Birhanu Eshete

Assistant Professor

Department of Computer & Information Science
University of Michigan-Dearborn
CIS 229, 4901 Evergreen Rd., Dearborn, MI 48128
☎ *+1 (313) 583 6669*
✉ *birhanu@umich.edu*

Home Page: http://www-personal.umd.umich.edu/~birhanu

Research Interests

- Trustworthy machine learning (focus: security, privacy, transparency, fairness).
- Cybercrime analysis (focus: characterization, detection, forensics).
- Cyber threat intelligence (focus: characterization, measurement, forensics).

Education

2009–2013 **Ph.D., Computer Science**, *University of Trento*, Italy.

Thesis: *Effective Analysis, Characterization, and Detection of Malicious Activities on the Web*

Supervisor: Adolfo Villafiorita, Ph.D.

Synopsis: contributed to defense against web-borne malware by developing techniques and tools for (i) holistic detection of malicious web pages (ii) evolution-aware detection of malicious web pages and (iii) behavioral fingerprinting and detection of exploit kits.

2005–2007 **M.Sc., Computer Science**, *Addis Ababa University*, Ethiopia.

Thesis: *Context Information Refinement for Pervasive Medical Systems*

Supervisor: Dawit Bekele, Ph.D.

Synopsis: contributed to pervasive computing by developing a context-awareness framework for pervasive healthcare systems with emphasis on QoS and pervasive healthcare domain requirements.

1999–2003 **B.Sc., Computer Science**, *Addis Ababa University*, Ethiopia.

Experience

09/18–now: **Assistant Professor**, *University of Michigan, Dearborn*, U.S.A.
—research, teaching, and service in cybersecurity.

09/18–now: **Affiliated Faculty Member**, *Michigan Institute for Data Science (MIDAS), University of Michigan, Ann Arbor*, U.S.A.
—research on data-driven security.

06/19–07/19: **Analytics Scientist**, *Ford Motor Company*, U.S.A.
—research on AI-driven platform for stolen vehicle parts tracking.

02/14–08/18: **Postdoctoral Researcher**, *University of Illinois at Chicago*, U.S.A.
—carried out original research on systems security, cybercrime analysis, and advanced cyber-attacks.

04/13–09/13 **Visiting Researcher**, *University of Illinois at Chicago*, U.S.A.
—developed a novel system for behavioral fingerprinting and detection of exploit kits.

08/09–12/13 **Research Assistant**, *Fondazione Bruno Kessler*, Italy.
—developed three novel techniques and tools to analyze and detect web-borne malware.

09/07–06/09 **Executive Committee Member**, *Ethiopian IT Professionals Association*, Ethiopia.
—served as treasurer of the executive committee.

06/06–12/06 **Main Research Engineer**, *United Nations Economic Commission for Africa*, Ethiopia.
—developed a prototype mobile medical system to support mobility of physicians in a hospital.

09/04–05/06 **Part-time Instructor**, *Addis Ababa University*, Ethiopia.
—taught laboratory and lecture sessions of programming, operating systems, and introductory computer science.

06/04–04/05 **Junior Programmer**, *Ethio Telecom*, Ethiopia.
worked as a developer on a Customer Management System.

Honors, Grants & Awards

- **Sponsor: NSF**. Project: "CAREER: Towards Provenance-Driven Understanding of Machine Learning Robustness", Sole PI: Birhanu Eshete, Amount: $\$619,838$, Duration: 05/01/23 - 04/30/28.
- **Sponsor: NSF**. Project: "Elements: An Infrastructure for Software Quality and Security Issues Detection and Correction", PI: Marouane Kessentini, Co-PI: Birhanu Eshete, Amount: $\$599,999$ (Birhanu's Share: $\$270,000$), Duration: 05/01/22 - 04/30/25.
- **Sponsor: Dearborn AI Research Center (DAIR)**. Project: "Towards Robust Machine Learning Models via Moving Target Defense", PI: Birhanu Eshete, Amount: $\$10,000$, Duration: 09/01/21 - 07/31/23.
- **Sponsor: NSF**. Project: "MALDIVES: Developing a Comprehensive Understanding of Malware Delivery Mechanisms", Direct Sponsor: University of Illinois at Chicago, Amount: $\$54,263$, Duration: 8/16/19 - 9/30/20.
- **U-M/Ford Alliance Program**: Faculty Summer Sabbatical Awardee, Summer of 2019.
- **NSF ASSIST Travel Award**: 2019 Academic Research Leadership Symposium (ARLS) at the Annual Convention of the National Society of Black Engineers (NSBE), 2019.
- **CSAW'18 US-Canada Finalist**: for the paper "NAVEX: Precise and Scalable Exploit Generation for Dynamic Web Applications", Applied Research Competition at CSAW, NYU Tandon School of Engineering, 2018.
- **Distinguished Paper Award**: for the paper "NAVEX: Precise and Scalable Exploit Generation for Dynamic Web Applications", USENIX Security Symposium, The USENIX Association, Baltimore, MD, USA, Aug. 2018.
- **USENIX Travel Grant**: for attending the USENIX Security Symposium, The USENIX Association, Washington D.C., USA, Aug. 2013.
- **Best Paper Award**: for the paper "Context Information Refinement for Pervasive Medical Systems", International Conference on Digital Society (ICDS), 2010.
- **Ph.D. Study Grant**: €43, 450 full scholarship for 3 years Ph.D. research in Web Security, Fondazione Bruno Kessler, Trento, Italy, Nov. 2010 - Oct. 2013.
- **Project Study Grant**: €15,750 for the project "Tool for Security Testing of Web Applications", Fondazione Bruno Kessler, Trento, Italy, Nov. 2009 - Oct. 2010.

Publications

1. Abderrahmen Amich, Birhanu Eshete, Vinod Yegneswaran, Nguyen Phong Hoang. DeResistor: Toward Detection-Resistant Probing for Evasion of Internet Censorship. *In Proceedings of the 32nd USENIX Security Symposium (SEC'23)*, 2023. **Acceptance Rate**: 18%
2. Ismat Jarin, Birhanu Eshete. MIAShield: Defending Membership Inference Attacks via Preemptive Exclusion of Members. *In Proceedings of the 23rd Privacy Enhancing Technologies Symposium (PETS)*, 2023. **Acceptance Rate**: 25%
3. Probir Roy, Birhanu Eshete, Pengfei Su. Designing Secure Performance Metrics for Last Level Cache. *In Proceedings of the 28th International Workshop on High-Level Parallel Programming Models and Supportive Environments, (HIPS)*, 2023.
4. Abderrahmen Amich, Birhanu Eshete, Vinod Yegneswaran. Adversarial Detection of Censorship Measurements. *In Proceedings of the 20th ACM Workshop on Privacy in the Electronic Society (WPES'22), co-located with the 29th ACM Conference on Computer and Communications Security (CCS)*, 2022. **Acceptance Rate**: 20.3%
5. Ismat Jarin, Birhanu Eshete. DP-UTIL: Comprehensive Utility Analysis of Differential Privacy in Machine Learning. *In Proceedings of the 12th ACM Conference on Data and Application Security and Privacy (ACM CODASPY)*, 2022. **Acceptance Rate**: 18%
6. Abderrahmen Amich, Birhanu Eshete. EG-Booster: Explanation-Guided Booster for ML Evasion Attacks. *In Proceedings of the 12th ACM Conference on Data and Application Security and Privacy (ACM CODASPY)*, 2022. **Acceptance Rate**: 18%
7. Abderrahmen Amich, Birhanu Eshete. Morphence: Moving Target Defense Against Adversarial Examples. *In Proceedings of the 37th Annual Computer Security Applications Conference (ACSAC)*, 2021. **Acceptance Rate**: 24.5%
8. Birhanu Eshete. Making Machine Learning Trustworthy. *Science*, Vol. 373, Issue. 6556, pp. 743–744, American Association for the Advancement of Science (AAAS), 13 August 2021. **Impact Factor**: 63.74.
9. Abderrahmen Amich, Birhanu Eshete. Explanation-Guided Diagnosis of Machine Learning Evasion Attacks. *In Proceedings of the 17th EAI International Conference on Security and Privacy in Communication Networks (SecureComm)*, 2021. **Acceptance Rate**: 34%
10. Ismat Jarin, Birhanu Eshete. PRICURE: Privacy-Preserving Collaborative Inference in a Multi-Party Setting. *In Proceedings of the 7th ACM International Workshop on Security and Privacy Analytics (IWSPA'21), co-located with the 11th ACM Conference on Data and Application Security and Privacy (CODASPY)*, 2021. **Acceptance Rate**: 29%
11. Abdullah Ali, Birhanu Eshete. Best-Effort Adversarial Approximation of Black-Box Malware Classifiers. *In Proceedings of the 16th EAI International Conference on Security and Privacy in Communication Networks (SecureComm)*, 2020. **Acceptance Rate**: 50%
12. Sadegh M. Milajerdi, Birhanu Eshete, Rigel Gjomemo, V.N. Venkatakrishnan. Poirot: Aligning Attack Behavior with Kernel Audit Records for Cyber Threat Hunting. *In Proceedings of the 26th ACM Conference on Computer and Communications Security (ACM CCS)*, 2019. **Acceptance Rate**: 16%
13. Sadegh M. Milajerdi, Rigel Gjomemo, Birhanu Eshete, R. Sekar, V.N. Venkatakrishnan. HOLMES: Real-time APT Detection through Correlation of Suspicious Information Flows. *In Proceedings of the 40th IEEE Symposium on Security and Privacy (Oakland)*, 2019. **Acceptance Rate**: 12%
14. Sadegh M. Milajerdi, Birhanu Eshete, Rigel Gjomemo, V.N. Venkatakrishnan. ProPatrol: Attack Investigation via Extracted High-Level Tasks. *In Proceedings of the 14th International Conference on Information Systems Security (ICISS)*, 2018. **Acceptance Rate**: 47%

15. Abeer Alhuzali, Rigel Gjomemo, Birhanu Eshete, V.N. Venkatakrishnan. NAVEX: Precise and Scalable Exploit Generation for Dynamic Web Applications. *In Proceedings of the USENIX Security Symposium (USENIX SEC)*, 2018. * Distinguished Paper Award * , * Finalist: CSAW'18 Applied Research Competition North America (US-Canada) *. **Acceptance Rate**: 19.1%
16. Md Nahid Hossain, Sadegh M. Milajerdi, Junao Wang, Birhanu Eshete, Rigel Gjomemo, R. Sekar, Scott Stoller, V.N. Venkatakrishnan. SLEUTH: Real-time Attack Scenario Reconstruction from COTS Audit Data. *In Proceedings of the USENIX Security Symposium (USENIX SEC)*, 2017. **Acceptance Rate**: 16.3%
17. Birhanu Eshete, V.N. Venkatakrishnan. DynaMiner: Leveraging Infection Dynamics Analytics for On-the-Wire Malware Detection. *In Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2017. **Acceptance Rate**: 24.5%
18. Abeer Alhuzali, Birhanu Eshete, Rigel Gjomemo, V.N. Venkatakrishnan. Chainsaw: Chained Automated Workflow-based Exploit Generation. *In Proceedings of Computer and Communications Security (ACM CCS)*, 2016. **Acceptance Rate**: 16.5%
19. Birhanu Eshete, Abeer Alhuzali, Maliheh Monshizadeh, Phillip Porras, V.N. Venkatakrishnan, Vinod Yegneswaran. EKHunter: A Counter-Offensive Toolkit for Exploit Kit Infiltration. *In Proceedings of Network and Distributed Systems Security Symposium (ISOC NDSS)*, 2015. **Acceptance Rate**: 16.9%
20. Birhanu Eshete, V.N. Venkatakrishnan. WebWinnow: Leveraging Exploit Kit Workflows to Detect Malicious URLs. *In Proceedings of Conference on Data and Application Security and Privacy (ACM CODASPY)*, 2014. **Acceptance Rate**: 16%
21. Birhanu Eshete, Komminist Weldemariam, Adolfo Villafiorita, Mohammad Zulkernine. EINSPECT: Evolution-Guided Analysis and Detection of Malicious Web Pages. *In Proceedings of the International Conference on Computer Software and Applications (IEEE COMPSAC)*, 2013. **Acceptance Rate**: 23%
22. Birhanu Eshete, Komminist Weldemariam, Adolfo Villafiorita, Mohammad Zulkernine. ConfEagle: Automated Analysis of Security Configuration Vulnerabilities in Web Applications. *In Proceedings of the International Conference on Security and Reliability (IEEE SERE)*, 2013. **Acceptance Rate**: 30%
23. Birhanu Eshete. Effective Analysis, Characterization, and Detection of Malicious Web Pages. *In Proceedings of the International Conference on World Wide Web (ACM WWW) Companion*, 2013. **Acceptance Rate**: 14%
24. Aaron Ciaghi, Birhanu Eshete, Pietro Molini, Adolfo Villafiorita. SAMo: experimenting a social accountability web platform. *In Proceedings of the ACM Symposium on Computing for Development (ACM DEV)*, 2013. **Acceptance Rate**: 33%
25. Birhanu Eshete, Adolfo Villafiorita, Komminist Weldemariam. BINSPECT: Holistic Analysis and Detection of Malicious Web Pages. *In Proceedings of the International Conference on Security and Privacy in Communication Networks (EAI SECURECOMM)*, 2012. **Acceptance Rate**: 28.8%
26. Aaron Ciaghi, Birhanu Eshete, Pietro Molini, Adolfo Villafiorita. Social Accountability for Mozambique: an Experience Report from the Moamba District. *In Proceedings of the International IEEE EAI Conference on e-Infrastructure and e-Services for Developing Countries (IEEE AFRICOMM)*, 2012.
27. Birhanu Eshete, Komminist Weldemariam, Adolfo Villafiorita. Early Detection of Security Misconfiguration Vulnerabilities in Web Applications. *In Proceedings of the International Conference on Availability, Reliability and Security (IEEE ARES)*, 2011. **Acceptance Rate**: 25%

28. Birhanu Eshete, Adolfo Villafiorita, Komminist Weldemariam. Malicious Website Detection: Effectiveness and Efficiency Issues. *In Proceedings of the System Security Workshop (IEEE SysSec)*, 2011.
29. Valentino Sartori, Birhanu Eshete, Adolfo Villafiorita. Measuring the Impact of Different Metrics on Software Quality: A Case Study in the Open Source Domain. *In Proceedings of the International Conference on Digital Society (IEEE ICDS)*, 2011.
30. Birhanu Eshete, Dawit Bekele, Komminist Weldemariam, Adolfo Villafiorita. Context Information Refinement for Pervasive Medical Systems. *In Proceedings of the International Conference on Digital Society (IEEE ICDS)*, 2010. *Best Paper Award Winner!*
31. Biniyam Asfaw, Dawit Bekele, Birhanu Eshete, Komminist Weldemariam, Adolfo Villafiorita. Host-based Anomaly Detection for Pervasive Medical Systems. *In Proceedings of the International Conference on Risks and Security of Internet and Systems (IEEE CRiSIS)*, 2010. **Acceptance Rate**: 44%
32. Birhanu Eshete, Komminist Weldemariam, Adolfo Villafiorita, Andrea Mattioli. ICT for Good: Opportunities, Challenges and the Way Forward. *In Proceedings of the International Conference on Digital Society (IEEE ICDS)*, 2010.

Patents

- System and Method Associated with Expedient Detection and Reconstruction of Cyber Events in a Compact Scenario Representation Using Provenance Tags and Customizable Policy. Inventors: Ramasubramanian Sekar, Junao Wang, Md Nahid Hossain, Sadegh M. Milajerdi, **Birhanu Eshete**, Rigel Gjomemo, V. N. Venkatakrishnan, Scott Stoller. Patent number: 11601442. Type: Grant. Filed: August 19, 2019. Date of Patent: March 7, 2023.

Teaching

Graduate

- **Winter 2023**: *Advanced Computer & Network Security (CIS 584)*, University of Michigan-Dearborn.
- **Fall 2022**: *Data Security and Privacy (CIS 545)*, University of Michigan-Dearborn.
- **Fall 2022**: *Foundations of Information Security (CIS540)* , University of Michigan-Dearborn.
- **Winter 2022**:*Compiler Design (CIS 574)*, University of Michigan-Dearborn.
- **Fall 2021**: *Data Security and Privacy (CIS 545)*, University of Michigan-Dearborn.
- **Fall 2021**: *Foundations of Information Security (CIS540)*, University of Michigan-Dearborn.
- **Winter 2021**: *Compiler Design (CIS 574)*, University of Michigan-Dearborn.
- **Fall 2020**: *Data Security and Privacy (CIS 545)*, University of Michigan-Dearborn.
- **Fall 2020**:*Foundations of Information Security (CIS 540)*, University of Michigan-Dearborn.
- **Winter 2020**:*Compiler Design (CIS 574)*, University of Michigan-Dearborn.
- **Fall 2019**: *Data Security and Privacy (CIS 545)*, University of Michigan-Dearborn.
- **Winter 2019**: *Compiler Design (CIS 574)*, University of Michigan-Dearborn.
- **Fall 2018**: *Data Security and Privacy (CIS 545)*, University of Michigan-Dearborn.
- **Spring 2018:** *Network Security (CS591)* with Venkat Venkatakrishnan, University of Illinois at Chicago.
- **Spring 2016:** *Advanced and Persistent Threats (CS594)* with Venkat Venkatakrishnan and Rigel Gjomemo, University of Illinois at Chicago.

Undergraduate

- **Winter 2022:** *Design Seminar I (CIS 4951)*, University of Michigan-Dearborn.

- **Winter 2022:** *Design Seminar II (CIS 4952)*, University of Michigan-Dearborn.
- **Winter 2022:***Compiler Design (CIS 474)*, University of Michigan-Dearborn.
- **Fall 2021:** *Data Security and Privacy (CIS 4851)*, University of Michigan-Dearborn.
- **Winter 2021:** *Compiler Design (CIS 474)*, University of Michigan-Dearborn.
- **Winter 2021:** *Digital Forensics II (CIS 467)*, University of Michigan-Dearborn.
- **Fall 2020:** *Data Security and Privacy (CIS 4851)*, University of Michigan-Dearborn.
- **Winter 2020:** *Compiler Design (CIS 474)*, University of Michigan-Dearborn.
- **Fall 2019:** *Data Security and Privacy (CIS 4851)*, University of Michigan-Dearborn.
- **Winter 2019:** *Compiler Design (CIS 474)*, University of Michigan-Dearborn.
- **Fall 2018:** *Data Security and Privacy (CIS 4851)*, University of Michigan-Dearborn.

Student Advising

Doctoral

- **2023** - : Firas Ben Hmida, University of Michigan-Dearborn.
- **2023** - : Philemon E. Hailemariam, University of Michigan-Dearborn.
- **2019** - **2024 (expected)**: Abderrahmen Amich, University of Michigan-Dearborn.
- **2019** - **2022**: Ismat Jarin, University of Michigan-Dearborn.

Master's Theses

- **2023:** By Christine Carlton. "AI Risk Management Framework for Autonomous Vehicles", University of Michigan-Dearborn.
- **2023:** By Jon-Nicklaus Jackson. "Exploring Training Provenance for Clues of Data Poisoning in Machine Learning", University of Michigan-Dearborn.
- **2022:** By Olajide David. "CYTAG: Multi-Source Behavioral Aggregation of Natural Language Cyber Threat Intelligence", University of Michigan-Dearborn.
- **2019:** By Abdullah Ali. "Adversarial Approximation of a Black-Box Malware Detector", University of Michigan-Dearborn.
- **2015:** By Stefano Arseni. "Hyper-Sift: Multi-Family Analysis and Detection of Exploit Kits", University of Illinois at Chicago.

Master's Projects

- **2023:** By Hassaan Ali "Large-Scale Correlation Analysis of Public Information of Notable Individuals with Security Questions on Websites", University of Michigan-Dearborn.
- **2023:** By Ata Kaboudi. "Code Property Graph-Based Security Vulnerability Analysis", University of Michigan-Dearborn.
- **2022:** By Hassan Ali. "Empirical Characterization of Benign and Adversarial Predictions of a Neural Network", University of Michigan-Dearborn.
- **2021:** By Majed Chamseddine. "Automated Characterization of Decision Provenance in Neural Networks", University of Michigan-Dearborn.
- **2015:** By Sai Kommini. "Architectural Isolation of Plugins in Web Applications", University of Illinois at Chicago.

Undergraduate Independent Studies

- **2022:** By Chevy Pawlik. Project Title: "Correlation and Temporal Analysis of Malware Infection Traffic and APT Reports"
- **2022:** By Ata Kaboudi. Project Title: "Morphence-2.0: Evasion-Resilient Moving Target Defense Powered by Out-of-Distribution Detection"

- **2021:** By Zeineb Moalla. Project Title: "Building a Behavior-Based Malware Detector and Evaluating its Adversarial Robustness"

Bachelor's Capstone Projects

Senior Design II: Winter 2022 (with Dr. Bruce Maxim): 14 Teams

- By Murfiq Ali, Nick Shute, Jeffrey Neal, Aashray Thakuri. Project Title: "Translation Networks"
- By Ali Baydoun, Othman Alaansi, Ali Shuhait. Project Title: "MICDROP"
- By Sydney Taylor, Trevor Johnson, Grant Saylor, Clarisa Summers, Deekshita Balaji. Project Title: "LandInfo Dashboard"
- By Amaya Gushiniere, Ingrid Camille Lagman, Brendan Kacic, Christopher Bourn, Sukun Patel. Project Title: "PolliNation ID: Interactive Pollination App"
- By Abdullah Babor, Anthony Gordon, Hassan Ibrahim, Alexander Kostoff, Alexander Rago. Project Title: "Maestro Analyzer"
- By Azal Ahmed, Bishal Bogati, Anish Simkhada, Upama Uprety, Jessica Sterly. Project Title: "Victory for Veterans"
- By Johnathan Khalil, Owen Rowader, Nathan Lipski, Clayton DeClue, Hadi Daana . Project Title: "Dearborn Police Department Database Project"
- By Muhaddatha Abdulghani, Jason Soltis, Dalia Nasr, Melissa Paul. Project Title: "EIC Scheduler"
- By Jeffery Fishman, Michelle Liu, Kevin Marzolo, Joseph Nelson, Harold Tudtud. Project Title: "Oplogic Messaging App"
- By Donovan Farrell, Amr Mashrah, Talal Al Fahad, Ronnie Kina. Project Title: "Cover Fanz"
- By Ali Banihashemi, Justin Beharry, Muhammad Ali Haidar, Christopher Hill, Kyle Ponikiewski. Project Title: "Land.Info Simulation"
- By Aaron Guzman, Jacob Travis, Tomas Kinolli, Bailey Merritt, Justin Kusch. Project Title: "7 Seas Game"
- By Rachel Kennelly, Sid Stainbrook, Aleksandra Shor, Ryan Hendershot, Emma Zorn. Project Title: "HiRoad Social Mobile App"
- By Malak Al-Delahmawi, Faras AlKhurasi, Ahmad Mazeh, Leila Fawaz, Basel Fawaz. Project Title: "Bring A Flatbed"

Senior Design I: Winter 2022 (with Dr. Bruce Maxim): 11 Teams

- By James Bordeau, Avery Girven, Justin Klump, Mustafa Ayyad. Project Title: "Art Match"
- By Mark LaFreniere, Ali Bazzi, John Bellfi, Shahriar Sagor. Project Title: "KAPTURE: Digital Forensic Case Management"
- By Abdallah Alallaf, Matthew Braden, Jeffrey Ambler, Gurnoor Sandhu. Project Title: "Legal App"
- By Ryan Shanerberger, Taylor Landdicho, Will Gaderick, Jordan Gilbert. Project Title: "SOLVED!: Crypto Game Platform"
- By Dua Atoui, Raghad Hajar, Matthew Smith, Thomas Metaxas. Project Title: "Scholarship App"
- By Nathan Yomtoob, Chris Sauer, Micheal Berry, Tanim Ahmed. Project Title: "Stock Companion App"
- By Nathan Baines, Abidul Chowdury, Nathanael Butler, Anna Mitrofan. Project Title: "The Casting Guru"
- By Jawad Kazma, Hady Mahfouz, Christian Hanchett, Chevy Pawlik. Project Title: "AUTOMATIC"
- By Lubna Tattan, Ahsan Virk, Basmalah Algahmi, Khodr Salman. Project Title: "FullScan Home Inspection App"
- By Brannon Alcantar, Erik Arney, Trenton Stebner-Hoang, Galen O'Donnell. Project Title:

"Tower of Babel: HathiTrust Edtion"
- By Jason Bean, Afraz Jaweed, Jack MacDonald, Kassim Ballout. Project Title: "While You're Out App"

University of Illinois at Chicago:
- **2014:** By Patric Tam on "Dynamic Crawling Infrastructure to Harvest Potentially Malicious URLs".
- **2014:** By Sohaib Choudhry on "Trend Based Web Crawler to Harvest Potentially Malicious URLs".

University of Trento:
- **2010:** By Valentino Sartori on "Definition of Predictive Models of Software Quality: Evaluation and Characterization of Open Source Web Applications"
- **2010:** By Claudio Frigo on "Misconfiguration Vulnerability Analysis in Web Applications".

Thesis Committees

Doctoral

- **Candidate**: Linxi Zhang. **Dissertation Title**: Intrusion Detection Systems to Secure In-Vehicle Networks. **Advisor**: Dr. Di Ma.
- **Candidate**: Robert Kaster. **Dissertation Title**: Automotive Remote Attestation: Self, Remote, Peer Challenges. **Advisor**: Dr. Di Ma
- **Candidate**: Weixing Zhou. **Dissertation Title**: Correlation Algorithm Method Based Vehicle CAN Network Identification Mapping. **Advisor**: Dr. Di Ma.

Master's

- **Candidate**: Magdalena Spinu. **Thesis Title**: A Comprehensive Review of Machine Learning Methods in Stock Market. **Advisor**: Dr. Jin Lu. 2022.
- **Candidate**: Francesco E. Mangano. **Thesis Title**: Modernization of Manufacturing with Cybersecurity at the Forefront. **Advisor**: Dr. Di Ma. 2018.

Professional Service

Organization Committee Member

- **43rd IEEE Symposium on Security & Privacy - Diversity, Equity, and Inclusion Co-Chair**. 2022.
- **Dearborn AI Symposium - Poster and Demo Track Co-Chair**: University of Michigan, Dearborn, Nov 05 – Nov 06, 2020.
- **Dearborn Cybersecurity Day**: University of Michigan, Dearborn, April 01, 2019.

Program Committee Member

- **CAI**: The 15^{th} International Workshop on Cyberspace Security and Artificial Intelligence, 2023.
- **USENIX SEC**: The USENIX Security Symposium, 2023.
- **IEEE EuroS&P**: IEEE European Symposium on Security and Privacy, 2023.
- **ACM CODASPY**: ACM Conference on Data and Application Security and Privacy, 2023.
- **USENIX SEC**: The USENIX Security Symposium, 2022.
- **USENIX SEC**: The USENIX Security Symposium, 2020.
- **SECURECOMM**: Security and Privacy in Communication Networks, 2020.
- **SECURECOMM**: Security and Privacy in Communication Networks, 2019.
- **SECURECOMM**: Security and Privacy in Communication Networks, 2018.

- **SECURECOMM**: Security and Privacy in Communication Networks, 2017.
- **MAICS**: Modern Artificial Intelligence and Cognitive Science Conference, 2017.
- **SECURECOMM**: Security and Privacy in Communication Networks, 2016.
- **MAICS**: Modern Artificial Intelligence and Cognitive Science Conference, 2016.

Invited Journal Article Reviewer

- **IJIS**: International Journal of Information Security, 2022.
- **TDSC**: IEEE Transactions on Dependable and Secure Computing, 2021.
- **IJIS**: International Journal of Information Security, 2020.
- **ITS**: IEEE Intelligent Transportation Systems Magazine, 2019.
- **TDSC**: IEEE Transactions on Dependable and Secure Computing, 2018.
- **TIFS**: IEEE Transactions on Information Forensics & Security, 2018.
- **TDSC**: IEEE Transactions on Dependable and Secure Computing, 2017.
- **IJIS**: International Journal of Information Security, 2016.
- **NEPL**: Neural Processing Letters, 2015.
- **TDSC**: IEEE Transactions on Dependable and Secure Computing, 2015.
- **ESEJ**: e-Informatica Software Engineering Journal, 2015.
- **JSS**: Journal of Systems and Software, 2013.

External Conference Reviewer

- **CCS**: Computer and Communication Security, 2018.
- **NDSS**: Network and Distributed Systems Security Symposium, 2016.
- **QRS**: International Conference on Software Quality, Reliability & Security, 2015.
- **ICWE**: International Conference on Web Engineering, 2015.
- **NDSS**: Network and Distributed Systems Security Symposium, 2015.
- **ICISS**: International Conference on Information Systems Security, 2014.
- **SERE**: International Conference on Security and Reliability, 2014.

K-12 Outreach

- **Advisory Board Member**: Cybersecurity Program, Taylor High School, 2022 - present.

Professional Membership

- **Member**: Global OWASP Foundation
- **Member**: IEEE
- **Member**: ACM

Invited Talks & Presentations

- **State of the Model: Promising Progress and Remaining Challenges Towards Trustworthy Machine Learning,** Blacks in Cybersecurity (BIC) Village @ DEF CON 30, Las Vegas, NV, August, 2022.
- **State of the Model: Making Machine Learning Models Resilient Against Evasion and Inference Attacks,** SRI International, Menlo Park, CA, March, 2022.
- **Best-Effort Adversarial Approximation of Black-Box Malware Classifiers,** EAI SecureComm'20, Washington, DC, October, 2020.
- **Adventures with Cybercrime Toolkits: Insights for Pragmatic Defense,** USENIX ENIGMA Conference, San Francisco, CA, USA, January, 2020.

- **Real-time Detection of Advanced Persistent Threats using Correlation of Information Flows,** Computer and Information Science Research Seminar, College of Engineering and Computer Science, University of Michigan, Dearborn, MI, USA, October, 2018.
- **Intrusion Detection: Theoretical Foundations and Practical Flavors,** Graduate Seminar, Addis Ababa Institute of Technology (AAiT), Addis Ababa, Ethiopia, July, 2018.
- **Learning from Offline Infection Episodes for On-the-Wire Malware Detection,** 7th Greater Chicago Area Systems Research Workshop (GCASR), Chicago, IL, USA, April, 2018.
- **DynaMiner: Leveraging Offline Infection Analytics for On-the-Wire Malware Detection,** IEEE/IFIP DSN'17, Denver, CO, USA, June, 2017.
- **EKHunter: A Counter-Offensive Toolkit for Exploit Kit Infiltration,** GCASR'15, Chicago, IL, USA, April, 2015.
- **EKHunter: A Counter-Offensive Toolkit for Exploit Kit Infiltration,** NDSS'15, San Diego, CA, USA, February 2015.
- **WebWinnow: Leveraging Exploit Kit Workflows to Detect Malicious URLs,** CODASPY'14, San Antonio, TX, USA, March 2014.
- **Effective Analysis, Characterization, and Detection of Malicious Activities on the Web,** Computer Science Department, University of Illinois at Chicago, Chicago, IL, USA, April 2013.
- **Effective Analysis, Characterization, and Detection of Malicious Web Pages,** WWW'13, Rio De Janeiro, Brazil, May 2013.
- **Leveraging Exploit Kit Workflow to Detect Malicious URLs,** Computer Science Department, University of Illinois at Chicago, Chicago, IL, USA, August 2013.
- **BINSPECT: Holistic Analysis and Detection of Malicious Web Pages,** SECURECOMM'12, Padua, Italy, September 2012.
- **Early Detection of Security Misconfiguration Vulnerabilities in Web Applications,** Vienna, Austria, August 2011.
- **Malicious Website Detection: Effectiveness and Efficiency Issues,** SysSec'11, Amsterdam, Netherlands, July 2011.
- **Host-Based Anomaly Detection in Pervasive Medical Systems,** CRISIS'10, Montreal, Canada, October 2010.

In the News

- **August 2022: New Frontiers: Emerging Science and Technology Podcast:** Machine Learning for Environment with Bad Actors.
  Podcast Audio Link: https://open.spotify.com/embed/episode/7KzU6wCIKymhc4mdrDrQgo
- **August 2021: Science Magazine Podcast:** Attacks on Machine Learning.
  Podcast Audio Link: https://open.spotify.com/embed/episode/7wA4RpCKMsGhMjkYZw1JUo
- **June 2021: WXYZ Detroit:** How to strengthen your cybersecurity while working at home.
  Interview Video Link: https://www.youtube.com/watch?v=J4gse2oEeWU
- **June 2023: UM-Dearborn Reporter**: Is AI really a threat to human civilization?
  https://umdearborn.edu/news/ai-really-threat-human-civilization
- **April 2023: UM-Dearborn Reporter**: NSF CAREER Award Feature:
  https://umdearborn.edu/news/cybersecurity-researcher-birhanu-eshete-scores-prestigious-nsf-career-award
- **November 2021: UM-Dearborn Reporter**: Should we view cyberattacks as acts of war?
  https://umdearborn.edu/news/should-we-view-cyberattacks-acts-war
- **November 2021: UM-Dearborn Reporter**: Helping scientists become better coders
  https://umdearborn.edu/news/helping-scientists-become-better-coders

- **June 2021: UM-Dearborn Reporter**: Can we make artificial intelligence more ethical?
  https://umdearborn.edu/news/can-we-make-artificial-intelligence-more-ethical
- **July 2020: UM-Dearborn Reporter**: UM-Dearborn's 'Blue Bytes' group is helping students build-up their arsenal of cybersecurity skills
  https://umdearborn.edu/news/um-dearborns-blue-bytes-group-helping-students-build-their-arsenal-cybersecurity-skills
- **November 2019: UM-Dearborn Reporter**: A dispatch from the cybersecurity 'arms race'
  https://umdearborn.edu/news/dispatch-cybersecurity-arms-race