Joyanta Debnath

Website - jdebnath@cs.stonybrook.edu - LinkedIn - Google Scholar

BIOGRAPHY

My research interest lies at the intersection of computer security and automated reasoning. I have extensive experience on applying different techniques from formal verification to enhance security, reliability, and robustness of modern systems and protocols. I am also interested to automatically detect functional bugs in network protocols and safety-critical cyber-physical and IoT systems. Currently, I am investigating exploitable weaknesses in SSL/TLS protocol as well as analyzing the robustness of X.509 certificate validation implemented in various open-source implementations. I am committed to advancing the state-of-the-art in formal verification and computer security and making the digital world safer for everyone.

EDUCATION

Stony Brook University *New York, USA*
Doctor of Philosophy (Candidate), Computer Science *January 2023 - Present*

- Thesis Advisor: *Omar Chowdhury* (Ph.D.), CGPA: $4.00/4.00$
- Transferred from the Ph.D. program (*August 2018 - December 2022*) of **University of Iowa** to continue working with *Dr. Chowdhury*

Bangladesh University of Engineering and Technology *Dhaka, Bangladesh*
Bachelor of Science, Computer Science and Engineering *April 2012 - February 2017*

- Thesis Advisor: *Tanzima Hashem* (Ph.D.), CGPA: $3.70/4.00$

PUBLICATIONS

ARMOR: A Formally Verified Implementation of X.509 Certificate Chain Validation
With *Christa Jenkins, Yuteng Sun, Sze Yiu Chau, and Omar Chowdhury*
https://doi.ieeecomputersociety.org/10.1109/SP54263.2024.00182
Appeared in the 45^{th} IEEE Symposium on Security and Privacy (IEEE S&P 2024)

Towards a Correct-by-Construction Design of Integrated Modular Avionics
With *Baoluo Meng, Sarat Chandra Varanasi, Emmanuel Manoloios, Michael Durling, and Saswata Paul*
https://doi.org/10.34727/2023/isbn.978-3-85448-060-0_30
Appeared in the 23^{rd} Formal Methods in Computer-Aided Design (FMCAD 2023)

On Re-engineering the X.509 PKI with Executable Specification for Better Implementation Guarantees
With *Sze Yiu Chau, and Omar Chowdhury*
https://doi.org/10.1145/3460120.3484793
Appeared in the 28^{th} ACM Conference on Computer and Communications Security (ACM CCS 2021)
$\star\star$ Best Paper Award (Runners-up)

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*
https://doi.org/10.1145/3460120.3484569
Appeared in the 28^{th} ACM Conference on Computer and Communications Security (ACM CCS 2021)

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*
https://doi.org/10.1145/3460120.3485382
Appeared in the 28^{th} ACM Conference on Computer and Communications Security (ACM CCS 2021)

When TLS Meets Proxy on Mobile
With *Sze Yiu Chau, and Omar Chowdhury*
https://doi.org/10.1007/978-3-030-57878-7_19
Appeared in the 18^{th} International Conference of Applied Cryptography and Network Security (ACNS 2020)
$\star\star$ Best Paper Award (Winner)

AWARDS

- **Student Travel Award** from IEEE S&P 2024 conference
- **GE Impact Awards 2022, 2021** from GE Research
- **Best Paper Award (Runners-up)** from ACM CCS 2021 conference
- **Best Paper Award (Winner)** from ACNS 2020 conference

WORK EXPERIENCE

Research Assistant

Stony Brook University *June 2023 - Present*

- Developed the *first* formally verified X.509 certificate chain validation logic (CCVL) implementation *ARMOR* with machine-checked correctness guarantees for a large portion of RFC 5280. Compared *ARMOR* with 11 open-source X.509 implementations and an open-source certificate linter for its specificational accuracy and runtime overhead and detected several noncompliance issues in the tested implementations.

University of Iowa *August 2018 - December 2022*

- Re-engineered and formalized a widely used fragment of the X.509 standard specification, and then used it to develop a high-assurance X.509 CCVL implementation *CERES*. Compared with 3 mainstream open-source X.509 implementations based on 4 million test certificate chains and found that *CERES*, in many cases, rightfully rejects malformed and invalid certificates compared to the tested implementations.
- Performed a measurement study on the security implications of using 34 proxy-based Android browsers, specifically the scenario where they are entangled with TLS. Analysis showed that many of those browsers silently accept weak ciphers, weak TLS versions, and vulnerable certificates offered by a Web server.
- [1] Performed the *first* multifaceted measurement study to investigate the widespread practices employed by 7045 tertiary education institutes (TEIs) in 54 countries when offering WPA2-Enterprise Wi-Fi services. Analysis showed that majority of the TEIs rely on insecure configurations, and nearly 86% of those can suffer from credential thefts.
- [1] Developed an automatic, black-box testing approach called *Morpheus* to check the non-compliance of libraries implementing PKCS#1-$v1.5$ signature verification with the PKCS#1-$v1.5$ standard. With *Morpheus*, tested 45 implementations of PKCS#1-$v1.5$ signature verification and discovered that 6 of them are susceptible to variants of the Bleichenbacher-style low public exponent RSA signature forgery attack, 1 implementation has a buffer overflow, 33 implementations have incompatibility issues, and 8 implementations have minor leniencies.

Teaching Assistant

Stony Brook University *January 2023 - May 2023*

- Course Title: High-Assurance Software Design and Implementation

University of Iowa *January 2022 - May 2022*

- Course Title: Computer Security

[1] Not part of the Ph.D. thesis

Summer Internship

GE Vernova *June 2024 - August 2024*

- Performed a formal analysis of the design of Universal Utility Data Exchange (UUDEX) protocol, a recently proposed secure and flexible protocol for sharing power system measurement data between utility control centers in the grid environment. Analysis involved modeling the UUDEX protocol, checking 5 cryptographic security properties using the Tamarin protocol verifier, and 14 functional properties using the Kind2 model checker. Reported the strength of UUDEX in terms of security, underlying assumptions, and possible attacks when assumption are violated.

GE Research *June 2022 - August 2022*

- Developed a formal language and framework, *OYSTER*, which invokes Satisfiability Modulo Theories (SMT) solvers to automatically generate correct-by-construction architecture design for a GE Aviation use case - a fuel control system named Integrated Modular Avionics (IMA). Behaviors of applications running on IMA components and their safety properties are modeled in the Assume Guarantee REasoning Environment (AGREE) annex and checked by the Kind2 model checker. Verification results are guaranteed to be correct by the independently verifiable proof certificates produced by Kind2 model checker.

GE Research *June 2021 - August 2021*

- Extensively tested the effectiveness of a memory-based malware detection program (using Syzkaller - a kernel fuzzer, writing testsuites in Linux Test Project) when integrated in a Linux Kernel.
- Modeled the *Secure Boot* process and verified different properties of it to demonstrate an use case of the Cyber Resiliency Verifier (CRV) component of the VERDICT tool.

QA Engineer (Independent Contractor)

Veriflow Systems (Acquired by VMware in 2019) *May 2017 - June 2018*

- Conducted research on networking features and protocols, developed network equipment behavior modeling tools in Java, and implemented virtual test labs.

TECHNICAL STRENGTHS

- **Imperative Programming Languages:** C/C++, Python, Java, Android
- **Functional Programming Languages:** OCaml, Haskell, Agda, F*
- **Hybrid Programming Languages:** Dafny, Lustre
- **Theorem Provers:** Agda, F*, Tamarin Verifier
- **SMT Solvers:** CVC4, Z3
- **Model Checkers:** Kind2, SPIN, NuSMV, Alloy Analyzer
- **Architecture Modeling Languages:** AADL, AGREE
- **Web Technologies:** HTML, CSS, PHP
- **Databases:** Oracle, MySQL
- **Basic Software and Tools:** Linux, Mac, Windows, MS Office, Docker, Git, Latex, Wireshark, VirtualBox

ORGANIZATIONAL ROLES

Vice-President *February 2022 - December 2022*

Bangladeshi Student Association, University of Iowa

Treasurer *February 2021 - January 2022*

Bangladeshi Student Association, University of Iowa

EXTRACURRICULAR ACTIVITIES

- **Hobbies:** Singing, Hiking, Biking
- **Sports:** Cricket, Soccer, Badminton