

Yazan Boshmaf

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

Education

- 2009–2015 **Ph.D. Computer Eng.**, *University of British Columbia*, Vancouver, Canada.
Thesis: Security Analysis of Malicious Social Bots on the Web
- 2006–2008 **M.Sc. Information Tech.**, *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 Eng.**, *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.
Cyber Security team
- I'm leading the Cybersecurity Initiative for Blockchain Research (CIBR) at QCRI. Our research is focused on technical, multidisciplinary aspects of cybersecurity for cryptocurrencies and blockchain technologies. We work with our partners on research projects that support the thriving blockchain ecosystem in Qatar and abroad (see <https://qcri.github.io/cibr>).
 - In collaboration with the University of British Columbia, I developed a cloud-based service for analyzing cryptographic API (mis)use in Android applications. The service has been used to analyze more than 120K applications, which included apps of major stakeholders in Qatar who accordingly patched their apps.
 - In collaboration with Qatar University, I investigated the feasibility of deanonymizing Tor hidden service users by exploiting public Bitcoin information. Using Bitcoin addresses from 88 hidden services, 5B tweets, and 1M forum pages, we were able to link 125 unique users to various hidden services, including sensitive ones, such as The Pirate Bay, Silk Road, and WikiLeaks. We show that Bitcoin addresses should always be assumed as compromised and can be used to deanonymize users. Our research has been covered international news outlets (WIRED, New Scientist) and was presented to the U.S. Federal Trade Commission.
 - Along with the Cyber Security team, I built a real-time processing platform for analyzing DRDoS attacks. The system has been used to visualize analytics about such attacks that go through Qatar using locally deployed honeypots.
- Jun 2015–May 2016 **Software Engineer, Full Stack**, *Hootsuite*, Vancouver, BC, Canada.
Hootsuite Labs team
- Developed disruptive products, experimented with emerging technologies, and promoted lean innovation.
 - As a full stack engineer, I worked with a wide array of technologies and languages such as Python, Flask, Django, NGINX, Tornado, MongoDB, MySQL, RAML, Blueprint, PHP, Vagrant, Ansible, Javascript, AngularJS, React Native, PhoneGap/Cordova, Objective-C, Java, and Ionic.
 - Along with the Labs team, I developed and released Hootsuite Amplify, an employee advocacy app that resulted in millions of dollars in revenue.

- Sep 2009–May 2015 **Research Assistant, University of British Columbia, Vancouver, BC, Canada.**
LERSSE and NetSysLab groups
- Designed, implemented, and evaluated scalable and robust defense systems to fight against abusive automation on the (social) web. My research has been covered by many international news outlets (e.g., BBC, CBC, New Scientist), and is currently being used by online services to protect millions of users (e.g., Tuenti, Telefonica).
 - Designed, implemented, and evaluated a data-at-rest encryption system for smartphones. Along with LERSSE members, we deployed the system on iOS and Android with a wearable hardware token that decouples data privacy from smartphone locking.
- Jun–Aug 2014 **Research Intern, Microsoft Research Silicon Valley, Mountain View, USA.**
Distributed Systems team
- Designed, implemented, and evaluated a prototypical DBMS extension to Sketch, a distributed system for interactive exploration of large datasets.
 - Deployed the system on a shared-nothing MSSQL cluster, where it interactively delivered analytics results (e.g., summary statistic, histograms) from tera bytes of data that did not fit in the overall cluster memory. The system is used internally at Microsoft to debug server logs and analyze social data.
- Sep–Nov 2013 **Research Intern, Telefonica Research, Barcelona, Spain.**
Distributed Systems team
- Designed, implemented, and evaluated Integro, a scalable system for victim prediction and fake account detection in online social networks.
 - Along with the Site Integrity team at Tuenti, the largest Spanish social network with more than 15 million users, I deployed the system in beta on production servers, where it delivered an AUC > 0.92, which is up to 30% improvement over the state-of-the art, in addition to orders of magnitude speedup.
- Sep–Nov 2012 **Research Intern, Facebook, Menlo Park, CA, USA.**
Site Integrity team
- Designed, implemented, and evaluated Huddle, a defense system for IP address reputation and botnet detection for large social networks.
 - Deployed the system in beta on production servers, where it delivered an additional 25% in detection sensitivity when compared to existing detection systems.
- May–Aug 2012 **Research Intern, Sophos, Vancouver, BC, Canada.**
Sophos Labs team
- Designed, implemented, and evaluated Augur, an automated malware detection system that uses large-scale machine learning techniques to classify malware and generate signatures in Sophos Virus Definition Language.
 - Deployed the system in beta on production servers, where it achieved 99.99% specificity and 30% sensitivity in malware detection.
- 2008–2009 **Research Intern, High Performance Computing Center (HLRS), Stuttgart, Germany.**
Scalable Computing and Coupled Systems group
- Designed, implemented, and benchmarked Lattice Boltzmann numerical methods on a massively-parallel GPU cluster using CUDA.
 - Extended CUDA basic IO libraries to reduce memory-bank conflicts and coalescing.
 - Deployed the vectorized methods into an existing software framework for numerical methods on 700-node Intel Nehalem Cluster with Nvidia Tesla S1070 GPUs.

- 2007–2008 **Software Engineer (Outsourced)**, *SAP*, Walldorf, Germany.
SAP NetWeaver, TREX team
- Offered consultation and training on software vectorization using Intel SSE technology.
 - Designed and developed a vectorization framework for decompressing in-memory data structures in TREX, which is the SAP NetWeaver search and classification engine.
 - Deployed the framework into SAP NetWeaver, where it achieved up to 2.1x speedup when compared to a highly optimized sequential version.
- 2007–2008 **Application Engineer**, *Intel*, Walldorf, Germany.
SAP Onsite Engineering
- Performed performance analysis and code optimization for SAP NetWeaver.
 - Reported performance bugs in Intel C/C++ Compiler to Intel Compiler team.
 - Evangelized Intel software tools and technologies to the software community in SAP.
- 2006–2007 **Research Intern**, *University of Stuttgart*, Stuttgart, Germany.
Self-Organizing Software Systems group
- Developed Symbian C communication plug-ins for PCOM middleware.
 - Performed experiments and empirical analysis to improve weighted centroid localization in smart ubiquitous environments.
 - Designed and developed low-cost automatic configuration algorithms for component-based pervasive applications.
- 2005–2006 **Infrastructure Consultant (Outsourced)**, *Microsoft*, Muscat, Oman.
Microsoft Consulting Services, EMEA
- Designed, deployed, and tested Microsoft enterprise solutions and server infrastructure for mobile number portability across providers at Nawras, a mobile network operator.
 - Designed, deployed, and tested a virtualized product staging environment for business software development at Nawras.
- 2005–2006 **Associate Network Engineer**, *Estarta Solutions*, Amman, Jordan.
IT and Business Infrastructure team
- Offered Cisco and Microsoft solutions consultancy.
 - Lead a team of five to plan, design, implement, optimize, and operate a campus-wide IEEE 802.11 wireless networking solution for the University of Jordan.
 - Deployed a Cisco IP Telephony solution for the company, including PSTN integration.
 - Performed Microsoft SQL security auditing for the Housing Bank for Trade & Finance.
 - Offered technical training on computer networking and VoIP to clients and partners.

Scholarships and Awards

- Aug, 2013 **Best Paper Award**, *Advances in Social Networks Analysis and Mining Conference*, Niagara Falls, Canada.
The award includes an honorarium and is based on both the paper and the presentation at the conference [3].
- May, 2012 **Research Internship Award**, *MITACS Accelerate*, Vancouver, BC, Canada.
\$15,000 CAD for four months of research internship at a Canadian company.
- Dec, 2011 **Outstanding Paper Award**, *Annual Computer Security Applications Conference*, Florida, USA.
The award includes an honorarium and is based on both the paper and the presentation at the conference [8].
- 2009-2013 **Four Year Doctoral Fellowship**, *University of British Columbia*, Institutional, Vancouver, Canada.
\$22,000 CAD per year plus tuition for the first four years of PhD studies.

- 2009-2013 **Faculty of Applied Science Award**, *University of British Columbia*, Institutional, Vancouver, Canada.
\$4,000 CAD per year for the first four years of PhD studies.
- 2006-2008 **Full Tuition Scholarship for Outstanding Students**, *University of Stuttgart*, Provincial, Stuttgart, Germany.
Full tuition refund for the duration of M.Sc. studies.
- 2001-2005 **Royal Academic Sponsorship**, *Jordan University of Science and Technology*, National, Irbid, Jordan.
\$1,700 CAD plus tuition for the duration of B.Sc. studies.

Computer skills

Languages	C++, Java, C#, Python, JavaScript	Environments	Linux, Windows, Android, iOS
Frameworks	Django, Flask, Google Cloud, Ionic, Angular, Bootstrap	DBMS	Oracle, MySQL, MSSQL, MongoDB
Editors/IDEs	Eclipse, Tmux+Vim, Sublime	Big Data	Giraph, Mahout, Hadoop, Hive, Spark, ELK

References

Academic

- Konstantin Beznosov **PhD Supervisor**, *Professor*
Department of Electrical and Computer Engineering
2332 Main Mall, Vancouver, BC, Canada V6T 1Z4
Email: beznosov@ece.ubc.ca.
- Matei Ripeanu **PhD Supervisor**, *Professor*
Department of Electrical and Computer Engineering
2332 Main Mall, Vancouver, BC, Canada V6T 1Z4
Email: matei@ece.ubc.ca.
- Bill Aiello **PhD Examiner**, *Professor*
Department of Computer Science
201-2366 Main Mall, Vancouver, BC, Canada V6T 1Z4
Email: aiello@cs.ubc.ca.
- David Lie **PhD Examiner**, *Professor*
Department of Electrical and Computer Engineering
10 King's College Road, Toronto, ON M5S 3G4
Email: lie@eecg.toronto.edu.
- Kurt Rothermel **M.Sc. Supervisor**, *Professor*
Department of Distributed Systems
Universitätsstraße 38, 70569 Stuttgart, Germany
Email: kurt.rothermel@ipvs.uni-stuttgart.de.

Professional

- Dietrich Banschbach **Direct Manager**, *Director EMEA Developer & Scale Programs*
Intel
Email: upon request.

Franz Faerber **Indirect Manager, Software Architect**
SAP
Email: upon request.

Salim Naim **Lead Solutions Architect, Service Line Lead**
Microsoft
Email: upon request.

Yuchun Tang **Mentor, Software Engineer**
Facebook
Email: upon request.

Dmitry Samosseiko **Direct Manager, Director of Threat Research**
SophosLabs, Sophos Inc.
Email: upon request.

Dionysios Logothetis **Mentor, Research Scientist**
Telefonica Research, Telefonica Digital.
Email: upon request.

Mihai Budiu **Mentor, Senior Researcher**
Microsoft Research.
Email: upon request.

Matt Switzer **Indirect Manager, SVP Strategy & Corporate Development**
Hootsuite.
Email: upon request.

Selected Invited Talks and Guest Lectures

- Sep 2019 **Cryptocurrency Analytics: Bitcoin vs. Cybersecurity**, *Invited Talk*, Department of Computer Science and Technology, Peking University, Beijing, China.
 - A public presentation to the CS community at Peking University.
 - Host: Yao Guo, Associate Professor
- 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.
 - Hosts: Dan Salsburg.
- 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 (DARPA) and Tim Hwang (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, Edmonton, Canada.

- June 2012 **Design and Analysis of a Social Botnet**, *Invited Talk*, SRI International, 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.
- Spring 2012 **Socialbots: A Security Perspective**, *Guest Lecture*, University of Washington Bothell, WA, USA.
- Course: CSS 490B—Programming Social and Computational Intelligence for the Web.
 - Host: Joe McCarthy.
- May 2010 **Automated Social Engineering Attacks in Online Social Networks**, *Invited Talk*, The Office of the Privacy Commissioner of Canada, Ottawa, Canada.
- Host: Andrew Patrick.

Recent Academic Services

- Feb 2018 **Reviewer**, *Elsevier Computers and Security*.
- Jun 2017 **PC Member**, *3rd Workshop on Security and Privacy in the Cloud (SPC 2017)*.
- Jan 2017 **Judge**, *Qatar National Scientific Research Competition (NSRC)*.
- Dec 2016 **Reviewer**, *IEEE Transactions on Dependable and Secure Computing (TDSC)*.
- Nov 2016 **Poster PC Member**, *8th ACM Conference on Data and Application Security and Privacy (CODASPY 2017)*.
- Nov 2016 **PC Member**, *32nd International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2017)*.
- Nov 2016 **Reviewer**, *ACM Transactions on Privacy and Security (TOPS)*.
- Jun 2016 **PC Member**, *ACM Workshop on Privacy in the Electronic Society (WPES 2016)*.
- Jan 2016 **Publicity Chair**, *The 19th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2016)*.

Publications

- [1] Michael Aupetit, Yury Zhauniarovich, Giorgos Vasiliadis, Marc Dacier, and Yazan Boshmaf. Visualization of actionable knowledge to mitigate drdos attacks. In *Visualization for Cyber Security (VizSec), 2016 IEEE Symposium on*, pages 1–8. IEEE, 2016.
- [2] Yazan Boshmaf. *Security analysis of malicious socialbots on the web*. PhD thesis, The University of British Columbia (Vancouver), 2015.
- [3] Yazan Boshmaf, Konstantin Beznosov, and Matei Ripeanu. Graph-based sybil detection in social and information systems. In *Advances in Social Networks Analysis and Mining (ASONAM), 2013 IEEE/ACM International Conference on*. IEEE, 2013.
- [4] Yazan Boshmaf, Charitha Elvitigala, Husam Al Jawaheri, Primal Wijesekera, and Mashael Al Sabah. Investigating mmm ponzi scheme on bitcoin. *arXiv preprint arXiv:1910.12244*, 2019.
- [5] Yazan Boshmaf, Al Jawaheri Husam, and Al Sabah Mashael. Blocktag: Design and applications of a tagging system for blockchain analysis. In *Proc. of 34th International Conference on ICT Systems Security and Privacy Protection*. IFIP, 2019.
- [6] 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 *Proceedings of the Network and Distributed System Security Symposium (NDSS'15)*, 2015.
- [7] Yazan Boshmaf, Dionysios Logothetis, Georgos Sigamos, Jorge Lería, Jose Lorenzo, Matei Ripeanu, Konstantin Beznosov, and Hassan Halawa. Íntegro: Leveraging victim prediction for robust fake account detection in large scale osns. *Computers & Security*, 61:142–168, 2016.
 - [8] Yazan Boshmaf, Ildar Muslukhov, Konstantin Beznosov, and Matei Ripeanu. The socialbot network: when bots socialize for fame and money. In *Proceedings of the 27th Annual Computer Security Applications Conference, ACSAC '11*, pages 93–102, New York, NY, USA, 2011. ACM.
 - [9] Yazan Boshmaf, Ildar Muslukhov, Konstantin Beznosov, and Matei Ripeanu. Design and analysis of a social botnet. *Elsevier Computer Networks—Special Issue on Botnets*, 2012.
 - [10] Yazan Boshmaf, Ildar Muslukhov, Konstantin Beznosov, and Matei Ripeanu. Key challenges in defending against malicious socialbots. In *Proceedings of the 5th USENIX conference on Large-scale exploits and emergent threats, LEET'12*, Berkeley, CA, USA, 2012. USENIX Association.
 - [11] Yazan Boshmaf, Matei Ripeanu, Konstantin Beznosov, and Elizeu Santos-Neto. Thwarting fake osn accounts by predicting their victims. In *Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security*, pages 81–89. ACM, 2015.
 - [12] Mihai Budiu, Rebecca Isaacs, Derek Murray, Gordon Plotkin, Paul Barham, Samer Al-Kiswani, Yazan Boshmaf, Qingzhou Luo, and Alexandr Andoni. Interacting with large distributed datasets using sketch. In *Eurographics Symposium on Parallel Graphics and Visualization (EGPGV'16)*, 2016.
 - [13] 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 *Proceedings of the 2016 New Security Paradigms Workshop*, pages 11–22. ACM, 2016.
 - [14] Husam Al Jawaheri, Mashael Al Sabah, Yazan Boshmaf, and Aiman Erbad. Deanonymizing tor hidden service users through bitcoin transactions analysis. *arXiv preprint arXiv:1801.07501*, 2018.
 - [15] Ildar Muslukhov, Yazan Boshmaf, and Konstantin Beznosov. Source attribution of cryptographic api misuse in android applications. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, pages 133–146. ACM, 2018.
 - [16] Ildar Muslukhov, Yazan Boshmaf, Cynthia Kuo, Jonathan Lester, and Konstantin Beznosov. Understanding users' requirements for data protection in smartphones. In *ICDE Workshops, Washington DC, USA*. IEEE, 2012.
 - [17] Ildar Muslukhov, Yazan Boshmaf, Cynthia Kuo, Jonathan Lester, and Konstantin Beznosov. Know your enemy: The risk of unauthorized access in smartphones by insiders. In *Proceedings of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services, MobileHCI '13*, pages 271–280, New York, NY, USA, 2013. ACM.
 - [18] Ildar Muslukhov, San-Tsai Sun, Primal Wijesekera, Yazan Boshmaf, and Konstantin Beznosov. Decoupling data-at-rest encryption and smartphone locking with wearable devices. *Pervasive and Mobile Computing*, 32:26–34, 2016.
 - [19] 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)*, 2014.
 - [20] 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 '13*, New York, NY, USA, 2013. ACM.

- [21] San-Tsai Sun, Yazan Boshmaf, Kirstie Hawkey, and Konstantin Beznosov. A Billion Keys, but Few Locks: The Crisis of Web Single Sign-On. In *Proceedings of the New Security Paradigms Workshop (NSPW)*, pages 61–72, September 20–22 2010.
- [22] 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. *Proc. VLDB Endow.*, 2(1):385–394, 2009.
- [23] 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.