# Anupam Das                                        Curriculum Vitae

CONTACT
INFORMATION
School of Computer Science
4121 Wean Hall,                          *Cell:*+1-(662)312-9029
5000 Forbes Avenue,                      *Email:* anupamd@cs.cmu.edu
Pittsburgh, PA–15213, USA                http://cs.cmu.edu/~anupamd

RESEARCH
INTERESTS
Explore new opportunities and challenges in both security and privacy for emerging technologies: context-aware smart assistants, information leakage in IoT data streams, privacy-ware data fusion.

EDUCATION

**University of Illinois at Urbana-Champaign (UIUC)**, IL, USA

PhD in Computer Science,                                    08/2010 – 06/2016

- Thesis Title: Understanding and Mitigating the Privacy Risks of Smartphone Sensor Fingerprinting
- Supervisor: Nikita Borisov
- Committee Members: Matthew Caesar, Romit Roy Choudhury, Paris Smaragdis, Dan Boneh (Stanford Univ.)

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

Master of Science in Computer Science and Engineering,        04/2008 – 06/2010

- Thesis Title: Dynamic Trust Model for Multi-agent Systems
- Supervisor: Dr. M. Mahfuzul Islam

Bachelor of Science in Computer Science and Engineering,       02/2003 – 11/2007

- Senior Thesis Title: Evolution of Neural Network using Genetic Algorithm
- Supervisor: Dr. Md. Monirul Islam and Dr. Md. Shohrab Hossain

HONORS AND
AWARDS
- Fellowships
  ⋄ Finalist of 2015 *Symantec Research Lab Graduate Fellowship*.
  ⋄ *Fulbright Science and Technology* fellowship from 2010 – 2013.
- CS@Illinois Feng Chen Memorial award 2015.
- Best paper awards
  ⋄ ACM MMSys 2017
  ⋄ ASIACCS 2014
- Distinguished poster awards
  ⋄ SOUPS 2017
- Excellent TA award for Fall 2011 at UIUC.
- Bangladesh University of Engineering and Technology
  ⋄ Dean's award in each of the four academic years for excellent academic result
  ⋄ Academic merit scholarship in each of the eight semesters for outstanding result

RESEARCH
EXPERIENCES
*Carnegie Mellon University* (CMU): Postdoctoral Fellow          07/2016 – present
- Prof. Norman Sadeh
- Prof. Lujo Bauer

|                          |                                                                                     |                      |
|--------------------------|-------------------------------------------------------------------------------------|----------------------|
|                          | *University of Illinois at Urbana-Champaign*: Research Assistant                     | 01/2011 – 06/2016    |
|                          | • Prof. Nikita Borisov                                                               |                      |
|                          | • Prof. Matthew Caesar                                                               |                      |
|                          | *Bangladesh University of Engr. and Tech.*: Graduate Student                         | 03/2009 – 08/2010    |
|                          | • Dr. M. Mahfuzul Islam                                                              |                      |

| PROFESSIONAL EXPERIENCE | |
|---|---|

Assistant Professor, Dept. of Computer Sci. and Engr., BUET     04/2008 – 08/2010
  • Lectured different undergraduate-level courses ([link](link))
Google     01/2015 – 04/2015
  • Worked on continuous authentication system for smartphones
VMware     05/2014 – 08/2014
  • Developed an application whitelisting service for virtualized setting
DisruptDev (startup)     05/2013 – 08/2013
  • Worked on designing a secure storage system
NEC Labs America     05/2012 – 08/2012
  • Developed a middle-ware to boost Hadoop performance

## TEACHING EXPERIENCE

*Guest Lecturer, School of Computer Science, CMU*
  • Information Security and Privacy     Fall 2016
*Teaching Assistant, Department of Computer Science, UIUC*
  • CS 463 (Computer Security II),     Spring 2013
  • CS 105 (Introduction to Computing),     Fall 2011
*Lecturer, Department of Computer Science and Engineering, BUET*
  • CSE 321 (Computer Networks),     May 2010
  • CSE 209 (Digital Electronics and Pulse Techniques),     Oct. 2009
  • CSE 409 (Computer Graphics),     Mar. 2009
  • CSE 205 (Digital Logic Design),     July 2008
  • CSE 100 (Introduction to Computer Programming),     Apr. 2008
*Cisco Regional Academy Instructor, BUET*
  • CNNA Exploration Module 1 to 4     05/2008 – 08/2010

## MENTORING EXPERIENCE

*Mentoring Graduate Students at CMU*
  • Daniel Smullen; Project: Privacy-aware IoT infrastructure     Fall 2017 – present
  • Aerin Zhang; Project: Notification preference study     Spring 2017 – present
  • Zheng Zong, Ludi Li; Project: Privacy-aware indoor location service     Fall 2016
  • A. Shah, D. Shaji, T. Liu; Project: Privacy issues of facial recognition     Fall 2016
*Mentor for Promoting Undergraduate Research in Engineering at UIUC*
  • Jacob Trueb, Qiuhua Ding; Project: Personalized security questions     Fall 2014
  • Ziqiao Ding; Project: Bandwidth anomalies of Tor relays     Fall 2014
*Mentoring Undergraduate Independent Study at UIUC*
  • Jacob Trueb, Qiuhua Ding; Project: Profiling users' app behavior     Spring 2015
  • Edward Chou, Project: Mitigating motion sensors fingerprinting     Spring 2016

## PATENTS

[FlowComb](FlowComb): Boosting Big Data Processing with OpenFlow

## TRAININGS

• Cisco Certified Network Associate (CCNA), BUET 2008.
• Teachers' Appreciation Workshop, BUET 2009.

*Google Scholar*

### Journals

1. J. Wang, B. Amos, **A. Das**, P. Pillai, N. Sadeh, and M. Satyanarayanan. Enabling live video analytics with a scalable and privacy-aware middleware. *ACM Transactions on Multimedia Computing, Communications and Applications (TOMM)*, 14(3s), 2018

2. **A. Das**, N. Borisov, and E. Chou. Every move you make: Exploring practical issues in smartphone motion sensor fingerprinting and countermeasures. In *Proceedings of the 18th Privacy Enhancing Technologies Symposium (PoPETs)*, 2018. (to appear)

3. J. Juen, A. Johnson, **A. Das**, N. Borisov, and M. Caesar. Defending Tor from network adversaries: A case study of network path prediction. In *Proceedings of the 15th Privacy Enhancing Technologies Symposium (PoPETs)*, pages 171–187, 2015

4. **A. Das** and M. M. Islam. SecuredTrust: A dynamic trust computation model for secured communication in multiagent systems. *IEEE Transactions on Dependable and Secure Computing*, 9(2):261–274, 2012

### Magazine Article

1. **A. Das**, M. Degeling, N. Sadeh, and D. Smullen. Personal privacy assistants for the Internet of Things. *IEEE Pervasive Computing*, 2018

### Conference proceedings

1. W. Melicher, **A. Das**, M. Sharif, L. Bauer, and L. Jia. Riding out DOMsday: Towards detecting and preventing DOM cross-site scripting. In *Proceedings of the 25th Annual Network and Distributed System Security Symposium (NDSS)*, 2018. (to appear)

2. R. Tahir, M. Huzaifa, **A. Das**, M. Ahmad, C. Gunter, F. Zafar, M. Caesar, and N. Borisov. Mining on someone else's dime: Mitigating covert mining operations in clouds and enterprises. In *Proceedings of the 20th International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, 2017

3. J. Wang, B. Amos, **A. Das**, P. Pillai, N. Sadeh, and M. Satyanarayanan. A scalable and privacy-aware IoT service for live video analytics. In *Proceedings of the 8th ACM on Multimedia Systems Conference (MMSys)*, pages 38–49, 2017. <span style="color:red">(Best Paper Award)</span>

4. S. Ji, S. Yang, **A. Das**, X. Hu, and R. Beyah. Password correlation: Quantification, evaluation and application. In *Proceedings of the 36th IEEE Annual International Conference on Computer Communications (INFOCOM)*, 2017

5. M. Surbatovich, J. Aljuraidan, L. Bauer, **A. Das**, and L. Jia. Some recipes can do more than spoil your appetite: Analyzing the security and privacy risks of IFTTT recipes. In *Proceedings of the 26th International World Wide Web Conference (WWW)*, pages 1501–1510, 2017

6. **A. Das**, N. Borisov, and M. Caesar. Tracking mobile web users through motion sensors: Attacks and defenses. In *Proceedings of the 23rd Annual Network and Distributed System Security Symposium (NDSS)*, 2016

7. **A. Das**, N. Borisov, and M. Caesar. Do you hear what I hear? Fingerprinting smart devices through embedded acoustic components. In *Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS)*, pages 441–452, 2014

8. **A. Das**, N. Borisov, and M. Caesar. Analyzing an adaptive reputation metric for anonymity systems. In *Proceedings of the First ACM Symposium and Bootcamp on the Science of Security (HotSoS)*, pages 11:1–11:11, 2014

9. **A. Das**, N. Borisov, P. Mittal, and M. Caesar. $Re^3$: Relay reliability reputation for anonymity systems. In *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, pages 63–74, 2014. (Best Paper Award)

10. **A. Das**, J. Bonneau, M. Caesar, N. Borisov, and X. Wang. The tangled web of password reuse. In *Proceedings of the 21st Annual Network and Distributed System Security Symposium (NDSS)*, 2014

11. **A. Das** and N. Borisov. Securing anonymous communication channels under the selective DoS attack. In *Proceedings of the 17th Financial Cryptography and Data Security (FC)*, pages 362–370, 2013

12. **A. Das**, M. M. Islam, and G. Sorwar. Dynamic trust model for reliable transactions in multi-agent systems. In *Proceedings of the 13th IEEE International Conference on Advanced Communication Technology (ICACT)*, pages 1101–1106, 2011

13. **A. Das** and M. M. Islam. A novel feedback based fast adaptive trust model for P2P networks. In *Proceedings of the 35th IEEE Conference on Local Computer Networks (LCN)*, pages 552–559, 2010

14. **A. Das** and S. M. Abdullah. Evolving multilayer neural networks using permutation free encoding technique. In *Proceedings of the 2009 International Conference on Artificial Intelligence (ICAI)*, pages 32–38, 2009

15. **A. Das**, M. Hossain, S. M. Abdullah, and R. U. Islam. Permutation free encoding technique for evolving neural networks. In *Proceedings of the 5th International Symposium on Neural Networks: Advances in Neural Networks (ISNN)*, pages 255–265, 2008

### Workshop proceedings

1. **A. Das**, M. Degeling, X. Wang, J. Wang, N. Sadeh, and M. Satyanarayanan. Assisting users in a world full of cameras: A privacy-aware infrastructure for computer vision applications. In *Proceedings of the 30th IEEE Computer Vision and Pattern Recognition Workshops (CVPRW)*, pages 1387–1396, 2017

2. P. Pappachan, M. Degeling, R. Yus, **A. Das**, S. Bhagavatula, W. Melicher, P. E. Naeini, S. Zhang, L. Bauer, A. Kobsa, S. Mehrotra, N. Sadeh, and N. Venkatasubramanian. Towards privacy-aware smart buildings: Capturing, communicating, and enforcing privacy policies and preferences. In *Proceedings of the 37th IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW)*, pages 193–198, 2017

3. **A. Das**, C. Lumezanu, Y. Zhang, V. Singh, G. Jiang, and C. Yu. Transparent and flexible network management for big data processing in the cloud. In *Proceedings of the 5th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud)*, pages 1–6, 2013

### Technical reports

1. **A. Das**, N. Borisov, E. Chou, and M. H. Mughees. Smartphone fingerprinting via motion sensors: Analyzing feasibility at large-scale and studying real usage patterns. *CoRR*, abs/1605.08763, 2016. http://arxiv.org/abs/1605.08763

2. **A. Das**, N. Borisov, and M. Caesar. Exploring ways to mitigate sensor-based smartphone fingerprinting. *CoRR*, abs/1503.01874, 2015. http://arxiv.org/abs/1503.01874

3. **A. Das**, N. Borisov, and M. Caesar. Fingerprinting smart devices through embedded acoustic components. *CoRR*, abs/1403.3366, 2014. http://arxiv.org/abs/1403.3366

4. **A. Das** and N. Borisov. Securing tor tunnels under the selective-DoS attack. *CoRR*,

abs/1107.3863, 2011. http://arxiv.org/abs/1107.3863

### Posters

1. N. Sadeh, M. Degeling, **A. Das**, A. S. Zhang, A. Acquisti, L. Bauer, L. Cranor, A. Datta, and D. Smullen. A privacy assistant for the Internet of Things. In *the 13th USENIX Symposium on Usable Privacy and Security (SOUPS)*, 2017. https://www.usenix.org/sites/default/files/soups17_poster_sadeh.pdf (Distinguished Poster Award)

2. **A. Das** and N. Borisov. Fingerprinting smartphones through speakers. In *the 35th IEEE Symposium on Security and Privacy (SP)*, 2014. http://www.ieee-security.org/TC/SP2014/posters/DASAN.pdf

3. G. T. K. Nguyen, X. Gong, **A. Das**, and N. Borisov. PnP: Improving web browsing performance over tor using web resource prefetch-and-push. In *the 20th ACM Conference on Computer and Communications Security (CCS)*, 2013. http://hatswitch.org/~nikita/papers/pnp-poster-ccs13.pdf

### Theses

1. **A. Das**. *Understanding and Mitigating the Privacy Risks of Smartphone Sensor Fingerprinting*. Ph.D. thesis, Department of Computer Science, University of Illinois at Urbana-Champaign, 2016

2. **A. Das**. Feedback based dynamic trust model for secured communication in multi-agent systems. M.Sc. thesis, Department of Computer Science and Engineering, Bangladesh University of Engineering and Technology, 2010

3. **A. Das**. Evolving neural networks using evolutionary algorithm. B.Sc. thesis, Department of Computer Science and Engineering, Bangladesh University of Engineering and Technology, 2008

CONFERENCE
TALKS AND
TUTORIALS

### Conference/Workshop Talk

- Assisting users in a world full of cameras: A privacy-aware infrastructure for computer vision applications. *The First International Workshop on The Bright and Dark Sides of Computer Vision: Challenges and Opportunities for Privacy and Security* (CV-COPS 2017), Honolulu, HI, USA, July 2017.

- Tracking mobile web users through motion sensors: Attacks and defenses. *The Network and Distributed System Security Symposium* (NDSS), San Diego, CA, USA, Feb. 2016.

- Do you hear what I hear? Fingerprinting smart devices through embedded acoustic components. *ACM Conference on Computer and Communications Security* (CCS), Scottsdale, AZ, USA, Nov. 2014.

- $Re^3$: Relay reliability reputation for anonymity systems. *ACM Symposium on Information, Computer and Communications Security* (ASIACCS), Kyoto, Japan, June 2014.

- Analyzing an adaptive reputation metric for anonymity systems. *ACM Symposium and Bootcamp on the Science of Security* (HotSoS), Raleigh, NC, USA, Apr. 2014.

- The tangled web of password reuse. *The Network and Distributed System Security Symposium* (NDSS), San Diego, CA, USA, Feb. 2014.

- Securing anonymous communication channels under the selective-DoS attack. *Financial Cryptography and Data Security* (FC), Okinawa, Japan, Apr. 2013.

- A novel feedback based fast adaptive trust model for P2P networks. *IEEE Conference*

*on Local Computer Networks* (LCN), Denver, CO, USA, Oct. 2010.

**Tutorial**
- An overview of usable privacy technologies, tools and findings coming out of recent research at Carnegie Mellon University. *USENIX Symposium on Usable Privacy and Security* (SOUPS), Santa Clara, CA, USA, July 2017.

| Invited Talks | *Tracking mobile web users through motion sensors: Attacks and defenses* | |
|---|---|---|
| | • Keynote speech at the 5th ACM IH&MMSec | Jun. 2017 |
| | • Carnegie Mellon University, Host: Norman Sadeh | Oct. 2016 |
| | • UC Berkeley, Host: Grant Ho | Feb. 2016 |
| | • IBM T.J. Watson Research Center, Host: Ian Molloy | Feb. 2016 |
| | • Cornell University, Host: Elaine Shi | Jan. 2016 |
| | • UIUC, Host: Romit Roy Choudhury | Oct. 2015 |

Media/Online Coverage

- Some recipes can do more than spoil your appetite: Analyzing the security and privacy risks of IFTTT recipes
  - ◇ CyLab News
- Smartphone fingerprinting via motion sensors: Analyzing feasibility at large-scale and studying real usage patterns
  - ◇ Motherboard    ◇ ECE Newroom, UIUC
- The tangled web of password reuse
  - ◇ ZDNet    ◇ FastCompany
- Defending Tor from network adversaries: A case study of network path prediction
  - ◇ Tor Weekly News, October 15th, 2014

Professional Services

- **Program Co-chair**: ACM MMSys '18 Special session on IoT and Smart cites
- **Program Committee Member**: CCS '17, WWW '18, CV-COPS '18, WPES '19, PoPETS '19
- **Invited Reviewer**: IEEE Pervasive Computing '18, ACM TOPS '17, ACM TWEB '17, IEEE TIFS '17-18, Elsevier PMC '15, IEEE TPDS '13
- **External Conference Reviewer**: CHI '18, USENIX '17, IEEE S&P '17, SOUPS '17, USENIX '16, CCS '15, CCS '14, SigComm '14, NDSS '12, CCS '12, CCS '11, IEEE LCN '10, GECCO '09
- **Organizing Committee Member**: WALCOM 2010
- **Consultancy**: Bureau of Research, Testing and Consultation, BUET    2008 – 2010