Lotfi ben Othmane

Curriculum Vitae

January 2026

Phone: +5157085234
Email: lotfi.benothmane@unt.edu
WWW: https://facultyinfo.unt.edu/faculty-profile?query=Lotfi%20Ben%20Othmane&type=name&profile=lb0577

Research interests:	Support engineering secure cyber-physical systems.
Research funding:	≃ $ 655.4K.
Publications:	61 peer-reviewed papers, incl. 4 IEEE transactions papers, # citations 2136, H-index 24, I-index 37
Graduate students:	17 students with MS degree and 2 students with Ph.D. degree
Taught courses:	15 courses on cyber-security, software engineering, artificial intelligence, and cybersecurity fundamentals.
Fully developed courses:	7 courses: software engineering for AI, secure software engineering, software engineering, foundation of cybersecurity, software architecture, project management, and programming with Python.
Citizenship:	US permanent resident and Canadian citizen

Work Experience

Academia

2022-Present	Clinical Associate Professor, University of North Texas, USA
2017-2021	Assistant Teaching Professor, Iowa State University, USA Title changed from Lecturer in July 2019
2014-2016	Head of the Secure Software Engineering Department, Fraunhofer Secure Information Technology, Germany Research Scientist until Oct. 2015
2014-2016	Lecturer, Technical University Darmstadt, Germany
2011-2013	Postdoc, Eindhoven University of Technology, The Netherlands
2010-2011	Visiting Assistant Professor, Kalamazoo College, USA
2008-2011	Teaching and Research Assistant, Western Michigan University, USA

Industry

2020-Present	President, Brainsoft LLC, USA
2005-2007	System Analyst, ABA International, USA
2004-2005	Software Architect, International Air Transportation Association, Canada
2003-2004	Consultant, Gestion Informatique OKA LTEE, Canada
2001-2003	Applications Architect, Documens, Canada
1998-2001	Information and Methodology Director, "Les Laboratoires Reunis", Tunisia
1997-1998	Technical Analyst, "Societe des Services Generaux", Tunisia
1995-1996	Technology Manager, SNA (subsidiary of POULINA Group), Tunisia

Education

2010	Ph.D.	Western Michigan University (WMU), USA (Computer Science)
2000	M.Sc.	University of Sherbrooke, Canada (Computer Science)
1995	B.Sc.	University of Sfax, Tunisia (Computer Science Applied to Management)

Professional Development

- Certificate in the Effective Teaching Practice Framework, The Association of College and University Educators (ACUE), 2025
- Certificate of Excellence in Teaching Online, University of North Texas, 2025

- Online Course Development Training, University of North Texas, 2025

Initiated startups

1. Brainsoft–Develop and commercialize software for controlling physical objects using brainwaves.
2. SecureAuto–Develop and commercialize a platform to detect malicious attacks on connected vehicles.

Professional memberships

- IEEE Cybersecurity Ambassador, 2016-current
- IEEE Senior Member, since 2017

Research grants

1. Ademola Adesokan (BL), and Sanjay Madria (TL), Lotfi ben Othmane (IM), i-Corp - Disaster Management Enterprise Information Resource Planning(DisMEIRP) System for Disaster Response, NSF, 2024, $ 50 K.
2. Lotfi ben Othmane (PI), Using brainwaves in virtual reality applications - supplement, BioConnect, 2022-2024, $ 50 K
3. Lotfi ben Othmane (PI), Using brainwaves in virtual reality applications, NSF, 2022-2023, $ 276 K
4. Lotfi ben Othmane (PI), Secure function evaluation for time-sensitive data, Air Force Research Lab, Summer Faculty Visit, 2021, $14,832
5. Lotfi ben Othmane (PI), David Jiles and Mani Mina, Measurement of the reaction of the brain to transcranial magnetic stimulation: a new way to monitor brain reactions, College of Engineering, Iowa State University, 2021, $ 16,993
6. Lotfi ben Othmane (PI), Detection of cyber-attack on cars–proof of concept, Regents Innovation Fund, Iowa State University, 2020, $ 10 K
7. Lotfi ben Othmane (PI), Controlled data dissemination in suspicious environments, Air Force Research Lab, Summer Faculty Visit, 2020, $11,700
8. Lotfi ben Othmane (PI), Towards secure code changes, John Deere, 2017-2018, $ 38K
9. Lotfi ben Othmane (PI) and Manimaran Govindarasu, Towards resiliency of connected vehicles against cyber-attacks, Pacific Northwest National Laboratory, USA, 2017-2018, $ 38K
10. Eric Bodden and Lotfi ben Othmane (CO-PI) Security process analytics, Fraunhofer SIT, funded by SAP, Germany, 2014-2016, $ 150K
11. Lotfi ben Othmane (PI), Dissertation completion fellowship, The Graduate College, WMU, USA, 2009

Collaboration on grant proposals

1. Engineering Security and Performance Aware Vehicular Applications for Safer and Smarter Roads, Funded by Qatar Foundation, collaborated with Prof. Bharat Bhargava, Purdue University, 2015-2017, total amount $ 1 M
2. Monitoring-Based System for E2E Security Auditing and Enforcement in Trusted and Untrusted SOA, collaborated with Prof. Bharat Bhargava, funded by Northrup Grumman, USA, 2014-2015, $ 150K
3. End-to-End Security Policy Auditing and Enforcement in Service Oriented Architecture, collaborated with Prof. Bharat Bhargava, funded by Northrup Grumman, USA, 2013-2014, $ 150K

Taught Courses

University of North Texas, USA (2022-Present)
CSCE 5565, Secure Software Systems (22, 23, 24, 25)
CSCE 5214 - Software Engineering for Artificial Intelligence (22, 23, 24, 25)
CSCE 3440, Software Engineering (25)
CSCE 5430, Software Engineering (24)
CSCE 3550 Foundations of Cybersecurity (24, 25)
Iowa State University, USA (2017-2021)
CPRE 562X, Secure Software Engineering (20, 21)
SE 339 - Software Architecture and Design (2017, 2018, 2019, 2020, 2021)
SE 329 - Software Project Management (2017, 2018, 2019, 2020, 2021)
SE 491 - Senior Design I (2020, 2021)
SE 185 - Problem Solving in Software Engineering – Language C (S'17, F'17)
Technical University Darmstadt, Germany (2014-2016)
20-00-0936-vl–Secure Software Development (W'15)
20-00-0777-se–Secure Software Development (W'14)
20-00-0760-se–Tool-based approaches to Software Security (SS'14)
Kalamazoo College, USA (2010-2011)
COMP 486–Software Engineering(W'11)
CS 107–Pictures and Sounds: Programming with Multimedia-Lab (W'11)
COMP 110–Introduction to Programming in Java (F'10, W'11)
COMP 105–Introduction to Computer Science Using the Web - Lab (F'10)
Western Michigan University, USA (2008-2010)
CS2100–Script Programming with Python (S'09, S'10)
CS2100–.Net Framework (F'08)
CS1000–Fluency with Information Technology - Lab (SS'08)
CS1022–Introduction to Math Software - Lab (S'08)
CS5950–Computer Security and Information Assurance - Lab (S'08, F'08)

Publications

Patents

1. L. Ben Othmane and N. J. Schmidt, "System and method for controlling physical systems using brain waves," U.S. Patent 12 303 296, May 20, 2025.

Books

1. L. ben Othmane, M. G. Jaatun, and E. Weippl, Eds., *Empirical Research for Software Security: Foundations and Experience*. Taylor & Francis Group, LLC, 2017.

Journal articles

1. L. Ben Othmane, L. Dhulipala, N. Multari, and M. Govindarasu, On the performance of detecting injection of fabricated messages into the CAN bus, *IEEE Transactions on Dependable and Secure Computing*, **19**, (1), 468–481, Jan. 2022.
2. M. Jedh, L. Ben Othmane, N. Ahmed, and B. Bhargava, Detection of message injection attacks onto the CAN bus using similarities of successive messages-sequence graphs, *IEEE Transactions on Information Forensics and Security*, **16**, 4133–4146, Jul. 2021.
3. R. Ranchal, B. Bhargava, P. Angin, and L. ben Othmane, Epics: A framework for enforcing security policies in composite web services, *IEEE Transactions on Services Computing, Special Issue on Recent Advances in Web Services Research*, **12**, (3), May 2019.
4. L. ben Othmane, G. Chehrazi, E. Bodden, P. Tsalovski, and A. D. Brucker, Time for addressing software security issues: prediction models and impacting factors, *Data Science and Engineering*, **2**, (2), 107–124, Jun. 2017.

5. N. Al-hadhrami, B. Aziz, and L. ben Othmane, An incremental B-model for RBAC-controlled electronic marking system, *International Journal of Secure Software Engineering (IJSSE)*, **7**, (2), 37–64, May 2016.
6. H. Oueslati, M. M. Rahman, L. ben Othmane, and I. G. A. Arbain, Evaluation of the challenges of developing secure software using the agile approach, *International Journal of Secure Software Engineering (IJSSE)*, **7**, (1), Jan. 2016.
7. L. ben Othmane, R. Ranchal, R. Fernando, B. Bhargava, and E. Bodden, Incorporating attacker capabilities in risk estimation and mitigation, *Computers & Security*, **51**, 41–61, Jun. 2015, Elsevier.
8. J. Son, V. Bhuse, L. ben Othmane, and L. Lilien, Incorporating lab experience into computer security courses: Three case studies, *Global Journal of Enterprise Information System (GJEIS)*, **7**, (2), 2015.
9. L. ben Othmane, P. Angin, H. Weffers, and B. Bhargava, Extending the agile development approach to develop acceptably secure software, *IEEE Transactions on Dependable and Secure Computing*, **11**, (6), 497–509, Nov. 2014.
10. L. ben Othmane, R. Fernando, R. Ranchal, B. Bhargava, and E. Bodden, Likelihood of threats to connected vehicles, *International Journal of Next-generation Computing (IJNGC)*, **5**, (3), 290–303, Nov. 2014.
11. L. Lilien, L. ben Othmane, P. Angin, A. DeCarlo, R. Salih, and B. Bhargava, A simulation study of ad hoc networking of UAVs with opportunistic resource utilization networks, *Journal of Network and Computer Applications, special Issue Advanced Technologies for Homeland Defense and Security*, **38**, 3–15. Feb. 2014, Elsevier.
12. L. ben Othmane, H. Weffers, P. Angin, and B. Bhargava, A time-evolution model for the privacy degree of information disseminated in online social networks, *International Journal of Communication Networks and Distributed Systems*, **11**, (4), 412–430, 2013, Inderscience Publishers.

Conference proceedings

1. Y. Konapalli, L. Ben Othmane, C. Tunc, F. Benchellal, and L. Mudagere, Reverse engineering and control-aware security analysis of the ardupilot uav framework, in *Proc. 8th International Workshop on Software Engineering Research and Practices for the IoT (SERP4IoT)*, accepted, Rio DeJeneiro, Brazil, 2026.
2. K. Cheerla, L. Ben Othmane, and K. Morozov, Comparison of fully homomorphic encryption and garbled circuit techniques in privacy-preserving machine learning inference, in *Proc. IEEE Secure Development Conference*, Indianapolis, IN, 2025.
3. N. Pecka, L. Ben Othmane, and R. Bryce, Toward automated identification of potential threats to large software using association of threats to call graph cluster types, in *Proc. the 20th International Conference on Risks and Security of Internet and Systems (CRISIS 2025)*, Gatineau, Canada, 2025.
4. P. Calyam et al., Towards a domain-agnostic knowledge graph-as-a-service infrastructure for active cyber defense with intelligent agents, in *Proc. of the 52th Annual Applied Imagery Pattern Recognition workshop*, St. Louis, MO, 2023, pp.1–8.
5. M. B. Jedh, L. ben Othmane, and A. K. Somani, Improvement and evaluation of resilience of adaptive cruise control against spoofing attacks using intrusion detection system, in *Proc. the 18th International Conference on Risks and Security of Internet and Systems (CRISIS 2023)*, Rabat, Marocco, Dec. 2023.
6. L. ben Othmane and A.-M. Jamil, Self-confidence of undergraduate students in designing software architecture, in *Proc. The Annual Conference The American Society for Engineering Education*, Paper ID: 38158, Minneapolis, MN, Jun. 2022.
7. M. B. Jedh, J. Lee, and L. ben Othmane, Evaluation of the architecture alternatives for real-time intrusion detection systems for connected vehicles, in *Proc. the IEEE International Conference on Software Quality, Reliability, and Security*, Guangzhou, China, Dec. 2022.

8. N. Pecka, L. ben Othmane, and A. Valani, Privilege escalation attack scenarios on the devops pipeline within a kubernetes environment, in *Proc. the International Conference on Software and Systems Processes*, Pittsburgh, PA, May 2022, pp.45–49.
9. L. ben Othmane and N. Ahmed, Using garbled circuit for secure brokering, in *Proc. the 16th International Conference on Risks and Security of Internet and Systems (CRISIS 2021)*, Ames, USA, Nov. 2021, pp.108–117.
10. A.-M. Jamil, S. Khan, J. K. Lee, and L. ben Othmane, Towards automated threat modeling of cyber-physical systems, in *The 7th International Conference on Software Engineering and Computer Systems (ICSECS)*, Pekan, Malaysia, Aug. 2021, pp.614–619.
11. A.-M. Jamil, L. ben Othmane, and A. Valani, Threat modeling of cyber-physical systems in practice, in *Proc. the 16th International Conference on Risks and Security of Internet and Systems (CRISIS 2021)*, Ames, USA, Nov. 2021, pp.3–19.
12. A. Jamil, L. Ben Othmane, A. Valani, M. Abdelkhalek, and A. Tek, The current practices of changing secure software: An empirical study, in *Proc. the 35th Annual ACM Symposium on Applied Computing (SAC '20)*, Brno, Czech Republic, 2020, pp.1566–1575.
13. M. Abdelkhalek, L. Ben Othmane, and A. Jamil, Identification of the impacts of code changes on the security of software, in *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, Milwaukee, WI, USA, 2019, pp.569–574.
14. L. Ben Othmane and M. Lamm, Mindset for software architecture students, in *Proc. IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, vol. 2, Milwaukee, WI, USA, 2019, pp.306–311.
15. V. Mohan, L. ben Othmane, and A. Kres, BP: Security concerns and best practices for the automation of software deployment processes - an industrial case study, in *Proc. IEEE Cybersecurity Development Conference (SecDev)*, Cambridge, MA, Sep. 2018.
16. L. ben Othmane, V. Alvarez, K. Berner, M. Fuhrmann, W. Fuhrmann, A. Guss, and T. Hartsock, Demo: A low-cost fleet monitoring system, in *The Fourth IEEE Annual International Smart Cities Conference*, Kansas City, MO, Sep. 2018.
17. S. Sardesai, D. Ulybyshev, L. ben Othmane, and B. Bhargava, Impacts of security attacks on the effectiveness of collaborative adaptive cruise control mechanism, in *The Fourth IEEE Annual International Smart Cities Conference*, Kansas City, MO, Sep. 2018.
18. D. Ulybyshev, A. Oqab-Alsalem, B. Bhargava, S. Savvides, G. Mani, and L. ben Othmane, Secure data communication in autonomous v2x systems, in *IEEE 2018 International Congress on Internet of Things*, San Francisco, CA, Jul. 2018.
19. B. Pfretzschner and L. ben Othmane, Identification of dependency-based attacks on node.js, in *Proc. of the 12th International Conference on Availability, Reliability and Security (ARES)*, Reggio Calabria, Italy, Sep. 2017.
20. A. Ali and L. ben Othmane, Towards effective security assurance for incremental software development - the case of zen cart application, in *Proc. of the 11th International Conference on Availability, Reliability and Security (ARES)*, Salzburg, Austria, Sep. 2016, pp.564–571.
21. R. Fernando, R. Ranchal, B. An, L. ben Othmane, and B. Bhargava, Consumer oriented privacy preserving access control for electronic health records in the cloud, in *IEEE cloud*, in press (acceptance rate 16,7%), San Francisco, USA, Jun. 2016.
22. V. Mohan and L. B. Othmane, SecDevOps: Is it a marketing buzzword? mapping research on security in devops, in *Proc. of the 11th International Conference on Availability, Reliability and Security (ARES)*, Salzburg, Austria, Sep. 2016, pp.542–547.
23. B. Pfretzschner and L. ben Othmane, Dependency-based attacks on node.js, in *2016 IEEE Cybersecurity Development (SecDev)*, Boston, MA, USA, Nov. 2016, pp.66.
24. L. ben Othmane, T. Cerqueus, A. Thiery, M. Salehie, N. Noel, A. Labaere, R. Domingues, A. Cordier, A. Ventresque, L. Pasquale, P. Perry, and B. Nuseibeh, Response to emergency situations in a traffic management system, in *Proc. of The 2nd World Congress on Computer Applications and Information Systems (WCCAIS'2015)*, Hammamet, Tunisia, Jan. 2015.

25. L. ben Othmane, G. Chehrazi, E. Bodden, P. Tsalovski, A. Brucker, and P. Miseldine, Factors impacting the effort required to fix security vulnerabilities, in *Proc. Information Security Conference (ISC 2015)*, Trondheim, Norway, Sep. 2015, pp.102–119.
26. N. Al-Hadhrami, B. Aziz, S. Sardesai, and L. ben Othmane, Incremental development of RBAC-controlled E-marking system using the b method, in *Proc. of the 10th International Conference on Availability, Reliability and Security (ARES)*, Toulouse, France, Aug. 2015, pp.532–539.
27. H. Oueslati, M. M. Rahman, and L. ben Othmane, Literature review of the challenges of developing secure software using the agile approach, in *Proc. of the 10th International Conference on Availability, Reliability and Security (ARES)*, Toulouse, France, Aug. 2015, pp.540–547.
28. K. Renaud, M. Volkamer, S. Flowerday, and L. ben Othmane, 'I Am Because We Are' developing and nurturing african digital security culture, in *Proc. African Cyber Citizenship Conference 2015 (ACCC 2015)*, Port Elizabeth, South Africa, Nov. 2015.
29. L. T. Lilien, L. ben Othmane, P. Angin, B. Bhargava, R. M. Salih, and A. DeCarlo, Impact of initial target position on performance of uav surveillance using opportunistic resource utilization networks, in *Proc. 33rd IEEE International Symposium on Reliable Distributed Systems Workshops (SRDSW)*, Montreal, Canada, Sep. 2015.
30. L. ben Othmane, P. Angin, and B. Bhargava, Using assurance cases to develop iteratively security features using scrum, in *Proc. of the 9th International Conference on Availability, Reliability and Security (ARES)*, Fribourg, Switzerland, Sep. 2014, pp.490–497.
31. L. ben Othmane, V. Bhuse, and L. Lilien, Incorporating labs into computer security courses, in *Proc. 2013 World Congress on Computer and Information Technology (WCCIT)*, Sousse, Tunisia, Jun. 2013, pp.1–4.
32. L. ben Othmane, H. Weffers, and M. Klabbers, Using attacker capabilities and motivations in estimating security risk, in *Workshop on Risk Perception in IT Security and Privacy*, URL: http://cups.cs.cmu.edu/soups/2013/risk/Cap.-Based-risk.pdf, Newcastle, UK., Jul. 2013.
33. L. ben Othmane, H. Weffers, R. Ranchal, P. Angin, B. Bhargava, and M. M. Mohamad, A case for societal digital security culture, in *Proc. 28th IFIP International Information Security and Privacy Conference (SEC 2013)*, Auckland, New Zealand, Jul. 2013, pp.391–404.
34. L. ben-Othmane, A. Al-Fuqaha, E. ben Hamida, and M. van den Brand, Towards extended safety in connected vehicles, in *Proc. 16th International IEEE Conference on Intelligent Transportation Systems (ITSC)*, The Hague, The Netherlands., Oct. 2013, pp.652–657.
35. B. Bhargava, R. Ranchal, and L. ben Othmane, Secure information sharing in supply chain collaboration, in *Proc. 3rd IEEE International Advance Computing Conference (IACC-2013)*, Ghaziabad, India, Feb. 2013, pp.1636–1640.
36. L. Lilien, M. Elbes, L. ben Othmane, and R. Salih, Simulation of emergency response operations for a static chemical spill within a building using an opportunistic resource utilization network, in *Proc. Of The 13th annual IEEE Conference on Technologies for Homeland Security (HST 13)*, Waltham, USA, Nov. 2013, pp.408–413.
37. M. Azarmi, B. Bhargava, P. Angin, R. Ranchal, N. Ahmed, A. Sinclair, M. Linderman, and L. ben Othmane, An end-to-end security auditing approach for service oriented architectures, in *Proc. 31st IEEE International Symposium on Reliable Distributed Systems (SRDS 2012)*, Irvine, CA, Oct. 2012, pp.279–284.
38. R. M. Salih, L. Lilien, and L. ben Othmane, Protecting patients electronic health records using enhanced active bundles, in *Proc. 6th International Conference on Pervasive Computing Technologies for Healthcare, Doctoral Consortium*, San Diego, CA, May 2012, pp.1–4.
39. R. Salih, L. ben Othmane, and L. Lilien, Privacy protection in pervasive healthcare monitoring systems with active bundles, in *Proc. Ninth IEEE International Symposium on Parallel and Distributed Processing with Applications Workshops (ISPAW 2011)*, Busan, Korea, May 2011, pp.311–315.
40. P. Angin, B. Bhargava, R. Ranchal, N. Singh, M. Linderman, L. ben Othmane, and L. Lilien, An entity-centric approach for privacy and identity management in cloud computing, in *Proc. 29th*

International Symposium on Reliable Distributed Systems (SRDS 2010), New Delhi, India, Nov. 2010, pp.177–183.

41. L. Lilien, A. Al-Alawneh, and L. ben Othmane, The pervasive trust foundation for security in next generation networks (a position paper), in *Proc. The New Security Paradigms Workshop (NSPW 2010)*, Concord, Massachusetts, Sep. 2010, pp.129–142.
42. R. Ranchal, B. Bhargava, L. ben Othmane, L. Lilien, A. Kim, M. Kang, and M. Linderman, Protection of identity information in cloud computing without trusted third party, in *Proc. 29th International Symposium on Reliable Distributed Systems (SRDS 2010)*, New Delhi, India, Nov. 2010, pp.368–372.
43. L. ben Othmane and L. Lilien, Protecting privacy of sensitive data dissemination using active bundles, in *World Congress on Privacy, Security, Trust and the Management of e-Business (CONGRESS '09)*, Aug. 2009, pp.202–213.
44. L. ben Othmane and L. Lilien, Protecting sensitive data throughout its life cycle, in *Graduate Students Symposium, Annual Conference on Privacy Security and Trust*, Fredericton, Canada, Oct. 2008.

Book chapters

1. D. S. Cruzes and L. ben Othmane, "Empirical research for software security: foundations and experience," in, L. ben Othmane, M. G. Jaatun, and E. Weippl, Eds. Taylor & Francis Group, LLC, 2017, ch. Threats to Validity in Software Security Empirical Research, pp. 275–300.
2. L. ben Othmane, A. D. Brucker, S. Dashevskyi, and P. Tsalovski, "Empirical research for software security: foundations and experience," in, L. ben Othmane, M. G. Jaatun, and E. Weippl, Eds. Taylor & Francis Group, LLC, 2017, ch. Data Analytics for Software Security: Foundations and Experience, pp. 69–94.
3. L. ben Othmane, H. Weffers, M. M. Mohamad, and M. Wolf, "Wireless sensor networks (WSN) for vehicular and space applications: Architecture and implementation," in, D. BenHaddou and A. Al-Fuqaha, Eds. Norwell, MA: Springer, 2015, ch. A Survey of Security and Privacy in Connected Vehicles, pp. 217–247.

PhD thesis

1. L. ben Othmane, "Active bundles for protecting confidentiality of sensitive data throughout their lifecycle," Ph.D. dissertation, Western Michigan University, Kalamazoo, MI, USA, Dec. 2010.

Tutorials

1. Threat Modeling of Cloud-based Solutions, IEEE Secure Development Conference, Atlanta, USA, 2022

Invited talks and keynotes

1. Transitioning Academic Research to the Market, Missouri University of Science and Technology, Rolla, MO, Nov. 2023
2. Improvement and Evaluation of Resilience of Adaptive Cruise Control Against Spoofing Attacks Using Intrusion Detection System, Symposium on the Science of Security (HotSoS), Presented by Ph.D. student Mubarek Jedh, Online, Apr. 2023
3. On Continuous Threat Modeling of Cyber-physical Systems, SecDevOps days, Washington DC, USA, 2021
4. Threat Modeling in Practice, The 7th International Workshop on Secure Software Engineering (SSE 2021), Digital, 2021 (keynote)
5. On the Security of Connected Vehicles , The 6th International Conference on Software Security and Assurance (ICSSA 2020), Altoona, PA, 2020 (keynote)

6. On the Security of Connected Vehicles , The 14th International Conference on Risks and Security of Internet and Systems, Hammamet, Tunisia, 2019 (Keynote)
7. Security Concerns and Best Practices for SecDevOps, DevSecOpsDays, Istanbul, Turkey, 2019
8. Secure Code Changes, 2018 Annual Computer Security Applications Conference, San Juan, Puerto Rico, USA, 2018.
9. Security Concerns and Best Practices for SecDevOps, 12th Central Area Networking and Security Workshop, Manhattan, USA, 2018.
10. What Will It Take to Develop Secure Software? Midwest Security Workshop, Urbana, April 14, 2018
11. Teaching Software Architecture Process to Undergraduate Students: A Case Study, International Workshop on Engineering IoT systems: Architectures, Services,
12. On the Limit of Security Protection Mechanisms, Iowa State University Research Day, USA, 2018.
13. What Roles Can Empirical Research Play to Advance Software Security Knowledge? Purdue University, USA, 2018.
14. Identification of Dependency-based Attacks on Node.js, 11th Central Area Networking and Security Workshop, Rolla, MO, USA, 2017.
15. What Roles Can Empirical Research Play to Advance Software Security Knowledge? University of Oslo, Norway, 2017.
16. What Will It Take to Develop Secure Software? SINTEF, Norway, Dec. 2016.
17. What Will It Take to Develop Secure Software? Ivoire Cybersecurity conference, Nov. 2016.
18. Likelihood of Threats to Connected Vehicles, Robert Bosch GmbH, Renningen, Germany, 2016.
19. Time for Addressing Software Security Issues: Prediction Models and Impacting Factors, OWASP AppSec Europe, Rome, Italy 2016.
20. Security Code Analysis of Truecrypt, Workshop "Softwarequalitat Sichtbar Machen," Leipzig, Germany, 2016
21. Empirical Research Methods for Secure Software Engineering, International Cyber Security Workshop and Certificate Program, Istanbul, Turkey, 2016.
22. Empirical Research Methods for Secure Software Development, Ninth International Crisis Management Workshop (CriM'15) and Oulu Winter School, Oulu, Finland, 2015.
23. Estimating Vulnerabilities Fixing Time, Cast Workshop hot topic "Big Data Security," Darmstadt, Germany, 2015.
24. Estimating Effort to fix Vulnerabilities at SAP, Workshop Recent Advances in Secure Software Engineering, Alghero, Italy, 2015.
25. An Example of the Science for Secure Software Development - Attacker-Capability-Based Risk Estimation, SINTEF, Trondheim, Norway, 2015.
26. Incorporating Attacker Capabilities in Risk Estimation and Mitigation, Purdue University, West Lafayette, IN, USA, 2014.
27. Three Examples of Cyber-physical Systems, Summer School on Cyber-Physical Systems, Grenoble, France, 2014.
28. Extending the Agile Development Life-cycle to Develop Secure Software, Fraunhofer Secure Information Technology, Darmstadt, Germany, 2013.
29. Extending the Agile Development Life-cycle to Develop Secure Software, Lero-The Irish Software Research Center, Limerick, Ireland, 2013.

30. Digital Security Culture for Organizations and the Society, Workshop Information Technology Security for Public Institutions, Hannover, Germany, 2013.
31. Towards Self-protecting Data, Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg, 2012.
32. Protecting Privacy in Sensitive Data Dissemination with Active Bundles, Purdue University, West Lafayette, IN, USA, 2010.

Panel Member

1. Entrepreneurial Insights, University of North Texas, CSE seminar, 2024
2. Integrate Threat Modeling into your DevOps Pipeline, Security Compass, Linkedin event, 2022.
3. Evolving Threat Modeling for Agility and Business Value with DevSecOps, SecDevOps days, Washington DC, 2021
4. Hackathon on Effective Threat Modeling, Microsoft, Online, 2021.
5. Maintain Software Security During Code Changes, Security Compass, Online, 2020.
6. Software Drives – Automotive Development 2030, Kugler Maag CIE, Germany, 2014.

Open-Source from Senior Design Projects

1. Security Assurance Case Design Tool, 2017. (Available in Github)
2. DevOps for Javascript-based Microservices, 2017-2018. (Available in Github)
3. Fleet Monitoring System, 2017-2018. (Available in Github)

Research Students

1. **Graduated PhD students**
   (a) Mubarek Jedh (Ph.D.), Attacks detection and cyber resilience: securing in-vehicle controller area network, Iowa State University, 2023.
   (b) Ameerah-Muhsinah Jamil (PhD), On engineering secure software for cyber-physical systems in practice, Iowa State University, 2021
2. **Graduated Master students**
   (a) Kalyan Cheerla, Comparison of Fully Homomorphic Encryption and Garbled Circuits Approaches in Privacy-Preserving Machine Learning, University of North Texas, 2025
   (b) Rishita Pappala (MSc), Using machine learning biofeedback-based approach for faster knee rehabilitation via surface electromyography, University of North Texas, 2024
   (c) Jian Lee (MSc), Evaluation of the architecture alternatives for real-time intrusion detection systems for connected vehicles, Iowa State University, 2022
   (d) Danny Yip (MSc), Empirical study on exploitation of dependency-based attacks in Node.js, Iowa State University, 2022
   (e) Nick Pecka (MSc), Attack scenarios on the DevOps pipeline within a Kubernetes environment, Iowa State University, 2022
   (f) Mubarek Jedh (Msc), Using messages precedence similarity to detect message injection in in-vehicle network, Iowa State University, 2020.
   (g) Nick Schmidt (Msc), Control of physical objects utilizing brain computer interfaces, Iowa State University, 2020.
   (h) Shifa Khan (MSc), Automated threat modeling for autonomous vehicle software - Apollo Auto, Iowa State University, 2019.
   (i) Sudharrshan Veeraraghavaramannijanaar (Msc), Security analysis of vehicle to vehicle Arada Locomate on board unit, Iowa State University, 2018.

(j) Srilalithadaksh Dhulipala (Msc), Detection of injection attacks on in-vehicle network using data analytics, Iowa State University, 2018.

(k) Prachi-Rajesh Patel (Msc), Existence of dependency-based attacks in Node.JS environment, Iowa State University, 2018.

(l) Brian Pfretzschner (Msc), Detection of dependency-based attacks on NodeJS environment, TU Darmstadt, 2016 (in collaboration with IBM Germany)

(m) Daniel Magin (Msc), Side-channel analysis of ABAP, TU Darmstadt, 2016 (in collaboration with HP Germany)

(n) Azmat Ali (Msc), Automated threat extraction from recovered architecture - the case of universAAL-based lighting example, TU Darmstadt, 2016

(o) Vaishnavi Mohan (Msc), Transformation of a waterfall-oriented manual code deployment process to secure DevOps, TU Darmstadt, 2016 (in collaboration with IBM Germany)

(p) Martin Mory (Msc), Evaluating the precision of malware in detecting analysis environments, TU Darmstadt, 2016 (in collaboration with HP Germany)

(q) Shantanu Sardesai (Msc), Impacts of security attacks on the effectiveness of collaborative adaptive cruise control system, TU Darmstadt, 2015

Ph.D. examination : Abdullah Ayed Algarni (QUT, Australia, 2016).

Awards and Honors

2024 Mentor, Second place Capture-the-Flag (CTF) Competition at the 17th Central Area Networking and Security Workshop (CANSec 2024) for Students Kalyan Cheerla and Naveen Karasu

2022 Mentor, First place Capture-the-Flag (CTF) Competition at the 15th Central Area Networking and Security Workshop (CANSec 2022) for Students Mubarek Jedh, Danny Yip, and Jian Lee

2011 All-University Graduate Research and Creative Scholar Award, The Graduate College, Western Michigan University (WMU)

2010 Department Teaching Effectiveness Award, Department of Computer Science, WMU

2010 Department Graduate Research and Creative Scholar Award, Department of Computer Science, WMU

2010 Doctoral Excellence in Research Award, Department of Computer Science, WMU

2009 Department Teaching Effectiveness Award, The Graduate College, WMU

2009 Department Graduate Research and Creative Scholar Award, The Graduate College, WMU

2009 Outstanding Service Award, Department of Computer Science, WMU

2008 Best Student Paper Award, Graduate Student Symposium, Sixth Annual Conference on Privacy, Security and Trust (PST2008), Fredericton, New Brunswick, Canada

Professional Activities

Education program development and assessment

1. Co-created Graduate Certificate on Cyber Artificial Intelligence, University of North Texas, 2025.
2. External Assessor for the MS in Cyber Security Analytics program, University of Exeter, UK. 2020.
3. Contributor to the online MS in Cybersecurity, University Wisconsin System, Extended Campus, USA, 2019.

Grant review

1. National Defense Science and Engineering Graduate Fellowship Program, Department of Defense, 2025
2. MITACs, Canada, 2023.

3. Department of Homeland Security (DHS), 2023.
4. National Science Foundations **NSF**, 2018, 2022(2), 2025(2).

Project review and mentoring

1. Industry mentor for NSF I-Corp, project DisMEIRP, 2024.
2. Advisory Board member for the EU project RASEN, 2015.

Department and university services

1. **University of North Texas (2022-Present)**
   (a) Group III representative on the Faculty Senate (2023-present)
   (b) Chair, Personnel Affairs Committee (PAC) (2023-2024/2025-2026)
   (c) Co-Chair, Outreach Committee (2025-2026)
   (d) Member, Professional Faculty Promotion Committee (2025-2026)
   (e) Committee on Faculty Participation in Governance (2025)
   (f) Faculty Development Leave Committee (2025)
   (g) Member, Personnel Affairs Committee (PAC) (2024-2025)
   (h) Chair, AdHoc committee on Professional Faculty Research (2024-Present)
   (i) Chair, AdHoc committee on Professional Faculty Promotion Policy (PAC) (2024-2025)
   (j) Member, Scholarship Committee of the Faculty Senate (2024-2025)
   (k) Member, Teaching Effectiveness Committee of the Faculty Senate (2023-2025)
   (l) Chair of the external awards committee (2023-2025)
   (m) Co-director of the MS degree in Cyber-security (2023)
   (n) Chair, Personnel Affairs Committee (PAC) (2023)
   (o) member, Search Committee (2023, 2025)
   (p) Academic Integrity Ad Hoc Committee (2022-2023)
2. **Iowa State University (2017-2021)**
   (a) Committee member for the Zaffarano Prize for Graduate Student Research(2021)
   (b) Member of the ISU Big Data Brain initiative (2019-2021)
   (c) Faculty of the Software Engineering Program (2017-2021)
   (d) Member of the Information Assurance Center (2017-2021)
   (e) Member of the Infrastructure Planning and Development Committee (2017-2021)
   (f) Senior Design Committee (2019)
   (g) Member of the Software Engineering Strategic Planning Committee (2018-2019)
   (h) Member of the Software Engineering Petition Committee (2017/2020)
3. **External services**
   (a) Faculty Promotion review, Purdue University (2025).

Journals editing

1. Special issue of Journal of Information Security and Applications, Elsevier, 2020, guest editor.
2. Special issue of the EURASIP Journal on Information Security, Springer, 2019, guest editor.
3. Special issue the journal Computers & Security, Elsevier, 2019, guest editor.
4. Special issue of the International Journal of Secure Software Engineering (IJSSE), IGI-group, Jan./Feb. 2016, Guest Co-editor.
5. The Hilltop Review–A Journal of Western Michigan University Graduate Research, published by the Graduate Student Advisory Committee (GSAC), WMU, 2009-2010, Editor-in-chief

Event organization

1. The 16th International Conference on Risks and Security of Internet and Systems (CRISIS), Ames, IA, 2021.
2. The 13th Central Area Networking and Security Workshop (CANSec), Iowa State University, Ames, IA, 2019.

Conference steering committee

1. The 16th International Conference on Risks and Security of Internet and Systems, Ames, IA, 2021.
2. The 13th Central Area Networking and Security Workshop (CANSec), Iowa State University, Ames, IA, 2019, Co-organizer.

Event chair

1. International Workshop on Secure Software Engineering (SSE), 2015 to 2022, Co-chair.
2. Central Area Networking and Security Workshop (CANSec), Ames, IA, 2019, Co-chair
3. Workshop on Empirical Research Methods in Information Security, Montreal, Canada, 2016, Co-chair.
4. Summer School on Cyber-Physical Systems, Grenoble, France, 2014, chair of a session.
5. World Congress on Computer and Information Technology (WCCIT), Sousse, Tunisia, 2013, chair of a session.
6. Workshop Information Technology Security for Public Institutions, Eindhoven, Netherlands, 2013, chair of a session.

Conference/Workshop Program Committee Member (Partial list)

CAI(2026), HotSoS(2026), IEEE COMPSAC (2025,2024,2023, 2021, 2020, 2019), SERP4IoT/ICSE (2025, 2024, 2023, 2022, 2021), CRISIS (2025, 2024, 2023, 2022, 2021), IEEE ITS (2023), AAAI symp. (2022), ASEE Annual Conf. (2022, 2021), FIE (2025,2024,2023), IEEE SecDev (2022, 2021, 2020, 2018), ISC2 (2022, 2021, 2019, 2018), ICSSA (2021, 2020, 2019, 2018), IEEE VTC (2020, 2018), Wireless Days (2019), IMCET(2018), IEEE CIT (2017), IEEE SRDS (2015, 2011), MCS (2015), CSE (2014), ADCONS (2013), CASoN (2013, 2012, 2011), ICCIT (2013), DVCOMP (2011), MESH (2011), SAHNS (2011), PST (2011).

Reviewer of journals (Partial list)

1. IEEE Transactions on Intelligent Transportation Systems, 2023, 2026
2. Internet of Things, Elsevier, 2025
3. Journal of Grid Computing, Springer, 2025
4. Engineering Applications of Artificial Intelligence, Elsevier, 2025
5. Journal of Open Innovation: Technology, Market, and Complexity, Elsevier, 2025
6. Physical Communication, Elsevier, 2024
7. International Journal of Critical Infrastructure Protection, Elsevier, 2024
8. Computers in Human Behavior Reports, Elsevier, 2024
9. IEEE Transactions on Services Computing, IEEE 2015, 2024
10. IEEE Internet of Things Journal, 2018, 2019, 2020, 2024
11. Security and Privacy, Wiley, 2023
12. Public Library of Science (PLOS) ONE, 2023
13. IEEE Transactions on Information Forensics & Security, 2011, 2022

14. IEEE Transactions on Network and Service Management, 2017, 2020
15. IEEE Transactions on Dependable and Secure Computing, 2016, 2017, 2019
16. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2017
17. IEEE Software, 2017
18. IEEE Systems Journal, IEEE, 2014
19. Empirical Software Engineering, Springer, 2021
20. Mobile Networks and Applications, Springer, 2013
21. Telecommunication Systems, Springer, 2013
22. Transactions on Computational Science, Springer, 2010
23. Information Systems Frontiers (ISF), Springer, 2010
24. Computers & Security, Elsevier, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021
25. Arabian Journal for Science and Engineering (AJSE), Elsevier, 2018, 2019, 2020
26. Computational and Structural Biotechnology Journal, Elsevier, 2018, 2019
27. Computer Communications, Elsevier, 2018
28. Computers & Electrical Engineering, Elsevier, 2014
29. Ad Hoc Networks, Elsevier, 2014
30. Journal of Network and Computer Applications, Elsevier, 2012, 2013, 2014
31. Journal of Systems and Software, Elsevier, 2010
32. Information Sciences, Elsevier, 2010, 2011, 2012
33. Security and Communication Networks (SCN), John Wiley, 2010, 2011, 2012, 2013, 2014
34. Software: Practice and Experience, Wiley, 2015
35. Journal of Computer Security, IOS Press, 2015
36. IBM Journal of Research and Development, 2015
37. SAE International Journal of Passenger Cars: Electronic and Electrical Systems, 2019