Yazan Boshmaf

+974 5060 4467
yboshmaf@hbku.edu.qa
boshmaf.github.io

Summary

I'm a research scientist who's passionate about tackling real-world problems and developing practical solutions. I equally enjoy writing academic papers and software code. I'm interested in the security and privacy of social and information networks, focusing on problems that impact the way people use technology and the Internet.

Education

2009–2015 **Ph.D. Computer Engineering**, *University of British Columbia*, Vancouver, Canada.
Thesis: Security Analysis of Malicious Social Bots on the Web.

2006–2008 **M.Sc. Information Technology**, *University of Stuttgart*, Germany.
Thesis: Design and Analysis of a Partial Application Configuration Algorithm for Pervasive Computing Environments using 3PC PCOM Middleware.

2001–2005 **B.Sc. Computer Engineering**, *Jordan University of Science and Technology*, Jordan.
Thesis: Proximity-based e-Coupon Delivery Platform for Bluetooth-enabled Smartphones.

Experience

June 2016 – Now **Scientist**, *Qatar Computing Research Institute, HBKU*, Doha, Qatar.
I joined the Cyber Security group under Ting Yu to lead a number of research projects on topics that are especially important to Qatari stakeholders. As such, my research is quite diverse tackling problems in applied cryptography, Web security, anonymity networks, and blockchain technology.

Jun 2015 – May 2016 **Software Engineer**, *Hootsuite*, Vancouver, BC, Canada.
I joined the Labs team to develop new products, experiment with emerging technologies, and promote lean innovation. As a full stack engineer, I worked with a wide array of tech stacks, languages, and frameworks, spanning from low-level backend services to high-level frontend designs.

Jun–Aug 2014 **Research Intern**, *Microsoft*, Mountain View, USA.
I joined the Distributed Systems team under Mihau Budui to work on sketching algorithms for interactive exploration of large datasets.

Sep–Nov 2013 **Research Intern**, *Telefonica*, Barcelona, Spain.
As part of my PhD research, I joined the Distributed Systems group under Dionysios Logothetis to work on fake account detection in online social networks.

Sep–Nov 2012 **Research Intern**, *Facebook*, Menlo Park, CA, USA.
I joined the Site Integrity team under Yuchun Tang to work on IP address reputation and botnet detection in online social networks.

May–Aug 2012 **Research Intern**, *Sophos*, Vancouver, BC, Canada.
I joined Sophos Labs team under David Cornell to work on ML-based malware detection and signature generation for fast and robust binary classification in endpoint security solutions.

Sep 2008 – Aug 2009 **Research Intern**, *High Performance Computing Center (HLRS)*, Stuttgart, Germany.
I joined the Scalable Computing and Coupled Systems group under Rolf Rabenseifner to work on vectorized Lattice Boltzmann numerical methods on a massively-parallel GPU cluster using CUDA.

Sep 2007 – Aug 2008 **Research Engineer (Outsourced)**, *SAP*, Walldorf, Germany.
I joined the TREX team under Franz Faerber to work on vectorized decompression of in-memory data structures for business intelligence search engines.

Sep 2007 – Aug 2008 **Software Engineer**, *Intel*, Walldorf, Germany.
I joined SAP Onsite Engineering team to analyze the performance and optimize the implementation of SAP NetWeaver. I reported performance bugs in Intel C/C++ Compiler to Intel Compiler team and evangelized Intel software tools and technologies to the software community at SAP.

Sep 2006 – Aug 2007 **Research Intern**, *University of Stuttgart*, Stuttgart, Germany.
As part of M.Sc. research, I joined the Distributed Systems group under Stephan Schuhmann to work on low-cost automatic configuration of component-based pervasive applications.

Nov 2005 – Aug 2006 **Infrastructure Consultant (Outsourced)**, *Microsoft*, Muscat, Oman.
I joined the Consulting Services division to help Nawras, an Omani mobile network operator, deploy Microsoft enterprise solutions and server infrastructure for mobile number portability across providers.

Jul 2005 – Aug 2006 **Network Engineer**, *Estarta Solutions*, Amman, Jordan.
I joined the Infrastructure team to provide Cisco and Microsoft solutions consultancy, networking and IP telephony solutions, software security auditing, and technical training to clients and partners.

Honours and Awards

Feb 2018 **Technology Fellowship Award**, *Katara Cultural Village Foundation*, Doha, Qatar.
The award includes an honorarium and is based on contributions to Katara Technology Forum.

Aug 2015 **Doctoral Dissertation Award – Honourable Mention**, *ACM SIGSAC*, Denver, CO, USA.
The award recognizes excellent research by PhD candidates in the field of computer and information security at the annual ACM CSS conference. My PhD dissertation was honourably mentioned as one of the top ten dissertations of the year.

Aug 2013 **Best Paper Award**, *IEEE/ACM ASONAM*, Niagara Falls, Canada.
The award includes an honorarium and recognizes the best paper at the conference

May 2012 **Research Internship Award**, *MITACS Accelerate*, Vancouver, BC, Canada.
$15,000 for four months of research internship at a Canadian company.

Dec 2011 **Outstanding Paper Award**, *ACSAC*, Florida, USA.
The award includes an honorarium and recognizes the best paper at the conference.

2009–2013 **Four Year Doctoral Fellowship**, *University of British Columbia*, Vancouver, Canada.
$22,000 per year plus tuition for the first four years of PhD studies.

2009–2013 **Faculty of Applied Science Award**, *University of British Columbia*, Vancouver, Canada.
$4,000 per year for the first four years of PhD studies.

2006–2008 **Outstanding Student Scholarship**, *University of Stuttgart*, Stuttgart, Germany.
Full tuition refund for the duration of M.Sc. studies.

2001–2005 **Royal Academic Sponsorship**, *Jordan University of Science and Technology*, Irbid, Jordan.
$1,700 plus tuition for the duration of B.Sc. studies.

Grants

2021–2022 **QNRF Technology Development Fund**, *Scalable Blockchain Security Analytics for the Masses*, Lead Principle Investigator, $70K for one year.

2020–2025 **QNRF National Priorities Research Program**, *A Secure End-to-End Blockchain-Based Solution to Finance Trade: The Legal, Technological, and Economic Framework*, Principle Investigator, $2.57M for five years.

2019–2022 **TÜBİTAK/QNRF Funding Program**, *A Defense-in-Depth Cyber Intelligence Platform to Defend against Emerging Cyber Attacks*, Principle Investigator, $1.65M for three years.

Systems

2019–Now **Dizzy+Toshi**, *Qatar Computing Research Institute*, Project Lead.
Patent-pending, ML-powered, systems for scalable blockchain security analytics. Dizzy and Toshi are currently used by the Financial and Electronic Crime Combating Unit at Qatar's Ministry of Interior to investigate cryptocurrency fraud and ransomware attacks. The systems have been selected by Qatar Research, Development, and Innovation Council for expedited commercialization.

2018 **BinSight**, *Qatar Computing Research Institute*, Project Member.
A cloud-based service for analyzing cryptographic API (mis)use in Android application. BinSight was used to analyze more than 120K apps in Google Play Store, focusing on those owned by key Qatari stakeholders. Several Qatari apps were flagged with severe security vulnerabilities and I worked with their security teams to fix and release patched versions.

2017 **Hemaya**, *Qatar Computing Research Institute*, Project Lead.
A data-driven security platform that is used by several projects at the Cyber Security group, including IPv4 scanning with Hemaya-IPs, malicious domain detection with Hemaya-Domains, and cyber security news aggregation and alerts with Hemaya-News.

2016 **VizFilt**, *Qatar Computing Research Institute*, Project Member.
An interactive data processing platform for analyzing Distributed Reflection Denial of Service (DrDoS) attacks. VizFilt was used to visualize, assess, and limit the impact of such attacks using honeypots deployed at Ooredoo, a Qatari Internet service provider.

2014 **Sketch-DB**, *Microsoft Research Silicon Valley*, Project Member.
A shared-nothing distributed DBMS extension to Sketch, which is a system for interactive exploration of large datasets using sketching algorithms. Sketch-DB was deployed on a MSSQL cluster, where it interactively computed analytics results (e.g., histograms) from 100s of terabytes of data which don't fit in the overall cluster memory. Sketch-DB is used internally at Microsoft to debug Azure server logs and analyze social media data for Microsoft Outlook.

2012–2013 **Íntegro**, *Telefonica Research*, Project Lead.
A patent-pending, scalable, and infiltration-resilient system for victim prediction and fake account detection in online social networks. Íntegro was deployed on production servers at Tuenti, the largest Spanish social network with more than 15 million users, where it delivered an AUC of 0.92, a 30% improvement over the used state-of-the art, in addition to orders of magnitude speedup in detection.

2012 **Huddle**, *Facebook*, Project Lead, Classified.
A scalable and robust defense system for IP address reputation and botnet detection in online social networks. Huddle was deployed on production servers at Facebook, where it delivered an additional 25% in detection sensitivity when compared to detection systems used by the Site Reliability team.

2012 **Augur**, *Sophos*, Project Lead.
An automated malware detection system that uses large-scale machine learning techniques to classify malware and generate malware signatures in Sophos Virus Definition Language. Augur was deployed on production servers at SophosLabs, where it achieved 99.99% specificity and 30% sensitivity in malware detection.

2007–2008 **SIMD-Scan**, *SAP and Intel*, Project Lead.
A software vectorization framework for decompressing in-memory data structures used in DBMS system. SIMD-Scan was deployed in TREX, SAP NetWeaver's search and classification engine, where it achieved up to 2.1x speedup when compared to a highly optimized sequential version.

2006–2007 **PCOM-PAC**, *University of Stuttgart*, Project Member.
A low-cost Partial Application Configuration (PAC) framework for component-based pervasive applications. PCOM-PAC was integrated into 3PC PCOM, a middleware for component-based pervasive computing, where it reduced the configuration latency by up to 66%.

Impact and Highlights

2016–2021 **Qatar Computing Research Institute**, *Leadership, Partnership, and Technology Transfer*.
- Started the Cybersecurity Initiative for Blockchain Research (CIBR), where I grew the team to eight affiliated researchers and engineers from different groups at QCRI and HBKU.
- Organized and hosted three CIBR workshops with more than 50 participants, including several key stakeholders. Each workshop included invited talks, a panel discussion, and a networking session.
- Led the effort to sign collaboration agreements with three major Qatari stakeholders, namely Ministry of Interior, Qatar Financial Center Regulatory Authority, and Qatar Central Bank, in addition to the United Nations Development Program and PeckShield.
- Led successful research collaborations with top universities (e.g., UC Berkeley, UBC).
- Along with Qatari stakeholders, released three systems out of which one is patent-pending and chosen by QRDI for expedited commercialization through its Technology Development Fund.
- Attracted international news coverage (e.g., WIRED, BBC), interviews (e.g., New Scientist, Al Jazeera), and invited talks (e.g., Qatar Central Bank, US FTC) about CIBR-related research.

Mar 2016 **Hootsuite**, *Leadership and Technology Transfer*.
Released Hootsuite Amplify, an employee advocacy app that resulted in millions of dollars in revenue.

Aug 2014 **Microsoft**, *Technology Transfer*.
Released Sketch-DB as part of Microsoft Outlook, adding social media intelligence to email content.

Nov 2013 **Telefonica**, *Technology Transfer*.
Released Íntegro as part of Tuenti Site Reliability Services, saving nearly €100K a year in person-hours for manual verification by Tuenti analysts.

Nov 2012 **Facebook**, *Partnership and Technology Transfer*.
- Released Huddle as part of Facebook Immune System, improving its overall effectiveness.
- Led the effort to sign partnerships with anti-malware companies to cleanup infected user machines.

Aug 2012 **Sophos**, *Technology Transfer*.
Released Augur as part of Sophos Labs Malware Detection System, resulting in faster response time to incidents and significant time savings in manual reverse engineering by malware engineers.

Sep 2008 **Intel**, *Partnership and Technology Transfer*.
- Released SIMD-Scan as part of SAP NetWeaver, which resulted in faster performance.
- Led the effort for added investment by SAP into Intel's server-grade hardware and software tools.

Selected Invited Talks and Guest Lectures

Sep 2019 **Cryptocurrency Analytics: Bitcoin versus Cyber Security**, *Invited Talk*, Department of Computer Science and Technology, Peking University, Beijing, China.
- A public presentation to the Computer Science community at Peking University.
- Host: Yao Guo, Associate Professor at Peking University.

Feb 2018 **Deanonymizing Dark Web Users Through Bitcoin Transaction Analysis**, *Invited Talk*, The U.S. Federal Trade Commission, Washington, DC, USA.
- An internal presentation through the Office of Technology Research and Investigation.
- Host: Dan Salsburg, Chief Counsel and Acting Chief, FTC Office of Tech Research & Investigation.

Feb 2018 **Introduction to Blockchain Technology**, *Invited Talk*, Katara Tech Forum, Doha, Qatar.
- An public presentation to the tech community at Katara, Qatar's cultural hub.
- Host: Taoufik Homri, Researcher, Katara Tech Forum.

March 2014 **Thwarting Fake Accounts in OSNs by Predicting their Victims**, *Invited Talk*, AAAI 2014 Spring Symposium Series, Stanford, USA.
- At the Social Hacking and Cognitive Security on the Internet and New Media track.
- Hosts: Rand Waltzman (Program Manger, DARPA) and Tim Hwang (Founder, PacSocial).

November 2012 **Protecting the Social Web From Large-Scale Malicious Automation**, *Invited Talk*, Humboldt Colloquium, Toronto, Canada.
- As an Early Career Researcher at the Theoretical Sciences Interdisciplinary Workshop, and under the theme of "Excellence in Research".
- Chair: Kevin Beach, University of Alberta.

June 2012 **Design and Analysis of a Social Botnet**, *Invited Talk*, SRI Int., Menlo Park, USA.
- At the The Infosec Technology Transition Council (ITTC), which is jointly organized by the U.S. Department of Homeland Security Science and Technology (S&T) Directorate and nonprofit research organization SRI International.
- Host: Ulf Lindqvist, Program Director, Computer Science Laboratory at Stanford Research Institute (SRI) International.

March 2012 **Socialbots: A Security Perspective**, *Guest Lecture*, University of Washington, WA, USA.
- Course: CSS 490B—Programming Social and Computational Intelligence for the Web.
- Host: Joe McMarthy, Assistant Professor, University of Washington.

May 2010 **Automated Social Engineering Attacks in Online Social Networks**, *Invited Talk*, Office of the Privacy Commissioner of Canada, Ottawa, Canada.
- Host: Andrew Patrick, IT Research Analyst, Office of the Privacy Commissioner of Canada.

Selected Research/Academic Services

Jul 2021 **Reviewer**, *Trans. on Dependable and Secure Computing*, IEEE TDSC.
Jan 2021 **Judge**, *Innovation Coupon Startup Fund*, QRDI Counsel.
Aug 2020 **Reviewer**, *Computers & Security*, Elsevier.
Jun 2020 **Judge**, *Summer Internship Program*, QCRI.
Mar 2020 **PC Member**, *Annual Computer Security Applications Conference*, ACSAC '20.
Sep 2019 **Reviewer**, *Trans. on Privacy and Security*, ACM TOPS.
Sep 2018 **Mentor**, *Summer Internship Program*, QCRI.
Feb 2018 **Reviewer**, *Computers & Security*, Elsevier.
Jan 2018 **Judge**, *Qatar National Scientific Research Competition*, NSRC '18.
Jun 2017 **PC Member**, *Workshop on Security and Privacy in the Cloud*, IEEE SPC '17.
Jan 2017 **Judge**, *Qatar National Scientific Research Competition*, NSRC '17.
Dec 2016 **Reviewer**, *Trans. on Dependable and Secure Computing*, IEEE TDSC.
Nov 2016 **PC Member**, *Conf. on Data and Application Security and Privacy*, ACM CODASPY '17.
Nov 2016 **PC Member**, *Int. Conf. on ICT Systems Security and Privacy Protection*, IFIP SEC '17.
Nov 2016 **Reviewer**, *Trans. on Privacy and Security*, ACM TOPS.
Jul 2016 **Lecturer**, *Computer and Network Security*, ICT Graduate Program, HBKU.
Jun 2016 **PC Member**, *Workshop on Privacy in the Electronic Society*, ACM WPES '16.
Jan 2016 **Publicity Chair**, *Int. Symp. on Research in Attacks, Intrusions and Defenses*, RAID '16.

Publications

Conferences

[1] Yazan Boshmaf et al. "Investigating MMM Ponzi Scheme on Bitcoin". In: *Asia Conference on Computer and Communications Security*. ASIA CCS '20. ACM. 2020, pp. 519–530.

[2] Yazan Boshmaf, Al Jawaheri Husam, and Al Sabah Mashael. "BlockTag: Design and Applications of a Tagging System for Blockchain Analysis". In: *International Conference on ICT Systems Security and Privacy Protection*. SEC '19. IFIP. 2019.

[3] Ildar Muslukhov, Yazan Boshmaf, and Konstantin Beznosov. "Source Attribution of Cryptographic API Misuse in Android Applications". In: *Asia Conference on Computer and Communications Security*. ASIA CCS '18. ACM. 2018, pp. 133–146.

[4] Husam Al Jawaheri, Al Sabah Mashael, and Yazan Boshmaf. "Measurement and Analysis of Bitcoin Transactions of Ransomware". In: *Qatar Foundation Annual Research Conference*. ARC '18. HBKU Press. 2018.

[5] Michael Aupetit et al. "Visualization of Actionable Knowledge to Mitigate DRDoS Attacks". In: *Symposium on Visualization for Cyber Security*. VizSec '16. IEEE. 2016, pp. 1–8.

[6] Mihai Budiu et al. "Interacting with Large Distributed Datasets using Sketch". In: *Symposium on Parallel Graphics and Visualization*. EGPGV '16. Eurographics Association, 2016.

[7] Yazan Boshmaf et al. "Íntegro: Leveraging Victim Prediction for Robust Fake Account Detection in OSNs". In: *Network and Distributed System Security Symposium*. NDSS '15. Internet Society, 2015.

[8] Hootan Rashtian et al. "To Befriend Or Not? A Model of Friend Request Acceptance on Facebook". In: *Symposium on Usable Privacy and Security*. SOUPS '14. 2014.

[9] Ildar Muslukhov et al. "Know Your Enemy: The Risk of Unauthorized Access in Smartphones by Insiders". In: *International Conference on Human-computer Interaction with Mobile Devices and Services*. MobileHCI '13. ACM, 2013, pp. 271–280.

[10] Yazan Boshmaf, Konstantin Beznosov, and Matei Ripeanu. "Graph-based Sybil Detection in Social and Information Systems". In: *International Conference on Advances in Social Networks Analysis and Mining*. ASONAM '13. IEEE/ACM. 2013.

[11] Yazan Boshmaf et al. "The Socialbot Network: When Bots Socialize for Fame and Money". In: *Annual Computer Security Applications Conference*. ACSAC '11. ACM, 2011, pp. 93–102.

Journals

[12] Husam Al Jawaheri et al. "Deanonymizing Tor Hidden Service Users Through Bitcoin Transactions Analysis". In: *Computers & Security* 89 (2020), pp. 101–146.

[13] Ildar Muslukhov et al. "Decoupling Data-at-Rest Encryption and Smartphone Locking with Wearable Devices". In: *Pervasive and Mobile Computing* 32 (2016), pp. 26–34.

[14] Yazan Boshmaf et al. "Íntegro: Leveraging Victim Prediction for Robust Fake Account Detection in Large Scale OSNs". In: *Computers & Security* 61 (2016), pp. 142–168.

[15] Yazan Boshmaf et al. "Design and Analysis of a Social Botnet". In: *Computer Networks* 57 (2012), pp. 556–578.

[16] Thomas Willhalm et al. "SIMD-scan: ultra fast in-memory table scan using on-chip vector processing units". In: *Proceedings of the VLDB Endowment* 2.1 (2009), pp. 385–394.

[17] Stephan Schuhmann et al. "Adaptive composition of distributed pervasive applications in heterogeneous environments". In: *ACM Transactions on Autonomous and Adaptive Systems (TAAS)* 8.2 (2013), pp. 1–21.

Workshops

[18] Hassan Halawa et al. "Harvesting the Low-Hanging Fruits: Defending Against Automated Large-Scale Cyber-Intrusions by Focusing on the Vulnerable Population". In: *New Security Paradigms Workshop*. NSPW '16. ACM. 2016, pp. 11–22.

[19] Yazan Boshmaf et al. "Thwarting Fake OSN Accounts by Predicting their Victims". In: *Workshop on Artificial Intelligence and Security*. AISec '15. ACM. 2015, pp. 81–89.

[20] Yazan Boshmaf et al. "Key Challenges in Defending Against Malicious Socialbots". In: *Conference on Large-scale exploits and emergent threats*. LEET'12. USENIX Association, 2012.

[21] Ildar Muslukhov et al. "Understanding Users' Requirements for Data Protection in Smartphones". In: *International Conference on Data Engineering*. ICDE Workshops '12. IEEE, 2012.

[22] Yazan Boshmaf et al. "Augur: Aiding Malware Detection Using Large-Scale Machine Learning". In: *Workshop on Hot Topics in Security*. HotSec '12. USENIX Association, 2012.

[23] San-Tsai Sun et al. "A Billion Keys, but Few Locks: The Crisis of Web Single Sign-On". In: *New Security Paradigms Workshop*. NSPW '10. 2010, pp. 61–72.

Patents

[24] Yazan Boshmaf, Mashael Al Sabah, and Mohamed Nabeel. "Phishing Domain Detection Systems and Methods". US Patent App. 17/229,386. 2021.

[25] Yazan Boshmaf, Husam Al Jawaheri, and Mashael Al Sabah. "Full-Stack System and Method for Blockchain Analytics". US Patent App. 16/880,575. 2020.

[26] Yazan Boshmaf, Dionysios Logothetis, and Georgios Siganos. "Method and System for Predicting Victim Users and Detecting Fake User Accounts in Online Social Networks". US Patent App. 14/140,965. 2015.

Theses

[27] Yazan Boshmaf. "Security Analysis of Malicious Socialbots on the Web". PhD thesis. The University of British Columbia (Vancouver), 2015.

[28] Yazan Boshmaf. "Development of an Advanced Configuration Algorithm for PCOM Using Partial Application Configurations". MA thesis. University of Stuttgart, 2008.

Technical Reports

[29] Isuranga Perera and Yazan Boshmaf. "Dizzy: Large-Scale Crawling and Analysis of Onion Services". arXiv preprint arXiv:2007.0342. 2021.

[30] Mashael Al Sabah et al. "Phishing Domains Analysis using Certificate Transparency Logs and Passive DNS Records". arXiv preprint arXiv:2034.0211. 2021.

[31] Yury Zhauniarovich et al. "Characterizing Bitcoin Donations to Open Source Software on GitHub". arXiv preprint arXiv:1907.04002. 2019.