

Deepak Kumar

<https://kumarde.com> | [LinkedIn](#) | debug12@gmail.com | (248)-231-3575

Interdisciplinary researcher with over six years of experience conducting large-scale, data studies to improve end-user security and safety on the Internet. Thrilled to join an organization that values data-driven decision making to improve trust & safety outcomes for their users.

EDUCATION

University of Illinois, Urbana Champaign

Aug 2020

Ph.D. in Computer Science

See <https://kumarde.com> for full list of publications

University of Michigan

Bachelor of Science in Engineering, Computer Science and Engineering

May 2016

SKILLS and TECHNOLOGIES

- Experienced at working towards ambitious goals with ambiguous research requirements
- Able to manage large scale, real-world datasets to drive insights, system design, and policy
- Strong verbal and written technical communication skills through presentations and publications
- Solid understanding of statistical methods, hypothesis testing, Bayesian statistics, A/B testing
- Proficient at machine learning model creation, training, and evaluation
- **Languages: Python, Golang, Node.js, Javascript, R, C, C++**
- **Services and Frameworks: Google Cloud, AWS, Scikit-learn, Hugging Face, PyTorch, Keras**

WORK EXPERIENCE

Stanford University, Postdoctoral Scholar

Aug 2020 – Present

- Authored 10 research papers at top-tier computer science conferences focused on anti-abuse technology, misinformation, and Internet safety
- Built and deployed large-scale data management and NLP pipelines with Python, Golang, and Google Cloud to develop new algorithms for detecting abuse and misinformation on the Internet
- Wrote and won two grants – NSF \$300K, Brown Institute Magic Grant \$150K – for research in building better anti-abuse tools for end-users
- Developed and co-taught a full graduate level course focused on modern Internet protocols at Stanford
- Advised 16 undergraduate, masters, and Ph.D. students leading to 9 new research publications
- Organized 1st IEEE Workshop on Security for Harassment Online, Protections, Empowerment (SecHOPE), a venue that brings researchers and practitioners together to improve anti-abuse technologies

University of Illinois, Graduate Student Researcher

Aug 2016 – Aug 2020

Advisor: [Michael Bailey](#)

- Authored 9 research papers at top-tier computer science conferences focused on IoT security, network security, and Internet measurement
- Developed ZLint, an open-source HTTPS Certificate Linter now deployed at the world's top certificate authorities like Let's Encrypt, Google, Digicert, and Sectigo (<https://github.com/zmap/zlint>)
- Discovered "Skill Squatting," an attack against real-world speech-to-text ML systems that enables attackers to launch complex phishing attacks against end-users; vulnerabilities were patched by Amazon and Google
- Advised 6 undergraduate and master's students leading to 4 research publications in top security venues
- Taught computer security principles like application security, web security fundamentals (SQL injection, XSS), and network security (DDoS, DNS cache poisoning) to 200+ students for three different semesters

Google, Research Intern

Summer 2018

Mentor: Kurt Thomas

- Developed personalized, *on-device* deep-learning models with Keras and Tensorflow.js to detect online hate and harassment geared towards end-users
- Contributed to source code of leading in-browser deep learning libraries, like Tensorflow.js
- Designed and deployed a Chrome extension using Vue.js that performed real-time hate and harassment detection on social platforms (Twitter, Reddit, Disqus) for end-users

Microsoft, Software Engineering Intern

Summer 2015, 2016

- Built new protocols for quickly flashing Microsoft HoloLens devices with Windows OS in factory settings
- Developed new functionality that brought pivot table interactivity to Microsoft Excel on Android devices

SELECT PUBLICATIONS

Understanding the Behaviors of Toxic Accounts on Reddit

Deepak Kumar, Jeff Hancock, Kurt Thomas, Zakir Durumeric.

ACM Web Conference (WebConf). May 2023.

Designing Toxic Content Classification for a Diversity of Perspectives

Deepak Kumar, Patrick Gage Kelley, Sunny Consolvo, Joshua Mason, Elie Bursztein, Zakir Durumeric, Kurt Thomas, Michael Bailey.

USENIX Symposium on Usable Privacy and Security (SOUPS). August 2021.

SoK: Hate, Harassment, and the Changing Landscape of Online Abuse

Kurt Thomas, Devdatta Akhawe, Michael Bailey, Elie Bursztein, Dan Boneh, Sunny Consolvo, Nicki Dell, Zakir Durumeric, Patrick Gage Kelley, Deepak Kumar, Damon McCoy, Sarah Meiklejohn, Thomas Ristenpart, Gianluca Stringhini.

IEEE Symposium on Security and Privacy (Oakland). May 2021.

Happenstance: Utilizing Semantic Search to Track Russian State Media Narratives about the Russo-Ukrainian War on Reddit

Hans Hanley, Deepak Kumar, Zakir Durumeric.

International Conference on Web and Social Media (ICWSM). June 2023.

On the Infrastructure Providers that Support Misinformation Websites

Catherine Han, Deepak Kumar, Zakir Durumeric.

International Conference on Web and Social Media (ICWSM). June 2022.

Skill Squatting Attacks on Amazon Alexa

Deepak Kumar, Riccardo Paccagnella, Paul Murley, Eric Hennenfent, Joshua Mason, Adam Bates, Michael Bailey.

27th USENIX Security Symposium (USENIX Security). August 2018.

Tracking Certificate Misissuance in the Wild

Deepak Kumar, Zhengping Wang, Matthew Hyder, Joseph Dickinson, Joshua Mason, Michael Bailey, Gabrielle Beck, David Adrian, Zakir Durumeric, J. Alex Halderman.

39th IEEE Symposium on Security and Privacy (Oakland). May 2018.