Ivan De Oliveira Nunes

Assistant Professor, Rochester Institute of Technology (RIT), Rochester, NY
(Email) ivanoliv@mail.rit.edu • (Phone) 213-713-1549 • (Website) http://ivan.csec.rit.edu • (Skype) ivanolive1

Research Interests

Security & Privacy; Embedded Systems; Computer Networks; Applied Cryptography; Distributed Systems.

Education

Ph.D., Networked Systems 2016 - 2021
University of California Irvine (UCI) *Irvine, CA*
- Dissertation: "Verifiable Integrity for Code and Execution in Resource-Constrained Embedded Systems"
- Advisor: Dr. Gene Tsudik

M.Sc., Computer Science 2014 - 2016
Federal University of Minas Gerais (UFMG) *Belo Horizonte, Brazil*
- Thesis: "Understanding Mobility to Improve D2D Communication"
- Advisors: Dr. Antonio Loureiro and Dr. Pedro Vaz de Melo

B.Eng., Computer Engineering 2009 - 2014
Federal University of Espirito Santo (UFES) *Vitoria, Brazil*
- Included 1 year abroad as an exchange student at University of California Irvine

Professional Experience

Assistant Professor – RIT 2021 - Present
Affiliations at RIT:
- Golisano College of Computing and Information Sciences (GCCIS)
- Computing Security Department (CSEC)
- Global Cybersecurity Institute (GCI)
- Computing and Information Sciences PhD Program

Research Assistant – UCI 2016 - 2021
Project: "Verifiable Integrity for Code and Execution in Resource-Constrained Embedded Systems"
- Supervisor: Dr. Gene Tsudik
- Systematic hardware/software co-design of novel and formally verified security services targeting resource-constrained embedded (a.k.a. IoT/CPS) devices. Examples of such services include Remote Attestation, Control-Flow Attestation, Secure Software Updates, and Provable Code Execution. These services are designed to remain effective even under the assumption of full compromise of the IoT/CPS device's software-state.

Research Intern – Visa Research Summer, 2020
Project: "Formal Verification of Fairness Properties in Secure Multi-Party Computation Protocols"
- Supervisors: Dr. Mihai Christodorescu and Dr. Rohit Sinha
- Despite the theoretical impossibility (in the standard model) of fairness in secure multi-party computation (MPC) protocols with dishonest majorities, recent work has shown that a combination of novel technologies – i.e., Trusted Execution Environments (TEEs) and Public Ledgers – enable fair MPC even if all but one party are actively malicious. In this project, we developed formal protocol models (using the Tamarin-Prover) and use formal verification to obtain symbolic proofs, attacks, and fixes to these recently proposed "fair MPC" protocols.

Research Intern – Visa Research Summer, 2019
Project: "Oblivious Extractors for Enhanced Biometric-Based User Authentication"
- Supervisors: Dr. Mihai Christodorescu and Dr. Maliheh Shirvanian

- We propose a new cryptographic construction, namely Oblivious Extractors (OEs), that enhances the security of biometric-based authentication systems. OEs enable biometric template confidentiality (provably at the same security level as regular Fuzzy Vaults) while enhancing the security of the authentication system against offline statistical guessing attacks.

Research Intern – SRI International Spring & Summer, 2018

Project: "SCaaS: Secure (Multi-Party) Computation as a Service".

- Supervisor: Dr. Karim Eldefrawy
- The SCaaS project implements a prototype of an online service that leverages virtualization to generate on-demand secure multi-party computation (MPC) circuits, according to configurable parameters chosen by the MPC participants. For instance, configurable parameters define the type of computation (or function), the number of parties, the threat model (semi-honest, covert, malicious), and the corruption threshold (number of tolerated corrupt parties).

Research Intern – SRI International Summer, 2017

Project: "Biometric-Based Authentication with Non-Interactive Re-Enrollment".

- Supervisor: Dr. Karim Eldefrawy
- Traditional cryptographic primitives used for biometric authentication, such as fuzzy vaults (FV) and fuzzy extractors (FE), enable confidentiality of biometric templates stored in back-end servers. However, one challenge for systems implemented atop these primitives is called "non-interactive user re-enrollment". Systems utilizing FV and FE, an update to cryptographic secrets and credentials associated to a given user may require active in-person user involvement. To effectively address this problem, we combine secure multi-party computation (MPC) techniques with existing FV and FE primitives, enabling secure non-interactive user re-enrollment at scale.

Research Intern – LG Electronics Sep. 2015 - Mar. 2016

Project: "AoT: Authentication and Access Control For the Entire IoT Device Life-Cycle".

- Supervisors: Dr. Leonardo Barbosa and Dr. Antonio Loureiro
- Authentication of Things (AoT) consists of a suite of protocols for assuring secure authentication and authorization through the IoT device life-cycle. AoT relies on identity- and attribute-based cryptography to obviate the need for certificate verification, which can be cost-prohibitive to many resource-constrained IoT devices.

Research Assistant – UFMG 2014 - 2016

Project: "Understanding Mobility to Improve D2D Communication".

- Supervisors: Dr. Antonio Loureiro and Dr. Pedro Vaz de Melo
- We statistically characterize of human mobility patterns with the goal of improve routing cost-effectiveness in Device-To-Device (D2D) networks. In particular, metrics for individual and collective/social mobility are extracted from real-world human mobility data-sets, and applied to design novel opportunistic routing protocols (GROUPS-NET and SAMPLER) and a social-aware human mobility model (Group Regularity Mobility Model).

Teaching Experience

Instructor of Record

CSEC 741 - SCADA and Sensor Security, RIT Spring, 2022

Class Details: grad level, 28 students

CSEC 559 & 659 - Trusted Computing and Trusted Execution, RIT Fall, 2021

Class Details: undergrad/grad level, 16 students

Teaching Assistant

CS202 - Computer & Network Security (Grad. level), UCI Spring, 2019

Class Details: graduate level, approximately 40 students, 1 TA

CS134 - Computer & Network Security (Undergrad. level), UCI Winter, 2018

Class Details: senior undergrad level course, approximately 130 students, 2 TAs

CS161 - Design & Analysis of Algorithms (Undergrad. level), UCI Winter, 2017
Class Details: senior undergrad level course, approximately 300 students, 4 TAs

Computer Networks, UFMG 2015
Class Details: senior undergrad level course, approximately 120 students, 2 TAs

Publications

REFEREED CONFERENCE PAPERS

(C1) Ivan De Oliveira Nunes, Seoyeon Hwang, Sashidhar Jakkamsetti, Gene Tsudik. **Privacy-from-Birth: Protecting Sensed Data from Malicious Sensors with VERSA.** IEEE Symposium on Security and Privacy (Oakland). 2022.

(C2) Adam Caulfield, Norrathep Rattanavipanon, Ivan De Oliveira Nunes. **ASAP: Reconciling Asynchronous Real-Time Operations and Proofs of Execution in Simple Embedded Systems.** ACM/IEEE Design Automation Conference (DAC). 2022.

(C3) Esmerald Aliaj, Ivan De Oliveira Nunes, and Gene Tsudik. **GAROTA: Generalized Active Root-Of-Trust Architecture (for Tiny Embedded Devices).** 31th USENIX Security Symposium (USENIX Security 22). 2022.

(C4) Mahmoud Ammar, Bruno Crispo, Ivan De Oliveira Nunes, and Gene Tsudik. **Delegated Attestation: Scalable Remote Attestation of Commodity CPS by Blending Proofs of Execution with Software Attestation.** ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec). 2021.

(C5) Ivan De Oliveira Nunes, Sashidhar Jakkamsetti, Norrathep Rattanavipanon, and Gene Tsudik. **On the TOCTOU Problem in Remote Attestation.** ACM Conference on Computer and Communications Security (CCS). 2021.

(C6) Ivan De Oliveira Nunes, Sashidhar Jakkamsetti and Gene Tsudik. **DIALED: Data Integrity Attestation for Low-end Embedded Devices.** Design Automation Conference (DAC). 2021.

(C7) Ivan De Oliveira Nunes, Xuhua Ding, and Gene Tsudik. **On the Root of Trust Identification Problem.** In 20th ACM/IEEE Conference on Information Processing in Sensor Networks (IPSN). 2021.

(C8) Ivan De Oliveira Nunes, Sashidhar Jakkamsetti, and Gene Tsudik. **Tiny-CFA: A Minimalistic Approach for Control Flow Attestation Using Verified Proofs of Execution.** In Design, Automation & Test in Europe Conference & Exhibition (DATE). 2021.

(C9) Ivan De Oliveira Nunes, Karim Eldefrawy, Norrathep Rattanavipanon, and Gene Tsudik. **APEX: A Verified Architecture for Proofs of Execution on Remote Devices under Full Software Compromise.** In 29th USENIX Security Symposium (USENIX Security 20). 2020.

(C10) Ivan De Oliveira Nunes, Karim Eldefrawy, Norrathep Rattanavipanon, Michael Steiner, and Gene Tsudik. **VRASED: A verified hardware/software co-design for remote attestation.** In 28th USENIX Security Symposium (USENIX Security 19), pp. 1429-1446. 2019.

(C11) Ivan De Oliveira Nunes, Ghada Dessouky, Ahmad Ibrahim, Norrathep Rattanavipanon, Ahmad-Reza Sadeghi, and Gene Tsudik. **Towards systematic design of collective remote attestation protocols.** In 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), pp. 1188-1198. IEEE, 2019.

(C12) Ivan De Oliveira Nunes, Karim Eldefrawy, Norrathep Rattanavipanon, and Gene Tsudik. **PURE: Using Verified Remote Attestation to Obtain Proofs of Update, Reset and Erasure in low-End Embedded Systems.** In IEEE/ACM International Conference On Computer Aided Design (ICCAD), pp. 1-8. 2019.

(C13) Ivan O. Nunes and Gene Tsudik. **KRB-CCN: Lightweight Authentication and Access Control for Private Content-Centric Networks.** In International Conference on Applied Cryptography and Network Security (ACNS), pp. 598-615. Springer, Cham, 2018.

(C14) Ivan De Oliveira Nunes, Karim Eldefrawy, and Tancrede Lepoint. **Secure Non-interactive User Re-enrollment in Biometrics-Based Identification and Authentication Systems.** In International Symposium on Cyber Security Cryptography and Machine Learning (CSCML), pp. 162-180. Springer, Cham, 2018.

(C15) Ivan O. Nunes, Gene Tsudik, and Christopher A. Wood. **Namespace tunnels in content-centric networks.** In 2017 IEEE 42nd Conference on Local Computer Networks (LCN), pp. 35-42. IEEE, 2017.

(C16) Ivan O. Nunes, Clayson Celes, Michael D. Silva, Pedro OS Vaz de Melo, and Antonio AF Loureiro. **GRM: Group Regularity Mobility Model.** In Proceedings of the 20th ACM International Conference on Modelling, Analysis and Simulation of Wireless and Mobile Systems (MSWIM), pp. 85-89. 2017.

(C17) Michael D. Silva, Ivan O. Nunes, Raquel AF Mini, and Antonio AF Loureiro. **ST-Drop: A novel buffer management strategy for D2D opportunistic networks.** In 2017 IEEE Symposium on Computers and Communications (ISCC), pp. 1300-1305. IEEE, 2017.

(C18) Antonio L. Maia Neto, Artur LF Souza, Italo Cunha, Michele Nogueira, Ivan Oliveira Nunes, Leonardo Cotta, Nicolas Gentille et al. **Aot: Authentication and access control for the entire iot device life-cycle.** In Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems (SenSys), pp. 1-15. 2016.

(C19) Ivan Oliveira Nunes, Pedro OS Vaz de Melo, and Antonio AF Loureiro. "Group mobility: Detection, tracking and characterization." In 2016 IEEE International Conference on Communications (ICC), pp. 1-6. IEEE, 2016.

REFEREED JOURNAL & MAGAZINE ARTICLES

(J1) Ivan De Oliveira Nunes, Karim Eldefrawy, and Tancrede Lepoint. **SNUSE: A secure computation approach for large-scale user re-enrollment in biometric authentication systems.** Future Generation Computer Systems 98 (2019): 259-273.

(J2) Ivan O. Nunes, Clayson Celes, Igor Nunes, Pedro OS Vaz de Melo, and Antonio AF Loureiro. **Combining spatial and social awareness in D2D opportunistic routing.** IEEE Communications Magazine 56, no. 1 (2018): 128-135.

(J3) Ivan O. Nunes, Clayson Celes, Pedro OS Vaz de Melo, and Antonio AF Loureiro. **GROUPS-NET: Group meetings aware routing in multi-hop D2D networks.** Computer Networks 127 (2017): 94-108.

(J4) Ivan O. Nunes, Pedro OS Vaz de Melo, and Antonio AF Loureiro. **Leveraging D2D multihop communication through social group meeting awareness.** IEEE Wireless Communications 23, no. 4 (2016): 12-19.

BOOK

(B1) I authored chapters 1, 7 and 8 of the `C` programming book **An Introduction to Programming: A New Approach Using C** (published in Portuguese) Elsevier, 2015. ISBN-13: 978-85-352-8011-1

PATENTS

(P1) Barbosa e Oliveira, L. et al. (2019). **System and Method for Authentication of Things.** U.S. Patent No. 10,523,437. Washington, DC: U.S. Patent and Trademark Office.

(P2) Eldefrawy, K., Nunes, I. D. O., & Tanguy, T. (2019). **Biometric authentication with template privacy and non-interactive re-enrollment.** U.S. Patent Application No. 16/373,355.

Awards & Honors

CSAW Applied Research Competition – North America Finalist 2019
One of the 10 Best Applied Security Papers in North America (out of 80 candidate papers)

M.Sc. Scholarship 2016
M.Sc. Scholarship for the Brazilian research agency FAPEMIG

M.Sc. Scholarship 2014-2015
Scholarship from the Brazilian's research agency CAPES

IEEE Latin American Robotics Competition - VSSS Autonomous Robot Soccer 2014
3rd Place out of 18 teams (Team leader)

Highest GPA 2014
Computer Engineering Graduating Class at UFES

SINDINFO Award for best bachelor's thesis in technology 2014
3rd Place

Science Without Borders Grant 2012-2013
Full Funding from the Brazilian Government to Study abroad at UCI for 1 year.

IEEE Latin American Robotics Competition - SEK Category 2010
1st place out of 33 teams

Peer Review Service

Conference Technical Program Committees
ISOC NDSS'22; ACM AsiaCCS'22.

External Reviewer
USENIX Security'20; NDSS'20; ACM CCS'20; WiSec'19; ACM CCS'18; NDSS-DISS'18; IEEE CNS'18; ASIACCS'17.

Journal Reviewers
ACM TODAES'20; Springer Computing'20; Elsevier Ad-Hoc Networks'17; IEEE ICC'17; IEEE WCM'16.

Student Organizations & Service

UFES Robotics Team – ERUS (Co-Founder & Member) 2012 - 2015

Student organization dedicated to use robotics as a means of outreach to undergraduates and local elementary and high schools. Activities include courses, workshop, and organization of local robotics competitions.

Tutorial Educational Program – PET (Member) 2009 - 2012

University group devoted to developing activities to bring University's research and educational projects closer to the local communities through a variety of outreach programs.

Pointers

Google Scholar: https://scholar.google.com/citations?user=2ITEX20AAAAJ&hl=en
DBLP: https://dblp.org/pid/173/5375.html
Research Gate: https://www.researchgate.net/profile/Ivan_De_Oliveira_Nunes2
LinkedIn: https://www.linkedin.com/in/ivan-de-oliveira-nunes-b74b82127/

Professional References

Available upon request.