Prashant Anantharaman

Doctor of Philosophy (Ph.D.) Candidate,
Department of Computer Science,
Dartmouth College, NH, USA.

Phone: (510) 904-8439
Email: pa@cs.dartmouth.edu
Web: https://prashant.at
Google Scholar: https://prashant.at/gscholar
LinkedIn: https://linkedin.com/in/prashant-a
Github account: https://github.com/prashantbarca

Education

- **Doctor of Philosophy (Ph.D.)** in Computer Science **June 2022 (Expected)**
  Dartmouth College, NH, USA
  Research Area: Securing Data Formats, Formally Verified Parsers
  Thesis: Protecting Systems from Exploits using Language-theoretic Security
  Advisors: Dr. Sean W. Smith and Dr. Sergey Bratus
- **Master of Science** in Computer Science **June 2017**
  Dartmouth College, NH, USA.
  Research Area: Internet of Things and Power Grid Security
  Advisors: Dr. Sean W. Smith and Dr. Sergey Bratus
- **Bachelor of Engineering** in Computer Science and Engineering **May 2015**
  College of Engineering Guindy, Chennai, India
  Research Area: Compilers and Systems
  Thesis: Code Compaction in LLVM IR.
  TCS Best Senior Thesis Award.
  Advisor: Dr. Arul Siromoney

Research Interests – Social Aspects of Privacy, Internet of Things (IoT)

- Conduct Vignette studies (on mTurk and via interviews) to better inform security and privacy decisions and policy
- Understand privacy attitudes of users towards various types of IoT devices
- Protect IoT devices and their users from exploits by building *secure* and *safe* software

My main contributions so far have been in the fields of (a) Language-theoretic Security: building new parsing methodologies and demonstrating them on various network formats and file formats, (b) Internet of Things: Behavioral analysis of various commercial IoT devices.

Highlights

- **Publications:** 15+ peer-reviewed papers in top conferences and journals (IoT, NSPW, SPW, IEEE S&P)
- **Awards:** Best Paper Award and Best Paper Award Nomination at ACM IoT Conference, TCS Best Senior Thesis Award, Dartmouth Graduate Student Scholarship
- **Service:** TPC and Reviewer at top-tier IEEE and ACM journals and conferences (WF-IoT, IEEE/ACM Networking, LangSec)
- **Collaborations:** Multiple ongoing and past collaborations with Industry (SRI International, Narf Industries, GE Research) and universities (UIUC, NYU) funded by the US DoE and DARPA

Experience

- **Student Research Associate** **June 2018 – September 2018**
  IoT Security and Privacy Center, SRI International, New York, NY, USA
  Advisors: Dr. Michael Locasto, Dr. Gabriela Ciocarlie, Dr. Ulf Lindqvist.
  Research: Device identification and fingerprinting in Internet-of-Things networks using clustering.
- **Student Research Associate** **June 2017 – September 2017**
  IoT Security and Privacy Center, SRI International, Menlo Park, CA, USA
  Advisors: Dr. Bogdan Copos, Dr. Michael Locasto, Dr. Ulf Lindqvist.
  Research: Designing *composite-metrics* to understand the security of Internet-of-Things ecosystems.
- **Student Research Associate** **June 2016 – September 2016**
  IoT Security and Privacy Center, SRI International, Menlo Park, CA, USA
  Advisors: Dr. Michael Locasto, Dr. Gabriela Ciocarlie, Dr. Ulf Lindqvist.
  Research: Building *Language-theoretic security* compliant clients for application layer Internet-of-Things protocols.
- **Student Trainee/Intern** **May 2013 – July 2013**
  Samsung R&D Institute, Bangalore, India – Intelligent Search Team
  Advisor: Mohan Sundar B.
  Research: Designing a graph searching system using Neo4J and Apache Giraph.

Current Projects

- Expert elicitation study to understand desired features in data description languages: A qualitative study to derive expert-desired properties using the Delphi Method (interviewed 20 experts)
- An mTurk study examining how users evaluate URLs: A large-scale (over 1100 participants hired on mTurk) quantitative study to determine what are some unsafe URL structures to which users are most susceptible
- Verified parser generators for file formats using Dafny
- FPGA-based parsers using Dafny and VHDL to validate and serialize parsers at line-speed
- Traffic validator for Smart Grid networks using Language-theoretic Security

---

Publications

Book Chapters

B1. **Prashant Anantharaman** et al.
"Intent as a Secure Design Primitive"
Modeling and Design of Secure Internet of Things
John Wiley and Sons, Inc.
DOI: https://doi.org/10.1002/9781119593386.ch23

B2. I. Agadakos, **Prashant Anantharaman** et al.
"Securing Smart Cities: Implications and Challenges"
Modeling and Design of Secure Internet of Things
John Wiley and Sons, Inc.
DOI: https://doi.org/10.1002/9781119593386.ch9

Patents

P1. Gabriela F Ciocarlie, Ioannis Agadakos, Chien-Ying Chen, Matteo Campanelli, **Prashant Anantharaman**, Monowar Hasan, Ulf Lindqvist, Michael Locasto, Bogdan Copos, Tancrède Lepoint, Matthew Filippone
"Modeling cyber-physical attack paths in the internet-of-things"
2020/5/21: US Patent number 16634591

Magazine Articles

M1. Sameed Ali, **Prashant Anantharaman**, Zephyr S. Lucas and Sean W. Smith
"What We Have Here Is Failure to Validate: Summer of LangSec."
IEEE Security and Privacy
May/June 2021
DOI: https://doi.org/10.1109/MSEC.2021.3059167

Conferences and Workshops

C1. Zephyr S. Lucas, Joanna Liu, **Prashant Anantharaman**, Sean W. Smith
"Pegmatite: Parsing PEGs with Length Fields in Software and Hardware"
Seventh Language-theoretic Security (LangSec) IEEE Security and Privacy Workshop, Virtual.
May 2021
DOI: https://doi.org/10.1109/SPW53761.2021.00026

C2. **Prashant Anantharaman***, Liwei Song*, Ioannis Agadakos, Bogdan Copos, Gabriela Ciocarlie, Ulf Lindqvist, Michael E. Locasto
"IoTHound: Environment-agnostic Device Identification and Monitoring"
10th International Conference on the Internet of Things (IoT 2020), Malmo, Sweden
★ *Best Paper Award (Top 1 paper out of 84 submitted papers)*
October 6-9th, 2020.
**Equal Contributions*
DOI: https://doi.org/10.1145/3410992.3410993

C3. S. Ali, **Prashant Anantharaman** and S.W. Smith
"Armor Within: Defending against Vulnerabilities in Third-Party Libraries"
Sixth Language-theoretic Security (LangSec) IEEE Security and Privacy Workshop
May 2020.
DOI: https://doi.org/10.1109/SPW50608.2020.00063

C4. P. Mundkur, **Prashant Anantharaman**, S. Ali, L. Briesemeister, N. Shankar and S.W. Smith.
"The Parsley Data Format Definition Language"
Sixth Language-theoretic Security (LangSec) IEEE Security and Privacy Workshop.
May 2020.
DOI: https://doi.org/10.1109/SPW50608.2020.00064

C5. I.R. Jenkins, **Prashant Anantharaman**, R. Shapiro, J.P. Brady, S. Bratus and S.W. Smith.
"Ghostbusting: Mitigating Spectre with Intraprocess Memory Isolation"
7th Annual Symposium and Bootcamp on Hot Topics in the Science of Security (HotSoS '20).
April 2020.
DOI: https://doi.org/10.1145/3384217.3385627

C6. **Prashant Anantharaman**, Kartik Palani, Sean W. Smith
"Scalable Identity and Key Management for Publish-Subscribe Protocols in the Internet-of-Things"
9th International Conference on Internet of Things (IoT 2019), Bilbao, Spain
October 22-25th, 2019.
★ *Nominated for the Best Paper Award, and received an Honorable Mention Award for the Top 3 papers (Top 3 papers out of 84 submitted papers)*
DOI: https://doi.org/10.1145/3365871.3365883

C7. **Prashant Anantharaman**, Vijay Kothari, J. Peter Brady, Ira Ray Jenkins, Sameed Ali, Michael C. Millian, Ross Koppel, Jim Blythe, Sergey Bratus, and Sean W. Smith
"Mismorphism: The Heart of the Weird Machine"
Twenty-seventh International Workshop on Security Protocols, Trinity College, Cambridge, UK
April 12–14th, 2019.
DOI: https://doi.org/10.1007/978-3-030-57043-9_11

C8. Vijay Kothari, **Prashant Anantharaman**, J. Peter Brady, Ira Ray Jenkins, Sameed Ali, Michael C. Millian, Ross Koppel, Jim Blythe, Sergey Bratus, and Sean W. Smith
"Human-Computability Boundaries"

Twenty-seventh International Workshop on Security Protocols, Trinity College, Cambridge, UK April 12–14th, 2019.
DOI: https://doi.org/10.1007/978-3-030-57043-9_15

C9. Michael C. Millian, **Prashant Anantharaman**, Sergey Bratus, Sean W. Smith, Michael E. Locasto
"Converting an Electric Power Utility Network to Defend Against Crafted Inputs"
Thirteenth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, Arlington, VA
March 11–12th, 2019.
DOI: https://doi.org/10.1007/978-3-030-34647-8_4

C10. **Prashant Anantharaman**, Kartik Palani, Rafael Brantley, Galen Brown, Sergey Bratus, Sean W. Smith
"PhasorSec: Protocol Security Filters for Wide Area Measurement Systems"
IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, Aalborg, Denmark
October 29-31, 2018.
DOI: https://doi.org/10.1109/SmartGridComm.2018.8587501

C11. **Prashant Anantharaman**, J. Peter Brady, Patrick Flathers, Vijay H. Kothari, Michael C. Millian, William G. Nisen, Jason Reeves, Nathan Reitinger, Sean W. Smith.
"Going Dark: A Retrospective on the North American Blackout of 2038"
New Security Paradigms Workshop (NSPW '18), Windsor, UK
August 28-31, 2018.
DOI: https://doi.org/10.1145/3285002.3285011

C12. Ioannis Agadakos*, Chien-Ying Chen*, Matteo Campanelli*, **Prashant Anantharaman***, Monowar Hasan*, Bogdan Copos*, Tancrede Lepoint, Michael Locasto, Gabriela F. Ciocarlie, Ulf Lindqvist
** Equal Contributions*
"Jumping the Air Gap: Modeling Cyber-Physical Attack Paths in the Internet-of-Things"
3rd ACM CCS Cyber-Physical Systems Security and Privacy Workshop
November 2017.
DOI: https://doi.org/10.1145/3140241.3140252

C13. **Prashant Anantharaman**, Michael M. Millian, Sergey Bratus, Meredith L. Patterson.
"Input Handling Done Right: Building Hardened Parsers using Language-theoretic Security"
2nd IEEE Cybersecurity Development Conference, Boston, MA
September 2017.
DOI: https://doi.org/10.1109/SecDev.2017.12

C14. **P. Anantharaman**, M. Locasto, G. Ciocarlie, U. Lindqvist.
"Building hardened Internet-of-Things implementations using Language-theoretic Security"
IEEE Symposium on Security and Privacy – Language-theoretic Security Workshop.
May 2017.
DOI: https://doi.org/10.1109/SPW.2017.36

C15. **P. Anantharaman**, K. Palani, D. Nicol, S.W. Smith.
"I am Joe's Fridge: Scalable Identity in the Internet of Things"
IEEE International Conference on Internet of Things.
December 2016.
DOI: https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.47

C16. G. Ramakrishnan, **P. Anantharaman**, and S. Mukherjee.
"Proactive Resource Provisioning Model for Cloud Federation"
International Conference on Distributed Computing and Internet Technology.
January 2016.
DOI: https://doi.org/10.1007/978-3-319-28034-9_22

Talks and Presentations

- *IoTHound: Environment-agnostic Device Identification and Monitoring*
  10th International Conference on Internet of Things (IoT 2020)

October 8th, 2020

- *Building Hardened IoT Implementations with LangSec*
  Nullcon Security Conference, Goa, India
  March 2nd, 2019
- *Ghostbusters: A tale of ELF, ABI and Spectre*
  BSidesAugusta
  Augusta, GA
  September 20th, 2018
- *Going Dark: A Retrospective on the Blackout of 2038*
  New Security Paradigms Workshop
  Windsor, UK
  August 28th, 2018
- *LangSec for Critical Infrastructure: SSP21, a secure lightweight SCADA protocol*
  5th LangSec Workshop at IEEE Symposium on Security and Privacy (Oakland)
  San Francisco, CA
  May 24th, 2018
- *Input Handling Done Right: Building Hardened Parsers using Language-theoretic Security*
  IEEE Cybersecurity Development Conference
  Boston, MA
  September 24th 2017
- *Building Hardened Internet-of-Things Clients using Language-theoretic Security*
  4th LangSec Workshop at IEEE Symposium on Security and Privacy (Oakland)
  San Jose, CA
  May 25th 2017
- *Building vertically hardened Industrial-Control-Systems applications using Language-theoretic security*
  2nd CREDC Industrial Workshop
  Tempe, AZ
  March 28th 2017
- *Scalability Identity in the Internet of Things*
  IEEE International Conference on Internet of Things
  Chengdu, China
  December 18th 2016

Teaching Experience

Sep. '16 – Nov. '16	Teaching Assistant for *Programming Languages (COSC 59)* Instructor – Dr. Sergey Bratus
Jun. '15	*Ruby on Rails* Instructor at FSFTN Summer Camp Number of participants: 120 Venue: IIT Madras, Chennai, India
Sep. '13 – May '15	Lecturer at CEG's GNU/Linux Users Group Topics covered: Ruby, Python, Git, Vim, Emacs Number of participants: 70

Advising

Prashant has advised the following Masters and undergraduate research students in collaboration with Prof. Sean W. Smith and Prof. Sergey Bratus at Dartmouth College.

Masters

2021 Anmol Chachra (LangSec: RADICS Project)

2019 Sameed Ali (LangSec)

Undergrads

2021 Patrick Norton (Verified Parsing)
2021 Shikhar Sinha (Senior Thesis: FPGA Parsing)
2021 Joanna Liu (FPGA Parsing)
2020 Andrew Truong (MQTT Security)
2020 Celina Tala (Safedocs)
2020 Syed H. Tanveer (LangSec: RADICS Project)
2018 Patrick J. Flathers (LangSec)
2017 Rafael Brantley (PhasorSec)
2017 Galen Brown (PhasorSec)

Select Fellowships and Awards

2020 Best Paper Award at the International Conference on Internet of Things (IoT'20)
2019 Honorable Mention Award at the International Conference on Internet of Things (IoT'19)
2015 TCS Award for Best Senior Thesis

Press and News Coverage

Quotes on Ransomware Attacks

2021 WCAX TV News Live Interview – "How can UVM Health Network prevent future cyberattacks?" – https://www.wcax.com/2021/05/28/how-can-uvm-health-network-prevent-future-cyberattacks/

2021 Vox Recode Quoted in the article – "What you need to know about ransomware and the future of cyberattacks" – https://www.vox.com/recode/22527272/ransomware-cyberattacks-bitcoin-explained

PhasorSec

2019 Dartmouth Press Dartmouth's PhasorSec Protects Power Grids from Cyberattack – https://www.dartmouth.edu/press-releases/dartmouths_phasorsec_protects_power-grids_from_cyberattack.html

Spectre V1 Defenses

2018 Dartmouth News Graduate Students Create Computer-Chip Security Fix – https://news.dartmouth.edu/news/2018/10/graduate-students-create-computer-chip-security-fix

2018 Bleeping Computer Academics Announce New Protections Against Spectre and Rowhammer Attacks – https://www.bleepingcomputer.com/news/security/academics-announce-new-protections-against-spectre-and-rowhammer-attacks/

2018 The Register Spectre rises from the dead to bite Intel in the return stack buffer – https://www.theregister.co.uk/2018/07/23/spectre_return_stack_buffer/

2018 SlashDot Academics Publish New Software-Level Protections Against Spectre and Rowhammer Attacks – https://it.slashdot.org/story/18/07/23/1613217/academics-publish-new-software-level-protections-against-spectre-and-rowhammer-attacks

---

Professional Service

Organizing Committee

2022 New Security Paradigms Workshop (NSPW) Local Chair
2021 New Security Paradigms Workshop (NSPW) Local Chair
2020 New Security Paradigms Workshop (NSPW) Local Chair

Program Committee Member

2021 International Conference on Internet Monitoring and Protection (ICIMP)
2020 International Conference on Internet Monitoring and Protection (ICIMP)

Reviewer

2021 IEEE IoT World Forum
2020 IEEE/ACM Transactions on Networking
2018 IEEE SmartGridComm
2017 LangSec Workshop

Community Service

2020–21 **Dartmouth's Graduate Student Council**
Elected Representative of the Computer Science Department

2019–20 **PhD Student Ambassador**
Served as a mentor for incoming Computer Science PhD students

---

Programing Environments

- **Languages:** Ruby, Python, Dafny, Rust, C, C++, VHDL, HTML, CSS, Javascript, Go, Java, Lisp, R
- **Plaforms:** Unix (Linux, Solaris), Windows
- **Tools:** Scapy, Rails, Django, Flask, Docker, Wireshark, Linux, Alloy Model Checker, Scikit-Learn, Hammer, Spin
- **Databases:** Mysql, Postgresql, Oracle
- **Editors:** Vim, Emacs, VS Code, Xilinx Vivado, Android Studio, Atom

---

References

Sean W. Smith
Professor, Computer Science, Dartmouth College
sws@cs.dartmouth.edu

Sergey Bratus
Research Associate Professor, Computer Science, Dartmouth College
sergey.l.bratus@dartmouth.edu