Anindya Maiti

NPB 3.374, One UTSA Circle, San Antonio, TX 78249, USA

anindya@maiti.info
+1 (316) 243 6204
https://maiti.info/anindya

About Me

I am a security researcher by profession, and a technology enthusiast by hobby. At SPriTELab, I am currently researching privacy and security of Internet-connected home appliances, and advising multiple PhD students on new research directions. My research and teaching interests lie primarily in the areas of privacy and security in cyber-physical systems, cryptography and network security, blockchains, and applied machine learning and artificial intelligence. Outside of work, I advocate for a free (as in freedom), open, and secure Internet.

Education

Doctor of Philosophy in **Electrical Engineering and Computer Science** — May 2018

Wichita State University, Wichita, USA

Dissertation: *Security and Privacy of Cyber and Physical User Interactions in the Age of Wearable Computing*

Master of Science in **Electrical Engineering** — July 2014

Wichita State University, Wichita, USA • **Outstanding Master's Thesis Award**

Thesis: *Context-Aware Access Control: An Alternate Privacy Protection Mechanism for Online Social Networks*

Bachelor of Technology in **Computer Science and Engineering** — May 2012

Vellore Institute of Technology, Vellore, India

Work Experience

Postdoctoral Fellow — July 2018 – Present

University of Texas at San Antonio, San Antonio, USA

Institute for Cyber Security • SPriTELab

Research Fellow — February 2018 – May 2018

University of Texas at San Antonio, San Antonio, USA

Department of Computer Science

Graduate Research Assistant — August 2013 – December 2017

Wichita State University, Wichita, USA

Department of Electrical Engineering and Computer Science

Summer Intern — June 2011 – July 2011

Indian Institute of Technology Kharagpur, Kharagpur, India

Integrated Circuits and Systems Engineering Lab

Awards and Honors

- Proof-of-Concept Award from the Office of Commercialization and Innovation at UTSA — March 2019
- ACM Replicability Award — ACM WiSec 2018
- ACM Travel Grant — ACM WiSec 2018

- Apple **Best Paper Award** — IEEE WristSense 2018
- Fellow of the Eta Kappa Nu — Epsilon Xi Chapter • 2017
- Student Government Association Travel Grants — ACM UbiComp/ISWC 2015, IEEE EuroS&P 2017
- National Science Foundation Travel Grants — IEEE/IFIP DSN 2014, IEEE PerCom 2017
- Boeing Global Engineering Award — ACM AsiaCCS 2016
- **Outstanding Master's Thesis Award** — Wichita State University • 2015
- Fellow of the Golden Key International Honour Society — 2013

Research

At University of Texas at San Antonio — February 2018 – Present

- Currently researching privacy and security of light-emitting IoT devices. Developed an adversarial framework (based on algorithms such as OSB and DTW) to infer smart light users' media consumption habits, and used infrared-enabled smart bulbs to covertly exfiltrate users' private data (applying encoding techniques such as M-ary ASK).

  Research outcomes: **A5** (publication list below)

- Collaborating with faculties and advising PhD students on several new research topics, such as game-theoretic analysis of shard-based blockchains, and applying wearable computing for pedestrian safety in urban streets.

  Research outcomes: **A2**, **A3**, **P7**
  External sponsors and collaborators: **National Science Foundation (NSF)**

At Wichita State University — August 2013 – December 2017

- Discovered multiple security and privacy vulnerabilities faced by users of wearable devices. Developed novel side-channel attack frameworks using various machine-learning tools and algorithms (such as Regression, Naive Bayes, Random Forest, Nearest Neighbors, SVM, Neural Networks) to infer private information, such as PIN codes, passwords, and padlock and safe combinations, from zero-permission sensor data captured on wrist-wearables.

  Research outcomes: **A4**, **P2**, **P3**, **P8**, **P9**, **P10**
  External sponsors and collaborators: **Air Force Research Lab (AFRL)**, **Google**, **National Science Foundation (NSF)**

- Designed defense mechanisms against some of the above attacks, and tested their usability (using SUS and NASA-TLX).

  Research outcomes: **P4**, **P6**
  External sponsors and collaborators: **National Science Foundation (NSF)**

- Studied user awareness and concerns regarding mobile and wearable device motion sensors leaking private information. Responses from 500+ participants were statistically analyzed using Chi-Square, Friedman, and Wilcoxon tests.

  Research outcomes: **P5**
  External sponsors and collaborators: **Air Force Research Lab (AFRL)**, **National Science Foundation (NSF)**

- Developed and evaluated two new surveillance-resistant access control frameworks for online social networks, using context-aware policies which can easily integrate with existing platforms like Facebook.

  Research outcomes: **P1**

- Collaborated with fellow PhD students on different research topics, such as ANN-based energy load prediction in smart grids to minimize energy over-generation and maximize consumers' household privacy.

  Research outcomes: **A1**
  External sponsors and collaborators: **Power Systems Engineering Research Center (PSERC)**

Teaching

- Guest lecturer for CS5323: **Principles of Computer and Information Security** — UTSA • Spring 2019
- Guest lecturer for CS3873: **Computer Networks** — UTSA • Fall 2018
- Teaching Assistant for CS766: **Information Assurance & Security** — Wichita State University • Fall 2015

Inventions and Entrepreneurship

- Co-inventor of CryptoMiner: A Blockchain-inspired Card Game of Strategy (UTSA TDF 2019-010).
  - Received $3,203 as Proof-of-Concept Award from the University of Texas at San Antonio — March 2019
  - Utility patent pending — As of March 2019
  - Trademark received — November 2018

Press Coverage

- MIT Technology Review: "***The Best of the Physics arXiv***" — 2018
- PJ Media: "***Your Internet-Enabled Smart Lights May Be Able to Spy on You***" — 2018
- Bleeping Computer: "***Novel Attack Technique Uses Smart Light Bulbs to Steal Data***" — 2018
- Internet of Business: "***Smart Lightbulbs Can Be Used to Steal Secure Data, Finds Report***" — 2018
- KAKE (ABC) News: "***Group Tackles Cyber Security at Wichita Forum***" — 2017
- The Wichita Eagle: "***Is Your Smartwatch Watching You?***" — 2015
- Government Technology News: "***Can Smartwatch Sensors Make Hacking Easier?***" — 2015

Services and Affiliations

- Member of ACM and IEEE since 2010. Member of IAENG since 2009.
- Reviewed journal articles for:
  - IEEE Transactions on Information Forensics and Security
  - IEEE Transactions on Mobile Computing
  - ACM Transactions on Intelligent Systems and Technology
  - Elsevier Computers & Security
  - ACM Transactions on Privacy and Security
  - Springer Cluster Computing
  - IEEE Access
- Reviewed conference papers for:
  - PETS 2019
  - ACM UbiComp 2018-19
  - IEEE ICCCN 2018
  - IEEE NAS 2018
  - IEEE IPCCC 2014-18
  - IEEE SmartGridComm 2016
- Serving as a Program Committee Member for SKM 2019 and SACMAT 2019
- Served as a Judge at the College of Sciences Research Conference, UTSA — October 2018
- Invited Graduate Research Seminar talk at the Department of Computer Science, UTSA — March 2018
- Speaker at the Kansas Linux Fest, Wichita — 2016, 2017
- Seminar talk for the Cybersecurity Association, Wichita State University — February 2016

Publications

Journal Articles

A5. Anindya Maiti, and Murtuza Jadliwala, "Light Ears: Information Leakage via Smart Lights", under revision at Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT, formerly ACM UbiComp). Preprint: https://arxiv.org/abs/1808.07814

A4. Anindya Maiti, Murtuza Jadliwala, Jibo He, and Igor Bilogrevic, "Side-Channel Inference Attacks on Mobile Keypads using Smartwatches", IEEE Transactions on Mobile Computing, Volume 17, Issue 9, 2018.

A3. Mohammad Hossein Manshaei, Murtuza Jadliwala, Anindya Maiti, and Mahdi Fooladgar, "A Game-Theoretic Analysis of Shard-Based Permissionless Blockchains", IEEE Access, Volume 6, 2018.

A2. Nisha Vinayaga-Sureshkanth, Anindya Maiti, Murtuza Jadliwala, Kirsten Crager, Jibo He, and Heena Rathore, "A Practical Framework for Preventing Distracted Pedestrian-related Incidents using Wrist Wearables", IEEE Access, Volume 6, 2018.

A1. Arash Boustani, Anindya Maiti, Sina Yousefian Jazi, Murtuza Jadliwala, and Vinod Namboodiri, "Seer Grid: Privacy and Utility Implications of Two-Level Load Prediction in Smart Grids", IEEE Transactions on Parallel and Distributed Systems, Volume 28, Issue 2, 2017.

Conference and Workshop Papers

P10. Raveen Wijewickrama, Anindya Maiti, and Murtuza Jadliwala, "deWristified: Handwriting Inference Using Wrist-Based Motion Sensors Revisited", ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), Miami, Florida, USA, May 2019.

P9. Anindya Maiti, Ryan Heard, Mohd Sabra, and Murtuza Jadliwala, "Towards Inferring Mechanical Lock Combinations using Wrist-Wearables as a Side-Channel", ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), Stockholm, Sweden, June 2018. **ACM Replicability Award**

P8. Mohd Sabra, Anindya Maiti, and Murtuza Jadliwala, "Keystroke Inference Using Ambient Light Sensor on Wrist-Wearables: A Feasibility Study", IEEE MobiSys Workshop on Wearable Systems and Applications (WearSys), Munich, Germany, June 2018.

P7. Nisha Vinayaga-Sureshkanth, Anindya Maiti, Murtuza Jadliwala, Kirsten Crager, Jibo He, and Heena Rathore, "Towards a Practical Pedestrian Distraction Detection Framework using Wearables", IEEE PerCom Workshop on Sensing Systems and Applications using Wrist Worn Smart Devices (WristSense), Athens, Greece, March 2018. **Best Paper Award**

P6. Anindya Maiti, Kirsten Crager, Murtuza Jadliwala, Jibo He, Kevin Kwiat, and Charles Kamhoua, "RandomPad: Usability of Randomized Mobile Keypads for Defeating Inference Attacks", IEEE EuroS&P Workshop on Innovations in Mobile Privacy & Security (IMPS), Paris, France, April 2017.

P5. Kirsten Crager, Anindya Maiti, Murtuza Jadliwala, and Jibo He, "Information Leakage through Mobile Motion Sensors: User Awareness and Concerns", European Workshop on Usable Security (EuroUSEC), Paris, France, April 2017.

P4. Anindya Maiti, Murtuza Jadliwala, and Chase Weber, "Preventing Shoulder Surfing using Randomized Augmented Reality Keyboards", IEEE PerCom Workshop on Security, Privacy and Trust in the Internet of Things (SPT-IoT), Kona, Hawaii, USA, March 2017.

P3. Anindya Maiti, Oscar Armbruster, Murtuza Jadliwala, and Jibo He, "Smartwatch-Based Keystroke Inference Attacks and Context-Aware Protection Mechanisms", ACM Symposium on Information, Computer and Communications Security (AsiaCCS), Xi'an, China, May 2016.

P2. Anindya Maiti, Murtuza Jadliwala, Jibo He, and Igor Bilogrevic, "(Smart)Watch Your Taps: Side-Channel Keystroke Inference Attacks using Smartwatches", ACM International Symposium on Wearable Computers (ISWC), Osaka, Japan, September 2015.

P1. Murtuza Jadliwala, Anindya Maiti, and Vinod Namboodiri, "Social Puzzles: Context-Based Access Control in Online Social Networks", IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Atlanta, Georgia, USA, June 2014.

References

- Dr. **Murtuza Jadliwala**, University of Texas at San Antonio, San Antonio, USA
  murtuza.jadliwala@utsa.edu • +1 (210) 458 5693
- Dr. **Igor Bilogrevic**, Google, Zurich, Switzerland
  ibilogrevic@google.com • +41 79 693 92 51
- Dr. **Mohammad Hossein Manshaei**, Isfahan University of Technology, Isfahan, Iran
  manshaei@cc.iut.ac.ir • +98 (313) 391 9067
- Dr. **Vinod Namboodiri**, Wichita State University, Wichita, USA
  vinod.namboodiri@wichita.edu • +1 (316) 978 3922
- Dr. **Jibo He**, Wichita State University, Wichita, USA
  jibo.he@wichita.edu • +1 (217) 417 3830