

Curriculum Vitae

Manuel Egele

September 14, 2021

1 Personal Information

Name: Manuel Egele
Address (work): Department of Electrical & Computer Engineering
Boston University
8 St. Mary's Street
Boston, MA, 02215
Email: megele@bu.edu
Web: <https://megele.io>

2 Education

10/2007–01/2011

Dr.techn. (Ph.D.) in Computer Science from Vienna University of Technology, Vienna, Austria.

Advisors: Prof. Dr. Christopher Kruegel (UC Santa Barbara) & Prof. Dr. Engin Kirda (Northeastern University)

Thesis Title: *Protecting Web Clients from Internet Threats*

10/2000–10/2006

Dipl.-Ing. (M.Sc.) in Computer Science from Vienna University of Technology, Vienna, Austria.

Advisors: Prof. Dr. Christopher Kruegel & Prof. Dr. Engin Kirda

Thesis Title: *Behavior-Based Spyware Detection Using Dynamic Taint Analysis*

3 Professional Appointments

05/2021–present

Associate Professor, Dept. of Electrical & Computer Engineering, Boston University, Boston, MA.
(Since 09/2015: Affiliated Faculty in the Dept. of Computer Science, Boston University)

09/2014–05/2021

Assistant Professor, Dept. of Electrical & Computer Engineering, Boston University, Boston, MA.

03/2013–06/2014

Systems Scientist, CyLab, Carnegie Mellon University, Pittsburgh, PA.

10/2012–03/2013

Post-doctoral Researcher, CyLab, Carnegie Mellon University, Pittsburgh, PA, working with Prof. David Brumley.

01/2011–10/2012

Post-doctoral Researcher, Department of Computer Science, University of California, Santa Barbara, CA, working with Prof. Giovanni Vigna, Richard Kemmerer, and Christopher Kruegel.

7/2009–01/2011

Visiting Researcher, Department of Computer Science, University of California, Santa Barbara, CA, working with Prof. Giovanni Vigna, Richard Kemmerer, and Christopher Kruegel.

10/2008–7/2009

Visiting Researcher, Ecole d'Ingénieurs & Centre de Recherche, Eurécom, Sophia Antipolis, France, working with Prof. Engin Kirda and Davide Balzarotti.

10/2007–10/2008

Research Assistant, Intl. Secure Systems Lab (Inst. of Computer Aided Automation), Vienna University of Technology, Vienna, Austria, working with Prof. Engin Kirda and Christopher Kruegel.

4 Awards and Nominations

1. *2019-20 Boston University College of Engineering, Early Career Research Award.*
2. *Junior PI Award* of the Austrian Scientists in Northern America (AScINA) network for B. Zhou, A. Gupta, R. Jahanshahi, M. Egele, and A. Joshi. Hardware Performance Counters Can Detect Malware: Myth or Fact? In *Proceedings of the ACM Asia Conference on Computer and Communications Security (ASIACCS)*, Incheon, Korea, June 2018.
3. *Best Paper Award* for B. Kaleli, M. Egele, and G. Stringhini. On the Perils of Leaking Referrers in Online Collaboration Services. In *Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA)*, Gothenburg, Sweden, June 2019.
4. *Best Artifact Award* for E. Ates, O. Tuncer, A. Turk, V. J. Leung, J. Brandt, M. Egele, and A. K. Coskun. Taxonomist: Application Detection through Rich Monitoring Data. In *Proceedings of the International European Conference on Parallel and Distributed Computing (EUROPAR)*, Turin, Italy, Aug. 2018.
5. *Best Paper Award* for B. Zhou, A. Gupta, R. Jahanshahi, M. Egele, and A. Joshi. Hardware Performance Counters Can Detect Malware: Myth or Fact? In *Proceedings of the ACM Asia Conference on Computer and Communications Security (ASIACCS)*, Incheon, Korea, June 2018.
6. *Distinguished Reviewer Award* at the 39th IEEE Symposium on Security and Privacy (Oakland), 2018
7. *Finalist, CSAW'17 Applied Research Competition* for E. Kolodenker, W. Koch, G. Stringhini, and M. Egele. PayBreak: Defense against cryptographic ransomware. In *Proceedings of the ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, Abu Dhabi, Apr. 2017.

8. *Gauss Center of Supercomputing Award* for O. Tuncer, E. Ates, Y. Zhang, A. Turk, J. Brandt, V. J. Leung, M. Egele, and A. K. Coskun. Diagnosing Performance Variations in HPC Applications Using Machine Learning. In *Proceedings of the ISC High Performance Conference*, Frankfurt, Germany, June 2017.
9. *Distinguished Paper Award* for M. Egele, C. Kruegel, E. Kirda, and G. Vigna. PiOS: Detecting Privacy Leaks in iOS Applications. In *Proceedings of Network and Distributed Systems Security Symposium (NDSS)*, San Diego, CA, Feb. 2011.

5 List of Publications

Journal Publications

- [1] B. Zhou, A. Gupta, R. Jahanshahi, M. Egele, and A. Joshi. A Cautionary Tale about Detecting Malware Using Hardware Performance Counters and Machine Learning. *IEEE Design & Test*, Mar. 2021.
- [2] V. J. M. Manès, H. Han, C. Han, S. K. Cha, M. Egele, E. J. Schwartz, and M. Woo. The Art, Science, and Engineering of Fuzzing: A Survey. *IEEE Transactions on Software Engineering (TSE)*, pages 1–21, Oct. 2019.
- [3] O. Tuncer, E. Ates, Y. Zhang, A. Turk, J. Brandt, V. J. Leung, M. Egele, and A. K. Coskun. Online Diagnosis of Performance Variation in HPC Systems Using Machine Learning. *Proceedings of the IEEE Transactions on Parallel and Distributed Systems (TPDS)*, Sept. 2018.
- [4] L. Delshadtehrani, S. Eldridge, S. Canakci, M. Egele, and A. Joshi. Nile: A Programmable Monitoring Coprocessor. *IEEE Computer Architecture Letters*, pages 1–4, Dec. 2017.
- [5] M. Egele, G. Stringhini, C. Kruegel, and G. Vigna. Towards detecting compromised accounts on social networks. *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 14(4):447–460, Sept. 2015.
- [6] G. Stringhini, M. Egele, C. Kruegel, and G. Vigna. Poultry markets: On the underground economy of twitter followers. *SIGCOMM Computer Communications Review*, 42(4):527–532, Sept. 2012.
- [7] M. Egele, A. Moser, C. Kruegel, and E. Kirda. PoX: Protecting users from malicious Facebook applications. *Elsevier Computer Communications*, 35(12):1507–1515, July 2012.
- [8] M. Egele, T. Scholte, E. Kirda, and C. Kruegel. A survey on automated dynamic malware-analysis techniques and tools. *ACM Computing Surveys*, 44(2):1–42, Mar. 2012.
- [9] M. Egele, C. Kolbitsch, and C. Platzer. Removing web spam links from search engine results. *Journal in Computer Virology*, 7(1):51–62, Feb. 2011.

Conference Publications (peer reviewed)

- [10] O. Zungur, A. Bianchi, G. Stringhini, and M. Egele. APPJITSU: Investigating the Resiliency of Android Applications. In *Proceedings of the IEEE European Symposium on Security and Privacy (EuroS&P)*, Vienna, Austria, Sept. 2021.
- [11] A. Bulekov, R. Jahanshahi, and M. Egele. Sapphire: Sandboxing PHP Applications with Tailored System Call Allowlists. In *Proceedings of the USENIX Security Symposium*, Vancouver, BC, Aug. 2021.

- [12] A. Aliyeva and M. Egele. Oversharing Is Not Caring: How CNAME Cloaking Can Expose Your Session Cookies. In *Proceedings of the ACM Asia Conference on Computer and Communications Security (ASIACCS)*, Hong Kong, China, June 2021.
- [13] A. Fasano, T. Ballo, M. Muench, T. Leek, A. Bulekov, B. Dolan-Gavitt, M. Egele, A. Francillon, L. Lu, N. Gregory, D. Balzarotti, and W. Robertson. SoK: Enabling Security Analyses of Embedded Systems via Rehosting. In *Proceedings of the ACM Asia Conference on Computer and Communications Security (ASIACCS)*, Hong Kong, China, June 2021.
- [14] L. Delshadtehrani, S. Canakci, M. Egele, and A. Joshi. Efficient Sealable Protection Keys for RISC-V. In *Proceedings of the Design, Automation & Test in Europe Conference (DATE)*, page 7, Grenoble, France, Feb. 2021.
- [15] B. Kaleli, B. Kondracki, M. Egele, N. Nikiforakis, and G. Stringhini. To Err.Is Human: Characterizing the Threat of Unintended URLs in Social Media. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, Feb. 2021.
- [16] R. Jahanshahi, A. Doupé, and M. Egele. You shall not pass: Mitigating SQL Injection Attacks on Legacy Web Applications. In *Proceedings of the ACM Asia Conference on Computer and Communications Security (ASIACCS)*, Taipei, Taiwan, Oct. 2020.
- [17] L. Delshadtehrani, S. Canakci, B. Zhou, S. Eldridge, A. Joshi, and M. Egele. PHMon: A Programmable Hardware Monitor and Its Security Use Cases. In *Proceedings of the USENIX Security Symposium*, Boston, MA, Aug. 2020.
- [18] O. Zungur, G. Stringhini, and M. Egele. LIBSPECTOR : Context-Aware Large-Scale Network Traffic Analysis of Android Applications. In *Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Valencia, Spain, June 2020.
- [19] B. Kondracki, A. Aliyeva, M. Egele, J. Polakis, and N. Nikiforakis. Meddling Middlemen: Empirical Analysis of the Risks of Data-Saving Mobile Browsers. In *Proceedings of the IEEE Symposium on Security and Privacy*, San Francisco, CA, May 2020.
- [20] W. Blair, A. Mambretti, S. Arshad, M. Weissbacher, E. Kirda, W. Robertson, and M. Egele. HotFuzz: Discovering Algorithmic Denial-of-Service Vulnerabilities Through Guided Micro-Fuzzing. In *Proceedings of Network and Distributed Systems Security Symposium (NDSS)*, San Diego, CA, Feb. 2020.
- [21] O. Sahin, A. Aliyeva, H. Mathavan, A. K. Coskun, and M. Egele. RandR: Record and Replay for Android Applications via Targeted Runtime Instrumentation. In *Proceedings of the International Conference on Automated Software Engineering (ASE)*, San Diego, CA, Nov. 2019.
- [22] E. Ates, Y. Zhang, B. Aksar, J. Brandt, V. J. Leung, M. Egele, and A. K. Coskun. HPAS: An HPC Anomaly Suite for Reproducing Performance Variations in HPC Systems. In *Proceedings of the International Conference on Parallel Processing (ICPP)*, Kyoto, Japan, Aug. 2019.
- [23] B. Kaleli, M. Egele, and G. Stringhini. On the Perils of Leaking Referrers in Online Collaboration Services. In *Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA)*, Gothenburg, Sweden, June 2019 (Best Paper Award).
- [24] O. Zungur, G. Suarez-Tangil, G. Stringhini, and M. Egele. BORDERPATROL: Securing BYOD using fine-grained contextual information. In *Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Portland, OR, June 2019.

- [25] O. Sahin, A. K. Coskun, and M. Egele. Proteus: Detecting Android Emulators from Instruction-level Profiles. In *Proceedings of the International Symposium on Research in Attacks, Intrusions, and Defenses (RAID)*, Heraklion, Greece, Sept. 2018.
- [26] E. Ates, O. Tuncer, A. Turk, V. J. Leung, J. Brandt, M. Egele, and A. K. Coskun. Taxonomist: Application Detection through Rich Monitoring Data. In *Proceedings of the International European Conference on Parallel and Distributed Computing (EUROPAR)*, Turin, Italy, Aug. 2018 (Best Artifact Award).
- [27] B. Zhou, A. Gupta, R. Jahanshahi, M. Egele, and A. Joshi. Hardware Performance Counters Can Detect Malware: Myth or Fact? In *Proceedings of the ACM Asia Conference on Computer and Communications Security (ASIACCS)*, Incheon, Korea, June 2018 (Best Paper Award).
- [28] B. Zhou, M. Egele, and A. Joshi. High-performance low-energy implementation of cryptographic algorithms on a programmable SoC for IoT devices. In *Proceedings of the High Performance Extreme Computing Conference (HPEC)*, pages 1–6, Waltham, MA, Sept. 2017.
- [29] W. Koch, A. Chaabane, M. Egele, W. Robertson, and E. Kirda. Semi-Automated Discovery of Server-Based Information Oversharing Vulnerabilities in Android Applications. In *Proceedings of the ACM International Symposium on Software Testing and Analysis (ISSTA)*, Santa Barbara, CA, July 2017.
- [30] O. Tuncer, E. Ates, Y. Zhang, A. Turk, J. Brandt, V. J. Leung, M. Egele, and A. K. Coskun. Diagnosing Performance Variations in HPC Applications Using Machine Learning. In *Proceedings of the ISC High Performance Conference*, Frankfurt, Germany, June 2017.
- [31] E. Kolodenker, W. Koch, G. Stringhini, and M. Egele. PayBreak: Defense against cryptographic ransomware. In *Proceedings of the ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, Abu Dhabi, Apr. 2017.
- [32] E. Mariconti, J. Onaolapo, S. S. Ahmad, N. Nikiforou, M. Egele, N. Nikiforakis, and G. Stringhini. What’s in a Name? Understanding Profile Name Reuse on Twitter. In *Proceedings of the World Wide Web Conference (WWW)*, Perth, Australia, Apr. 2017.
- [33] S. Duman, K. Kalkan-Cakmakci, M. Egele, W. Robertson, and E. Kirda. EmailProfiler: Spearphishing Filtering with Header and Stylometric Features of Emails. In *Proceedings of the IEEE Computer Software and Applications Conference (COMPSAC)*, pages 408–416, Atlanta, GA, June 2016.
- [34] D. D. Chen, M. Egele, M. Woo, and D. Brumley. Towards Automated Dynamic Analysis for Linux-based Embedded Firmware. In *Proceedings of Network and Distributed Systems Security Symposium (NDSS)*, San Diego, CA, Feb. 2016.
- [35] S. Hao, K. Borgolte, N. Nikiforakis, G. Stringhini, M. Egele, M. Eubanks, B. Krebs, and G. Vigna. Drops for Stuff: An Analysis of Reshipping Mule Scams. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, pages 1081–1092, Denver, CO, Nov. 2015.
- [36] G. Stringhini, P. Mourlanne, G. Jacob, M. Egele, C. Kruegel, and G. Vigna. EvilCohort: Detecting communities of malicious accounts on online services. In *Proceedings of the USENIX Security Symposium*, Washington, D.C., Aug. 2015.
- [37] Y. Fratantonio, A. Bianchi, W. Robertson, M. Egele, C. Kruegel, E. Kirda, and G. Vigna. On the Security and Engineering Implications of Finer-Grained Access Controls for Android Developers and Users. In *Proceedings of the Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA)*, Milano, Italy, July 2015.

- [38] Y. Cao, Y. Fratantonio, A. Bianchi, M. Egele, C. Kruegel, G. Vigna, and Y. Chen. EdgeMiner: Automatically Detecting Implicit Control Flow Transitions through the Android Framework. In *Proceedings of Network and Distributed Systems Security Symposium (NDSS)*, San Diego, CA, Feb. 2015.
- [39] M. Egele, M. Woo, P. Chapman, and D. Brumley. Blanket Execution: Dynamic Similarity Testing for Program Binaries and Components. In *Proceedings of the USENIX Security Symposium*, San Diego, CA, Aug. 2014.
- [40] M. Egele, D. Brumley, Y. Fratantonio, and C. Kruegel. An empirical study of cryptographic misuse in android applications. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, pages 73–84, Berlin, Germany, Nov. 2013.
- [41] G. Stringhini, G. Wang, M. Egele, C. Kruegel, G. Vigna, H. Zheng, and B. Y. Zhao. Follow the green: Growth and dynamics in twitter follower markets. In *Proceedings of the ACM Internet Measurement Conference (IMC)*, pages 163–176, Barcelona, Spain, Oct. 2013.
- [42] M. Egele, G. Stringhini, C. Kruegel, and G. Vigna. Compa: Detecting Compromised Accounts on Social Networks. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, Feb. 2013.
- [43] G. Stringhini, M. Egele, A. Zarras, T. Holz, C. Kruegel, and G. Vigna. B@bel: Leveraging Email Delivery for Spam Mitigation. In *Proceedings of the USENIX Security Symposium*, pages 16–32, Bellevue, WA, Aug. 2012.
- [44] L. Davi, A. Dmitrienko, M. Egele, T. Fischer, T. Holz, R. Hund, S. Nürnberger, and A.-R. Sadeghi. MoCFI: A Framework to Mitigate Control-Flow Attacks on Smartphones. In *Proceedings of Network and Distributed Systems Security Symposium (NDSS)*, San Diego, CA, Feb. 2012.
- [45] A. Doupé, M. Egele, B. Caillat, G. Stringhini, G. Yakin, A. Zand, L. Cavedon, and G. Vigna. Hit'em where it hurts: A live security exercise on cyber situational awareness. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, pages 51–61, Orlando, FL, Dec. 2011.
- [46] M. Egele, C. Kruegel, E. Kirda, and G. Vigna. PiOS: Detecting Privacy Leaks in iOS Applications. In *Proceedings of Network and Distributed Systems Security Symposium (NDSS)*, San Diego, CA, Feb. 2011. (*Distinguished Paper Award*)
- [47] N. Childers, B. Boe, L. Cavallaro, L. Cavedon, M. Cova, M. Egele, and G. Vigna. Organizing large scale hacking competitions. In *Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA)*, pages 132–152, Bonn, Germany, July 2010.
- [48] M. Balduzzi, M. Egele, E. Kirda, D. Balzarotti, and C. Kruegel. A solution for the automated detection of clickjacking attacks. In *Proceedings of the ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, Beijing, China, Apr. 2010.
- [49] M. Egele, L. Bilge, E. Kirda, and C. Kruegel. Captcha smuggling: Hijacking web browsing sessions to create captcha farms. In *Proceedings of the ACM Symposium on Applied Computing (SAC)*, pages 1865–1870, Sierre, Switzerland, Mar. 2010.
- [50] M. Egele, P. Wurzinger, C. Kruegel, and E. Kirda. Defending browsers against drive-by downloads: Mitigating heap-spraying code injection attacks. In *Proceedings of the Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA)*, pages 88–106, Milan, Italy, July 2009.

- [51] M. Egele, C. Kruegel, and E. Kirda. Removing web spam links from search engine results. In *Proceedings of the European Institute for Computer Antivirus Research Conference*, Berlin, Germany, May 2009.
- [52] H. Yin, D. Song, M. Egele, C. Kruegel, and E. Kirda. Panorama: Capturing system-wide information flow for malware detection and analysis. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, pages 116–127, Alexandria, VA, Oct. 2007.
- [53] M. Egele, C. Kruegel, E. Kirda, H. Yin, and D. X. Song. Dynamic Spyware Analysis. In *Proceedings of the USENIX Annual Technical Conference (ATC)*, pages 233–246, Santa Clara, CA, June 2007.
- [54] M. Egele, M. Szydlowski, E. Kirda, and C. Kruegel. Using static program analysis to aid intrusion detection. In *Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA)*, pages 17–36, Berlin, Germany, July 2006.

Workshop Publications (peer reviewed)

- [55] L. Delshadtehrani, J. Appavoo, M. Egele, A. Joshi, and S. Eldridge. Varanus: An Infrastructure for Programmable Hardware Monitoring Units. In *Proceedings of the Boston Area ARChitecture Workshop (BARC)*, Cambridge, MA, Jan. 2017.
- [56] D. Orikogbo, M. Büchler, and M. Egele. CRiOS : Toward Large-Scale iOS Application Analysis. In *Proceedings of the ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*, Vienna, Austria, Oct. 2016.
- [57] E. Mariconti, J. Onaolapo, S. S. Ahmad, N. Nikiforou, M. Egele, N. Nikiforakis, and G. Stringhini. Why Allowing Profile Name Reuse Is A Bad Idea. In *Proceedings of the European Workshop on System Security (EUROSEC)*, London, UK, Apr. 2016.
- [58] G. Stringhini, M. Egele, C. Kruegel, and G. Vigna. Poultry markets: On the underground economy of twitter followers. In *Proceedings of the ACM Workshop on Online Social Networks (WOSN)*, pages 1–6, Helsinki, Finland, Aug. 2012.
- [59] M. Szydlowski, M. Egele, C. Kruegel, and G. Vigna. Challenges for dynamic analysis of iOS applications. In *Proceedings of the iNetSec Workshop on Open Research Problems in Network Security*, Luzerne, Switzerland, June 2011.
- [60] L. Davi, A. Dmitrienko, M. Egele, T. Fischer, T. Holz, R. Hund, S. Nürnberger, and A.-R. Sadeghi. CFI goes mobile: Control-flow integrity for smartphones. In *Proceedings of the International Workshop on Trustworthy Embedded Devices (TrustED)*, Leuven, Belgium, Sept. 2011.
- [61] M. Egele, A. Moser, C. Kruegel, and E. Kirda. PoX: Protecting users from malicious Facebook applications. In *Proceedings of the IEEE International Workshop on Security and Social Networking (SESOC)*, Seattle, WA, Mar. 2011.
- [62] M. Egele, E. Kirda, and C. Kruegel. Mitigating drive-by download attacks: Challenges and open problems. In *Proceedings of the iNetSec Workshop on Open Research Problems in Network Security*, Zurich, Switzerland, Apr. 2009.

Theses

- [63] M. Egele. *Protecting Web Clients from Internet Threats*. PhD thesis, Vienna University of Technology, Vienna, Austria, 2011.
- [64] M. Egele. *Behavior-Based Spyware Detection Using Dynamic Taint Analysis*. Master's Thesis, Vienna University of Technology, Vienna, Austria, 2006.

6 Selected Invited Talks

1. Vulnerability Analysis for the IoT & Architectural Enhancements for Software Security, *MIT Lincoln Laboratory — Secure, Resilient Systems and Technology Group, Lexington, MA*, July 2019.
2. Securing the Internet of Things Through Dynamic Program Analysis, Keynote at *Workshop on Data-Centric Dependability and Security (DCDS)*, June 2019.
3. IoT Security via Broad Strokes & Fine-tooth Combs, *IBM Research, Thomas J. Watson Research Center, Yorktown Heights, New York*, November 2018.
4. From Mobile Systems to the IoT: Analysis for Security and Privacy, *Concordia University, Montreal, Quebec, Canada*, March 2017.
5. Static Analysis of Mobile Apps for Security and Privacy, *MIT Lincoln Laboratory — Secure, Resilient Systems and Technology Group, Lexington, MA*, March 2016.
6. Where's the Money in Cyber-Crime, *Vorarlberg University of Applied Sciences, Dornbirn, Austria*, March 2016.
7. Opposites Attract – Static Analysis on Mobile Apps for Security and Privacy, *Ecole d'Ingénieurs & Centre de Recherche, Eurécom, Sophia Antipolis, France*, June 2013.
8. Mobile Security iOS & Android, *ETH Zürich, Switzerland*, August 2012.
9. The State of Mobile Security, Keynote at the *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Crete, Greece*, July 2012.
10. On the Importance of Detecting Compromised Accounts on Social Networks, *Communications and Digital Signal Processing Research Workshop, Boston, MA*, April 2012.

7 Professional Activities

Board & Chair Service

- 1 Editorial Board Member, *ACM Transactions on Security and Privacy (TOPS)*, since 2018
- 2 Program Chair *International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, 2020

- 3 Program Co-Chair International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2019
- 4 Chair of the Artifact Evaluation Committee, Annual Computer Security Applications Conference (ACSAC), 2017, 2018
- 5 Area Chair (Application & Web Security) at ACM Conference on Computer and Communications Security (CCS), 2018 – 2020
- 6 Poster Chair at the ACM Symposium on Information, Computer and Communications Security (ASIACCS), 2019

Selected Program Committee Memberships

- 7 IEEE Symposium on Security and Privacy (Oakland), 2018 – 2020, 2022
- 8 USENIX Security Symposium, 2015 – 2022
- 9 ISOC Network and Distributed Systems Security Symposium (NDSS), 2015 – 2022
- 10 ACM Conference on Computer and Communications Security (CCS), 2014 – 2016, 2018 – 2020
- 11 Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), 2012, 2013, 2015 – 2019
- 12 International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2016 – 2018
- 13 Annual Computer Security Applications Conference (ACSAC), 2015 – 2021
- 14 IEEE International Conference on Distributed Computing Systems (ICDCS), 2017
- 15 ACM Conference on Data and Application Security and Privacy (CODASPY), 2016 – 2019
- 16 USENIX Workshop on Offensive Technologies (WOOT), 2013, 2017, 2018

Selected Journal Reviewer

- 17 ACM Computing Surveys (CSUR)
- 18 ACM Transactions on Information and System Security (TISSEC)
- 19 ACM Transactions on Privacy and Security (TOPS)
- 20 IEEE Transactions on Dependable and Secure Computing (TDSC)
- 21 The Computer Journal
- 22 IEEE Journal of Internet Computing
- 23 Elsevier Computers & Security (COSE)
- 24 Elsevier Journal of Systems and Software (JSS)
- 25 Springer International Journal of Information Security (IJIS)