

Aditya Basu

https:// adityabasu.me
github:// [mitthu](https://github.com/mitthu)
google scholar:// [NjtxVEoAAAAJ](https://scholar.google.com/citations?user=NjtxVEoAAAAJ)
orcid:// [0000-0002-9760-0912](https://orcid.org/0000-0002-9760-0912)

☎ (814) 862-8300
✉ ab.aditya.basu@gmail.com

- Education**
- PhD Candidate** in *Computer Science* May 2025
at *Pennsylvania State University*, PA, USA
GPA: 3.85 (of 4). Advised by Trent Jaeger.
- B.Tech.** in *Information and Communication Technology* August 2014
from *Dhirubhai Ambani Institute (DAIICT)*, Gujarat, India
GPA: 9.52 (of 10) in major, 8.55 overall
- Work Experience**
- Research Scientist**, Meta (Facebook), Menlo Park, CA, USA July 8, 2024 - current
Automated fetching cryptographic keys that are needed for decrypting user data during AI training with strict lifecycle management. The system ensures that even with physical hardware access, an untrusted vendor cannot get hold of unencrypted data.
Skills: C++ • Python • Apache Thrift • Filesystem Security
- Research Intern**, Microsoft Research, Redmond, WA, USA May 16 – Aug. 5, 2022
Integrated HDFS with our Nimble framework (published in OSDI '23) to detect rollback attacks by untrusted cloud providers.
Skills: Golang • Java • HDFS • Bash • LXC Containers • Docker | **Code:** github.com/mitthu/hadoop-nimble
- Software Engineering Intern**, Google, Cambridge, MA, USA May 13 – Aug. 16, 2019
Added support for Intel VT-d to the Akaros kernel allowing any PCI/PCIe device to be placed in the address space of a process or a VM. Also wrote a driver for Intel's DMA accelerator (IOAT).
Skills: C • QEMU • GDB • x86 Assembly | **Code:** github.com/brho/akaros
- Product Security Intern**, NIO, San Jose, CA, USA May – Aug. 2018
Pen-tested ES8's (SUV) firmware via the OBD-II diagnostics port and wrote a driver for an on-board network switch.
Skills: C • Python
- System Operations**, Media.net, Mumbai, India Jul. 2014 – Jul. 2016
Managed the web crawling infrastructure that served >100 million reqs./day. Also conducted training sessions on Linux and networking.
Skills: C • Python • Java • Bash • AWS • Puppet • Ansible • Docker • Mesos • Hadoop
- Software Developer Intern**, DAIICT, Gandhinagar, India June–July of '13, '14 & '15
Developed the university's admissions portal to generate merit-lists and wait-lists of candidates based on their module preferences and standardized test scores.
Skills: Python • Django Framework • HTML • CSS • JavaScript • PostgreSQL

Skills	<p>>10k lines: C • Python • Golang • bash • \LaTeX (macros) • HTML</p> <p>5k – 10k lines: x86 Assembly • C++ • Java • BPF • Django • Puppet • Ansible • CSS</p> <p>Utilities: make • git • Docker • strace • GDB • Protocol Buffers</p> <p>Others: Linux • Mac OS X • Markdown • HDFS • IDA Hex-Rays • Intel[®] Processor Trace</p>
Research Artifacts	<p>Collision detector identifies name collisions from Auditd traces [Golang • bash]</p> <p>Nimble-aware Hadoop detects rollback attacks on HDFS [Java • Protobuf]</p> <p>Printable Shellcode Compiler transforms shellcode: binary → printable [C • x86 asm]</p> <p>Alpha Loader transforms shellcode: binary → compact ASCII [C • x86 asm • Python • Bash]</p>
Publications	<ol style="list-style-type: none"> 1. TALISMAN: Tamper Analysis for Reference Monitors. Frank Capobianco, Quan Zhou, Aditya Basu, Trent Jaeger, Danfeng Zhang. In <i>Network and Distributed System Security Symposium (NDSS)</i>. 2024. Acceptance rate: 15%, or 104/694 • Publication 2. Unsafe at Any Copy: Name Collisions from Mixing Case Sensitivities. Aditya Basu, Jack Sampson, Zhiyun Qian, Trent Jaeger. In <i>21st USENIX Conference on File and Storage Technologies (FAST)</i>. 2023. Acceptance rate: 23%, or 28/122 • Recipient of USENIX Student Grant • Publication • Code 3. Nimble: Rollback Protection for Confidential Cloud Services. Sebastian Angel, Aditya Basu, Weidong Cui, Trent Jaeger, Stella Lau, Srinath Setty, Sudheesh Singanamalla. In <i>17th USENIX Symposium on Operating Systems Design and Implementation (OSDI)</i>. 2023. Acceptance rate: 19.6%, or 50/255 • Publication • Code (HDFS) • Code (Nimble) 4. Automatic Generation of Compact Printable Shellcodes for x86. Dhruvil Patel, Aditya Basu, Anish Mathuria. In <i>14th USENIX Workshop on Offensive Technologies (WOOT)</i>. 2020. Acceptance rate: 33.33%, or 12/36 • Publication • Code 5. Hardware Assisted Buffer Protection Mechanisms for Embedded RISC-V. Asmit De, Aditya Basu, Swaroop Ghosh, Trent Jaeger. In <i>IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems</i>. 2020. Impact factor: 2.168 • DOI: 10.1109/TCAD.2020.2984407 6. FIXER: Flow Integrity Extensions in Embedded RISC-V. Asmit De, Aditya Basu, Swaroop Ghosh and Trent Jaeger. In <i>Proceedings of Design, Automation and Test in Europe (DATE)</i>. 2019. Acceptance rate: 24% • DOI: 10.23919/DATE.2019.8714980 7. Automatic Generation of Compact Alphanumeric Shellcodes for x86. Aditya Basu, Anish Mathuria, Nagendra Chowdary. In <i>Proceedings of 10th International Conference on Information Systems Security (ICISS)</i>. 2014. Acceptance rate: 19%, or 25/129 • DOI: 10.1007/978-3-319-13841-1_22 • Code
Posters & Demos	<p>Detecting and Preventing Resource Naming Attacks at <i>Collaborative Research Alliance (CRA), Delaware</i>. Poster. 2023.</p> <p>Provenance using Process Introspection at <i>Collaborative Research Alliance (CRA) Bootcamp, University of California, Irvine</i>. Poster. 2022.</p> <p>Flexible Process Monitoring with the Process Firewall at <i>Total Platform Cyber Protection (TPCP) Software Security Summer School (SSSS)</i>. Demo. 2020.</p>

Execution Integrity at *Total Platform Cyber Protection (TPCP)*, Northeastern University. Poster. 2019.

CFI Enforcement on the Linux Kernel at *Industry Day – Institute for Network and Security Research (INSR)*, PennState. Poster. 2017.

Peer Reviewer	2025 ACM Transactions on Embedded Computing Systems	x 1
	2023 IEEE Transactions on Aerospace and Electronic Systems	x 1
	2022 IEEE Computer Architecture Letters	x 2
	2018 IEEE Computer Architecture Letters	x 1
Assistantships	Research Assistant , PennState	2017-2023 (except when TA)
	Lead Teaching Assistant , PennState – Operating Systems	Spring 2023, Spring 2024
	Teaching Assistant , PennState – Operating Systems	Fall 2016, Spring 2018
	Teaching Assistant , DAIICT – Systems Software	Spring 2014
Extracurriculars	President of <i>Shotokan Karate-do Club</i> at PennState	2022-23
	President of <i>Social Dance Club</i> at PennState	2022-23
	Co-ordinator of <i>Argentine Tango</i> at PennState	2019-20
	Started the <i>Linux Pack Club</i> at DAIICT	2013