Hasini Gunasinghe

@ huralali@purdue.edu www.hasinitg.net (765) 714-9268
www.linkedin.com/in/hasinitg github.com/hasinitg

Education

- **Ph.D. in Computer Science** — **Fall 2013 – Fall 2019 (expected)**
  Purdue University — *West Lafayette, IN, USA*
- **M.S. in Computer Science** — **Fall 2013 – Spring 2016**
  Purdue University — *West Lafayette, IN, USA*
- **B.Sc. (Honors) in Computer Science and Engineering** — **May 2006 – Sept 2010**
  University of Moratuwa — *Moratuwa, Sri Lanka*

Industry Experience

- **IBM T. J. Watson Research Center, Yorktown Heights, NY, USA** — *May 2017 – Aug. 2017*
  Research Intern - Information Security
  - Designed and developed a protocol for privacy preserving and secure exchange of digital identity assets in a decentralized identity ecosystem.
- **Salesforce.com, San Francisco, CA, USA** — *May 2016 – Aug. 2016*
  Software Engineering Intern - Infrastructure Security
  - Contributed to the development of next generation access control solution for Salesforce data centers.
- **WSO2 Inc., Sri Lanka** — *Sept 2010 – May 2013*
  Software Engineer - Security and Identity Management Team
  - Designed and developed standardized identity provisioning based on SCIM (System for Cross-domain Identity Management) for WSO2 Identity Server.
  - Represented WSO2 in the first SCIM interoperability event at IETF 83rd meeting held in Paris, France.
  - Participated in client engagements in USA and Germany.
  - Speaker in WSO2Con 2013 held in London, UK.
  - Managed three releases of WSO2 Identity Server (3.2.0, 3.2.3 and 4.0.0) as the release manager.
- **Wavenet International Pvt Ltd, Sri Lanka** — *Oct 2008 – March 2009*
  Software Engineering Intern
  - Designed and developed a SIP (Session Initiation Protocol) based soft phone with audio and video streams.

Research Experience

Designed and developed privacy preserving and secure online protocols for real world use cases, with special focus on digital identity management. Selected research projects:

- **PEBASI:** An efficient online biometric authentication scheme which protects users' biometric privacy from service providers and transaction privacy from identity providers. Different from traditional identity provider-centric authentication model, PEBASI is based on a user-centric authentication model. At the heart of the scheme is a novel biometric matching technique which outperforms the state-of-the-art by 35% in terms of execution time, which is based on a novel hybrid secure multiplication framework. PEBASI is biometric trait agnostic.
- **PrivIdEx:** A protocol enabling service providers to exchange users' verified identity information over a decentralized identity management platform which is backed by a permissioned blockchain network. The protocol makes identity verification scenarios such as KYC (Know Your Customer), which involve lengthy due diligence steps, more convenient and less expensive. It preserves both privacy (e.g. confidentiality, anonymity, unlinkability) and security (e.g. correctnes, ownership assurance, protection from counterfeits, financial fairness) properties which are conflicting yet critical requirements.
- **PrivBioMTAuth:** The first user-centric biometric authentication protocol enabling privacy preserving remote authentication from mobile phones. The main building blocks are zero knowledge proofs (ZKP) and machine learning classification. An approach protecting the ZKP protocols from mafia attacks is proposed as an independent contribution.

- **RahasNym:** A pseudonymous identity management system supporting unlinkable and accountable online transactions. A policy language combined with light weight cryptography makes it efficient for online transactions. RahasNym featured in the IEEE Computing Now - April 2017 theme article.

Publications

- **Journal Papers:**
  - H. Gunasinghe, E. Bertino. **PrivBioMTAuth: Privacy Preserving Biometrics-Based and User Centric Protocol for User Authentication from Mobile Phones.** IEEE Transactions on Information Forensics and Security, vol. 13, no. 4, p. 1042-1057, April, 2018. (*impact factor: 5.824*)
- **Conference Papers:**
  - H. Gunasinghe, M. Atallah, E. Bertino. **PEBASI: A Privacy preserving, Efficient Biometric Authentication Scheme based on Irises.** In submission.
  - H. Gunasinghe, A. Kundu, E. Bertino, H. Krawczyk, S. Chari, K. Singh, D. Song. **PrivIdEx: Privacy Preserving and Secure Exchange of Digital Identity Assets.** The World Wide Web Conference (WWW), May, 2019. (*acceptance rate: 18%*)
  - H. Gunasinghe, E. Bertino. [Invited Paper] **RahasNym: Pseudonymous Identity Management System for Protecting against Linkability.** The 2nd IEEE International Conference on Collaboration and Internet Computing, CIC 2016, Pittsburgh, PA, USA.
  - H. Gunasinghe, E. Bertino. **Privacy Preserving Biometrics-Based and User Centric Authentication Protocol.** The 8th International Conference in Network and System Security, NSS 2014, China.
- **Poster Papers:**
  - H. Gunasinghe, E. Bertino. [Poster Paper] **RahasNym: Protecting against Linkability in the Digital Identity Ecosystem.** The 35th IEEE International Conference on Distributed Computing Systems, ICDCS 2015, Columbus, OH, USA, June 2015.
- **Patents:**
  - S. Chari, H. Gunasinghe, HM. Krawczyk, A. Kundu, KK. Singh, D. Su. **Protection of Confidentiality, Privacy and Ownership Assurance in a Blockchain Based Decentralized Identity Management System**. US Patent 15/824,405.
  - S. Chari, H. Gunasinghe, A. Kundu, KK. Singh, D. Su. **Protection of confidentiality, privacy and financial fairness in a blockchain based decentralized identity management system**. US Patent 15/839,117.

Teaching Experience and Professional Service

- Served as a Graduate Teaching Assistant for Software Engineering (CS 307) and Senior Software Engineering (CS 407) courses at Purdue University (*Spring 2015 - Spring 2018*).
- Conducted a guest lecture on "Zero knowledge proofs and their applications in digital identity management" in the seminar course on Data Security and Privacy (CS 59000-DSP) at Purdue University (*Spring 2019*).
- Served as a reviewer/subreviewer for renowned journals (e.g. IEEE Transactions on Information Security and Forensics (*2018-2019*), IEEE Transactions on Dependable and Secure Computing (*2014-2019*)) and conferences (e.g. WWW-2019, ICDCS-2019, SACMAT-2015, AsiaCCS-2014, 2015, CODASPY-2015, 2018, 2019, etc.).

Awards

- Bisland Dissertation Fellowship awarded by the Graduate School, Purdue University. *2019*
- Emil Stefanov Memorial Partial Fellowship for originality and creative thinking in security research. *2019*
- Travel grant awarded by the ZKProof Steering Committee to attend the 2nd ZKProof Workshop. *2019*
- IBM PhD Fellowship. *2018*
- Summer Research Grant awarded by the Graduate School, Purdue University. *2018*
- Raymond Boyce Graduate Teacher Award by the Computer Science Department, Purdue University. *2017*

- Graduate Teaching Assistant Award (sponsored by Harris Corporation). *2016*
- Travel grant awarded by Purdue University to attend the Grace Hopper Conference. *2016*
- Travel grant awarded by NSF to attend the Summer School on Secure Computation. *2016*
- Best Poster Paper Award in the 35th IEEE International Conference on Distributed Computing Systems. *2015*
- Travel grant awarded by NSF to attend IEEE ICDCS 2015. *2015*
- Best Paper Award in the 8th International Conference on Network and Systems Security. *2014*
- Outstanding Contributor Award, WSO2 Inc. *2011, 2012*
- Second Runner Up in the Software Design Category of Imagine Cup-2008, Microsoft, Sri Lanka. *2008*

Technical Skills

- Programming Languages: *Java, Python*
- Cryptographic Tools: *Secure Multiparty Computation (e.g. Yao's Garbled Circuits using FastGC), Zero Knowledge Proofs (e.g. ZK-SNARKs using jsnark)*
- Blockchain Technologies: *Hyperledger Fabric*
- Operating Systems: *Linux, Windows, MacOS, Android*
- Development Tools: *Git, Subversion, Ant, Maven, Gradle, IntelliJ IDEA*
- Standards and Specifications: *SCIM, OpenID Connect, OAuth*

Open Source Contributions

- Google Summer of Code *Summer 2015*
  - Designed and developed an access control solution for Apache Airavata.
- Committer, Apache Software Foundation - Airavata Project. *Summer 2015*
- Committer, WSO2 Inc. *2010 - 2013*
- Committer, initial SCIM Working Group. *2012*

Other Activities

- Student Member, CERIAS at Purdue University. *2013 - present*
- 2nd ZKProof Workshop. *April, 2019*
  - Attended a three-day workshop organized by the ZKProof Steering Committee, which drives standardization of zero knowledge proofs by creating a framework for collaboration between academics, researchers, developers and industry experts.
- Summer School on Secure and Oblivious Computation and Outsourcing. *Summer 2016*
  - Attended a three-day workshop organized by the University of Notre Dame, on emerging topics in secure computation, oblivious algorithms and data structures, and secure and verifiable outsourcing.
- Member, Gavel Club (Affiliate of Toastmasters International) *2006–2007*