

EDUCATION	Doctoral Student - Computer Science University of Wisconsin – Madison	August 2021 - Present
	Bachelor of Science - Computer Engineering University of Wisconsin – Madison	August 2018 - May 2021
	Bachelor of Science - Computer Sciences University of Wisconsin – Madison	August 2018 - May 2021
	Dean's Honor List	2019, 2020, 2021
INTERESTS	Security & Privacy, Systems, Large Language Models, Multi-Modal Language Models, Computer Vision	
PUBLICATIONS (* = CO-AUTHORS)	<b>Experimental Security Analysis of Sensitive Data Access by Browser Extensions</b> <u>A. Nayak</u> *, R. Khandelwal*, Earlence Fernande, and K. Fawaz.	<a href="#">[Paper]</a> (TheWebConf'24)
	<b>Unpacking Privacy Labels: A Measurement and Developer Perspective on Google's Data Safety Section</b> R. Khandelwal*, <u>A. Nayak</u> *, P. Chung, and K. Fawaz.	<a href="#">[Paper]</a> (USENIX Security, 2024)
	<b>Comparing Privacy Labels of Applications in Android and iOS.</b> R. Khandelwal, <u>A. Nayak</u> , P. Chung, and K. Fawaz.	<a href="#">[Paper]</a> (WPES, CCS, 2023)
	<b>CookieEnforcer: Automated Cookie Notice Analysis and Enforcement.</b> R. Khandelwal, <u>A. Nayak</u> , H. Harkous, and K. Fawaz.	<a href="#">[Paper]</a> (USENIX Security, 2023)
	<b>Surfacing Privacy Settings Using Semantic Matching.</b> R. Khandelwal, <u>A. Nayak</u> , Y. Yao, and K. Fawaz.	<a href="#">[Paper]</a> (PrivateNLP, EMNLP 2020)
	<b>Automated Analysis of User Privacy Threats on Privacy Notices</b> <i>Mentors: Prof. Kassem Fawaz, Prof. Norman Sadeh</i> Designing and developing an automated framework to analyze privacy notices (eg: cookie notice, privacy settings) and detect User Privacy Threats present as defined in the <a href="#">UsersFirst</a> framework.	
UNDER REVIEW/ONGOING WORK		
WORK EXPERIENCE	<b>Research Assistant, Wisconsin Privacy and Security Group</b> <i>Mentors: Prof. Kassem Fawaz</i> Working on multi-modal analysis to detect dark patterns on websites and develop VLMs to understand Web-UI	June 2022 - Present
	<b>Visiting Researcher, Carnegie Mellon University</b> <i>Mentors: Prof. Norman Sadeh</i> Developing an LLM framework to analyze Privacy Threats on online platforms automatically, primarily focused on user privacy.	January 2025 - May 2025
	<b>Graduate Teaching Assistant, Department of Computer Sciences</b> Assisted with the development of class materials, homework, and term papers. Gave a guest lecture on Reinforcement Learning during the summer term.	Sept 2021 - Dec 2022
	<b>UGrad Research Assistant, Wisconsin Privacy and Security Group</b> As an Undergrad Research Assistant, I worked on the CookieEnforcer project. Next, I focused on developing a semantic clustering algorithm that could group similar privacy settings based on their meaning.	June 2020 - Aug 2021

## Automatically Detecting Online Deceptive Patterns in Real-time

Advisor: Prof. Kassem Fawaz

[[Arxiv Pre-print](#)]

- Designed a multi-modal framework to convert website screenshots into a machine-parsable format to perform Deceptive Pattern (or Dark Patterns) classifications in real-time.
- Developed a pipeline to generate realistic synthetic websites and extract the web-element location automatically.
- Finetuned **YOLOv10** models on **over 60K** synthetic websites on the web-element classification task.
- Developed an LLM-assisted human annotation framework to create a Deceptive Patterns (DP) dataset consisting of over 1000 websites
- Created a synthetic labelled dataset to distill smaller models on the DP detection task, consisting of over **10K websites**.
- Created a new pipeline to distill **T5** models on DP-Dataset, achieving high DP-detection accuracy. We also distilled **Qwen2.5-1.5B** model for this task.

## Experimental Security Analysis of Sensitive Data Access by Browser

Extensions

(*The Web Conference'24*)

Advisor: Prof. Kassem Fawaz

[[Paper](#)]

- Performed an extensive study to uncover security risks in browser extensions and demonstrated vulnerabilities in Chrome's review process by developing a proof-of-concept extension capable of bypassing Chrome WebStore review processes.
- Analyzed **over 10K** web domains and **160K** Chrome extensions, identifying critical security loopholes in password protection and extension permissions.
- Created an LLM-driven framework for advanced browser extension code analysis to detect sensitive data access and malicious code in extensions.

## Unpacking Privacy Labels: A Measurement and Developer Perspective on Google's Data Safety Section

(*USENIX'24*)

Advisor: Prof. Kassem Fawaz

[[Paper](#)]

- Designed and developed the methodology to examine Google's Data Safety Section using quantitative and qualitative methods, revealing inconsistencies and reporting trends. We analyzed **over 1.1M** apps on the Google Play Store.
- Conducted a user study uncovering app developers' struggles, strategies, and factors affecting DSS submissions, emphasizing the need for better resources and guidelines to enhance privacy label accuracy

## Comparison of Privacy Labels between Android and iOS apps

(*WPES, CCS'23*)

Advisor: Prof. Kassem Fawaz

[[Paper](#)]

- Created a system to detect cross-listed apps on App Store and Play Store and scrape their privacy labels.
- Performed analysis on the collected privacy labels to find inconsistencies and trends of these inconsistencies.

## Automated Cookie Notice Analysis and Enforcement

(*USENIX Security 2023*)

Advisor: Prof. Kassem Fawaz

[[Paper](#)]

- Designed and developed a browser plugin to automatically accept the most privacy-preserving choices for a cookie notice on any website
- Conducted a user study showing the reduction in user effort in interacting with cookie notices as well as the usability of the extension

## Surfacing Privacy Settings Using Semantic Matching

(*PrivateNLP@EMNLP 2020*)

Advisor: Prof. Kassem Fawaz

[[Paper](#)]

- Designed and developed an HTML parser to understand the relative positioning of web elements.
- Created a hierarchical clustering algorithm to merge sentences based on semantic matching into high-level categories

### **Increasing the accuracy of Sim2Real Transfer Learning**

- Developed a Reward Shaping function for better policy transfer in the Sim2Real domain
- Created custom environments with realistic physics

#### **SCHOLASTIC ACHIEVEMENTS**

- Recipient of first-year CS Departmental Scholarship (UW-Madison)
- Awarded Student Research Grant by the Graduate School (UW Madison, 2023)

#### **RESEARCH IN NEWS**

Our work on **Exposing and Addressing Security Vulnerabilities in Text Input Fields** was covered by BleepingComputer ([Link](#)), Malwarebytes ([Link](#)), TechRadar ([Link](#)), The Sun ([Link](#)), Mirror UK ([Link](#)) and India Times ([Link](#)). TV interview conducted by WISC-TV ([Link](#))

Our work on **Automating Cookie Notice Analysis and Enforcement** was covered by The Gradient ([Link](#)), Unite.AI ([Link](#)) and Techradar ([Link](#))

#### **TALKS**

- Sensitive Data Access by Browser Extensions, Supernova Technology, February 2024

#### **TECHNICAL SKILLS**

Generative AI, ML, LLM, VLM, Algorithms, Python, Java, JS, C++, Pytorch, Tensorflow, React

#### **SERVICE**

- Sub Reviewer: USENIX (2023, 2024), IEEE S&P (2024)
- Reviewer: ACM TWEB (2025)