

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](#) @Data-CSIRO, [@Google Scholar](#), & [@LinkedIn](#)

Education

- 09/2014 – 05/2018 **PhD in Electrical and Telecommunication Engineering**, UNSW, Australia.
 o *Thesis*: Analysis and Design of secure and privacy preserving systems. Advisor: **Mohamed Ali (Dali) Kaafar**
- 03/2008 – 02/2010 **M.Sc in Computer Engineering**, Ajou University, Korea.
 (GPA: 4.06/4.5) o *Thesis*: Design and analysis of a resource- and energy-efficient surveillance scheme for wireless sensor networks. Advisor: **Ki Hyung Kim**
- 12/2002 – 03/2007 **B.Sc in Computer Systems Engineering**, UET Peshawar, Pakistan.
 (GPA: 3.71/4.0) o *Project*: Simulation and implementation of CDMA transceiver with advanced access control mechanisms using MATLAB and field programmable graphics arrays. Advisor: **Mustafa Bari**

Professional experience

- 07/2018 – to date **Postdoctoral Scholar**, *Censored Planet*, University of Michigan, Ann Arbor, USA.
 o Analyzing server-side blocking in the wild
- 01/2018 – to date **Research Assistant (part-time)**, *Optus Macquarie University Cyber Security Hub*, Sydney, Australia.
 o Designed and analyzed testbed for investigating security and privacy issues in mobile applications
 o Analyzed graph-features of Android malware and designed ML-based scheme to detect malicious application in the wild
 o Tutored PenTesting course: "COMP350 Special Topics in Computing and Information Systems"
- 09/2014 – to date **Graduate Researcher**, Networks Group, CyberPhysical Systems Research Program, Data61-CSIRO, Australia.
 o Modeled and implemented an obfuscation resilient tool for detecting Android malware via behavior modeling of weighted directed Android API call graph
 o Design analysis framework for longitudinally analysis of invisible structures and information aggregation revealed through DNS
 o Designed and implemented data-analysis framework to comprehensively analyzed characterize sellers, buyers, and services of prominent underground marketplaces that involved in eCrime activities.
 o Empirically 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
 o Designed and implemented obfuscation-resilient malware detection framework to detect polymorphic malicious activities in softwares such as Android apps.
 o Designed and implemented a data-analysis and intelligence framework to retrieve and (Temporal-longitudinally) analyze malware in the wild.
 o 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.
 o 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.
 o 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.
 o 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.
 o Implemented monitoring systems to analyzing security and resiliency of p2p-based services.
 o 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.
 o 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)

Under Review Papers

- 1) Benjamin Zi Hao Zhao, **Muhammad Ikram**, Hassan Jameel Asghar, Abdelberi Chaa-bane, Kanchana Thilakarathna and Mohamed Ali Kaafar, "A Decade of Mal-activity: A Retrospective Analysis of Internet Malicious Activities", ACM IMC, 2018.
- 2) Noha Loizon, Rahat Masood, **Muhammad Ikram**, Gareth Tyson, and Mohamed Ali Kaafar, "The Chains of Implicit Trust: An Analysis of the Web Third-party Resources Loading", IMC, 2018.
- 3) Jingxiu Su, Zhenyu Li, Stephane Grumbach, **Muhammad Ikram**, Kave Salamatian and Gaogang Xie, "Web Tracking Cartography with DNS records", GlobeCom, 2018.

Peer-reviewed publications

- 1) Rahat Masood, Dinusha Vatsalan, **Muhammad Ikram** and Dali Kaafar, "Incognito: A Method for Obfuscating Web Data", WWW, 2018.
- 2) **Muhammad Ikram** and Mohamed Ali Kaafar, "A First Look at Ad-Blocking Apps on Google Play", IEEE NCA, 2017.
- 3) **Muhammad Ikram**, Lucky Onwuzurike, Shehroze Farooqi, Emiliano De Cristofaro, Arik Friedman, Guillaume Jourjon, Mohamed Ali Kaafar, M. Zubair Shafiq, "Combating Fraud in Online Social Networks: Measuring, Characterizing, and Detecting Facebook Like Farms", ACM TOPS, 2017.
- 4) **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", PETS, 2017.
- 5) 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", eCrime, 2017.
- 6) **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", ACM IMC, 2016.
- 7) **Muhammad Ikram**, Hassan Asghar, Mohamed Ali Kaafar and Anirban Mahanthi, "On the Intrusiveness of JavaScript on the Web", CoNEXT, 2014.

Technical Reports

- 1) Pierrick Beaume, **Muhammad Ikram**, and Mohamed Ali Kaafar, "DaDiDroid: An Obfuscation Resilient Tool for Detecting Android Malware via Behavior Modeling of Weighted Directed Call Graph", To be submitted to NDSS'18.
- 2) 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", <https://arxiv.org/abs/1506.00507>, 2017.
- 3) **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", <https://arxiv.org/abs/1506.00506>, 2016.
- 4) 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", <https://arxiv.org/abs/1505.01637>, 2015.

Security/Privacy Analysis Tools/Skills

Languages Python, JavaScript, Java, R, and BashScript

Platforms Linux, Mac OS X, Android OS, Contiki and TinyOS for Sensor Networks

Libraries/APIs Matplotlib, SciPy, Sklearn, Pandas, NumPy, BeautifulSoup, Scapy

Favorite Tools Eclipse, NetBeans, Android SDK, Kile, XCode, RStudio

Honor and Recognition

- In Media**
- 1) Our ACM SIGCOMM IMC'16 paper: "An analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps" and my proposal "Combating fraud in online social networks: detecting stealthy Facebook Like Farms" have attracted a significant media coverage in the top tech news websites and media outlets such as Electronic Frontier Foundation (EFF), ABC News, ZDNet, CIO Australia, itwire, The Register UK, LifeHacker, Yahoo News, Gizmodo Australia, and number of other [websites](#).
 - 2) Due to our 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) Our comprehensive analysis of security and privacy issues in mobile VPN apps triggered user awareness. 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, more [details](#).

09/2014 – 01/2018 **PhD Scholarship**, granted by UNSW and Data61-CSIRO.

07/2017 – 07/2017 **Student Travel Grant**, granted by Data61-CSIRO and UNSW, for PETS'17 & SOUPS'17.

09/2016 – 09/2016 **Student Travel Grant**, granted by Data61-CSIRO and UNSW, for IMC'16.

10/2015 – 11/2015 **Student Travel Grant**, granted by ACM and NICTA, for IMC'15.

03/2008 – 01/2010 **M.Sc Scholarship**, granted by IITA and Ajou University.

03/2002 – 03/2007 **Position Holder Scholarship**, secured top position (1%) in B.Sc eng., granted by UET, Peshawar, 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.

References

- **Mohamed Ali (Dali) Kaafar**, Group Leader, Information Security Group, Macquarie University and CSIRO-Data61. Email: Dali.Kaafar@data61.csiro.au.
- **Aruna Seneviratne, PhD**, Research Director, Connecting To The World Research Program, Data61-CSIRO. Email: Aruna.Seneviratne@data61.csiro.au.
- **Hassan Jameel Asghar** Research Scientist, Information Security Group, Macquarie University. Email: Hassan.Asghar@mq.edu.au
- **Zubair Shafiq** Assistant Professor, Dept. of Computer Science, The University of Iowa, USA. Email: zubair.shafiq@uiowa.edu.
- **Narseo Vallina-Rodriguez** Research Scientist, Networking and Security Group, International Computer Science Institute (ICSI), Berkeley, California, USA and Assistant Research Professor at IMDEA Networks, Madrid, Spain. Email: narseo@icsi.berkeley.edu or narseo.vallina@imdea.org.
- **Emiliano De Cristofaro, PhD**, Associate Professor, Dept. of Computer Science, University College London, United Kingdom. Email: e.decrisofaro@ucl.ac.uk