Steven Ullman

|  |  |
| --- | --- |
| steven.ullman@utsa.edustevenullman.github.io | Department of Information Systems and Cyber SecurityAlvarez College of Business, University of Texas at San AntonioOne UTSA Circle, San Antonio, TX 78249 |

# Academic Employment

|  |  |  |
| --- | --- | --- |
| 2024 – Present | Assistant Professor, Information Systems and Cyber Security | University of Texas at San Antonio |
| 2018 – 2024 | Research Associate, Artificial Intelligence (AI) Lab | University of Arizona |

# Education

|  |  |  |
| --- | --- | --- |
| Ph.D. | Management Information Systems (MIS) | 2024 |
|  | University of Arizona |
|  |  |
| MS | Management Information Systems (MIS) | 2019 |
|  | University of Arizona |
|  |  |
| MBA | Master of Business Administration | 2018 |
|  | Colorado State University-Pueblo |
|  |  |
| BS | Computer Information Systems | 2018 |
|  | Colorado State University-Pueblo |

# Research Interests

**Domain:** Cybersecurity, Vulnerability Assessment and Management, Enterprise Information Technology (IT) Security, Open-Source Software Security, Internet of Things (IoT) Security.

**Methods:** Deep Learning (Self-Supervised Learning, Multi-View Representation Learning, Contrastive Representation Learning), Machine Learning, Network Science (Graph Representation Learning, Graph Neural Networks), Design Science.

# Dissertation

**Title:** *“Artificial Intelligence-enabled Vulnerability Analysis and Management Enterprise IT Infrastructure: A Computational Design Science Approach”*

**Committee Members:** Dr. Hsinchun Chen (Chair), Dr. Jay F. Nunamaker Jr. (Member), Dr. Sue Brown (Member)

# Publications

**Journal Publications**

1. **S. Ullman**, S. Samtani, H. Zhu, B. Lazarine, H. Chen, and J.F. Nunamaker, Jr. (2024) “Enhancing Vulnerability Prioritization in Cloud Computing Using Multi-View Representation Learning” *Journal of Management Information Systems (JMIS), 41*(3), 708–743*.*
2. B. Ampel, **S. Ullman**. (2023) “Why Following Friends Can Hurt You: A Replication Study,” *AIS Transactions on Replication Research (TRR)*, 9(1):1–15.

*Journal Papers Under Review*

1. **S. Ullman**, H. Zhu, S. Samtani, and H. Chen “Linking Vulnerabilities in Cyberinfrastructure With Their Remediations: A Contrastive Representation Learning Approach” ***Under Review (Second Round) at Information Systems Research (ISR).***
2. A. Ndubizu, **S. Ullman**, S. Samtani, H. Zhu, and H. Chen “Generating Security Nutrition Labels for Internet of Things Device GitHub Repositories: A Multi-Label Classification Approach” ***Under Review (First Round) MIS Quarterly (MISQ).***

*Work-In-Progress Journal Papers*

1. C. Yang, **S. Ullman**, S. Samtani, H. Zhu, and H. Chen “Exploring the Propagation of Vulnerabilities in FinTech Payment Applications on GitHub: A Deep Node Ranking Approach” ***Preparing for Submission to Information Systems Research (ISR).***
2. B. Lazarine, S. Samtani, H. Zhu, **S. Ullman**, and H. Chen “Detecting and Grouping Vulnerable GitHub Repositories in Scientific Cyberinfrastructure: An Unsupervised Graph Embedding Approach” ***Preparing for Submission to Journal of Management Information Systems (JMIS).***
3. **S. Ullman**, “Replication of Internet Privacy Concerns in the Context of Smart Home Devices” ***Preparing for Submission to AIS Transactions on Replication Research (TRR).***
4. R. Reyes, **S. Ullman**, S. Samtani, and H. Chen “Identifying Vulnerability Persistence on Containers from Docker Hub: A Multi-View Learning Approach” ***Preparing for Submission to ACM Transactions on Management Information Systems (TMIS).***
5. **S. Ullman**, B. Lazarine, S. Samtani, and H. Chen “Securing Software Application Deployments in Cloud Computing: A Graph Contrastive Learning Approach” ***Preparing for Submission to MIS Quarterly (MISQ).***
6. B. Lazarine, **S. Ullman**, H. Zhu, and S. Samtani “Suggesting Alternatives for Insecure Machine Learning Repositories: A Multi-View Graph Transformer Approach” ***Preparing for Submission to MIS Quarterly (MISQ).***
7. A. Ndubizu, **S. Ullman**, S. Samtani, and H. Chen “Identifying Vulnerability Propagation in Quantum Source Code on GitHub: A Large-Language Model Code Clone Detection Approach” ***Preparing for Submission to MIS Quarterly (MISQ).***

**Refereed Conference Proceedings** (\* indicates I was the presenting author)

1. **S. Ullman**, B. Ampel, S. Samtani, S. Yang, and H. Chen. “The 4th Workshop on Artificial Intelligence-Enabled Cybersecurity Analytics” *In Proceedings of 2024 ACM Conference on Knowledge Discovery and Data Mining (KDD’24).* Barcelona, Spain. August, 2024.
2. **\*S. Ullman**, S. Samtani, H. Zhu, B. Lazarine, B. Ampel, M. Patton, and H. Chen “Smart Vulnerability Assessment for Scientific Cyberinfrastructure: An Unsupervised Graph Embedding Approach” *IEEE Intelligence and Security Informatics (ISI)*. Rosslyn, VA (Virtual). November 2020.
3. B. Ampel, S. Samtani, H. Zhu, **S. Ullman**, and H. Chen “Labeling Hacker Exploits for Proactive Cyber Threat Intelligence: A Deep Transfer Learning Approach” *IEEE Intelligence and Security Informatics (ISI)*. Rosslyn, VA (Virtual). November 2020. ***(Winner of the Best Paper Award).***
4. B.Lazarine, S. Samtani, M. Patton, H. Zhu, **S. Ullman**, B. Ampel, and H. Chen “Identifying Vulnerable GitHub Repositories and Users in Scientific Cyberinfrastructure: An Unsupervised Graph Embedding Approach” *IEEE Intelligence and Security Informatics (ISI)*. Rosslyn, VA (Virtual). November 2020.

**Refereed Workshop Papers (No Proceedings;** \* indicates I was the presenting author**)**

1. **\*S. Ullman** and H. Chen “VulnSSL: Identifying Relevant Vulnerability Remediation Strategies Using Self-Supervised Learning” *International Conference on Secure Knowledge Management (SKM)*. Tempe, AZ (Virtual). September 2023.
2. B. Ampel, S. Samtani, **S. Ullman**, H. Chen “Linking Common Vulnerabilities and Exposures to the MITRE ATT&CK Framework: A Self-Distillation Approach” *ACM KDD Workshop on AI-enabled Cybersecurity Analytics.* Virtual Event. August 2021.

**Poster Presentations**

1. M. Wisniewski, L. Irizarry, A. Hayes, S. DeHeart, K. Shu, **S. Ullman** “Automated Vulnerability Classification Using Supervised Machine Learning Methods” Colorado State University Pueblo 9th Annual Spring Symposium: A Celebration of Research, Scholarship, and Creative Activity. Pueblo, CO. April 2023.
2. M. Wisniewski, L. Irizarry, A. Hayes, S. DeHeart, K. Shu, **S. Ullman** “Cybersecurity Advisory Data Collection for Data-Driven Tools” Colorado State University Pueblo 9th Annual Spring Symposium: A Celebration of Research, Scholarship, and Creative Activity. Pueblo, CO. April 2023.

# Invited Talks and External Presentations

1. *University of Arizona MIS Department 50th Anniversary – Future of MIS.* **Presentation Title:** “Vulnerability Management for IT Infrastructure: An Artificial Intelligence-enabled Approach” March 22, 2024.
2. *INFORMS Annual Meeting*. **Presentation Title:** “Using Computational Design Science and Contrastive Self-Supervised Learning to Link Vulnerabilities and Their Remediations” October 15, 2023.
3. *Open Data Science Conference (ODSC) East 2023*. **Presentation Title:** “AI4Cyber: An Overview of Artificial Intelligence for Cybersecurity and an Open-Source Virtual Machine” May 9, 2023.
4. *56th Hawaii International Conference on System Sciences (HICSS)*. **Symposium Title:** “AI in Cybersecurity – Machine Learning/Deep Learning Data Analytics” January 3,2023.
5. *Open Data Science Conference (ODSC) West 2022*. **Presentation Title:** “AI4Cyber: An Overview of the Field and an Open-Source Virtual Machine for Research and Education” November 2, 2022.
6. *Inaugural University of Arizona MS Cybersecurity Board of Advisors Meeting*. **Presentation Title:** “Detecting and Grouping Vulnerable Virtual Machines in Public Clouds: A Multi-View Representation Learning Approach” April 8, 2022.
7. *NSF Cybersecurity Summit Vulnerability Management Workshop*. **Presentation Title:** “Detecting and Grouping Vulnerable Virtual Machines in Scientific Cyberinfrastructure” October 19, 2021.
8. *NSF Cybersecurity Summit Vulnerability Management Workshop*. **Presentation Title:** “Detecting and Linking Vulnerabilities in Scientific Cyberinfrastructure to MITRE ATT&CK” October 19, 2021.

# Professional Service

**Conference Committees**

* Workshop Co-Chair, 4th Workshop on Artificial Intelligence-enabled Cybersecurity Analytics (AI4Cyber-KDD), 2024.
* Program Committee, INFORMS Workshop on Data Science (WDS), 2022.
* Program Committee, ACM Conference on Computer and Communications Security (CCS) AISec Workshop, 2021.
* Program Committee, Workshop on Artificial Intelligence-enabled Cybersecurity Analytics (AI4Cyber-KDD), 2021, 2023.

**Ad-hoc Reviewer: Journal Publications**

* Information Systems Research (ISR), 2024.
* IEEE Transactions on Big Data (TBD), 2024.
* Journal of Management Information Systems (JMIS), 2024.
* IEEE Transactions on Engineering Management (TEM), 2024.
* Information Systems Frontiers, 2024.
* Computers & Security, 2022, 2023.
* IEEE Transactions on Dependable and Secure Computing (TDSC), 2021, 2023.
* IEEE Internet of Things Journal (IoTJ), 2023.
* ACM Digital Threats: Research and Practice (DTRAP), 2022, 2023.
* ACM Transactions on Management Information Systems (TMIS), 2019.

**Ad-hoc Reviewer: Refereed Conference Proceedings**

* Hawaii International Conference on System Sciences (HICSS), 2021, 2023, 2024.
* Pacific Asia Conference on Information Systems (PACIS), 2020-2023.
* International Conference on Information Systems (ICIS), 2020, 2021.
* IEEE Security and Privacy Deep Learning and Security Workshop (DLS) 2020.
* ICDM Workshop on Deep Learning for Cyber Threat Intelligence (DL-CTI), 2020.
* INFORMS Workshop on Data Science (WDS), 2022.

# Honors and Awards

**Awards:**

* Moshe Dror Research Excellence Award. 2024.
* James F. LaSalle Teaching Excellence Award. 2024.
* Doctoral Consortium, Americas Conference on Information Systems (AMCIS). 2023.
* Paul S. and Shirley Goodman Award in International Computer Technology. 2022.
* Samtani-Garcia MIS Ph.D. Commitment Scholarship. 2022.
* Best Paper Award, IEEE Intelligence and Security Informatics (ISI). 2020.
* Nunamaker-Chen Doctoral Student Scholarship. 2020.

# Teaching Experience

**Instructor:**

University of Texas at San Antonio – IS 4893 **“Cyber Security Capstone”**

* Fall 2024 (16 students, online synchronous)

University of Arizona – MIS 689 **“Cyber Warfare Capstone”**

* Spring 2024 (22 students, online asynchronous)
* Fall 2023 (10 students, online asynchronous)
* Spring 2023 (27 students, online asynchronous)
* Fall 2022 (11 students, online asynchronous)
* Spring 2022 (16 students, online asynchronous)
* Fall 2021 (13 students, online asynchronous)
* Spring 2021 (4 students, online asynchronous)

Colorado State University-Pueblo – CIS 490 **“Special Projects: AI for Cybersecurity”**

* Spring 2024 (14 students, online synchronous)
* Spring 2023 (5 students, online synchronous)

**Graduate Teaching Assistant:**

University of Arizona – MIS 611D **“Topics in Data and Web Mining”**

* Spring 2023, Instructor: Dr. Hsinchun Chen (12 students)

University of Arizona – MIS 464 **“Data Analytics”**

* Spring 2023, Instructor: Dr. Hsinchun Chen (43 students)

University of Arizona – MIS 689 **“Cyber Warfare Capstone”**

* Fall 2020, Instructor: Dr. Hsinchun Chen (17 students)
* Spring 2020, Instructor: Dr. Hsinchun Chen (3 students)
* Fall 2019, Instructor: Dr. Hsinchun Chen (15 students)
* Spring 2019, Instructor: Dr. Hsinchun Chen (3 students)

**External:**

* **AZ Cyber Initiative – Cyber Bootcamp** (High School Bootcamp). 2021 (Inaugural Year), 2022. Instructor.

# Grant Experience

* **Year:** 2024. **Funding Source:** National Science Foundation. **Grant Title:** “CICI: TCR: Enhancing the Resilience of Open Source Artificial Intelligence Software: Vulnerability Detection and Deep Learning-based Linkage and Remediation” **Funding Amount:** $1,199,998. **Role:** Co-PI. **Status:** Under Review.
* **Year:** 2023. **Funding Source:** National Science Foundation. **Grant Title:** “CICI: UCSS: Enhancing the Usability of Vulnerability Assessment Results for Open-Source Software Technologies in Scientific Cyberinfrastructure: A Deep Learning Perspective” **Funding Amount:** $600,000. **Role:** Assisting Grant Writer. **Status:** Awarded.
* **Year:** 2022. **Funding Source:** National Science Foundation. **Grant Title:** “CICI: UCSS: Enhancing the Usability of Vulnerability Assessment Results for Open-Source Software Technologies in Scientific Cyberinfrastructures: A Deep Learning Perspective” **Funding Amount:** $600,000. **Role:** Assisting Grant Writer. **Status:** Not Funded (Low Competitive).
* **Year:** 2022. **Funding Source:** National Science Foundation. **Grant Title:** “CISE-MSI: DP: SaTC: MSI Research Capacity Building for Artificial Intelligence (AI)-enabled Vulnerability Assessment and Remediation in Cyberinfrastructure” **Funding Amount:** $600,000. **Role:** Lead Author. **Duration:** 2022-2025. **Status:** Awarded.
* **Year:** 2021. **Funding Source:** National Science Foundation. **Grant Title:** “CCRI: New: CCRI for Cybersecurity: An Artificial Intelligence (AI)-enabled Cybersecurity Analytics Perspective” **Funding Amount:** $2,000,000. **Role:** Assisting Grant Writer. **Status:** Not Funded (Competitive).
* **Year:** 2020. **Funding Source:** National Science Foundation. **Grant Title:** “CICI: SIVD: Proactively Detecting and Categorizing Configuration and Social Coding Vulnerabilities in Scientific Cyberinfrastructure: An AI-enabled Vulnerability Discovery Approach” **Funding Amount:** $492,000. **Role:** Assisting Grant Writer. **Status:** Not Funded (Competitive).
* **Year:** 2020. **Funding Source:** NSF XSEDE. **Grant Title:** “Exploratory Study of Scientific Cyberinfrastructure for Information Systems Research” **Funding Amount:** $2,000. **Role:** Allocation Manager. **Status:** Awarded.

# Work Experience

|  |  |
| --- | --- |
| **University of Arizona**  | 2018 – 2024 |
| *Graduate Research/Teaching Assistant* |  |
| **The MITRE Corporation**  | 2019 –2019 |
| *Cybersecurity Intern* |  |
| **Institutional Research (CSU-Pueblo)**  | 2017 –2018 |
| *Data Analytics Assistant* |  |

# Professional Affiliations

* Association for Information Systems (AIS), Member.
* Institute for Operations Research and Management Sciences (INFORMS), Member.
* Institute of Electrical and Electronics Engineers (IEEE), Member.
* Association for Computing Machinery (ACM), Member.

# Technical Skills

* **Databases:** Oracle, MySQL, MongoDB.
* **Programming Languages:** Python, R, Bash.
* **Visualization:** Tableau, Gephi.
* **Data Mining Tools:** RapidMiner, SPSS, scikit-learn.
* **Deep Learning Modules:** TensorFlow, Keras, PyTorch.
* **Security Tools:** Nmap, Wireshark, SQLMap, Metasploit, Meterpreter, Hydra, Nessus, BurpSuite.
* **Operating Systems:** Linux (Ubuntu, CentOS, Kali), Windows.