Sadia Afroz

Contact Information

International Computer Science Institute (ICSI)

Berkeley, CA 94704

Phone: (215) 200-9571

Email: sadia@icsi.berkeley.edu
Website: http://icsi.berkeley.edu/~sadia/

Research Interests

Adversarial machine learning; privacy and anonymity; cybercrimal network analysis

Honors and Awards

Runner up for the **ACM SIGSAC Dissertation Award**, 2014.
Award for Outstanding Research in Privacy Enhancing Technologies (**PET Award**) 2013.
Andreas Pftzmann PETS 2012 **Best Student Paper** Award.
Drexel University College of Engineering **Dean's Fellowship**, 2008 and 2009.
Dean's Merit List Award, 2003, Bangladesh University of Engineering and Technology.
BUET Admission Test Excellence Scholarship, 2002, Rank 60/4000.
General Scholarship (2001, 1999, 1996, 1993), Bangladesh Education Board.

Education

Drexel University, Philadelphia, PA

PhD in Computer Science, June 2014
Thesis: Deception in Authorship Attribution
Advisor: Rachel Greenstadt

Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh

B.Sc. in Engineering, Computer Science and Engineering, June 2007
Thesis: Effect of Diversity in Ensemble Learning
Advisor: Md. Monirul Islam

Journals

[J1] Michael Brennan, Sadia Afroz, and Rachel Greenstadt. Adversarial stylometry: Circumventing authorship recognition to preserve privacy and anonymity. *ACM Transactions on Information and System Security (TISSEC)*, 15(3):12, 2012 (**PET Award 2013**)

Conference Publications

[C13] Rebecca S. Portnoff, Danny Yuxing Huang, Periwinkle Doerfler, Sadia Afroz, and Damon McCoy. Backpage and bitcoin: Uncovering human traffickers. In *Proceedings of the 23rd ACM SIGKDD international conference on Knowledge discovery in data mining*. ACM, 2017

[C12] Rachee Singh, Rishab Nithyanand, Sadia Afroz, Paul Pearce, Michael Carl Tschantz, Phillipa Gill, and Vern Paxson. Characterizing the nature and dynamics of tor exit blocking. In *Proceedings of the 26th USENIX Security Symposium*. USENIX, 2017

[C11] Rebecca S. Portnoff, Sadia Afroz, Greg Durrett, Jonathan K. Kummerfeld, Taylor Berg-Kirkpatrick, Damon McCoy, Kirill Levchenko, and Vern Paxson. Automated analysis of cybercriminal markets. In *Proceedings of the 26th International Conference on World Wide Web*. ACM, 2017

[C10] Srikanth Sundaresan, Damon McCoy, Sadia Afroz, and Vern Paxson. Profiling underground merchants based on network behavior. In *Proceedings of the eleventh Symposium on Electronic Crime Research (eCrime)*, 2016

[C9] Brad Miller, Alex Kantchelian, Michael Carl Tschantz, Sadia Afroz, Rekha Bahwani, Riyaz Faizullabhoy, Ling Huang, Vaishaal Shankar, Tony Wu, George Yiu, et al. Reviewer integration and performance measurement for malware detection. In *Proceedings of the 2016 Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*, 2016

[C8] Michael Carl Tschantz, Sadia Afroz, Anonymous, and Vern Paxson. Sok: Towards grounding censorship circumvention in empiricism. In *Proceedings of the 35rd conference on IEEE Symposium on Security and Privacy*. IEEE, 2016

[C7] Sheharbano Khattak, David Fifield, Sadia Afroz, Mobin Javed, Srikanth Sundaresan, Vern Paxson, Steven J. Murdoch, and Damon McCoy. Do you see what i see?: Differential treatment of anonymous users. In *Network and Distributed System Security Symposium 2016*. IETF, 2016

[C6] Vaibhav Garg, Sadia Afroz, Rebekah Overdorf, and Rachel Greenstadt. Computer-supported cooperative crime. In *Proceedings of the 19th International Conference on Financial Cryptography and Data Security*, 2015

[C5] Marc Juarez, Sadia Afroz, Gunes Acar, Claudia Diaz, and Rachel Greenstadt. A critical evaluation of website fingerprinting attacks. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 263–274. ACM, 2014

[C4] Sadia Afroz, Aylin Caliskan-Islam, Ariel Stolerman, Damon McCoy, and Rachel Greenstadt. Doppelgänger finder: Taking stylometry to the underground. In *Proceedings of the 35rd conference on IEEE Symposium on Security and Privacy*, pages 212–226. IEEE, 2014

[C3] Ariel Stolerman, Rebekah Overdorf, Sadia Afroz, and Rachel Greenstadt. Breaking the closed-world assumption in stylometric authorship attribution. In *Advances in Digital Forensics X*, pages 185–205. Springer, 2014

[C2] Andrew WE McDonald, Sadia Afroz, Aylin Caliskan, Ariel Stolerman, and Rachel Greenstadt. Use fewer instances of the letter i: Toward writing style anonymization. In *Privacy Enhancing Technologies*, pages 299–318. Springer, 2012 (**Best Student Paper Award 2012**)

[C1] Sadia Afroz, Michael Brennan, and Rachel Greenstadt. Detecting hoaxes, frauds, and deception in writing style online. In *Security and Privacy (SP), 2012 IEEE Symposium on*, pages 461–475. IEEE, 2012

Peer-reviewed Workshop Publications

[W10] Alex Kantchelian, Michael Carl Tschantz, Sadia Afroz, Brad Miller, Vaishaal Shankar, Rekha Bachwani, Anthony D Joseph, and JD Tygar. Better malware ground truth: Techniques for weighting anti-virus vendor labels. *Proceedings of the 2015 ACM Workshop on Artificial Intelligence and Security. AISec*, 15, 2015

[W9] Sadia Afroz, David Fifield, Michael Carl Tschantz, Vern Paxson, and J. D. Tygar. Censorship arms race: Research vs. practice. *HotPETS*, 2015

[W8] Brad Miller, Alex Kantchelian, Sadia Afroz, Rekha Bachwani, Edwin Dauber, Ling Huang, Michael Carl Tschantz, Anthony D Joseph, and JD Tygar. Adversarial active learning. In *Proceedings of the 2014 Workshop on Artificial Intelligent and Security Workshop*, pages 3–14. ACM, 2014

[W7] Alex Kantchelian, Sadia Afroz, Ling Huang, Aylin Caliskan Islam, Brad Miller, Michael Carl Tschantz, Rachel Greenstadt, Anthony D Joseph, and JD Tygar. Approaches to adversarial drift. In *Proceedings of the 2013 ACM workshop on Artificial intelligence and security*, pages 99–110. ACM, 2013

[W6] Sadia Afroz, Vaibhav Garg, Damon McCoy, and Rachel Greenstadt. Honor among thieves: A common's analysis of cybercrime economies. In *eCrime Researchers Summit (eCRS), 2013*, pages 1–11, 2013

[W5] Sadia Afroz, Aylin Caliskan Islam, Jordan Santell, Aaron Chapin, and Rachel Greenstadt. How privacy flaws affect consumer perception. In *Socio-Technical Aspects in Security and Trust (STAST), 2013 Third Workshop on*, pages 10–17. IEEE, 2013

[W4] Alex Kantchelian, Justin Ma, Ling Huang, Sadia Afroz, Anthony Joseph, and JD Tygar. Robust detection of comment spam using entropy rate. In *Proceedings of the 5th ACM workshop on Security and artificial intelligence*, pages 59–70. ACM, 2012

[W3] Knarig Arabshian, Peter J Danielsen, and Sadia Afroz. Lexont: A semi-automatic ontology creation tool for programmable web. In *AAAI Spring Symposium: Intelligent Web Services Meet Social Computing*. AAAI, 2012

[W2] Sadia Afroz and Rachel Greenstadt. Phishzoo: Detecting phishing websites by looking at them. In *Semantic Computing (ICSC), 2011 Fifth IEEE International Conference on*, pages 368–375. IEEE, 2011

[W1] Rachel Greenstadt, Sadia Afroz, and Michael Brennan. Mixed-initiative security agents. In *Proceedings of the 2nd ACM workshop on Security and artificial intelligence*, pages 35–38. ACM, 2009

Technical reports

[T4] Brad Miller, Alex Kantchelian, Michael Carl Tschantz, Sadia Afroz, Rekha Bahwani, Riyaz Faizullabhoy, Ling Huang, Vaishaal Shankar, Tony Wu, George Yiu, et al. Back to the future: Malware detection with temporally consistent labels. *arXiv preprint arXiv:1510.07338*, 2015

[T3] Michael Carl Tschantz, Sadia Afroz, Vern Paxson, and J. D. Tygar. On modeling the costs of censorship. Technical Report arXiv:1409.3211v1, ArXiv, September 2014

[T2] Sadia Afroz and Rachel Greenstadt. Toward generalizing comment quality prediction in online communities. Technical Report DU-CS-14-01, Drexel University, 2014

[T1] Sadia Afroz and Rachel Greenstadt. Phishzoo: An automated web phishing detection approach based on profiling and fuzzy matching. Technical Report DU-CS-09-03, Drexel University, 2009

Research Grant

PI: Adversarially Robust Machine Learning, Center for Long-Term Cybersecurity, UC Berkeley, Duration: 01/15/2017–12/31/2017, Award Amount: $15,000.

PI: NSF 1651857: EAGER: Collaborative Research: Exploring Internet Balkanization through the Lens of Regional Discrimination, Duration: 10/1/2016–09/30/2017, Award Amount: $300,000

PI: Large Scale Automated Analysis of Cybercriminal Networks, Center for Long-Term Cybersecurity, UC Berkeley, Duration: 01/15/2016–07/31/2017, Award Amount: $50,000.

I participated in writing two National Science Foundation grants:

NSF 1347151: EAGER: Cybercrime Science, Duration: 09/01/2013-08/31/2015, Award Amount: $188,676.

NSF 1518918: TWC: TTP Option: Large: Collaborative: Towards a Science of Censorship Resistance, Duration: 09/01/2015-08/31/2019, Award Amount: $4,897,402.

Source Code

Doppelgänger Finder: `https://github.com/sheetal57/doppelganger-finder`
JStylo-Anonymouth: `https://github.com/sheetal57/jstylo`

Work Experience

International Computer Science Institute (ICSI), CA
Research Scientist **Jan 2016 - Current**

University of California, Berkeley, CA
Postdoctoral Researcher **Jan 2014 - Dec 2015**
I work with Anthony Joseph, J. D. Tygar and Vern Paxson.

University of California, Berkeley, CA
Summer Intern **Summer 2013, 2012**
I worked with J. D. Tygar and Anthony Joseph on social spam detection and adversarial machine learning.

Bell Labs, Murray Hill, New Jersey
Summer Intern **Summer 2011**
I worked with Knarig Arabshian at the Bell Laboratories Service Infrastructure research domain in semi-automatic ontology generation project.

Drexel University, Philadelphia, Pennsylvania
Research Assistant and Teaching Assistant **Sep 2008 - Dec 2013**
I was a teaching assistant for Introduction to Computing (CS 161), and Computer Network and security (CS 475).

Vonair Software Services, Dhaka, Bangladesh
Junior Software Engineer **Jun 2007- Jun 2008**
I worked as a Software Developer on VoIP related projects.

Service

Reviewer for an NSF panel, 2017, 2016, 2015

Program Co-Chair for the Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETS) 2016, 2017

Program Committee member for
ACM Conference on Computer and Communications Security (CCS), 2017
International World Wide Web Conference (WWW), 2017, 2016
Symposium on Electronic Crime Research, 2017, 2016
IEEE Symposium on Security and Privacy, 2016
USENIX Security, 2015
Privacy Enhancing Technologies Symposium (PETS), 2016, 2015
Women Empowerment through ICT, Bangladesh, 2014
Workshop on Usable Security, 2013, 2012.

Organizing committee member for Security and Privacy Workshops (SPW), 2013.

External Reviewer for
ACM Conference on Computer and Communications Security (CCS), 2015, 2009
Privacy Enhancing Technologies Symposium (PETS), 2011-14, 2009
ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD), 2014
ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM), 2013
ACM Conference for Human-Computer Interaction (CHI), 2013
AAAI Conference on Artificial Intelligence (AAAI), 2011
Financial Cryptography, 2011

President of Drexel University Women in Computing Society (WiCS), 2010-2011.

Secretary of Drexel University IEEE Graduate Forum, 2010-2011.

Invited Talks

Twitter, 2016
Electronic Frontier Foundation (EFF), 2016
Conference on Information Sciences and Systems (CISS), Princeton University, 2016
ISAT/DARPA Workshop: Technological Disruptions of Societies and Organizations: Communications Networks, Computational Trust, Reputation, Anonymity, and Beyond, 2016
Bangladesh University of Engineering and Technology, 2015
Indiana University, 2015
Intel Research, 2015
IBM TJ Watson, 2015
NSF-funded meeting on IRB, privacy and big data in learning 2014
NSF review at UC San Diego 2014
Google Abuse Summit, Mountain View, CA 2014
Grace Hopper Celebration of Women in Computing 2014, 2012
Intel ISTC Retreat 2013, 2012

DataPhilly meetup, Philadelphia 2013
Chaos Communication Congress, Germany 2012, 2011
Stanford Security Seminar, Stanford University 2012
Duquesne university, Pittsburgh 2012
Girls Geek Dinner Philadelphia, 2012

Press

Articles on **cybercrime research**:

[1] Barron's Editorial Commentary, November 30, 2013: Efficiency Makes Crime Pay

Articles on **Doppelgänger Finder**:

[1] SC Magazine (Australian edition), Hacker News, and Slashdot, January 9, 2013: Linguistics identifies anonymous users

[2] Security Affairs blog, January 10, 2013: Stylometric analysis to track anonymous users in the underground

[3] Sydney Morning Herald, January 13, 2013: Why hackers should be afraid of how they write

[4] Schneier on Security blog, January 24, 2013: Identifying People from their Writing Style

Articles on **Anonymouth**:

[1] Slashdot, August 5, 2013: Project Anonymizes Your Writing Style To Hide Your Identity

[2] The New Republic, July 31, 2013: This Computer Program Turns Famous Writers Into Anonymous Hacks

[3] i-programmer, August 4, 2013: Anonymouth Hides Identity

[4] NYtimes Bits Blog, January 3, 2012: Software Helps Identify Anonymous Writers or Helps Them Stay That Way

[5] Der Spiegel, December 30, 2011: Wer Hemingway imitiert, schreibt anonym (Translation: "Whoever imitates Hemingway writes anonymously")

[6] BoingBoing, Dec 29, 2011: State of Adversarial Stylometry: can you change your prose-style?