Arkaprabha Bhattacharya

The Bloomberg Center
Cornell University

+1 425-445-4782
ab2956@cornell.edu
https://arkabhat.github.io

EDUCATION

2024 – Present **P.h.D in Computer Science**
Cornell University, New York, NY
Faculty Advisors: Professor Nicola Dell, Professor Thomas Ristenpart

2021–2022 **M.S. in Computer Science and Engineering**
University of Washington, Seattle, WA
Faculty Advisors: Professor Franziska Roesner, Professor Tadayoshi Kohno

2018–2021 **B.S. in Computer Science and Engineering**
University of Washington, Seattle, WA

PUBLICATIONS

2026 P.1 **Arkaprabha, Bhattacharya**, Alaa Daffalla, Kevin Lee, Rosanna Bellini, Nicola Dell, and Thomas Ristenpart. Inconsistent, Incomplete, and Insecure: A Survey of Account Security Interfaces. *To appear in: 35th USENIX Security Symposium (USENIX Security 26)*, 2026

2025 P.1 Alaa Daffalla, **Arkaprabha, Bhattacharya**, Jacob Wilder, Rahul Chatterjee, Nicola Dell, Rosanna Bellini, and Thomas Ristenpart. A framework for abusability analysis: The case of passkeys in interpersonal threat models. In *34th USENIX Security Symposium (USENIX Security 25)*, pages 7819–7838, 2025

P.2 Vijay Prakash, Kevin Lee, **Arkaprabha, Bhattacharya**, Danny Yuxing Huang, and Jessica Staddon. Learned, lagged, llm-splained: Llm responses to end user security questions. In *2025 Annual Computer Security Applications Conference (ACSAC)*. IEEE, 2025

2024 P.1 **Arkaprabha, Bhattacharya**, Kevin Lee, Vineeth Ravi, Jessica Staddon, and Rosanna Bellini. Shortchanged: Uncovering and analyzing intimate partner financial abuse in consumer complaints. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, pages 1–20, 2024

P.2 Kaiming Cheng, **Arkaprabha, Bhattacharya**, Michelle Lin, Jaewook Lee, Aroosh Kumar, Jeffery F Tian, Tadayoshi Kohno, and Franziska Roesner. When the User Is Inside the User Interface: An Empirical Study of UI Security Properties in Augmented Reality. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 2707–2723, 2024

2023 P.1 Peter Ney, **Arkaprabha, Bhattacharya**, Luis Ceze, Karl Koscher, Tadayoshi Kohno, and Jeff Nivala. Cybersecurity across the dna-digital boundary: Dna samples to genomic data. In *Cyberbiosecurity: A New Field to Deal with Emerging Threats*, pages 95–114. Springer, 2023

2022 P.1 Peter Ney, **Arkaprabha Bhattacharya**, David Ward, Luis Ceze, Tadayoshi Kohno, and Jeff Nivala. Doctoring Direct-to-Consumer Genetic Tests with DNA Spike-Ins. *bioRxiv*, 2022

RESEARCH EXPERIENCES

2024 – **Cornell University**, Research Assistant
Faculty Advisors: Prof. Nicola Dell & Prof. Tom Ristenpart
Additional Collaborators: Dr. Kevin Lee, Dr. Rosanna Bellini, Alaa Daffalla
Researching topics in computer security, trust and safety, and human-computer interaction.

- Lead a measurement study surveying account security interfaces on 100 services.
- Leading a project surveying vulnerabilities of account remediation tools and advice.

2023 – 24 **JP Morgan Chase**, Senior Research Associate
Supervisor: Dr. Jessica Staddon
Additional Collaborators: Dr. Rosanna Bellini, Dr. Kevin Lee, Simran Lamba, Vineeth Ravi
Started and collaborated on research projects in user safety, security, and privacy in the context of consumer finance.

- Built an automated pipeline for assessing consumer privacy concerns with banking services.

2021 – 22 **University of Washington**, Research Assistant
Faculty Advisors: Prof. Franziska Roesner & Prof. Tadayoshi Kohno
Additional Collaborators: Dr. Kaiming Cheng
Developing a testbed to explore vulnerabilities in Augmented Reality technologies.

- Performed a systematic analysis on the sets of properties of AR systems that could play into the threat model of current and future AR development and systems.
- Developed sample test applications for ARCore, ARKit, and WebXR platforms to test various properties of AR systems. Used these test applications to rigorously test the outcome of certain properties that could inform future compromises.
- Creating proof-of-concept compromises using the results from our aforementioned testbed to highlight the importance of considering the handling of these properties in AR platforms and inform future development standards and practices.

2022 **JP Morgan Chase**, Summer Research Associate
Supervisor: Dr. Jessica Staddon
Additional Collaborators: Dr. Rosanna Bellini, Dr. Kevin Lee, Vineeth Ravi
Spearheaded research project to better understand financial abuse caused by intimate partners. Collaborated with a cross-functional team of external academics, NLP and User Safety researchers, and leaders in fraud/risk domains.

- Drew from prior work to use sentence transformer models and unsupervised non-hierarchical and density-based clustering techniques to understand how language models can identify the complexities of financial abuse by an intimate partner.
- Developed a set of rigorous labelling guidelines to label over 4000 complaints for financial abuse and financial abuse by intimate partners in consumer complaint narratives for a dataset for future research. Found 527 positively labeled instances of financial abuse by an intimate partner described in CFPB data.

2019–21 **University of Washington**, Research Assistant
Faculty Advisors: Prof. Luis Ceze, & Prof. Tadayoshi Kohno
Additional Collaborators: Dr. Peter Ney, Dr. Jeff Nivala
Engineered the first experimental Trojan Horse attack on a DNA sequencer. Explored the integrity of Genetic Inference Systems as a Mary Gates Research Scholar.

- Worked with collaborators to create a rigorous threat model that considers novel vectors of communication that bypass airgaps and are unique to molecular processing and wetlab systems.
- Used notions from aforementioned threat model to create a proof of concept Trojan that used commands and data encoded in physical DNA molecules. This work is awaiting publication.
- Explored the integrity and robustness of genetic inference models used for services such as Direct-To-Consumer (DTC) genetic testing and DNA phenotyping.
- Collaboratively identified the possibility of modifying Single Nucleotide Polymorphisms to drastically change the predictions presented by DNA phenotyping and genetic testing models. This work is currently on bioRxiv (P.1).

ADDITIONAL PROFESSIONAL EXPERIENCES

2022 **NVIDIA**, Software Engineering Intern
Improving and maintaining driver systems for NVIDIA's GPU stack.

- Lead the design of a fuzzing interface to fuzz communication channels between NVIDIA drivers and GPU resources. Set up the baseline for implementation of this fuzzer.
- Resolved versioning and communications issues pertaining to the introduction of new hardware in newer NVIDIA GPU architectures.

2021 **Microsoft**, Software Engineering Intern
Hardening authentication protocols in enterprise Windows systems.

- Developed and tested a feature to improve security of enterprise authentication workflows by switching the authentication handshake to use the Kerberos cryptographic protocol.
- Discovered, reported, and addressed a critical security vulnerability pertaining to authentication.

HONORS AND AWARDS

2025 Digital Life Initiative (DLI) Fellow 2024-2025

2021 Mary Gates Research Scholar (University of Washington)

INVITED TALKS

2022 **Using Large Language Models to understand Consumer Financial Protection Bureau complaints of Intimate Partner Financial Abuse.**
User Safety in AI and Finance Workshop (USAIF) 2022 (11/02/2022)
https://sites.google.com/view/usaif22/program

TEACHING EXPERIENCE

2025 **CS 5682 HCI and Design**
Teaching Assistant for Profs. Nicola Dell and Thijs Roumen, Cornell University

2024 **CS 5433 Blockchains, Cryptocurrencies, and Smart Contracts**
Teaching Assistant for Prof. Ari Juels, Cornell University

2021 **CSE P 590 A**
Teaching Assistant for Adam Shostack, University of Washington

2021 **CSE 484 Computer Security**
Teaching Assistant for Tadayoshi Kohno, University of Washington

Updated March 2026