), 2011
33. 14th International Symposium on Recent Advances in Intrusion Detection (RAID), 2011
34. International Conference on Distributed Computing Systems (ICDCS), Security and Privacy, 2011
35. Web 2.0 Security and Privacy Workshop (W2SP), 2011
36. IEEE Symposium on Security and Privacy, 2011
37. Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), 2011
38. Usenix Workshop on Large-Scale Exploits and Emergent Threats (LEET), 2011
39. ACM Conference on Computer and Communications Security (CCS), Publicity Chair, 2010
40. Usenix Workshop on Hot Topics in Security (HotSec), 2010
41. Usenix Workshop on Offensive Technologies (WOOT), 2010
42. IEEE Symposium on Security and Privacy, 2010
43. Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), 2010
44. European Workshop on Systems Security (EuroSec), 2010
45. 17th Network and Distributed System Security Symposium (NDSS), 2010
46. ACM Conference on Computer and Communications Security (CCS), Publicity Chair, 2009
47. 18th Usenix Security Symposium, 2009
48. New Security Paradigms Workshop (NSPW), 2009
49. 12th International Symposium on Recent Advances in Intrusion Detection (RAID), 2009
50. Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), 2009
51. Usenix Workshop on Hot Topics in Security (HotSec), 2009
52. European Workshop on Systems Security (EuroSec), 2009
53. Usenix Workshop on Large-Scale Exploits and Emergent Threats (LEET), 2009
54. 29th International Conference on Distributed Computing Systems (ICDCS), Security and Privacy, 2009
55. 17th International World Wide Web Conference (WWW), Security and Privacy Track, 2009
56. 16th Network and Distributed System Security Symposium (NDSS), 2009
57. ACM Conference on Computer and Communications Security (CCS), 2008
58. European Conference on Computer Network Defense (EC2ND), 2008
59. 13th European Symposium on Research in Computer Security (ESORICS), 2008
60. IEEE International Conference on Security and Privacy for Emerging Areas in Communication Networks (Securecomm), 2008
61. Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), 2008

62. Trust Conference (TRUST), 2008
63. IEEE Symposium on Security and Privacy, 2008
64. Usenix Workshop on Large-Scale Exploits and Emergent Threats (LEET), 2008
65. 17th International World Wide Web Conference (WWW), Security, Privacy, Reliability, and Ethics Track, 2008
66. European Workshop on Systems Security (EuroSec), 2008
67. 15th Network and Distributed System Security Symposium (NDSS), 2008
68. International Conference on Information Security and Cryptography (ICISC), 2007
69. ACM Conference on Computer and Communications Security (CCS), 2007
70. European Conference on Computer Network Defense (EC2ND), 2007
71. 12th European Symposium on Research in Computer Security (ESORICS), 2007
72. IEEE International Conference on Security and Privacy for Emerging Areas in Communication Networks (Securecomm), 2007
73. International Conference on Security and Cryptography (SECRYPT), 2007
74. Mathematical Methods, Models and Architectures for Computer Networks Security (MMM-ACNS), 2007
75. 16th Usenix Security Symposium, 2007
76. Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), 2007
77. International Conference on Networking and Services (ICNS), 2007
78. IEEE Symposium on Security and Privacy, 2007
79. 16th International World Wide Web Conference (WWW), Security, Privacy, Reliability, and Ethics Track, 2007
80. 2nd Workshop on Dependability Aspects on Data Warehousing and Mining applications (DAWAM), 2007
81. Workshop on Secure Software Engineering (SecSE), 2007
82. 8th International Conference on Information and Communications Security (ICICS), 2006
83. International Conference on Software Engineering Advances (ICSEA), 2006
84. IEEE International Conference on Security and Privacy for Emerging Areas in Communication Networks (Securecomm), 2006
85. International Conference on Information System Security (ICISS), 2006
86. International Conference on Security and Cryptography (SECRYPT), 2006
87. 9th International Symposium on Recent Advances in Intrusion Detection (RAID), 2006
88. International Conference on Networking and Services (ICNS), 2006
89. ICSE Workshop on Software Engineering for Secure Systems (SESS), 2006
90. Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), 2006
91. IEEE Symposium on Security and Privacy, 2006
92. International Conference on IP and Web Applications (ICIW), 2006
93. IEEE International Conference on Security and Privacy for Emerging Areas in Communication Networks (Securecomm), 2005
94. International Conference on Information System Security (ICISS), 2005
95. 3rd ACM CCS Workshop on Rapid Malcode (WORM), 2005
96. 8th International Symposium on Recent Advances in Intrusion Detection (RAID), 2005
97. International Conference on Networking and Services (ICNS), 2005
98. ICSE Workshop on Software Engineering for Secure Systems (SESS), 2005
99. 12th Network and Distributed System Security Symposium (NDSS), 2005

100. Workshop on Privacy Respecting Incident Management (PRIMA), 2005
101. Workshop on Safety, Reliability, and Security of Industrial Computer Systems (WSRS), 2004
102. 7th International Symposium on Recent Advances in Intrusion Detection (RAID), 2004
103. Workshop on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), 2004
104. 6th International Symposium on Recent Advances in Intrusion Detection (RAID), 2003
105. 8th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2001