Muhammad Ahmad Bashir (Curriculum Vitae)

Postdoctoral Research Fellow
International Computer Science Institute (ICSI)
1947 Center Street, Ste. 600
Berkeley, CA 94704

Email: mahmad@icsi.berkeley.edu
www: https://ahmadbashir.com
in: linkedin.com/in/mahmadb

Research Interests

Security & Privacy on Web/Mobile; Limiting Fraud & Abuse; Internet Measurement; Trust and Safety

Education

Ph.D. in Computer Science - Northeastern University, Boston, MA 2014 - 2019
B.S. in Computer Science - LUMS, Lahore, Punjab, Pakistan 2008 - 2012

Relevant Courses: Machine Learning, Advanced Algorithms, Computer Security, Intensive Computer Systems

Professional Experience

International Computer Science Institute - Postdoctoral Research Fellow — OCT 2019 - Present

I drive multiple research projects in the area of security and privacy. A key part of these projects involves forming new collaborations and mentoring undergraduate and graduate students.

Facebook Inc. - Security Engineering Intern / Threat Infrastructure — JUN 2017 - SEP 2017

I worked with Facebook's ThreatExchange platform to build a recommendation engine for the threat-intelligence data. Through this tool, participating companies can discover new threats (Indicators of Compromise) that are similar to the ones they have already faced.

Facebook Inc. - Security Engineering Intern / Online Safety — May 2016 - Aug 2016

I worked with Facebook's internal investigators to build tools that were used to discover abuse on the platform and protect vulnerable people by identifying harmful actors.

Max Planck Institute for Software Systems, Saarbrucken, Germany - Research Intern — OCT 2012 - JAN 2013

Developed techniques to detect 'tampered' computations in Online Social Networks. For example, a Twitter user with a majority of 'bought' followers or a Yelp business with a majority of fake reviews. Detected abuse on Twitter, Yelp, and Facebook. Collected and worked with public data of 300M Twitter users, 30K Yelp businesses with 341K business reviews, and more than 50K Facebook users.

Key Skills

Programming Languages: Python JavaScript SQL Java Hack C++ R MATLAB
Web Development: Nodejs Express React Django HTML5 CSS jQuery
Miscellaneous: SPARK Web Automation (e.g., Selenium) Browser Extension Development

Selected Research Projects / Publications

Cross Site Tracking via First Party Cookies — Ongoing

Large-Scale Analysis of Cross Device Tracking — Ongoing

Differentiating between Permissions Accessed by the APP and the SDKs — Ongoing

A Longitudinal Analysis of the ads.txt Standard — IMC '19

- Conducted a 15-month long study to analyze the adoption of the ads.txt advertising standard.
- Data from this study, spanning more than 200K websites, is made publicly available.
- Currently working on expanding this study to the mobile apps as well.

Evaluating User Interest Profiles Using Ad Preference Managers — NDSS '19

- A Large-scale study of the "interests" inferred by ad networks using Ad Preference Managers.
- 220 users contributed their 'interest' data from popular ad preference managers (e.g., Facebook, Google) and participated in a survey via a browser extension I developed.
- This study investigates how user interests are inferred and how useful they are according to the users. It also highlights they key limitations of pervasive tracking and targeted advertisements.

How Tracking Companies Circumvented Ad Blockers Using WebSockets — IMC '18

- This study investigates how certain tracking companies abused a bug in Chrome's *WebRequest* API to bypass ad and tracker blocking extensions.
- Conducted a longitudinal study on top-100K websites before and after the bug was patched.

Diffusion of User Tracking Data in the Online Advertising Ecosystem — PETS '18

- Proposed a novel graph structure to represent the advertising graph and modeled how user tracking data propagates in the advertising ecosystem via *Real Time Bidding (RTB)* auctions.
- Through my graph model, I demonstrated how user information is shared among ad networks even when the user is using popular ad and tracker blocking extensions.
- This work received *Best Student Paper* award in a national competition.

Tracing Information Flows Between Ad Exchanges Using Retargeted Ads — USENIX SECURITY '16

- Proposed a novel methodology to detect information-sharing between ad networks.
- Detected 31% of information-sharing partners which were missed by prior methods.

Detection of Anomalous User Behavior in Online Social Networks — COSN '15 & USENIX SECURITY '14

- Developed techniques to detect 'tampered' computations in OSNs. For example, a Twitter user with a majority of 'bought' followers or a Yelp business with a majority of fake reviews.
- Detected abuse on Twitter, Yelp, and Facebook. Collected and worked with public data of 300M Twitter users, 30K Yelp businesses (341K reviews), and more than 50K Facebook users.

Honors & Awards

1. **Privacy Papers for Policymakers Award –** Future of Privacy Forum — 2019
2. **Best Paper Award –** Conference on Online Social Networks — 2015
3. **Best Paper Award –** Conference on Security and Cryptography — 2015
4. **Best Senior Year Project –** Ericsson – PTA Mobile Excellence Award — 2011