TUDOR A. DUMITRAŞ

Dept. of Electrical and Computer Engineering
University of Maryland
5109 Brendan Iribe Center for Computer Science and Engineering
8125 Paint Branch Drive
College Park, MD 20742

Phone: +1-301-405-7466
Email: tudor@umd.edu
Web: http://www.umiacs.umd.edu/~tdumitra

RESEARCH OVERVIEW

My research focuses on data-driven security: I study real-world adversaries empirically, I build machine-learning systems for detecting attacks and predicting security incidents, and I investigate the security of machine learning in adversarial environments. I collaborate frequently with industry partners to deploy and evaluate my research results in an industrial setting. My work has been featured in the Research Highlights of the Communications of the ACM and has been widely cited in the media, for example in The Economist, the MIT Technology Review, Forbes, and The Register. I also enjoy creating innovative pedagogical strategies, to meet the needs of a diverse student body, and giving TED-style talks, to explain our work to broad audiences.

EDUCATIONAL BACKGROUND

Carnegie Mellon University, Pittsburgh, PA
Ph.D. in Electrical and Computer Engineering — December 2010
Advisor: Prof. Priya Narasimhan
Dissertation: Improving the Dependability of Distributed Systems through AIR Software Upgrades

Ecole Polytechnique, Paris, France
Diplôme d'Ingénieur (Computer Science Major) — July 2001

"Politehnica" University, Bucharest, Romania
B.S. in Computer Science — July 2001

ACADEMIC APPOINTMENTS AT UMD

University of Maryland, College Park, ECE Department — July 2019 – present
Associate Professor

University of Maryland, College Park, ECE Department — August 2013 – July 2019
Assistant Professor

OTHER EMPLOYMENT

Symantec Research Labs, Herndon, VA — Nov 2010 – Jul 2013
Sr. Research Engineer

Research, Scholarly, Creative and/or Professional Activities

HONORS AND AWARDS

Young Faculty Award, DARPA	2019
Research Highlights, Communications of the ACM* (for IMC'14 paper)	2018
Best Scientific Cybersecurity Paper, Honorable mention, NSA (for CCS'12 paper)	2013
A.G. Jordan Award, Carnegie Mellon ECE Department (for outstanding Ph.D. thesis and service)	2011
John Vlissides Award, ACM SIGPLAN (for significant promise in applied software research)	2009
1st Place, ACM Student Research Competition, OOPSLA'09	2009
Graduate Student Service Award, Carnegie Mellon University	2006
Best Paper Award, Asia and South Pacific Design Automation Conference	2003
Excellence scholarship, French government's EIFFEL program	1999–2001

PUBLICATIONS

Journal Articles

[1] B. Kwon, M. Petrișor, V. Srinivas, A. Deshpande, and T. Dumitraș, 'Beewolves: Unsupervised Detection of Silent Delivery Campaigns in Parallel.' Under review at *IEEE Transactions on Information Forensics and Security (**TIFS'18**)*, 2018.

[2] C. Sabottke, D. Chen, L. Layman, and T. Dumitraş, 'How to Trick the Borg: Threat Models against Manual and Automated Techniques for Detecting Network Attacks.' Accepted for publication at *Elsevier Computers and Security (**COSE'18**)*, 2018.

[3] S. Hong, A. Nicolae, A. Srivastava, and Tudor Dumitraş, 'Peek-a-Boo with Xen: Inferring Program Behaviors in a Virtualized Infrastructure without Introspection.' Accepted for publication at *Elsevier Computers and Security (**COSE'18**)*, 2018.

[4] L. Zhang, D. Choffnes, T. Dumitraş, D. Levin, A. Mislove, A. Schulman, and C. Wilson. 'Analysis of SSL certificate reissues and revocations in the wake of Heartbleed.' In *Communications of the ACM, Research Highlights **(CACM'18)***, March 2018.

[5] M. Ovelgonne, T. Dumitraș, A. Prakash, V. S. Subrahmanian, and B. Wang, 'Understanding the Relationship between Human Behavior and Susceptibility to Cyberattacks: A Data-Driven Approach,' *ACM Transactions on Intelligent Systems & Technology (**TIST'16**)*, vol. 8, no. 4, Mar 2017.
- **46 citations**†

[6] E. Papalexakis, T. Dumitraș, D.H. Chau, A. Prakash and C. Faloutsos. `SharkFin: Spatio-temporal mining of software adoption and penetration.' In *Social Network Analysis and Mining (**SNAM'14**)*, vol. 4, no. 1, article 240, Dec 2014, Springer.

[7] T. Dumitraș and P. Narasimhan. 'A Study of Unpredictability in Fault-Tolerant Middleware.' *Computer Networks (**COMNET'13**)*, vol. 57, no. 3, pp. 682–698, Feb 2013, Elsevier.

[8] P. Bogdan, T. Dumitraș and R. Mărculescu. 'Stochastic Communication: A New Paradigm for Fault-Tolerant Networks-on-Chip.' *Hindawi **VLSI Design***, Special Issue on Networks-on-Chip, 2007.
- **100 citations**

[9] P. Narasimhan, T. Dumitraș, A. M. Paulos, S. M. Pertet, C. F. Reverte, J. G. Slember and D. Sriva-

* Communications of the ACM, the flagship publication of the Association for Computing Machinery, highlights two outstanding research articles in each issue, selected across the broad spectrum of computing research.
† Citation counts retrieved from Google Scholar on 12 October 2021.

stava. 'MEAD: Support for Real-Time, Fault-Tolerant CORBA.' *Concurrency and Computation: Practice and Experience (**CC:PS'05**)*, vol. 17, no. 12, pp. 1527-1545, Oct 2005, Wiley and Sons.
- **93 citations**

Peer-Reviewed Conference Publications[‡]

[10] O. Suciu, C. Nelson, Z. Lyu, T. Bao, and T. Dumitraș. 'Expected exploitability: Predicting the development of functional vulnerability exploits.' In *USENIX Security Symposium (**USENIX Security'22**)*, Boston, MA, 2022.

[11] S. Hong, M. Panaitescu-Liess, Y. Kaya, T. Dumitraș. 'Qu-ANTI-zation: Exploiting Quantization Artifacts for Achieving Adversarial Outcomes.' In *Neural Information Processing Systems (**NeurIPS'21**)*, Online, 2021.

[12] E. Avllazagaj, Z. Zhu, L. Bilge, D. Balzarotti, and T. Dumitraș. 'When Malware Changed Its Mind: An Empirical Study of Variable Program Behaviors in the Real World.' In *USENIX Security Symposium (**USENIX Security'21**)*, Online, 2021.

[13] Y. Kaya, and T. Dumitraș. 'When Does Data Augmentation Help with Membership Inference Attacks?' In *International Conference on Machine Learning (**ICML'21 Spotlight**)*, Online, 2021.

[14] D. Kim, H. Cho, Y. Kwon, A. Doupé, S. Son, G-J Ahn, and T. Dumitraș. 'Security Analysis on Practices of Certificate Authorities in the HTTPS Phishing Ecosystem.' In *ACM Asia Conference on Computer and Communications Security (**ASIACCS '21**)*, Online, 2021.

[15] S. Hong, Y. Kaya, I. Modoranu, T. Dumitraș. 'A Panda? No, It's a Sloth: Slowdown Attacks on Adaptive Multi-Exit Neural Network Inference.' In *International Conference on Learning Representations (**ICLR'21 Spotlight**)*, Online, 2021.

[16] S. Hong, M. Davinroy, Y. Kaya, D. Dachman-Soled, T. Dumitraș. 'How to 0wn NAS in Your Spare Time.' In *International Conference on Learning Representations (**ICLR'20**)*, Online, 2020.
- **10 citations**

[17] S. Hong, P. Frigo, Y. Kaya, C. Giuffrida, and T. Dumitraș. 'Terminal Brain Damage: Exposing the Graceless Degradation in Deep Neural Networks Under Hardware Fault Attacks.' In *USENIX Security Symposium (**USENIX Security'19**)*, Santa Clara, CA, 2019.
- **60 citations**

[18] Y. Kaya, S. Hong, and T. Dumitraș. 'Shallow-Deep Networks: Understanding and Mitigating Network Overthinking.' In *International Conference on Machine Learning (**ICML'19**)*, 2019.
- **57 citations**

[19] A. Shafahi, W. R. Huang, M. Najibi, O. Suciu, C. Studer, T. Dumitraș, and T. Goldstein, 'Poison Frogs! Targeted Clean-Label Poisoning Attacks on Neural Networks.' In *Neural Information Processing Systems (**NIPS'18**)*, Montreal, Canada, 2018.
- **347 citations**

[20] E. Redmiles, Z. Zhu, D. Kuchhal, T. Dumitraș, and M. Mazurek, 'Asking for a Friend: Evaluating Response Biases in Security User Studies.' In *ACM Conference on Computer and Communications Security (**CCS'18**)*, Toronto, Canada, 2018. (16.7% acceptance rate)
- **28 citations**

[21] O. Suciu, R. Mărginean, Y. Kaya, H. Daumé III, and T. Dumitraș, 'When Does Machine Learning FAIL? Generalized Transferability for Evasion and Poisoning Attacks.' In *USENIX Security Symposium* (**USENIX Security'18**), Baltimore, MD, Aug 2018. (19% acceptance rate)
- **112 citations**

[‡] The premier publication venues in my field are IEEE S&P, ACM CCS, USENIX Security, NDSS, IMC, RAID, Euro S&P. These conferences are peer-reviewed and accept fewer than 20% of the papers submitted.

[22] D. Kim, B. J. Kwon, K. Kozák, C. Gates, and T. Dumitraș, 'The Broken Shield: Measuring Revocation Effectiveness in the Windows Code-Signing PKI.' In *USENIX Security Symposium* (**USENIX Security'18**), Baltimore, MD, Aug 2018. (19% acceptance rate)
- **16 citations**

[23] C. Xiao, A. Sarabi, Y. Liu, B. Li, M. Liu, and T. Dumitraș, 'From Patching Delays to Infection Symptoms: Using Risk Profiles for an Early Discovery of Vulnerabilities Exploited in the Wild.' In *USENIX Security Symposium* (**USENIX Security'18**), Baltimore, MD, Aug 2018. (19% acceptance rate)
- **19 citations**

[24] Z. Zhu and T. Dumitraș, 'ChainSmith: Automatically Learning the Semantics of Malicious Campaigns by Mining Threat Intelligence Reports.' In *IEEE European Symposium on Security and Privacy (**Euro S&P'18**),* London, United Kingdom, Apr 2018. (22.9% acceptance rate)
- **40 citations**

[25] D. Kim, B. J. Kwon, and T. Dumitraș, 'Certified Malware: Measuring Breaches of Trust in the Windows Code-Signing PKI.' In *ACM Conference on Computer and Communications Security (**CCS'17**)*, Dallas, TX, 2017. (18.1% acceptance rate)
- **50 citations**

[26] W. Lawson, S. Secules, S. Bhattacharyya, A. Elby, W. Hawkins, T. Dumitraș, and N. Ramirez, 'Traditional versus Hardware-driven Introductory Programming Courses: a Comparison of Student Identity, Efficacy and Success.' In *ASEE Annual Conference & Exposition (**ASEE'17**)*, Columbus, OH, Jun 2017.

[27] A. Sarabi, Z. Zhu, C. Xiao, M. Liu, and T. Dumitraș, 'Patch Me If You Can: A Study on the Effects of Individual User Behavior on the End-Host Vulnerability State.' In *Passive and Active Measurement Conference (**PAM'17**)*, Sydney, Australia, Mar 2017.
- **21 citations**

[28] B. Kwon, V. Srinivas, A. Deshpande, and T. Dumitraș, 'Catching worms, trojan horses and PUPs: Unsupervised detection of silent delivery campaigns.' In *Network and Distributed System Security Symposium (**NDSS'17**)*, San Diego, CA, Feb 2017. (16.1% acceptance rate)
- **31 citations**

[29] S. Indela, M. Kulkarni, K. Nayak, and T. Dumitraș, 'Helping Johnny Encrypt: Toward Semantic Interfaces for Cryptographic Frameworks.' In *ACM SPLASH Onward! Conference (**Onward!'16**)*, Amsterdam, Netherlands, Nov 2016.
- **15 citations**

[30] S. Indela, M. Kulkarni, K. Nayak, and T. Dumitraș, 'Toward Semantic Cryptography APIs.' In *IEEE Secure Development Conference (**SecDev'16**)*, Boston, MA, Nov 2016.

[31] Z. Zhu and T. Dumitraș, 'FeatureSmith: Automatically Engineering Features for Malware Detection by Mining the Security Literature.' In *ACM Conference on Computer and Communications Security (**CCS'16**)*, Vienna, Austria, Oct 2016. (16.5% acceptance rate)
- **89 citations**

[32] K. Saur, T. Dumitraș, and M. Hicks, 'Evolving NoSQL Databases Without Downtime.' In *IEEE International Conference on Software Maintenance and Evolution (**ICSME'16**)*, Raleigh, NC, Oct 2016.
- **34 citations**

[33] H. Hang, A. Bashir, M. Faloutsos, C. Faloutsos and T. Dumitraș, 'Infect-me-not: A user-centric and site-centric study of web-based malware.' *IFIP Networking Conference (**NETWORKING'16**)*, Vienna, MAY 2016

[34] B. Kwon, J. Mondal, L. Bilge, J. Jang, and T. Dumitraș. 'The Dropper Effect: Insights into Malware Distribution with Downloader Graph Analytics.' In *ACM Conference on Computer and Communications Security (**CCS'15**)*, Denver, CO, Oct 2015. (19% acceptance rate)
- **116 citations**

[35] C. Sabottke, O. Suciu, and T. Dumitraş. 'Vulnerability disclosure in the age of social media: Exploiting Twitter for predicting real-world exploits.' In *USENIX Security Symposium* (**USENIX Security'15**), Washington, DC, Aug 2015. (16% acceptance rate)
- **230 citations**

[36] A. Nappa, R. Johnson, L. Bilge, J. Caballero, and T. Dumitraş. 'The attack of the clones: A study of the impact of shared code on vulnerability patching.' In *IEEE Symposium on Security and Privacy* (**IEEE S&P'15**), San Jose, CA, May 2015. (14% acceptance rate)
- **123 citations**

[37] L. Zhang, D. Choffnes, T. Dumitraş, D. Levin, A. Mislove, A. Schulman, and C. Wilson. 'Analysis of SSL certificate reissues and revocations in the wake of Heartbleed.' In *ACM Internet Measurement Conference **(IMC'14)***, Vancouver, Canada, Nov 2014. (23% acceptance rate)
- **105 citations**
- **Selected for CACM Research Highlights**

[38] K. Nayak, D. Marino, P. Efstathopoulos, and T. Dumitraș. 'Some vulnerabilities are different than others: Studying vulnerabilities and attack surfaces in the wild.' In *International Symposium on Research in Attacks, Intrusions and Defenses **(RAID'14)***, Gothenburg, Sweden, Sep 2014. (19% acceptance rate)
- **88 citations**

[39] E. Papalexakis, T. Dumitraș, D.H. Chau, A. Prakash and C. Faloutsos. 'Spatio-temporal Mining of Software Adoption & Penetration.' In *IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (**ASONAM'13**)*, Niagara Falls, CA, Aug 2013.
- **32 citations**

[40] L. Bilge and T. Dumitraş. 'Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World.' In *USENIX ACM Conference on Computer and Communications Security (**CCS'12**)*, Raleigh, NC, Oct 2012. (19% acceptance rate)
- **568 citations**
- **NSA Best Scientific Cybersecurity Papers of 2012, Honorable Mention**

[41] T. Dumitraș and P. Efstathopoulos. 'The Provenance of WINE.' In *European Dependable Computing Conference (**EDCC'12**)*, Sibiu, Romania, May 2012.

[42] T. Dumitraș, E. Tilevich and P. Narasimhan. 'To Upgrade or Not To Upgrade: Impact of Online Upgrades Across Multiple Administrative Domains.' In *ACM Onward! Conference (**Onward'10**)*, Reno/Tahoe, NV, Oct 2010. (23% acceptance rate)
- **38 citations**

[43] T. Dumitraș and P. Narasimhan. 'Why Do Upgrades Fail And What Can We Do About It? Toward Dependable, Online Upgrades in Enterprise Systems.' In *ACM/IFIP/USENIX Conference on Middleware (**Middleware'09**)*, Urbana-Champaign, IL, Nov–Dec 2009. (19% acceptance rate)
- **103 citations**

[44] T. Dumitraș and P. Narasimhan. 'Got Predictability? Experiences with Fault-Tolerant Middleware.' In *ACM/IFIP/USENIX Conference on Middleware (**Middleware'07**)*, Newport Beach, CA, Nov 2007. (24% acceptance rate)

[45] T. Dumitraș and P. Narasimhan. 'Fault-Tolerant Middleware and the Magical 1%.' In *ACM/IFIP/USENIX Conference on Middleware (**Middleware'05**)*, Grenoble, France, Nov–Dec

2005. (21% acceptance rate)
- **21 citations**

[46] T. Dumitraș, S. Kerner and R. Mărculescu. 'Enabling On-Chip Diversity through Architectural Communication Design.' In *Asia and South Pacific Design Automation Conference (**ASP-DAC'04**)*, Yokohama, Japan, Jan 2004.
- **11 citations**

[47] T. Dumitraș and R. Mărculescu. 'On-Chip Stochastic Communication.' In *Design, Automation and Test in Europe Conference (**DATE'03**)*, Munich, Germany, Mar 2003. (17% acceptance rate)
- **137 citations**

[48] T. Dumitraș, S. Kerner and R. Mărculescu. 'Towards on-chip fault-tolerant communication.' In *Asia and South Pacific Design Automation Conference (**ASP-DAC'03**)*, Kitakyushu, Japan, Jan 2003, pp. 225–232.
- **210 citations**
- **Best Paper Award**

Books

[49] V.S. Subrahmanian, M. Ovelgonne, T. Dumitras, B. A. Prakash, 'The Global Cyber-Vulnerability Report.' Springer International, 2015.
- **44 citations**

Book Chapters (peer-reviewed)

[50] T. Dumitraș, 'Understanding the Vulnerability Lifecycle for Risk Assessment and Defense Against Sophisticated Cyber Attacks.' In Cyber Warfare: Building the Scientific Foundation, S. Jajodia, P. Shakarian, V. S. Subrahmanian, V. Swarup, and C. Wang, eds., Springer, 2015.

[51] T. Dumitraș, D. Roșu, A. Dan and P. Narasimhan, 'Ecotopia: An Ecological Framework for Change Management in Distributed Systems.' In *Architecting Dependable Systems Vol. IV (**ADS IV**)*, C. Gacek, A. Romanovsky and R. de Lemos, eds., Springer-Verlag, 2007.
- **14 citations**

[52] T. Dumitraș, D. Srivastava and P. Narasimhan. 'Architecting and Implementing Versatile Dependability.' In *Architecting Dependable Systems Vol. III (**ADS III**)*, C. Gacek, A. Romanovsky and R. de Lemos, eds., Springer-Verlag, 2005.
- **21 citations**

[53] T. Dumitraș and R. Mărculescu. 'On-Chip Stochastic Communication.' In *Embedded Software for SoC*, A. Jerraya, S. Yoo, D. Verkest and N. When, eds., Kluwer, 2003, pp. 373-386.

Workshop Papers (peer-reviewed)

[54] S. Hong, A. Srivastava, W. Shambrook, and T. Dumitraș, 'Go Serverless: Securing Cloud via Serverless Design Patterns.' In *USENIX Workshop on Hot Topics in Cloud Computing (**HotCloud'18**)*, Jul 2018.

[55] K. Kozák, B. J. Kwon, D. Kim, and T. Dumitraș, 'Issued for Abuse: Measuring the Underground Trade in Code Signing Certificates.' In *Workshop on the Economics of Information Security (**WEIS'18**)*, Jun 2018.

[56] T. Dumitraș, Y. Kaya, R. Mărginean, and O. Suciu. 'Too Big to FAIL: What You Need to Know Before Attacking a Machine Learning System.' In *International Security Protocols Workshop (**SPW'18**)*, Cambridge, United Kingdom, Mar 2018.

[57] R. Stevens, O. Suciu, A. Ruef, S. Hong, M. Hicks, and T. Dumitraş. 'Summoning Demons: The Pursuit of Exploitable Bugs in Machine Learning.' In *NIPS Workshop on Reliable Machine Learning in the Wild (**WildML'16**)*, Barcelona, Spain, Dec 2016.

[58] T. Dumitraș and P. Efstathopoulos. 'Ask WINE: Are We Safer Today? Evaluating Operating System Security through Big Data Analysis.' In *USENIX Workshop on Large-Scale Exploits and Emerging Threats (**LEET'12**)*, San Jose, CA, Apr 2012.

[59] I. Neamtiu and T. Dumitraș. 'Cloud Software Upgrades: Challenges and Opportunities.' In *IEEE International Workshop on the Maintenance and Evolution of Service-Oriented and Cloud-Based Systems (**MESOCA'11**)*, Williamsburg, VA, Sep 2011.
- **56 citations**

[60] T. Dumitraș and I. Neamtiu. 'Experimental Challenges in Cyber Security: A Story of Provenance and Lineage for Malware.' In *USENIX Workshop on Cyber Security Experimentation and Test (**CSET'11**)*, San Francisco, CA, Aug 2011.
- **30 citations**

[61] T. Dumitraș and D. Shou. 'Toward a standard benchmark for computer security research: The Worldwide Intelligence Network Environment (WINE).' In *EuroSys Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (**BADGERS'11**),* Salzburg, Austria, Apr 2011.
- **122 citations**

[62] T. Dumitraș, J. Tan, Z. Gho and P. Narasimhan, 'No More *HotDep*endencies: Toward Dependency-Agnostic Upgrades in Distributed Systems.' In *Workshop on Hot Topics in System Dependability (**HotDep'07**)*, Edinburgh, Scotland, Jun 2007.
- **17 citations**

[63] T. Dumitraș, D. Roșu, A. Dan and P. Narasimhan. 'Impact-Sensitive Framework for Dynamic Change-Management.' In *DSN Workshop on Architecting Dependable Systems (**WADS'06**)*, Philadelphia, PA, Jun 2006.

[64] T. Dumitraș, P. Narasimhan. 'An Architecture for Versatile Dependability.' In *DSN Workshop on Architecting Dependable Systems (**WADS'05**)*, Florence, Italy, Jun 2004.

Other Publications

[65] T. Dumitraș. 'The WINE Platform for Experimenting with Big Data Analytics in Security.' In *Big Data Analytics for Security Intelligence*, Report of the Big Data Working Group, Cloud Security Alliance, Sep 2013.

[66] L. Bilge and T. Dumitraș. 'Investigating Zero-Day Attacks.' *USENIX ;login:*, vol. 38, no. 4, Aug 2013.

[67] T. Dumitraș, I. Neamtiu and E. Tilevich. 'Report on the Second ACM Workshop on Hot Topics in Software Upgrades.' *ACM SIGOPS Operating Systems Review (**OSR'10**)*, vol. 44, no. 4, Dec 2010.

[68] T. Dumitraș. 'Improving the Dependability of Distributed Systems through AIR Software Upgrades.' ***Ph.D. Thesis***, Carnegie Mellon University, Dec 2010.
Committee: P. Narasimhan (advisor), G. Ganger, B. Maggs, A. Dan.

[69] T. Dumitraș and P. Narasimhan. 'Upgrades-as-a-Service in Distributed Systems.' In *Work-in-Progress Session at FAST'10*, San Jose, CA, Jan 2010.

[70] T. Dumitraș and P. Narasimhan. 'Toward Upgrades-as-a-Service in Distributed Systems.' In *Poster Session at Middleware'09*, Urbana-Champaign, IL, Nov–Dec 2009.

[71] T. Dumitraș. 'Dependable, Online Upgrades in Distributed Systems,' In *Doctoral Symposium at OOPSLA'09*, Orlando, FL, Oct 2009 (**John Vlissides Award**).

[72] T. Dumitraș. 'Dependable, Online Upgrades in Distributed Systems,' In *ACM Student Research Competition at OOPSLA'09*, Orlando, FL, Oct 2009 (**First Place**).

[73] T. Dumitraș, I. Neamtiu and E. Tilevich, co-editors. *Proceedings of HotSWUp'09*, Orlando, FL, Oct 2009.

[74] T. Dumitraș and P. Narasimhan. 'No Downtime for Data Conversions: Rethinking Hot Upgrades,' Technical report CMU-PDL-09-106, Carnegie Mellon University, Jul 2009.
- **10 citations**

[75] T. Dumitraș, F. Eliassen, K. Geihs, H. Muccini, A. Polini and T. Ungerer. 'Testing Run-time Evolving Systems.' In *Self-Healing and Self-Adaptive Systems,* ***Dagstuhl Seminar*** *09201*, May 2009.

[76] T. Dumitraș, D. Dig and I. Neamtiu, co-editors. *Proceedings of HotSWUp'08*, Nashville, TN, Oct 2008.

[77] T. Dumitraș, A. Hanemann, B. Kratz and J. Pathak, co-editors. *Proceedings of the IBM Ph.D. Student Symposium at ICSOC'07*, Vienna, Austria, Sep 2007.

[78] T. Dumitraș. 'Dependency-Agnostic Online Upgrades in Distributed Systems,' In *Student Forum at DSN'07*, Edinburgh, Scotland, Jun 2007.

[79] A. Hanemann, B. Kratz, T. Dumitraș, and N. Mukhi, co-editors. Proceedings of the IBM Ph.D. Student Symposium at ICSOC'06, Chicago, IL, Dec 2006.

[80] T. Dumitraș, M. Lee, P. Quinones, A. Smailagic, D. Siewiorek and P. Narasimhan. 'Eye of the Beholder: Phone-Based Text-Recognition for the Visually-Impaired.' In *Poster Session at ISWC'06,* Montreux, Switzerland, Oct 2006, pp. 145–146.
- **24 citations**

[81] T. Dumitraș. 'On-Chip Stochastic Communication.' ***M.S. Thesis***. Carnegie Mellon University, May 2003. Committee: R. Mărculescu (advisor), P. Narasimhan.

TALKS

Peer-reviewed presentations

'How to Predict Which Vulnerabilities Will Be Exploited'
- **USENIX Enigma**,[§] Burlingame, CA — Jan 2019

'FeatureSmith: Learning to Detect Malware by Mining the Security Literature'
- **USENIX Enigma**, Oakland, CA — Jan 2017

Keynotes

'Measurements, predictions, and the puzzle of machine learning: What data from 10 million hosts can teach us about security,' **BalkanCryptSec'18** — Sep 2018

'The Impact of Shared Code on Vulnerability Patching,' **Qualcomm Security Summit'15** — Oct 2015

'Field Data Available at Symantec Research Labs,' **ASPLOS-EXERT'11** — Mar 2011

Invited talks

'The Shallow-Deep Network: A Generic, Input-Adaptive, Platform for CPS'
- **ARO Workshop on Assured Autonomy** — Jun 2020

'Research Challenges for the Security of Machine Learning'
- **IBM-MIT AI Meets Security Workshop** (invited talk) — Sep 2019
- **Workshop on Machine Learning and Applications at UMD** — Mar 2019

'How to Think About Cyber Risk'
- **Booz Allen Hamilton iHub** — Mar 2020
- **UMD Executive Cybersecurity Summit** — Apr 2019

[§] USENIX Enigma is a conference that focuses on communicating security ideas effectively through TED-style presentations. The topics are selected competitively by a Program Committee, and the presentations undergo extensive peer review and coaching following TED guidelines.

'Measurements, predictions, and the puzzle of machine learning: What data from 10 million hosts can teach us about security'

- **CISPA Helmholtz Center for Information Security** (host: Michael Backes) Mar 2019
- **UC San Diego** (host: Geoff Voelker) Nov 2019
- **UC Santa Barbara** (host: Giovanni Vigna) Jun 2018
- **Dropbox** (host: Devdatta Akhave) May 2018
- **Ecole Polytechnique Fédérale de Lausanne** (host: Carmela Troncoso) Apr 2018
- **Max Planck Institute for Software Systems** (host: Krishna Gummadi) Apr 2018
- **Berkeley** (host: Raluca Popa) Apr 2018

'Research Challenges for the Security of Machine Learning'

- **ARO/IARPA Workshop on Adversarial Machine Learning** (invited talk) May 2018

'Challenging Security Assumptions: The Capabilities and Limitations of Real-World Adversaries'

- **ETH Zurich** (host: Adrian Perrig) Mar 2018

'How to Measure Security?'

- **NSF Workshop on Self-Running Networks** (invited talk) Feb 2018

'Before We Knew It: From Measurements to Predictions of Security in the Real World'

- **Stony Brook University** (host: Nick Nikiforakis) Feb 2018
- **Cornell Tech NYC** (host: Thomas Ristenpart) Feb 2018

'Automatic Feature Engineering by Mining the Computer Security Literature'

- **AI for Security and the Security of AI Workshop** (invited talk) Jan 2020
- **Carnegie Mellon University** (host: Lujo Bauer) Dec 2017
- **Georgia Tech** (host: Maria Konte) Sep 2017
- **University of Michigan, Ann Arbor** (host: Mingyan Liu) May 2017
- **Laboratory of Telecommunication Sciences** (host: Gerry Baumgartner) Jan 2017
- **MC2 Symposium** (invited talk) Dec 2016
- **IBM T. J. Watson Research Center** (host: Jiyong Jang) Sep 2016

'FeatureSmith: Learning to Detect Malware by Mining the Security Literature'

- **With The Best** online conference (invited talk) Oct 2017

'The Impact of Shared Code on Vulnerability Patching'

- **Northeastern University** (host: Cristina Niță Rotaru) Jan 2016

'Machine Learning Techniques for Preventing the Global Malware Dissemination'

- **EBSIS Summer School on Distributed Event Based Systems** (invited talk) Jul 2016
- **Qualcomm Research, Silicon Valley** (host: Anil Gathala) Mar 2016
- **University of North Carolina, Charlotte** (host: Ehab Al-Shaer) Feb 2016
- **Boston University/Lincoln Lab Cybersecurity Series: Cybersecurity Applications of Big Data** (host: Hamed Okhravi) Jan 2016
- **Symantec Research Labs** (host: Kevin Roundy) Nov 2015
- **AT&T Security Research Center** (host: Gustavo de los Reyes) Oct 2015

'Predicting Vulnerability Exploits with Twitter Analytics'

- **Messaging, Malware, Mobile Anti-Abuse Working Group** (invited talk) Jun 2016
- **Romanian Cryptology Days Workshop** (invited talk) Sep 2015

'Understanding the Vulnerability Lifecycle: A Big Data Approach'

- **Fraunhofer Center for Experimental Software Engineering** (host: Adam Porter) Apr 2015
- **Northwestern University** (host: Yan Chen) Mar 2015
- **Hughes Network Systems** (host: Chi-Jiun Su) Aug 2014
- **Qualcomm** (host: Alex Gantman) Aug 2014
- **National Institute of Standards and Technology** (host: Peter Mell) May 2014

'Cyber Security: Understanding Threats with Big Data Analytics'

- **ExecSense** (invited webinar) Aug 2014

'Cyber Data Suitable for Academic Research: Where to Get Them and How to Use Them'

- **Army Research Lab** (host: Alex Kott) May 2014

'Security and (In)Security: A Big Data Approach'

- **ARO Invitational Workshop on Cyber Warfare** (invited talk) Mar 2014

'Improving System Security with Big Data Techniques'

- **"Politehnica" University, Bucharest, Romania** (host: Costin Raiciu) Mar 2014
- **Technical University of Cluj-Napoca, Romania** (host: Rodica Potolea) Mar 2014
- **"Politehnica" University, Timisoara, Romania** (host: Bogdan Groza) Mar 2014
- **University of Toronto** (host: David Lie) Feb 2014
- **DC Anonymity, Privacy and Security workshop** (invited talk) Jan 2014
- **EURECOM** (host: Davide Balzarotti) Jan 2014
- **Laboratory of Telecommunication Sciences** (host: Gerry Baumgartner) Jul 2013
- **Microsoft Research, Redmond** (host: Navendu Jain) May 2013
- **University of Maryland, College Park** (host: Gang Qu) Apr 2013
- **IMDEA Software Institute** (host: Anindya Banerjee) Apr 2013
- **Virginia Tech** (host: Charles Clancy) Mar 2013
- **Cambridge University** (host: Robert Mullins) Feb 2013
- **Carnegie Mellon University** (host: David Brumley) Jan 2013

'Before we knew it: An empirical study of zero-day attacks in the real world'

- **HotSoS'14** (invited talk) Apr 2014
- **ISACA North America joint ISRM / IT GRC conference** (invited "hot topics" talk) Oct 2012

'The Worldwide Intelligence Network Environment (WINE)'

- **Duke** (host: Bruce Maggs) Oct 2012
- **University of North Carolina, Chapel Hill** (host: Mike Reiter) Oct 2012
- **NC State** (host: Ting Yu) Oct 2012
- **Stanford Security Seminar** (host: Ankur Taly) May 2012
- **Rutgers** (host: Tina Eliassi-Rad) Mar 2012
- **Princeton** (host: Jennifer Rexford) Mar 2012
- **Virginia Tech** (host: Eli Tilevich) Mar 2012
- **University of Maryland** (host: Michael Hicks) Nov 2011
- **UC Riverside** (host: Iulian Neamtiu) Apr 2011

'Improving the end-to-end dependability of distributed systems'

- **USC** (host: Ramesh Govindan) Jan 2011
- **Purdue** (host: Cristina Niță-Rotaru) Jul 2010
- **UIUC** (host: Indranil Gupta) Jun 2010
- **VMware** (host: Orran Krieger) Jun 2010
- **Stevens Institute of Technology** (host: Hong Man) Apr 2010
- **Caltech** (host: Adam Wierman) Apr 2010
- **UCLA** (host: Carlo Zaniolo) Apr 2010
- **IBM Research, Almaden** (host: Joseph Slember) Mar 2010
- **Microsoft Research, Silicon Valley** (host: Mihai Budiu) Feb 2010
- **HP Labs** (host: Lucy Cherkasova) Feb 2010
- **IBM Research, T.J. Watson** (host: Peter Sweeney) Jan 2010
- **AT&T Labs** (hosts: Matti Hiltunen and Rick Schlichting) Jan 2010

'Toward Dependable, Online Upgrades in Enterprise Systems'

- **Software Engineering Institute**, Carnegie Mellon University (host: Charles Weinstock) Jun 2009
- **EPFL**, Switzerland (host: Willy Zwaenepoel) May 2009

- **Vanderbilt University** (host: Anirüddhā Gokhālé) Oct 2008
- **Oracle Corporation** (host: Alan Downing) Jun 2008
- **Cambridge University**, UK (host: Jon Crowcroft) Jun 2007
- **Newcastle University**, UK (host: Graham Morgan) Jun 2007

'Why Do Upgrades Fail and What Can We Do About It?,' **Dagstuhl Seminar 09201** May 2009

'Patch Management Sandboxing,' **VMware Inc.** (host: Suresh Ravoor) Jul 2006

'Distributed, Impact-Sensitive Dynamic Change-Management'

- **CNRS-LAAS**, France (host: Jean-Charles Fabre) Dec 2005
- **IBM Research** (host: Asit Dan) Aug 2005

Completed Creative Works

USENIX Enigma Talk 2017

https://www.youtube.com/watch?v=ikaDWJhSMIU

Delivered TED-style talk titled 'FeatureSmith: Learning to Detect Malware by Mining the Security Literature' at USENIX Enigma, a conference that focuses on communicating security ideas effectively.

Data Sets Released

- ChainSmith (Web application backed by the system described in [**Euro S&P'18**]) 2018
  http://ioc-chainsmith.org/
- Digitally signed malware (due to breaches of trust in the code-signing PKI [**CCS'17**]) 2017
  http://signedmalware.org/
- Beewolf (relationships among actors in the malware delivery ecosystem [**NDSS'17**]) 2017
  http://www.beewolf.org/
- FeatureSmith (automatically engineered features [**CCS'16**]) 2016
  http://featuresmith.org/
  In use at :
  - University of Illinois at Urbana-Champaign, USA
  - University of Melbourne, Australia
  - Shanghai Jiao Tong University, China
  - University of Virginia, USA
  - The Hong Kong Polytechnic University, China
  - Chinese Academy of Sciences, China
  - Bangladesh University of Engineering & Technology, Bangladesh
  - University of Maryland, Baltimore County, USA
  - Daffodil International University, Bangladesh
  - FAST National University of Computer and Emerging Sciences, Peshawar, Pakistan

The Worldwide Intelligence Network Environment (WINE) 2012

http://www.umiacs.umd.edu/~tdumitra/blog/old/worldwide-intelligence-network-environment/

Built the WINE platform for conducting data intensive experiments in cyber security. Nine academic groups have conducted experimental research using WINE in 2012 and 2013, and the reference data sets defined in these experiments remain available for future research and independent verification.

Middleware for Embedded Adaptive Dependability (MEAD) 2006

http://www.ece.cmu.edu/~mead

Built and released the MEAD middleware system, which served as the main fault-tolerance platform for the DARPA-ARMS II and DARPA-PCES II programs.

Discussions and Reviews of Work

- **CCS'17 paper:** featured in Ars Technica, The Register, Threat Post, Schneier on Security, The Hacker News, Tech Wire Asia, Cyberdefense Magazine

- **WildML'16 paper**: featured in the MIT Technology Review and The Register
- **IEEE S&P'15 paper**: featured in Schneier on Security and GCN
- **IMC'14 paper**: featured in Science Daily, The Register, The Diamondback
- **RAID'14 paper**: featured in Threat Post
- **CCS'12 paper**: featured in The Economist, Forbes, eWEEK, The Register, Slashdot, Schneier on Security, Dark Reading, SC Magazine, Ars Technica, Threat Post, Channelnomics, Tech Target, CSO Magazine, Info Security Magazine, Security Affairs
- **LEET'12 paper**: featured in the editorial ('Musings') of the August edition of USENIX ;login:

RESEARCH FUNDING

Between 2014–2018, I have been PI or co-PI on projects that have secured funding adding up to $5,478,343 (*my share: $3,190,692*).

Sponsored Research – single PI

- **IARPA**, $116,615 07/01/2020–06/30/2021
  Backdoor Detection via Eigenvalues, Hessians, Internal Behaviors, and Robust Statistics
  Co-PI: Michael Mahoney (ICSI)
  My share: $116,615
- **DARPA**, $489,591 07/01/2019–06/30/2021
  Young Faculty Award
  Transferable Factors of Updating Behavior for Predicting Vulnerability Patching and Exploitation
  My share: $489,591
- **Laboratory of Telecommunication Sciences**, $270,488 02/01/2019–1/31/2021
  Functional and Semantic Understanding of Deep Learning
  My share: $270,488
- **Laboratory of Telecommunication Sciences**, $403,192
  Threat Intelligence through Social Media Analytics (continuation) 02/01/2019–1/31/2021
  My share: $403,192
- **Laboratory of Telecommunication Sciences**, $169,592 01/16/2018 – 01/15/2019
  Automatically Learning the Semantics of Security Threats
  My share: $169,592
- **Laboratory of Telecommunication Sciences**, $169,592 01/16/2018 – 01/15/2019
  Threat Intelligence through Social Media Analytics (continuation)
  My share: $169,592
- **Laboratory of Telecommunication Sciences**, $174,440 3/1/2017 – 2/28/2018
  Threat Intelligence through Social Media Analytics
  My share: $174,440
- **National Science Foundation**, Award 1464163, $170,340 05/1/2015 – 04/30/2017
  CRII: SaTC: Empirical and Analytical Models for the Deployment of Software Updates in Large Vulnerable Populations
  My share: $170,340
- **Laboratory of Telecommunication Sciences**, $93,840 03/24/2015 – 03/25/2016
  Document Retrieval from Unstructured Web Data
  My share: $93,840
- **Laboratory of Telecommunication Sciences**, $169,760 03/24/2015 – 03/25/2016
  Feature Identification for Streaming Detection of Malware
  My share: $169,760

Sponsored Research – Co-PI

- **National Science Foundation**, Award 1564143, $600,000 7/1/2016 – 6/30/2020
  TWC: Medium: Collaborative: Measuring and Improving the Management of Today's PKI

Co-PIs: Dave Levin (UMD), David Choffnes, Alan Mislove, Christo Wilson (Northeastern)
My share: $300,000

- **Maryland Procurement Office**, $290,637 5/1/2016 – 4/30/2017
  Establishing a Science of Security Research Lablet at the University of Maryland: Task Empirical Models for Vulnerability Exploits
  Co-PI: Marshini Chetty (UMD)
  My share: $168,569
- **Maryland Procurement Office**, $191,426 5/1/2016 – 4/30/2017
  Establishing a Science of Security Research Lablet at the University of Maryland: Task Human Behavior and Cyber Vulnerabilities
  Co-PIs: VS Subrahmanian (UMD), Aditya Prakash (Virginia Tech)
  My share: $72,742
- **Maryland Procurement Office**, $178,250 03/28/2015 – 03/27/2016
  Establishing a Science of Security Research Lablet at the University of Maryland: Task Empirical Models for Vulnerability Exploits
  Co-PI: Marshini Chetty (UMD)
  My share: $129,231
- **Maryland Procurement Office**, $188,805 03/28/2015 – 03/27/2016
  Establishing a Science of Security Research Lablet at the University of Maryland: Task Human Behavior and Cyber Vulnerabilities
  Co-PIs: VS Subrahmanian (UMD), Aditya Prakash (Virginia Tech)
  My share: $71,746
- **Maryland Procurement Office,** $251,856 02/07/2014 - 07/31/2015
  Establishing a Science of Security Research Lablet at the University of Maryland: Task Empirical Models for Vulnerability Exploits
  Co-PI: Marshini Chetty (UMD)
  My share: $146,077
- **Maryland Procurement Office**, $221,972 02/07/2014 - 07/31/2015
  Establishing a Science of Security Research Lablet at the University of Maryland: Task Human Behavior and Cyber Vulnerabilities
  Co-PIs: VS Subrahmanian (UMD), Aditya Prakash (Virginia Tech)
  My share: $84,349
- **National Science Foundation**, Award 1429404, $600,000 08/01/2014 – 07/31/2017
  MRI: Development of Augmentarium: High Performance Visual Computing Infrastructure with Adaptive Displays
  Co-PIs: Amitabh Varshney, Lee Mundy, Kayo Ide, Peter Bajcsy, Antonio Cardone, Ramani Duraiswami, Catherine Plaisant, Rama Chellappa, Joseph JaJa, Rao Gullapalli
  My share: $0 (infrastructure award)

Fellowships, Gifts, and Other Funded Research

- **Amazon**, $25,000 2017
  AWS Cloud Credits for Research
  Co-PIs: Dave Levin, Jonathan Katz, Michael Hicks, Jeff Foster, Michelle Mazurek, Charalampos Papamanthou
  My share: $3,571.43
- **Adobe Corporation**, $50,000 2017
  Adobe Research Award
  Co-PI: Leman Akoglu (CMU)
  My share: $25,000

- **Symantec Corporation**, **$75,000** 2015-2016
  Unrestricted gifts
  My share: $75,000
- **Amazon**, $50,000 2015
  Amazon Web Services (AWS) credit
  Co-PIs: Michael Hicks, Dave Levin, Michelle Mazurek, Charalampos Papamanthou, Elaine Shi, Atif Memon
  My share: $7,142.86

PATENTS

- L. Yumer, T. Dumitraș, Systems and methods for analyzing zero-day attacks, United States Patent 9,158,915, 13 Oct 2015
- T. Dumitraș, P. Efstathopoulos, Systems and methods for determining malicious-attack exposure levels based on field-data analysis, United States Patent 9,043,922, 26 May 2015

RESEARCH PROJECTS

Data-Driven Security 2010 – present
http://www.umiacs.umd.edu/~tdumitra/research-wine.html
Built WINE, Symantec's platform for conducting *data intensive experiments in cyber security* [**BADGERS'11, LEET'12, EDCC'12**]. Designed WINE from the ground up for collecting, sampling and aggregating petabyte-size data sets, for supporting experiments at scale and for ensuring experimental reproducibility.
Used WINE and other data collection platforms to conduct empirical studies on the capabilities of real-world adversaries, including *large scale measurements* of *zero-day attacks* [**CCS'12**], of *exploitation ratios and attack surfaces in the wild* [**RAID'14**], of *reissues and revocations of potentially compromised SSL certificates* [**IMC'14**], of *vulnerability patching* [**IEEE S&P'15**], and of *breaches of trust in the Windows code-signing PKI* [**CCS'17**]. These studies highlighted previously unknown threats that become visible in global-scale data. Utilizing these insights, built machine-learning and data-mining systems for detecting malware and attacks [**USENIX Security'15**, **CCS'15, NDSS'17,**] and developed techniques for addressing key challenges for using machine learning in security [**CCS'16, Euro S&P'18**].

AIR Software Upgrades in Distributed Systems (Ph.D. Dissertation) 2007 – 2010
http://www.umiacs.umd.edu/~tdumitra/research-upgrades.html
Identified the leading causes of *both planned and unplanned downtime* resulting from software upgrades, which account for 66%–86% of the total service unavailability in distributed systems [**Middleware'09**]. Defined the *AIR properties* (atomicity, isolation, runtime-testing) for dependable software upgrades in the cloud; identified the anomalies that may occur when relaxing these properties, such as *mixed-version race conditions* [**Onward!'10**]. Defined methods for benchmarking the dependability of upgrade techniques.

Transparent Adaptation in Fault-Tolerant Middleware 2003 – 2006
http://www.umiacs.umd.edu/~tdumitra/research-mead.html
Introduced mechanisms for resource-aware adaptation to crash, communication and timing faults (e.g., switching between active and passive replication on-the-fly, automatic configuration knobs) [**Middleware'05, ADS III**]. Developed the *MEAD system*, which served as the main fault-tolerance platform for the DARPA-ARMS II and DARPA-PCES II programs [**CC:PS'05**]. Conducted empirical study of *unpredictability* in 16 distributed systems relying on fault-tolerant middleware [**COMNET'12**].

On-Chip Stochastic Communication (M.S. Thesis) 2001 – 2003
http://www.umiacs.umd.edu/~tdumitra/research-noc.html

Proposed new communication paradigm for *networks on chip*, based on randomized gossip. This approach marks a departure from traditional chip design by providing fault tolerance at the system level, through the design of the communication protocol [**ASP-DAC'03, DATE'03, VLSI Design'07**].

Teaching, Mentoring and Advising

Teaching Innovations

Curriculum development

- **ENEE 657 - Computer Security** 2017, 2019
  Proposed and developed a new entry-level graduate security course, to be offered regularly in ECE. The course aims to fill a gap in our curriculum (a graduate security course had not been taught regularly in ECE since 2007) by providing students with a broad foundation in cybersecurity. The course is designed to be relevant to graduate students in both Computer Engineering and in related ECE areas (e.g., Communications).
- **ENEE 140 – Introduction to Programming Concepts for Engineers** 2014–2021
  Developed new teaching materials to cover security topics, aiming to emphasize the importance of secure programming early on in the engineering curriculum. ENEE 140 provides an excellent opportunity for developing a security mindset in our students, as the class teaches the C programming language (a low-level language with few safeguards against programming errors), and for most of the students taking ENEE 140, this is their first encounter with programming.

Innovative pedagogical strategies

- **Debate-oriented active learning** 2014–2017
- Developed a structured discussion format for the student participation component of graduate ECE classes, drawing from my experience in competitive debating. When discussing research papers in class, two teams of students take turns debating the technical merits and the weaknesses of each paper. In addition to making the class more fun and engaging, this format improves the students' communication skills and teaches them to think adversarially, in order to characterize the security properties of a complex system. Tested the format in ENEE 657 and ENEE 757.

Courses Taught

ENEE 657 – Computer Security Fall 2017, 2019
- Enrollment: 12 students

ENEE 757 – Network and Distributed System Security Fall 2014, 2015
- Enrollment 15–17 students
- Course projects resulted in two publications in top-tier security conferences [**USENIX Security'15**, **CCS'15**].

ENEE 140 – Introduction to Programming Concepts for Engineers Fall 2016, 2018, 2020; Spring 2014, 2015, 2016, 2017, 2019
- Enrollment: 35–90 students

ENEE 759D – Security Data Science Fall 2013
- Enrollment: 13 students

Tutorials

'Security Data Science: Improving Security with Big Data Techniques,' **MC2 Symposium'14** Jun 2014
'Benchmarking Computer Security through WINE,' **ACM CCS'11** Oct 2011

Mentoring and Advising

Recruiting and Mentoring Activities to Enhance Student Diversity

- **Summer@MC2 internship program** 2014–present
  Organized paid summer internship program targeting top undergraduate students worldwide. The best performing interns are encouraged to apply for a Ph.D. at UMD. The need for recruiting top

students directly, through this program, stems from the fact that the Maryland Cybersecurity Center (MC2) was created recently and faces strong competition from peer universities with established reputations in security. Additionally, it has become challenging for the ECE department to attract graduate applications from certain geographical regions (e.g. Eastern Europe). Three former interns have subsequently joined Ph.D. programs at UMD: Octavian Suciu, Yiğitcan Kaya and Erin Avllazagaj.
http://legacydirs.umiacs.umd.edu/~tdumitra/summer-internship.html

Students Advised at UMD

- **BumJun Kwon** (PhD; Staff Engineer at Samsung Research) 2013–2018
- **Ziyun Zhu** (PhD; Research Scientist at Facebook) 2014–2019
- **Doowon Kim** (PhD; Assistant Professor at University of Tennessee, Knoxville) 2017–2020
- **Yantao Zhang** (MS) 2014–2015
- **Sanghyun Hong** (PhD; Assistant Professor at Oregon State University) 2015–2021
- **Octavian Suciu** (PhD) 2015–2021
- **Yiğitcan Kaya** (PhD) 2017–present
- **Erin Avllazagaj** (PhD) 2018–present

Undergraduate Students Mentored within Summer@MC2 Internship Program

- **Ionuț Modoranu** (summer intern) 2020
- **Michael Panaitescu-Liess** (summer intern) 2020
- **Khasmamad Shabanovi**, (summer intern) 2020
- **Alperen Keleș** (summer intern) 2020
- **Ionuț Modoranu** (summer intern) 2019
- **Ștefan Matcovici** (summer intern) 2019
- **Michael Davinroy** (summer intern) 2019
- **Gökberk Karaca** (summer intern) 2018
- **Erin Avllazagaj** (summer intern) — admitted to UMD PhD program in 2018 2017
- **Cip Baetu** (summer intern) 2017
- **Florina Barbu** (summer intern) 2017
- **Kristian Kozak** (summer intern) 2017
- **Maria Petrișor** (summer intern) 2017
- **Radu Mărginean** (summer intern) 2017
- **Dylan O'Reagan** (UMD-ECE) 2017
- **Yiğitcan Kaya** (summer intern) — admitted to UMD PhD program in 2017 2016
- **Tiberiu Iorgulescu** (summer intern) 2016
- **Alina Nicolae** (summer intern) 2016
- **Răzvan Bărbăscu** (summer intern) 2016
- **Octavian Suciu** (summer intern) — admitted to UMD PhD program in 2015 2014

Other Undergraduate Students Mentored

- **Derek Blahut** (UMD-URF) 2016
- **Salman Morshed** (UMD-ECE) 2016
- **Alexa Tavassoli** (UMD-ECE) 2016
- **Xiechen Zheng** (UMD-ECE) 2016
- **Grant Orndorff** (UMD-URF) 2015
- **Yang Fang** (UMD–CS) 2015
- **Jacob Eisenman** (UMD-ACES) 2015
- **Leonardo Santos** (UMD-ACES) 2015
- **Cristina Padró Juarbe** (REU) 2014
- **Emma LoBuono** (REU) 2014

- **Daniel Chen** (UMD-ACES) 2014-2015
- **Nicholas Chung** (UMD-ACES) 2014
- **Vyshakh Kandamath** (UMD-ACES) 2014
- **Dan Cuthbert** (UMD-ACES) 2014
- **Max Grable** (UMD-ACES) 2014
- **Lorenzo Randé** (Institut EURECOM) 2012
- **Abdalla Taha** (Institut EURECOM) 2012
- **Pierre Guilleminot** (Institut EURECOM) 2012
- **Alexandre Lachèze** (Institut EURECOM) 2012

Master's Students Mentored

- **Ciara Lynton** (UMD-ECE) – committee member 2018
- **Rock Stevens** (UMD-CS) – non-thesis scholarly paper, reviewer 2016
- **Matt Gilboy** (UMD – ECE) – committee member 2016
- **Frank Shawn Hemingway** (UMD-ECE) – committee member 2013
- **Tammy Tran** (UMD-CS) – non-thesis scholarly paper, reviewer 2013
- **Max Potasznik** (UMD-CS) – non-thesis scholarly paper, reviewer 2013

Doctoral Students Mentored

- **Danny Kim** (UMD-ECE) – committee member 2018
- **Armin Sarabi** (University of Michigan) – committee member 2017
- **Srijan Kumar** (UMD-CS) – committee member 2017
- **Evripidis Paraskevas** (UMD-ECE) – committee member 2016
- **Jayanta Mondal** (UMD-CS) – committee member 2015
- **Xiangyang Liu** (UMD-ECE) – committee member 2015
- **Karla Saur** (UMD-CS) – committee member 2015
- **Udayan Khurana** (UMD-CS) – committee member 2015
- **Jing Wu** (UMD-ECE) – committee member 2014
- **Bertrand Sobesto** (UMD-MechE) – committee member 2014
- **Leyla Bilge** (Symantec Graduate Research Fellowship) 2012
- **Jiyong Jang** (Symantec Graduate Research Fellowship) 2012

Service

Leadership Roles in Meetings and Conferences

- **International Symposium on Research in Attacks, Intrusions and Defenses (RAID)** 2021-2022
  Program Committee Chair
- **MC2 Workshop on Data-Driven Security** 2015, 2017
  Founded and organized biennial workshop aiming to build a community of researchers interested in studying security and privacy empirically, using data-driven techniques, and to establish a research agenda for the field. The 2015 and 2017 editions were organized at the Maryland Cybersecurity Center (MC2) and were attended by 23 and 28 researchers, respectively.
  http://www.umiacs.umd.edu/~tdumitra/data-driven
- **International Workshop on Hot Topics in Software Upgrades (HotSWUp)** 2008–2013
  Co-founded the HotSWUp series of workshops, which bring together researchers from multiple domains (e.g., systems, programming languages, software engineering, databases) who are interested in software upgrades. Through its first five editions, co-located with OOPSLA, ICDE, ICSE and USENIX ATC, HotSWUp has succeeded in establishing a focused research community and in engaging the software industry. Chaired HotSWUp in 2008 and 2009.
  http://www.hotswup.org/
- **ICSOC Ph.D. Symposium** 2006–2007
  Program Committee Chair

Service to the Research Community

Reviewing Activities for Agencies and Foundations

- National Science Foundation, Secure and Trustworthy Cyberspace program 2015, 2016
- Department of Energy, Office of Advanced Scientific Computing Research 2015
- Swiss National Science Foundation 2013

Program Committee Member**

- **IEEE Symposium on Security and Privacy (IEEE S&P)** **2017–2019**
- **ISOC Network and Distributed System Security Symposium (NDSS)** **2017–2020**
- **ACM Conference on Computer and Communications Security (CCS)** **2016–2020**
- **USENIX Security Symposium** **2016–2018**
- IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) 2016
- USENIX Enigma Conference 2016–2017
- Symposium and Bootcamp on the Science of Security (HotSoS) 2015
- USENIX Workshop on Cyber Security and Test (CSET) 2015
- ACM/IFIP/USENIX Middleware Conference 2012–2016
- International Symposium on Research in Attacks, Intrusions and Defenses (RAID) 2015, 2018
- International Conference on Cryptology and Network Security (CANS) 2015
- ACM SIGMETRICS 2014
- European Dependable Computing Conference (EDCC) 2014
- International Workshop on Hot Topics in Software Upgrades (HotSWUp) 2013
- IFIP Distributed Applications and Interoperable Systems (DAIS) 2013
- International Workshop on Software Engineering for Resilient Systems (SERENE) 2013
- IEEE International Conference on Cloud Computing (CLOUD) 2012

** The "Big 4" conferences—IEEE S&P, NDSS, CCS, and USENIX Security—are regarded as the most prestigious publication venues in the security community.

- International Workshop on Evolution and Change in Data Management (ECDM) 2012
- ISSRE Fast Abstracts 2010

Reviewing Activities for Journals

- IEEE Transactions on Parallel and Distributed Systems (TPDS); IEEE/ACM Transactions on Networking; IEEE Transactions on Dependable and Secure Computing (TDSC); IEEE Transactions on Computers (TC); ACM Object-Oriented Programming, Systems, Languages and Applications Conference (OOPSLA) 2010; International Journal of Computer Networks (COMNET); Distributed Computing; IBM Journal of Research and Development; ACM Transactions on the Web (TWEB); Service-Oriented Computing and Applications; IEEE Transactions on Very Large Scale Integration Systems (TVLSI); Architecting Dependable Systems Vol. V; IEEE Pervasive Computing.

CAMPUS SERVICE

Campus Service - Department

- Faculty search committee, ECE 2021
- Salary Committee, ECE 2020
- Department Council, ECE 2019-2020
- Lecturer search committee, ECE 2019-2020
- Faculty search committee, ECE 2017
- Committee for establishing a Computer Engineering Minor, ECE 2014

Campus Service - Other

- Co-Chair, Faculty Search Committee, Maryland Cybersecurity Center 2020
- Program Committee, UMD Executive Cybersecurity Summit 2018-2019
- ACES Director Review Committee, UMD Honors College 2017
- UMIACS Retreat Committee on High-Impact Research, UMIACS 2014

OUTREACH

Consultancies

- Council on Foreign Relations 2016
  Provided expertise on the duration and characteristics of zero-day attacks for a CFR Cyber Brief titled 'Using Incentives to Shape the Zero-Day Market'.
  http://www.cfr.org/cybersecurity/using-incentives-shape-zero-day-market/p38294

Other Outreach

- President, ECE Graduate Student Organization, CMU
- Founder and president, Romanian Students Association, CMU