

PERSONAL DATA



Name : DR. NORRATHEP RATTANAVIPANON
Position : Assistant Professor
Email : norrathep.r@phuket.psu.ac.th
Phone : 076276977
Website : <https://www.norrathep.com/>
ORCID : [0000-0003-1192-5079](https://orcid.org/0000-0003-1192-5079)
SCOPUS ID : [57194776707](https://scopus.com/authid/detail.uri?authorid=57194776707)

PUBLICATIONS SUMMARY

6

International Journal

21

International Proceedings

3

Research Grants

Total Publications: 30

EDUCATION

Ph.D. Degree	2019	University of California, Irvine
Master Degree	2015	University of California, Irvine
Bachelor Degree	2013	University of Michigan -- Ann Arbor

RESEARCH INTERESTS

*Embedded Systems Security**Machine Learning Systems Security**Software Systems Security*

RESEARCH PROJECTS

1. Embedded Systems and IoT Security

2. ML/AI Security
3. Binary Analysis

TEACHING

977-221 Module: Network and Security
977-330 Trusted Computing
977-210 Object-Oriented Programming

MSc/PhD STUDENTS

1. Amarin Laohajirapan, M.Sc., 2024-present
2. Raned Chuphueak, M.Sc., 2024-present

INTERNATIONAL JOURNAL ARTICLES

Norrathep Rattanavipanon, and Ivan De Oliveira Nunes. "[SLAPP: Poisoning Prevention in Federated Learning and Differential Privacy via Stateful Proofs of Execution](#)." *IEEE Transactions on Information Forensics and Security* (2025).

 3/2025

Rattanavipanon, Norrathep, Jakapan Suaboot, and Warodom Werapun. "A Toolchain for Assisting Migration of Software Executables Towards Post-Quantum Cryptography." *IEEE Access* (2024).

 1/2025

Ivan De Oliveira Nunes, Sashidhar Jakkamsetti, Norrathep Rattanavipanon, and Gene Tsudik, [Towards remotely verifiable software integrity in resource-constrained IoT devices](#), *IEEE Communications Magazine*, Volume 62, Issue 7, 2024.

 <https://ieeexplore.ieee.org/document/10400394>

 7/2024

Norrathep Rattanavipanon, Donlapark Ponnoprat, Hideya Ochiai, Kuljaree Tantayakul, Touchai Angchuan, and Sinchai Kamolphiwong, [Detecting Anomalous LAN Activities under Differential Privacy](#), *Hindawi Security and Communication Networks*, 2022.

 <https://doi.org/10.1155/2022/1403200>

 4/2022

N. Asokan, Thomas Nyman, Norrathep Rattanavipanon, Ahmad-Reza Sadeghi, and Gene Tsudik, [ASSURED: Architecture for Secure Software Update of Realistic Embedded Devices](#), *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)*, Volume 37, Issue 11, 2018.

 <https://ieeexplore.ieee.org/document/8493602>

 11/2018

Xavier Carpent, Norrathep Rattanavipanon, and Gene Tsudik. [Remote Attestation via Self-Measurement](#), *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, Volume 24, Issue 1, 2018.

 <https://dl.acm.org/doi/abs/10.1145/3279950>

 1/2018

INTERNATIONAL PROCEEDINGS

Adam Caulfield, Norrathep Rattanavipanon, and Ivan De Oliveira Nunes, Run-time Attestation and Auditing: The Verifier's Perspective, *ACM WiSec*, 2025.  <https://dl.acm.org/doi/10.1145/3734477.3734710>

 6/2025

Antonio Joia Neto, Norrathep Rattanavipanon, and Ivan De Oliveira Nunes, PEARTS: Provable Execution in Real-Time Embedded Systems, IEEE S&P,

2025.  <https://www.computer.org/csdl/proceedings-article/sp/2025/223600a047/21B7QzkFmY8>

 5/2025

Nasrin Sohrabi, Norrathep Rattanavipanon, and Zahir Tari, A Query Language to Enhance Security and Privacy of Blockchain as a Service (BaaS), ICSOC, 2024.

 12/2024

Adam Caulfield, Antonio Joia Neto, Norrathep Rattanavipanon, and Ivan De Oliveira Nunes, [TRACES: TEE-based Runtime Auditing for Commodity Embedded Systems](#), ACSAC, 2024

 12/2024

Ivan De Oliveira Nunes, Seoyeon Hwang, Sashidhar Jakkamsetti, Norrathep Rattanavipanon, and Gene Tsudik, [PARsel: Towards a Verified Root-of-Trust over sel4](#), ICCAD, 2023.

 11/2023

Nattawat Songsom, Warodom Werapun, Jakapan Suaboot, and Norrathep Rattanavipanon, [The SWC-based Security Analysis Tool for Smart Contract Vulnerability Detection](#), INCIT, 2022.

 10/2022

Adam Caulfield, Norrathep Rattanavipanon, and Ivan De Oliveira Nunes, [ASAP: Reconciling Asynchronous Real-Time Operations and Proofs of Execution in Simple Embedded Systems](#), DAC, 2022.

 <https://doi.org/10.1145/3489517.3530550>

 7/2022

Ivan De Oliveira Nunes, Sashidhar Jakkamsetti, Norrathep Rattanavipanon, and Gene Tsudik, [On the TOCTOU Problem in Remote Attestation](#), CCS, 2021.

 11/2021

Norrathep Rattanavipanon, Donlapark Ponnoprat, Hideya Ochiai, Kuljaree Tantayakul, Touchai Angchuan, and Sinchai Kamolphiwong, [Releasing ARP Data with Differential Privacy Guarantees For LAN Anomaly Detection](#), ECTI-CON 2021.

 5/2021

Karim Eldefrawy, Michael Locasto, Norrathep Rattanavipanon, and Hassen Saidi, [Towards Automated Augmentation and Instrumentation of Legacy Cryptographic Executables](#), Applied Cryptography and Network Security (ACNS), 2020.

 10/2020

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](#), USENIX Security, 2020.

 8/2020

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](#), IEEE/ACM ICCAD, 2019.

 10/2019

Ivan De Oliveira Nunes, Karim Eldefrawy, Norrathep Rattanavipanon, Michael Steiner, and Gene Tsudik, [VRASED: A Verified Hardware/Software Co-Design for Remote Attestation](#), in USENIX Security, 2019.

 8/2019

Ivan De Oliveira Nunes, Ghada Dessouky, Ahmad Ibrahim, Norrathep Rattanavipanon, Ahmad-Reza Sadeghi and Gene Tsudik, [Towards Systematic Design of Collective Remote Attestation Protocols](#), IEEE ICDCS, 2019.

 6/2019

N. Asokan, Thomas Nyman, Norrathep Rattanavipanon, Ahmad-Reza Sadeghi, and Gene Tsudik, [ASSURED: Architecture for Secure Software Update of Realistic Embedded Devices](#), EMSOFT, 2018.

 8/2018

Xavier Carpent, Karim Eldefrawy, Norrathep Rattanavipanon, Ahmad-Reza Sadeghi, and Gene Tsudik, [Invited:](#)

[Reconciling Remote Attestation and Safety-Critical Operation on Simple IoT Devices](#), DAC, 2018.

📅 8/2018

Xavier Carpent, Karim ElDefrawy, Norrathep Rattanavipanon, and Gene Tsudik, [Temporal Consistency of Integrity-Ensuring Computations and Applications to Embedded Systems Security](#), ACM ASIACCS, 2018.

📅 5/2018

Xavier Carpent, Norrathep Rattanavipanon, and Gene Tsudik, [Remote Attestation of IoT Devices via SMARM: Shuffled Measurements Against Roving Malware](#), IEEE HOST, 2018.

📅 4/2018

Xavier Carpent, Norrathep Rattanavipanon, and Gene Tsudik, [ERASMUS: Efficient Remote Attestation via Self-Measurement for Unattended Settings](#), DATE, 2018.

📅 4/2018

Karim ElDefrawy, Norrathep Rattanavipanon and Gene Tsudik, [HYDRA: HYbrid Design for Remote Attestation \(Using a Formally Verified Microkernel\)](#), ACM WiSEC 2017.

📅 10/2017

Xavier Carpent, Karim ElDefrawy, Norrathep Rattanavipanon, and Gene Tsudik, [Lightweight Swarm Attestation: A Tale of Two LISAs](#), ACM ASIACCS, 2017.

📅 4/2017

RESEARCH GRANTS

การตรวจจับซอฟต์แวร์ไบนารีที่เสี่ยงต่อการถูกโจมตีด้วยควอนตัมคอมพิวเตอร์: 599,060 baht funded by
เงินงบประมาณแผ่นดิน, 2025

📅 2025

การป้องกันการโจมตีแบบ Poisoning Attacks ในระบบ IoT แบบกระจายศูนย์: 281,580 baht funded by
หน่วยบริหารและจัดการทุนด้านการพัฒนากำลังคน และทุนด้านการพัฒนาสถาบันอุดมศึกษา การวิจัยและการสร้างนวัตกรรม
(บพค.), 2025

📅 2025

Securing Remote Attestation Against Time-of-Check Time-of-Use (TOCTOU) Attacks in Embedded/IoT
Devices (การป้องกันปัญหา TOCTOU ในระบบการยืนยันระยะไกลของอุปกรณ์ฝังตัว)

: 250,000 baht funded by Young Research Grant (ทุนนักวิจัยใหม่ ว.ท.), 2021

📅 2021

[Scan Me!! CV Online](#)



COLLEGE OF COMPUTING

Prince of Songkla University Phuket Campus

80 M.1 Vichitsongkram Road Kathu, Phuket 83120

Email: coc@phuket.psu.ac.th

Website: computing.psu.ac.th