Ryan Sheatsley

Litigation Experience

Trusted Knight Corporation v. International Business Northern District of California

Machines Corporation

3:19-cv-01206-EMC - *Patent* 2019–2022

Technical Associate assisting Dr. Patrick McDaniel

Quinn Emanuel Urquhart & Sullivan

Rimini Street, Inc. v. Oracle America, Inc. and Oracle District of Nevada

International Corporation

2:14-cv-01699-LRH-CWH - Other 2016–2020

Technical Associate assisting Dr. Patrick McDaniel

Bois, Schiller, & Flexner

Zito Vault, LLC v. International Business Machines Cor- Northern District of Texas

poration, and Softlayer Technologies, Inc.

3:16-cv-00962-M - Patent 2016–2018

Technical Associate assisting Dr. Patrick McDaniel

Quinn Emanuel Urquhart & Sullivan

Academic & Professional Experience

United States Army Research Laboratory

Research Scientist and Team Lead (mentored by Andrew Toth)

Summers of 2014–2018

Systems and Internet Infrastructure Security Labora- University Park, PA

tory

Systems Administrator 2015–2022

Penn State Learning Center University Park, PA

Writing Tutor (mentored by Dr. Jon Olson) 2012–2013

Education

University of Wisconsin-Madison

Madison, WI

Ph.D. in Computer Sciences

2022-2024

- O Thesis: Methods for Robust Models in Security-Critical Domains
- O Advisor: Prof. Patrick McDaniel
- Thesis committee: Prof. Patrick McDaniel, Prof. Kassem Fawaz, Prof. Rahul Chatterjee, Prof. Sharon
 Li

Pennsylvania State University

University Park, PA

Ph.D. in Computer Science and Engineering

2019-2022

- O Advisor: Prof. Patrick McDaniel
- Transfer to University of Wisconsin-Madison starting Fall 2022

Pennsylvania State University

University Park, PA

M.S. in Computer Science and Engineering

2016-2018

- Thesis: Adversarial Examples in Constrained Domains
- O Advisor: Prof. Patrick McDaniel
- O Thesis committee: Prof. Patrick McDaniel, Prof. Trent Jaeger, Prof. Nicolas Papernot

Pennsylvania State University

University Park, PA

B.S. in Computer Engineering

2011-2015

Publications

Conference Proceedings.....

Characterizing the Modification Space of Signature IDS Rules. Ryan Guide, Eric Pauley, Yohan Beugin, Ryan Sheatsley, Patrick McDaniel. Proceedings of the 2023 Military Communications Conference (MILCOM), Boston, MA. (2023)

The Space of Adversarial Strategies. *Ryan Sheatsley, Blaine Hoak, Eric Pauley, Patrick McDaniel*. Proceedings of the 32nd USENIX Security Symposium (USENIX), Anaheim, CA. (2023)

Measuring and Mitigating the Risk of IP Reuse on Public Cloud. Eric Pauley, Ryan Sheatsley, Blaine Hoak, Quinn Burke, Yohan Beugin, Patrick McDaniel. Proceedings of the 43rd IEEE Symposium on Security and Privacy (S&P), San Francisco, CA. (2022)

A Machine Learning and Computer Vision Approach to Geomagnetic Storm Forecasting. *Kyle Domico, Ryan Sheatsley, Yohan Beugin, Quinn Burke, Michael Patrick McDaniel.* Proceedings of the Second AGU Conference on Machine Learning in Heliophysics (ML-Helio), Boulder, CO. (2022)

Building a Privacy-Preserving Smart Camera System. *Yohan Beugin, Quinn Burke, Blaine Hoak, Ryan Sheatsley, Eric Pauley, Gang Tan, Syed Rafiul Hussain, Patrick McDaniel*. Proceedings on Privacy Enhancing Technologies Symposium (PETS), Sydney, Australia. (2022)

HoneyModels: Machine Learning Honeypots. *Ahmed Abdou, Ryan Sheatsley, Yohan Beugin, Tyler Shipp, Patrick McDaniel*. Proceedings of the 2021 Military Communications Conference (MILCOM), San Diego, CA. (2021)

On the Robustness of Domain Constraints. Ryan Sheatsley, Blaine Hoak, Eric Pauley, Yohan Beguin, Yohan Beugin, Michael Weisman, Patrick McDaniel. Proceedings of the 2021 Conference on Computer and Communications Security (CCS), Coex, Seoul, Republic of Korea. (2021)

Feature Engineering: A Case Study For Radiation Source Localization In Complicated Environments. *Matthew Durbin, Ryan Sheatsley, Patrick McDaniel, Azaree Lintereur*. Proceedings of the 62nd Annual Meeting of the Institute of Nuclear Materials Management (INMM), Virtual. (2021)

A Multi-Step Machine Learning Approach to Directional Gamma Ray Detection. *Matthew Durbin, Ryan Sheatsley, Patrick McDaniel, Azaree Lintereur*. Proceedings of the 61st Annual Meeting of the Institute of Nuclear Materials Management (INMM), Virtual. (2020)

Development of Machine Learning Algorithms for Directional Gamma Ray Detection. *Matthew Durbin, Ryan Sheatsley, Christopher Balbier, Tristan Grieve, Patrick McDaniel, Azaree Lintereur.* Proceedings of the 60th Annual Meeting of the Institute of Nuclear Materials Management (INMM), Palm Springs, CA. (2019)

Curie: Policy-based secure data exchange. *Z. Berkay Celik, Abbas Acar, Hidayet Aksu, Ryan Sheatsley, Patrick McDaniel, A Secuk Uluagac.* Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy (CODASPY), Richardson, TX. (2019)

Network Traffic Obfuscation: An Adversarial Machine Learning Approach. Gunjan Verma,

Ertugrul Ciftcioglu, Ryan Sheatsley, Kevin Chain, Lisa Scott. Proceedings of the 2018 Military Communications Conference (MILCOM), Baltimore, MD. (2018)

Detection under Privileged Information. *Z. Berkay Celik, Patrick McDaniel, Rauf Izmailov, Nicolas Papernot, Ryan Sheatsley, Raquel Alvarez, Ananthram Swami*. Proceedings of the 2018 Asia Conference on Computer and Communications Security (ASIACCS), Incheon, Republic of Korea. (2018)

Heterogeneous information sharing of sensor information in contested environments. *Jason A Wampler, Chien Hsieh, Andrew Toth, Ryan Sheatsley*. Proceedings of Volume 10190 Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR VIII (SPIE), Anaheim, CA. (2017)

Journals.....

Experimental tests of Gamma-ray Localization Aided with Machine-learning (GLAM) capabilities. *Matthew Durbin, Ryan Sheatsley, Patrick McDaniel, Azaree Lintereur*. Elsevier Journal of Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment (NIM-A). (2022)

Adversarial Examples for Network Intrusion Detection Systems. Ryan Sheatsley, Nicolas Papernot, Michael Weisman, Gunjan Verma, Patrick McDaniel. IOS Press Journal of Computer Security (JCS). (2022)

Physics-based Misbehavior Detection System for V2X Communications. *Alejandro Andrade Salazar, Patrick McDaniel, Ryan Sheatsley, Jonathan Petit*. SAE International Journal of Connected and Automated Vehicles. (2021)

Improving Radioactive Material Localization by Leveraging Cyber-Security Model Optimizations. Ryan Sheatsley, Matthew Durbin, Azaree Lintereur, Patrick McDaniel. IEEE Sensors. (2021)

Book Chapters.

Evading Machine Learning-based Network Intrusion Detection Systems with GANs. Bolor-Erdene Zolbayar, Ryan Sheatsley, Patrick McDaniel. In: Charles A Kamhoua, Christopher D. Kiekintveld, Fei Fang, Quanyan Zhu (Ed.). Game Theory and Machine Learning for Cyber Security. John Wiley & Sons, Incorporated, Hoboken, New Jersey. (2021)

Technical Reports.

Systematic Evaluation of Geolocation Privacy Mechanisms. *Alban Héon, Ryan Sheatsley, Quinn Burke, Blaine Hoak, Eric Pauley, Yohan Beugin, Patrick McDaniel*. (2023)

Generating Practical Adversarial Network Traffic Flows using NIDSGAN. Bolor-Erdene Zolbayar, Ryan Sheatsley, Patrick McDaniel, Michael Weisman, Sencun Zhu, Shitong Zhu, Srikanth Krishnamurthy. (2020)

Adversarial Planning. Valentin Vie, Ryan Sheatsley, Sophia Beyda, Sushrut Shringarputale, Kevin Chan, Trent Jaeger, Patrick McDaniel. (2020)

A Vision Toward an Internet of Battlefield Things (IoBT): Autonomous Classifying Sensor Network. John Zhu, Egan McClave, Quan Pham, Sujay Polineni, Sam Reinhart, Ryan Sheatsley, Andrew Toth. (2018)

Cleverhans v1.0.0: an adversarial machine learning library. *Nicolas Papernot, Ian Goodfellow, Ryan Sheatsley, Reuben Feinman, Patrick McDaniel.* (2016)

Analyzing GAIAN Database (GaianDB) on a Tactical Network. *Ryan Sheatsley, Andrew Toth.* (2015)

Thesis....

Methods for Robust Models in Security-Critical Domains. Ryan Sheatsley. (2018) Adversarial Examples in Constrained Domains. Ryan Sheatsley. (2018)

Honors

LEAP Dissertation Fellowship: Google and CMD-IT	2023
Robert M. Owens Memorial Scholarship: Pennsylvania State University	2017
Pathways Internship Program: United States Government	2015
Peer Tutor Faculty Recommendation: Pennsylvania State University	2011

Talks

On the Robustness of Domain Constraints: VMWare ML Approaches to Security Disc	cussion
Group	2023
Adversarial Machine Learning: Penn State CMPSC 443: Introduction to Computer and	nd Net-
work Security	2021
On the Robustness of Domain Constraints: ACM CCS	2021
On the Robustness of Domain Constraints: CTML Industrial Advisory Board Meetir	ıg 2021
Adversarial Examples in Constrained Domains: RIT Great Lakes Security Day	2020
Adversarial Examples in Constrained Domains: Cyber-CRA Webinar	2020

Professional Activities

Reviewer	
SATML: IEEE Symposium on Secure and Trustworthy Machine Learning	2023, 2024
MILCOM: IEEE Military Communications Conference Artificial Intelligence	e for Cyber Work-
shop	2023
IEEE Trans. Signal Process.: IEEE Transactions on Signal Processing	2023
Transp. Res. C: Transportation Research Part C: Emerging Technologies	2023
Ann. Telecommun.: Annals of Telecommunications	2023
IEEE S&P: IEEE Symposium on Security and Privacy	2023, 2023
JCS: IOS Press Journal of Computer Security	2022, 2023, 2024
ACM Comput. Surv.: ACM Computing Surveys	2022, 2023
SOFTW: IET Software	2022
TDSC: IEEE Transactions on Dependable and Secure Computing	2021
IC: IEEE Internet Computing	2021
TIP: IEEE Transactions on Image Processing	2020
TEM: IEEE Transactions on Engineering Management	2020
DKE: Data & Knowledge Engineering Journal	2020
GLOBECOM: IEEE Global Communications Conference	2019

Volunteer	
Dancing with Robots Penn State Summer Camp Coordinator	2019