Curriculum Vitae — Muhammad Ikram, PhD

Interests	I am passionate about data-driven analysis of online privacy & security issues and abuses in networked systems. I am keen in using statistical methods to derive salient features and use applied machine-learning algorithms to auto-detect these issues and abuses for vetting and correcting purposes.
Online Presence	Homepage, @Google Scholar, & @LinkedIn

Education

09/2014 – 05/2018 — **PhD in Electrical and Telecommunication Engineering**, UNSW, Australia.
- *Thesis*: Analysis and design of secure and privacy preserving systems. Mentor: **Mohamed Ali (Dali) Kaafar**

03/2008 – 02/2010 (GPA: 4.06/4.5) — **M.Sc in Computer Engineering**, *Ajou University*, Korea.
- *Thesis*: Design and analysis of a resource- and energy-efficient surveillance scheme for wireless sensor networks. Mentor: **Ki Hyung Kim**

12/2002 – 03/2007 (GPA: 3.71/4.0) — **B.Sc in Computer Systems Engineering**, *UET Peshawar*, Pakistan.
- *Project*: Simulation and implementation of CDMA transceiver with advanced access control mechanisms using MATLAB and field programmable graphics arrays. Mentor: **Mustafa Bari**

Professional experience

07/2018 – to date — **Postdoc Research Fellow**, *Censored Planet, University of Michigan*, Ann Arbor, USA.
- Designed and deployed systems to analyze server-side blocking and discriminations at scale
- Analyzed and characterized facets of blocking (or censorship) in Russia
- Analyzed and characterized the security and privacy issues of URL-shorters' redirections

09/2018 – to date — **Postdoc Research Fellow**, *Optus MQ Cyber Security Hub*, Sydney, Australia.
- Designing systems to characterize the security and privacy issues related to mobile apps' resource-loading
- Designing systems to analyze suspicious redirects of web traffic and prevent the inflicted harms
- Implemented systems to reveal vulnerabilities of network service libraries/APIs in iOS apps

10/2018 – to date — **Visiting Scientist**, *Data61, CSIRO*, Sydney, Australia.
- Research and development on optimizing the balance of data privacy and utility in the context of differential privacy

01/2018 – 09/2018 — **Research Associate**, *Optus Macquarie University Cyber Security Hub*, Sydney, Australia.
- Designed and analyzed testbed for investigating security and privacy issues in mobile applications
- Analyzed graph-features of Android malware and designed ML-based scheme to detect malicious application in the wild
- Tutored PenTesting course: "COMP350 Special Topics in Computing and Information Systems"

09/2014 – 06/2018 — **Graduate Researcher**, Networks Group, CyberPhysical Systems Research Program, Data61-CSIRO, Australia.
- Modeled and implemented an obfuscation resilient tool for detecting Android malware via behavior modeling of weighted directed Android API call graph
- Designed analysis framework for longitudinally analysis of invisible structures and information aggregation revealed through DNS
- Designed and implemented data-analysis framework to comprehensively analyzed characterize sellers, buyers, and services of prominent underground marketplaces that involved in eCrime activities.
- Analyzed the inefficiencies of state-of-the art spam detection systems and proposed as well as validated an NLP and machine-learning based system to efficiently detect (and prevent) even the most trickiest and stealthy spammer
- Designed and implemented obfuscation-resilient malware detection framework to detect polymorphic malicious activities in softwares such as Android apps.
- Designed and implemented a data-analysis and intelligence framework to retrieve and (Temporal-longitudinally) analyze malware in the wild.
- Designed and implemented an analysis framework to analyze privacy preserving systems for the Web and proposed as well as validated a machine-learning based systems with improved usability and efficiency.
- Designed and implemented data-collection and analysis framework to analyze security and privacy risks of security-promising systems (e.g., Android VPN apps and Ad-Blocking apps).

05/2014 – 08/2014 — **Software Engineer**, *Network Research Lab (NRL) NICTA*, Sydney, Australia.
- Implemented an analysis framework to extract syntactic and semantic features from JavaScript programs collected from Alexa's top 5K websites.

05/2013 – 12/2013	**Software Engineer**, *STU, Umm Al Qura University*, Makkah, Saudi Arabia. ○ Designed and implemented crowd sensing system to monitor crowd behavior in Hajj–one of the largest religious gatherings.
02/2010 – 01/2013	**Research Engineer**, *Peer-to-Peer Networks*, Technische Universität Darmstadt, Germany. ○ Implemented monitoring systems to analyzing security and resiliency of p2p-based services. ○ Contributed to research activities in QuaP2P (www.quap2p.de) project to benchmark security (attacks and countermeasures) against p2p-based systems.
11/2009 – 01/2010	**Software Engineer**, *GStorm*, Seoul, Korea. ○ Ported multi-media codec for Samsung Galaxy mobile phone at GStorm from propriety multi-media applications to Android OS.
07/2008 – 08/2008	**Software Engineer**, *Lanbrid Company*, Seoul, Korea. ○ Implemented security solutions, mainly IPSec, in network service processors i.e., propriety gateways and routers.
03/2008 – 01/2010	**Research Assistant**, *Information and Communication Security Lab*, Seoul, South Korea. ○ Programmed sensor node and deployed surveillance applications in sensor networks and collected multimedia monitored data. ○ Proposed efficient relay node placement scheme for two-tiered wireless sensor networks.
03/2007 – 03/2008	**Lab Instructor**, *DCSE, University of Engineering and Technology*, Peshawar, Pakistan. ○ Conducted lab courses including embedded system programming, Java-based object oriented software development, and image processing.

Selected publications (Complete list @GScholar)

Peer-reviewed publications

1) **Muhammad Ikram**, Rahat Masood, Gareth Tyson, Mohamed Ali Kaafar, Roya Ensafi, "The Chain of Implicit Trust: An Analysis of the Web Third-party Resources Loading", submitted to the World Wide Web (WWW), 2019.

2) Jingxiu Su, Zhenyu Li, Stephane Grumbach, **Muhammad Ikram**, Kave Salamatian and Gaogang Xie, "A Cartography of Web Tracking using DNS Records", in Journal of Computer Communications, 2018.

3) Jingxiu Su, Zhenyu Li, Stephane Grumbach, **Muhammad Ikram**, Kave Salamatian and Gaogang Xie, "Web Tracking Cartography with DNS Records", in International Performance Computing and Communications Conference (IPCCC), 2018.

4) Rahat Masood, Dinusha Vatsalan, **Muhammad Ikram** and Muhammad Ali Kaafar, "Incognito: A Method for Obfuscating Web Data", in proceeding of World Wide Web (WWW), 2018.

5) **Muhammad Ikram** and Mohamed Ali Kaafar, "A First Look at Mobile Ad-Blocking Apps", in proceeding of IEEE Network Computing and Applications (NCA), 2017.

6) **Muhammad Ikram**, Lucky Onwuzurike, Shehroze Farooqi, Emiliano De Cristofaro, Arik Friedman, Guillaume Jourjon, Mohamed Ali Kaafar, M. Zubair Shafiq, "Measuring, Characterizing, and Detecting Facebook Like Farms", in issue of ACM Transaction on Privacy and Security (TOPS), 2017.

7) **Muhammad Ikram**, Hassan Jameel Asghar, Mohamed Ali Kaafar, Balachander Krishnamurthy, and Anirban Mahanti, "Towards Seamless Tracking-Free Web: Improved Detection of Trackers via One-class Learning", in proceeding of Privacy Enhancing Technology Symposium (PETS), 2017.

8) Shehroze Farooqi, **Muhammad Ikram**, Emiliano De Cristofaro, Arik Friedman, Guillaume Jourjon, Mohamed Ali Kaafar, M. Zubair Shafiq, Fareed Zaffar, "Characterizing Key Stakeholders in an Online Black-Hat Marketplace", in proceeding of IEEE APWG Symposium on Electronic Crime Research (eCrime), 2017.

9) **Muhammad Ikram**, Narseo Vallina Rodriguez, Suranga Seneviratne, Mohamed Ali Kaafar, Vern Paxson, "An analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps", in proceeding of ACM SIGCOMM Internet Measurements Conference (IMC), 2016.

10) **Muhammad Ikram**, Hassan Asghar, Mohamed Ali Kaafar and Anirban Mahanthi, "On the Intrusiveness of JavaScript on the Web", Conference on emerging Networking EXperiments and Technologies (CoNEXT), 2014.

Technical Reports	1) Shehroze Farooqi, **Muhammad Ikram**, Emiliano De Cristofaro, Arik Friedman, Guillaume Jourjon, Mohamed Ali Kaafar, M. Zubair Shafiq, Fareed Zaffar, "The 1%: Identification and Role of Key Stakeholders in a Black-Hat Marketplace", 2017.
	2) **Muhammad Ikram**, Lucky Onwuzurike, Shehroze Farooqi, Emiliano De Cristofaro, Arik Friedman, Guillaume Jourjon, Mohammad Ali Kaafar, M. Zubair Shafiq, "Combating Fraud in Online Social Networks: Detecting Stealthy Facebook Like Farms", 2016.
	3) Shehroze Farooqi, **Muhammad Ikram**, Emiliano De Cristofaro, Arik Friedman, Guillaume Jourjon, Mohamed Ali Kaafar, M. Zubair Shafiq, Fareed Zaffar, "Characterizing Seller-Driven Black-Hat Marketplaces", 2015.
Under Review Papers	1) **Muhammad Ikram**, Benjamin Zi Hao Zhao, Hassan Asghar, Mohamed Ali Kaafar, "A Decade of Mal-Activity Reporting: A Retrospective Analysis of Internet Malicious Activity Blacklists", Asia Computer Communication and Security (AsiaCCS), 2019.
	2) Zhushou Tang, Sen Chen, Ke Tang, Minhui Xue, **Muhammad Ikram**, Yuan Tian, Tielei Wang, and Haojin Zhu, "iOS, Your OS, Everybody's OS: Vetting and Measuring Network Services of iOS Apps", Computer Communication and Security (CCS), 2019.
	3) **Muhammad Ikram**, Pierrick Beaume, and Mohamed Ali Kaafar, "DaDiDroid: An Obfuscation Resilient Tool for Detecting Android Malware via Behavior Modeling of Weighted Directed Call Graph", Security and Cryptography (Secrypt), 2019.

In Media

News Papers	1) My research work: "An analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps" was featured by the top tech news websites and media outlets: Electronic Frontier Foundation (EFF), SlashDot, Security Week, ZDNet (1, 2), ITwire, ArsTechnica, LifeHacker, Digital Trends, ABC News, and number of others (Full list of URLs to media coverage).
	2) Due to my research project, the VPN apps' developers leverage on third-party security auditors to ensure security/privacy claims and tighten the security to thwart potential abusers or malicious actors, more details.
	3) My comprehensive analysis of security and privacy issues in mobile VPN apps triggered user awareness and a complaint has been registered at Federal Trade Commission (FTC), US, to address and regulate the abusive methods employed in HotSpot Shield Free VPN app by AnchorFree.
	4) My research work "Combating fraud in online social networks: detecting stealthy Facebook Like Farms" was featured by The Register.

Honors and Awards

07/2018 – to date	**OTF Fellowship (250K USD)**, *grated by OTF to investigate server-side discriminations at scale.*
10/2018 – 09/2018	**Travel Grant (2K USD)**, *granted by OTF to attend and present my research project at OTF-Summit in Taiwan.*
09/2014 – 01/2018	**PhD Scholarship (Tuition Fee and Monthly Stipend)**, *granted by UNSW and Data61-CSIRO.*
07/2017 – 07/2017	**Student Travel Grant (2.5K USD)**, *granted by Data61-CSIRO and UNSW*, for attending PETS'17.
07/2017 – 07/2017	**Student Travel Grant (2.5K USD)**, *granted by Data61-CSIRO and UNSW*, for attending SOUPS'17.
09/2016 – 09/2016	**Student Travel Grant (1.5K USD)**, *granted by Data61-CSIRO and UNSW*, for IMC'16.
10/2015 – 11/2015	**Student Travel Grant (1.5K USD)**, *granted by ACM and NICTA*, for attending IMC'15.
03/2008 – 01/2010	**M.Sc Scholarship Stipend (20K USD))**, *granted by IITA*, ministry of IT, South Korea.
03/2008 – 01/2010	**M.Sc Scholarship Tuition Fee Scholarship**, *granted Ajou University*, South Korea.
03/2002 – 03/2007	**Position Holder Scholarship**, *secured top position (1%) in B.Sc Engineering*, granted by UET, Peshawar, Pakistan.

03/2002 – 03/2007	**B.Sc Tuition Fee and Stipend Scholarship**, *granted got 3rd position out of 50K+ students in intermediate school exams*, granted by BISE Mardan, Pakistan.
03/2002 – 03/2007	**Position Holder Bronze Medal and Scholarship**, *got 3rd position out of 50K+ students in intermediate school exams*, granted by BISE Mardan, Pakistan.

Mentoring and Advising Students

Master Theses

1) Kieran Wouterlood, Implementation and analysis of Machine-learning based Ad-Blocking plugin for Web platform, Oct. 2018. (co-advised with Prof. Muhammad Ali (Dali) Kaafar at Macquarie University)

2) Hasina Rahman, A data-driven analysis tool to investigate Content dependencies and Chains of malicious content injection on the Web, Oct. 2018. (co-advised with Prof. Muhammad Ali (Dali) Kaafar at Macquarie University)

3) Ben Zhou, Longitudinal Analysis of Malicious Activities on the Web, Dec., 2017. (co-advised with Prof. Muhammad Ali (Dali) Kaafar at Data61)

4) Malcolm Parsons, Security Analysis of Peer-to-Peer Overlays, Dec., 2011. (co-advised with Prof. Thorsten Strufe at TU Darmstadt)

5) Carola Schwinn, Resilient Monitoring Scheme for Mobile Crowd Missions, Jan. 2013. (co-advised with Prof. Thorsten Strufe at TU Darmstadt)

6) Mohsen Amoorezaei, Cheating Resistant P2P-based Gaming Overlays, Feb. 2013. (co-advised with Prof. Thorsten Strufe at TU Darmstadt)

Bachelor Theses

1) Oleksi Donet, Evaluation and Improvement of Routing Table-based Countermeasures in KAD Networks, Oct. 2012. (co-advised with Prof. Thorsten Strufe at TU Darmstadt)

2) Sven Ferse, Evaluation and Improvement of Identity-based Countermeasures in Kad Networks, Oct. 2012. (co-advised with Prof. Thorsten Strufe at TU Darmstadt)

3) Michael Markert, Amplifying Eclipse Attacks versus structured Peer-to-Peer Networks, Oct. 2012. (co-advised with Prof. Thorsten Strufe at TU Darmstadt)

4) Johannes Schwandke, Comparative Robustness Study of a Peer-to-Peer based SynchroPhasor Network Middleware, Oct. 2012. (co-advised with Prof. Thorsten Strufe at TU Darmstadt)

Internees

1) Noha Liozon, The Chains of Implicit Trust: An Analysis of the Web Third-party Resources Loading, Dec. 2017. (co-advised with Prof. Muhammad Ali (Dali) Kaafar at Data61)

2) Pierrick Beaume, DaDiDroid: An Obfuscation Resilient Tool for Detecting Android Malware via Behavior Modeling of Weighted Directed Call Graph, Dec. 2017. (co-advised with Prof. Muhammad Ali (Dali) Kaafar at Data61)

Community Services

1) I reviewed papers submitted to conferences/journals: IEEE S&P'19, Usenix Security'19, AsiaCCS'17, PETS'14, , PETS'15, PETS'16, PETS'17, PETS'18, PETS'18, DSN'17, IMC'17, NSDI, Computer Communications, IEEE Transactions on Parallel and Distributed Systems, and AI4Mobile'19.

2) I volunteered to organize conferences: WoWMoM'14, CoNext'14, PAM'17.

3) I am a program committee member of IEEE International Workshop on Artificial Intelligence for Mobile, 2019.

Teaching and Instructing

1) **COMP350:** I instructed 'Special Topics in Computing and Information Systems - COMP350' at Macquarie University in S1-2018 where I helped students in conducting practical penetration testing.

2) **ENGG411, ENGG805/6 :** I mentored a group of two students toward their Master Theses at Macquarie University. The work involved from formalizing research ideas, execution of plan of action, and final thesis writing.

3) I designed and taught Peer-to-Peer Networks Exercise in Winter Semester course at TU Darmstadt, Germany in WS 2011/2012.

4) Digital Signal Processing in Summer and Winter Semesters, 2007/08 at the Department of Computer System Engineering, University of Engineering and Technology, Peshawar, Pakistan.

References

○ **Mohamed Ali (Dali) Kaafar,** Group Leader, Information Security Group, Macquarie University and CSIRO-Data61. Email: Dali.Kaafar@data61.csiro.au.

○ **Roya Ensafi,** Research Assistant Professor, Computer Science & Engineering, University of Michigan, USA. Email: ensafi@umich.edu.

○ **Vern Paxson,** Professor, International Computer Science Institute (ICSI) and UC Berkeley, Berkeley, California, USA. Email: vern@icir.org

○ **Zubair Shafiq,** Assistant Professor, Dept. of Computer Science, The University of Iowa, USA. Email: zubair.shafiq@uiowa.edu.