

# Yazan Boshmaf

+974 5060 4467  
yazan.boshmaf@gmail.com  
boshmaf.com  
boshmaf

## 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

- Sep 2024 – **Co-Founder**, *MenaML*, London, UK  
Now I co-founded MenaML as a non-profit organization to advance AI education and innovation across the MENA region. We co-organize a flagship 6-day annual event along with top regional and international AI labs, such as Google DeepMind and QCRI. The event is designed to cultivate a vibrant network of AI practitioners and emerging local talent across the MENA region.
- Jun 2016 – **Research Scientist**, *Qatar Computing Research Institute, HBKU*, Doha, Qatar  
Now I joined the Cyber Security group under Marc Dacier to work on research projects that are especially important to Qatari stakeholders. As part of the Senior Staff, I'm leading core projects at QCRI on LLM attribution, AI safety and security, agentic AI, and blockchain analytics. This involves leading cross-functional development among teams of 10+ scientists and engineers, working with local stakeholders and focal points to scope out new use cases across various government and business entities, leading the development of quick MVPs for use case validation, reading and writing research papers in AI/ML, cybersecurity, and blockchain, leading the evaluation and benchmarking of products under development, meeting with internal and external stakeholders for status updates and feedback, and exploring commercialization opportunities.
- Mar 2020 – **Founder**, *QuickByte*, Doha, Qatar  
Aug 2021 Founded QuickByte as a remote-first tech venture studio to satisfy the market's need in Qatar. I raised a \$275k pre-seed from a well-known Family Office and built an amazing team that combined design/engineering expertise, operational support, and capital to turn ideas into lean startups. Notably, we bootstrapped Lobbyz, a social e-commerce app for food delivery, with a functional MVP and \$100K in pre-seed funding and 50+ onboarded merchants. I also contributed strategically in securing its partnership with Snoonu, a leading delivery super-app in Qatar.
- Jun 2015 – **Software Engineer**, *Hootsuite*, Vancouver, BC, Canada  
May 2016 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. Along with the Labs team, I developed and released Hootsuite Amplify, an employee advocacy app that resulted in millions of dollars in revenue.
- 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 developing machine learning-based victim prediction for effective 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 machine learning-based 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 automated, machine learning-based malware detection and signature generation for fast and robust binary file classification in endpoint security solutions.
- Sep 2008 – **Research Engineer, High Performance Computing Center (HLRS)**, Stuttgart, Germany  
Aug 2009 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 – **Research Engineer (Outsourced), SAP**, Walldorf, Germany  
Aug 2008 I joined the TREX team under Franz Faerber to work on vectorized decompression of in-memory data structures for business intelligence search engines using Intel SIMD architecture.
- Sep 2007 – **Software Engineer, Intel**, Walldorf, Germany  
Aug 2008 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 – **Research Intern, University of Stuttgart**, Stuttgart, Germany  
Aug 2007 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 – **Infrastructure Consultant (Outsourced), Microsoft**, Muscat, Oman  
Aug 2006 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 – **Network Engineer, Estarta Solutions**, Amman, Jordan  
Aug 2006 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

---

## Developed Systems

- 2024–Now **aiXamine**, *Qatar Computing Research Institute*, Project Lead  
aiXamine is an LLM safety and security evaluation platform. With 40+ tests across eight services, it provides the most comprehensive evaluation with a single command. aiXamine has been used to evaluate 50+ top LLM models through nearly 1.5K examinations, resulting in the detection of novel safety issues and security threats in models like GPT-4o, Gemini-2, and Grok-3.
- 2024–2025 **Fanar LLM-Attribution**, *Qatar Computing Research Institute*, Subproject Lead  
Fanar is Qatar's state-of-the-art Arabic Large Language Model (LLM) that is built from scratch at QCRI. Under Fanar, I led the development of the attribution service, which fact-checks Fanar responses and adds references to factual statements. The service is a distinguishing feature for Arab LLMs and it has received the higher user approval rating (> 95% like rate).
- 2019–2023 **Dizzy+Toshi+Kansa**, *Qatar Computing Research Institute*, Project Lead  
Patent-pending, ML-powered, systems for scalable blockchain security analytics. Dizzy, Toshi, and Kansa 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 HBKU Innovation Center for expedited commercialization through the Startup Program.
- 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–Now **Qatar Computing Research Institute**, *Leadership, Partnership, and Technology Transfer*
- Leading the applications of Fanar LLM with some of the most important local stakeholders.
  - 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 two are patent-pending and chosen by QRDI for expedited commercialization through its Technology Development Fund and later by HBKU Innovation Center for the Startup Program as a spin-off.
  - 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 Talks and Lectures

- Aug 2021 **Introduction to Virtual Currencies and FinTech**, *Invited Talk*, Qatar International Islamic Bank (QIIB), Doha, Qatar
- A private presentation to QIIB's board of directors as part of their training program.
  - Host: Aphrodite Hammad, Executive Director, HBKU Executive Education Center.
- 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.
- Mar 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 Manager, DARPA) and Tim Hwang (Founder, PacSocial).
- Nov 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.
- Jun 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.
- Mar 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 McCarthy, 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 Professional Services

### Organizing Committee Member

- Jan 2016 Int. Symp. on Research in Attacks, Intrusions and Defenses (RAID '16), *Publicity Chair*

### Program Committee Member

- Apr 2022 ACNS Workshop on Security in Mobile Technologies (SecMT '22)
- Jun 2017 IEEE Workshop on Security and Privacy in the Cloud (SPC '17)
- Nov 2016 ACM Conf. on Data and Application Security and Privacy (CODASPY '17), *Poster Session*
- Nov 2016 IFIP Int. Conf. on ICT Systems Security and Privacy Protection (IFIP SEC '17)
- Jun 2016 ACM Workshop on Privacy in the Electronic Society (WPES '16)

### Reviewer

Feb 2025 ACM Trans. on Privacy and Security (TOPS)  
 Aug 2024 ACM Trans. on Privacy and Security (TOPS)  
 Nov 2023 ACM Computing Surveys  
 Jun 2022 ACM Trans. on Privacy and Security (TOPS)  
 Jul 2021 IEEE Trans. on Dependable and Secure Computing (TDSC)  
 Aug 2020 Elsevier Computers & Security  
 Sep 2019 ACM Trans. on Privacy and Security (TOPS)  
 Feb 2018 Elsevier Computers & Security  
 Dec 2016 IEEE Trans. on Dependable and Secure Computing (TDSC)  
 Nov 2016 ACM Trans. on Privacy and Security (TOPS)

### Others

Sep 2025 3rd HBKU Thematic Research Grant, *Reviewer*, HBKU  
 Feb 2025 MenaML Winter School, *Co-Founder and Organizer*, MenaML (educational, non-profit)  
 Jan 2025 Qatar Foundation Alumni Fund, *Judge*, Qatar Foundation Alumni Office  
 Aug 2024 Innovative Business Discovery and Acceleration Fund, *Judge*, HBKU Innovation  
 Aug 2023 Qatar Financial Centre Digital Assets Regime, *Advisor*, QFC Authority  
 May 2022 Summer Internship Program, *Mentor*, QCRI  
 Jan 2021 Innovation Coupon Startup Fund, *Judge*, QRDl Counsel  
 Jun 2020 Summer Internship Program, *Judge*, QCRI  
 Sep 2018 Summer Internship Program, *Mentor*, QCRI  
 Jan 2018 Qatar National Scientific Research Competition (NSRC '18), *Judge*  
 Jan 2017 Qatar National Scientific Research Competition (NSRC '17), *Judge*  
 Jul 2016 Computer and Network Security, *Lecturer*, ICT Graduate Program, HBKU

### Taught Courses

Jul 2016 Computer and Network Security, *Graduate (Joint)*, CYSE-520, HBKU  
 Sep 2013 Discrete Structures and Algorithms, *Undergraduate*, EECE-320, UBC  
 Sep 2012 Introduction to Computation in Engineering Design, *Undergraduate*, APSC-160, UBC  
 Sep 2011 Introduction to Computation in Engineering Design, *Undergraduate*, APSC-160, UBC  
 Sep 2010 Introduction to Computation in Engineering Design, *Undergraduate*, APSC-160, UBC

### Publications

- \* Primary author
- \*\* Equal contribution as preceding authors

### Refereed Journal Articles

- [1] Husam Al Jawaheri, Masha'al Al Sabah, **Yazan Boshmaf\*\***, and Aiman Erbad. "Deanonymizing Tor Hidden Service Users Through Bitcoin Transactions Analysis". In: *Computers & Security* 89 (2020), pp. 101–146.
- [2] Ildar Muslukhov, San-Tsai Sun, Primal Wijesekera, **Yazan Boshmaf**, and Konstantin Beznosov. "Decoupling Data-at-Rest Encryption and Smartphone Locking with Wearable Devices". In: *Pervasive and Mobile Computing* 32 (2016), pp. 26–34.

- [3] **Yazan Boshmaf\***, Dionysios Logothetis, Georgos Siganos, Jorge Lería, Jose Lorenzo, Matei Ripeanu, Konstantin Beznosov, and Hassan Halawa. "Integro: Leveraging Victim Prediction for Robust Fake Account Detection in Large Scale OSNs". In: *Computers & Security* 61 (2016), pp. 142–168.
- [4] Stephan Schuhmann, Klaus Herrmann, Kurt Rothermel, and **Yazan Boshmaf**. "Adaptive composition of distributed pervasive applications in heterogeneous environments". In: *ACM Transactions on Autonomous and Adaptive Systems (TAAS)* 8.2 (2013), pp. 1–21.
- [5] **Yazan Boshmaf\***, Ildar Muslukhov, Konstantin Beznosov, and Matei Ripeanu. "Design and Analysis of a Social Botnet". In: *Computer Networks* 57 (2012), pp. 556–578.
- [6] Thomas Willhalm, Nicolae Popovici, **Yazan Boshmaf\*\***, Hasso Plattner, Alexander Zeier, and Jan Schaffner. "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.

## Refereed Conference Papers

- [7] **Yazan Boshmaf\***, Isuranga Perera, Udesch Kumarasinghe, Sajitha Liyanage, and Husam Al Jawaheri. "Dizzy: Large-Scale Crawling and Analysis of Onion Services". In: *International Conference on Availability, Reliability and Security*. ARES '22. ACM. 2023.
- [8] Mashael Al Sabah, Mohamed Nabeel, Euijin Choo, and **Yazan Boshmaf**. "Content-Agnostic Detection of Phishing Domains using Certificate Transparency and Passive DNS". In: *International Symposium on Research in Attacks, Intrusions and Defenses*. RAID '22. ACM. 2022.
- [9] **Yazan Boshmaf\***, Charitha Elvitigala, Husam Al Jawaheri, Primal Wijesekera, and Mashael Al Sabah. "Investigating MMM Ponzi Scheme on Bitcoin". In: *Asia Conference on Computer and Communications Security*. ASIA CCS '20. ACM. 2020, pp. 519–530.
- [10] **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.
- [11] 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.
- [12] Michael Aupetit, Yury Zhauniarovich, Giorgos Vasiladis, Marc Dacier, and **Yazan Boshmaf**. "Visualization of Actionable Knowledge to Mitigate DRDoS Attacks". In: *Symposium on Visualization for Cyber Security*. VizSec '16. IEEE. 2016, pp. 1–8.
- [13] Mihai Budiu, Rebecca Isaacs, Derek Murray, Gordon Plotkin, Paul Barham, Samer Al-Kiswany, **Yazan Boshmaf**, Qingzhou Luo, and Alexandr Andoni. "Interacting with Large Distributed Datasets using Sketch". In: *Symposium on Parallel Graphics and Visualization*. EGPGV '16. Eurographics Association, 2016.
- [14] **Yazan Boshmaf\***, Dionysios Logothetis, Georgos Siganos, Jorge Leria, Jose Lorenzo, Matei Ripeanu, and Konstantin Beznosov. "Integro: Leveraging Victim Prediction for Robust Fake Account Detection in OSNs". In: *Network and Distributed System Security Symposium*. NDSS '15. Internet Society, 2015.
- [15] Hootan Rashtian, **Yazan Boshmaf\*\***, Pooya Jaferian, and Konstantin Beznosov. "To Befriend Or Not? A Model of Friend Request Acceptance on Facebook". In: *Symposium on Usable Privacy and Security*. SOUPS '14. 2014.
- [16] Ildar Muslukhov, **Yazan Boshmaf\*\***, Cynthia Kuo, Jonathan Lester, and Konstantin Beznosov. "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.
- [17] **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.

- [18] **Yazan Boshmaf\***, Ildar Muslukhov, Konstantin Beznosov, and Matei Ripeanu. "The Socialbot Network: When Bots Socialize for Fame and Money". In: *Annual Computer Security Applications Conference. ACSAC '11*. ACM, 2011, pp. 93–102.

### Refereed Workshop Papers

- [19] Mohannad Alhanahnah and **Yazan Boshmaf**. "DepsRAG: Towards Agentic Reasoning and Planning for Software Dependency Management". In: *Workshop on Open-World Agents. OWA '24*, part of NeurIPS '24. ACM. 2024, pp. 8–18.
- [20] Mohannad Alhanahnah, **Yazan Boshmaf**, and Ashish Gehani. "SoK: Software Debloating Landscape and Future Directions". In: *Workshop on Forming an Ecosystem Around Software Transformation. FEAST '24*, part of ACM CCS '24. ACM. 2024, pp. 8–18.
- [21] Hassan Halawa, Konstantin Beznosov, **Yazan Boshmaf**, Baris Coskun, Matei Ripeanu, and Elizeu Santos-Neto. "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.
- [22] **Yazan Boshmaf\***, Matei Ripeanu, Konstantin Beznosov, and Elizeu Santos-Neto. "Thwarting Fake OSN Accounts by Predicting their Victims". In: *Workshop on Artificial Intelligence and Security. AISEC '15*, part of ACM CCS '15. ACM. 2015, pp. 81–89.
- [23] **Yazan Boshmaf\***, Ildar Muslukhov, Konstantin Beznosov, and Matei Ripeanu. "Key Challenges in Defending Against Malicious Socialbots". In: *Conference on Large-scale Exploits and Emergent Threats. LEET'12*, part of Usenix Sec '12. USENIX Association, 2012.
- [24] Ildar Muslukhov, **Yazan Boshmaf**, Cynthia Kuo, Jonathan Lester, and Konstantin Beznosov. "Understanding Users' Requirements for Data Protection in Smartphones". In: *International Conference on Data Engineering. ICDE Workshops '12*. IEEE, 2012.
- [25] San-Tsai Sun, **Yazan Boshmaf**, Kirstie Hawkey, and Konstantin Beznosov. "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

- [26] **Yazan Boshmaf\*** and Sajitha Liyanage. "System and Methods for Smart Contract Security Auditing". US Patent App. 18/535,740. 2022.
- [27] **Yazan Boshmaf\*** and Isuranga Perera. "System and Methods for Scalable Darkweb Analytics". US Patent App. 18/386,486. 2022.
- [28] Mashael Al Sabah, Mohamed Nabeel, and **Yazan Boshmaf**. "Phishing Domain Detection Systems and Methods". US Patent App. 17/229,386. 2021.
- [29] **Yazan Boshmaf\***, Husam Al Jawaheri, and Mashael Al Sabah. "Full-Stack System and Method for Blockchain Analytics". US Patent App. 16/880,575. 2020.
- [30] **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.

### Technical Reports / Under Review

- [31] Fatih Deniz, Dorde Popovic, **Boshmaf, Yazan**, Euisuh Jeong, Minhaj Ahmad, Sanjay Chawla, and Issa Khalil. "aiXamine: Simplified LLM Safety and Security". arXiv preprint arXiv:2504.14985. 2025.
- [32] Ummar Abbas, Mohammad Shahmeer Ahmad, Firoj Alam, Enes Altinisik, Ehsannedin Asgari, **Yazan Boshmaf**, Sabri Boughorbel, Sanjay Chawla, Shammur Chowdhury, et al. "Fonar: An Arabic-Centric Multimodal Generative AI Platform". arXiv preprint arXiv:2501.13944. 2025.
- [33] Yury Zhauniarovich, **Yazan Boshmaf\*\***, Husam Al Jawaheri, and Mashael Al Sabah. "Characterizing Bitcoin Donations to Open Source Software on GitHub". arXiv preprint arXiv:1907.04002. 2019.