

Joyanta Debnath

New York, USA, 319-512-0597, joyanta.debnath@stonybrook.edu

WEBSITES <https://www3.cs.stonybrook.edu/~jdebnath/>

BIOGRAPHY My research interests lie at the intersection of formal methods and security. I am interested in developing automated tools for enhancing the safety and reliability of complex systems.

EDUCATION

Jan 2023 — Present **Ph.D. Candidate** Computer Science

Stony Brook University

- Advisor: Professor *Omar Chowdbury*
- Transferred from the Ph.D. program of **University of Iowa** (August 2018 - December 2022)
- CGPA: 4.00/4.00

Apr 2012 — Feb 2017 **Bachelor of Science** Computer Engineering

Bangladesh University of Engineering and Technology

- Advisor: Professor *Tanzima Hashem*
 - CGPA: 3.70/4.00
-

WORK EXPERIENCE

Aug 2018 — Present **Research Assistant**

Stony Brook University, University of Iowa

Finding vulnerabilities in deployments of various network protocols, development of a formally verified implementation for X.509 PKI, and testing different open-source X.509 PKI implementations

- **Keywords:** Formal Verification, X.509 PKI, Differential Testing
- **Tools/Technologies:** Agda, CVC4, Python, C/C++

May 2022 — Aug 2022 **Summer 2022 Internship**

Formal Verification Team, GE Global Research

Developed a new language called OYSTER, which can be used as an annex to annotate a system architectural model with different types of constraints, in order to check the satisfiability of these constraints using SMT solver, and synthesize a complex architecture model from the user given simple system architecture model

- **Keywords:** Model Checking, Architecture Synthesis
- **Tools/Technologies:** Architecture Analysis & Design Language (AADL), Java, Z3 SMT Solver

May 2021 — Aug 2021 **Summer 2021 Internship**

Formal Verification Team, GE Global Research

Modeling system architecture, and modeling expected behavior of different system components with assume-guarantee contracts, which are used by Cyber Resiliency Verifier (CRV) tool to find vulnerabilities in system architecture design under various threat effects

- **Keywords:** Threat Effect Modeling, Model Checking, Cyber Resiliency Verification
- **Tools/Technologies:** Architecture Analysis & Design Language (AADL), Assume Guarantee Reasoning Environment (AGREE), OSATE, Kind2

May 2017 — Jun 2018 **QA Engineer**

Veriflow Systems

Development and testing of network equipment behavior modeling tool *Veriflow*, which checks network software or configuration for bugs prior to deployment

- **Keywords:** Network Device Configuration, Virtual Network Design, Bug Finding
 - **Tools/Technologies:** Java, Wireshark, GNS3, VMware, VirtualBox
-

PUBLICATIONS

Towards a Correct-by-Construction Design of Integrated Modular Avionics

with Baoluo Meng, Sarat Chandra Varanasi, Emmanuel Manolios, Michael Durling, Saswata Paul, Daniel Prince, Saif Alsabbagh, Richard Haadsma,

Craig McMillan, Chi Zhang, and Tim Oates; In Proceedings of the 23rd Conference on Formal Methods in Computer-Aided Design 2023 (FMCAD 2023); https://doi.org/10.34727/2023/isbn.978-3-85448-060-0_30

On Re-engineering the X.509 PKI with Executable Specification for Better Implementation Guarantees

with Sze Yiu Chau, and Omar Chowdhury; In Proceedings of the 28th ACM Conference on Computer and Communications Security 2021 (ACM CCS 2021); <https://doi.org/10.1145/3460120.3484793>

All your credentials are belong to us: On Insecure WPA2-Enterprise Configurations

with Man Hong Hue, Kin Man Leung, Li Li, Mohsen Minaei, M. Hammad Mazhar, Kailiang Xian, Endadul Hoque, Omar Chowdhury, and Sze Yiu Chau; In Proceedings of the 28th ACM Conference on Computer and Communications Security 2021 (ACM CCS 2021); <https://doi.org/10.1145/3460120.3484569>

Morpheus: Bringing The (PKCS) One To Meet the Oracle

with Moosa Yahyazadeh, Sze Yiu Chau, Li Li, Man Hong Hue, Sheung Chiu Ip, Li Chun Ngai, Endadul Hoque, and Omar Chowdhury; In Proceedings of the 28th ACM Conference on Computer and Communications Security 2021 (ACM CCS 2021); <https://doi.org/10.1145/3460120.3485382>

When TLS Meets Proxy on Mobile

with Sze Yiu Chau, and Omar Chowdhury; In 18th International Conference of Applied Cryptography and Network Security (ACNS 2020); https://doi.org/10.1007/978-3-030-57878-7_19

TECHNICAL STRENGTHS

- **Programming Languages:** Python, C/C++, Java, Android, OCaml
- **Formal Specification Languages:** Alloy, Lustre, Dafny, AGREE
- **Formal Verification Tools:** Alloy Analyzer, Kind2, Dafny
- **SMT Solvers:** Z3, CVC4
- **Architecture Description Languages:** AADL (OSATE)
- **Network Analyzers:** Wireshark, tshark, GNS3
- **Operating Systems:** Windows, Linux, Mac
- **Web Technologies:** HTML, CSS, PHP
- **Database:** MySQL, Oracle

KEY SKILLS AND EXPERTISE

Automated Reasoning
Formal Verification
Model Checking

Public Key Infrastructure (PKI)
SSL/TLS Protocol

AWARDS

- GE Impact Award 2022, 2021
- Runners-up of Best Student Paper Award in ACM CCS 2021
- Winner of Best Student Paper Award in ACNS 2020

EXTRA-CURRICULAR ACTIVITIES

Feb 2022 — Dec 2022

Vice-President

Bangladeshi Student Association, University of Iowa

Feb 2021 — Jan 2022

Treasurer

Bangladeshi Student Association, University of Iowa

HOBBIES

Singing, Hiking, Playing Soccer and Badminton