DECENTRALIZED MECHANISMS TO ATTEST, RECOVER AND UPDATE IOT NETWORKS

SAMUEL WEDAJ KIBRET

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY DELHI
NOVEMBER 2021

DECENTRALIZED MECHANISMS TO ATTEST, RECOVER AND UPDATE IOT NETWORKS

by

SAMUEL WEDAJ KIBRET

Department of Computer Science and Engineering

Submitted

in fulfillment of the requirements of the degree of
Doctor of Philosophy

to the

Indian Institute of Technology Delhi
November 2021

Certificate

This is to certify that the thesis titled **Decentralized Mechanisms to Attest, Recover and Update IoT Networks** being submitted by **Samuel Wedaj Kibret** for the award of **Doctor of Philosophy** in **Computer Science and Engineering** is a record of bona fide work carried out by her under my guidance and supervision at the Department of Computer Science and Engineering, Indian Institute of Technology Delhi. The work presented in this thesis has not been submitted elsewhere, either in part or full, for the award of any other degree or diploma.

Kolin Paul
Professor
Department of Computer Science and Engineering
Indian Institute of Technology Delhi
New Delhi - 110016

Vinay Joseph Ribeiro
Associate Professor
Department of Computer Science and Engineering
Indian Institute of Technology Bombay
Powai, Mumbai - 400076

Acknowledgements

First and foremost, I am very honored to have Prof. Kolin Paul and Prof. Vinay J. Ribeiro as my thesis advisors, and I would like to thank them for their continuous guidance, constant feedback, unconditional support, and motivation throughout the course of my doctorate.

I had the opportunity and pleasure to have worked together with many colleagues and students. I especially thank Sourav Das for his contribution to the thesis. I would also thank my friends and colleagues Solomon Abera, Samuel Kassaye, Rajshekar K., Rajesh Kedia, and Himanshu Gandhi for their help and support during my stay at IIT Delhi. I thank them for their feedback and inspiring discussions in the course of my Ph.D. I am also thankful to the lab and office staff in the Department of Computer Science and Engineering and School of IT, especially Mrs. Vandana, Mrs. Rekha, Mr. Hemant, Mr. Rajesh, and Mr. Suresh, for facilitating things and making several processes smoother for me.

I am extremely indebted to IIT Delhi for providing me the necessary facilities, support and creating a conducive environment for my research.

Finally, I am deeply thankful to my family for their support before and during my doctorate. I could not have made it without their encouragement. I am thankful to God for his grace.

Samuel Wedaj Kibret

Abstract

Embedded devices are pervasive and are critical for building systems used in safety and mission-critical Internet of Things (IoT) applications, from smart grids to robotics systems and process control systems. Such systems are characterized by large numbers of smart mobile and interconnected devices (i.e., device swarms). Thus, it is imperative to have a good verification mechanism that scales to device swarms and establishes trust among collaborating member devices.

Nowadays, Remote Attestation (RA) is being used as a viable technique for detecting attacks in Cyber-Physical Systems (CPS) and Internet of Things (IoT) devices. This security service requires a secure memory to store attestation-related code and signing keys and isolation guarantees for the execution of the attestation code. Such minimal hardware support is provided by various state-of-the-art architectures for secure and practical embedded systems remote attestations like SMART, TrustLite, ARM TrustZone's security extensions, etc.

Current state-of-the-art swarm attestation techniques have key limitations: having a single (central) verifier creates a single point of failure, lack of scalability for device swarms, they do not support device mobility, they only focus on the detection of the presence of malware, and they are all static, i.e., they only check the authenticity of the binary code loaded in the Random-access memory (RAM).

In this dissertation, we present a novel decentralized Attestation approach for device swarms. In light of making swarm attestation efficient and addressing the key security issue, our technique spreads the verifier's (verification) duties to swarm members. It is decentralized, has no single point of failure, and can handle changing topologies after nodes are compromised. The approach assures system resilience to node compromise/failure while guaranteeing only devices that execute

genuine code remain part of the group. We conduct performance measurements of run-time, communication, computation, memory, and energy, based on the TrustLite embedded systems architecture in the OMNeT++ simulation environment. We show that our approach is very effective and robust against various attacks.

We also present a novel decentralized, self-reliant, and re-configurable attestation scheme that executes in the SMM operating mode, available in IoT devices built with x86 CPUs. After successful attestation, our approach generates a trusted graph on which message exchanges rely. It is resilient to node compromise/failure and does not need additional hardware requirements. We evaluate performance using real-world embedded (cyber-physical) applications and demonstrate that the execution overhead is negligible. We also analyze security.

Furthermore, we also deal with the issue of disinfecting swarm members after device compromise. In this regard, we introduce a method and system to detect the application software's corruption on an IoT node and self corrects itself using its neighbors. This decentralized mechanism prevents the spread of self-propagating malware and can also be used to update application code on IoT devices. We assess the performance using the embedded systems security architecture of TrustLite in the OMNeT++ simulator. The results show that our approach scales up to thousands of devices, ensures the guaranteed update of the entire network, and can recover 95% of the nodes in 10 minutes in both internal and external propagation models. Moreover, we evaluate memory and communication costs and show that this approach is efficient and incurs very low overhead.

Additionally, we investigate recent efforts on runtime attestation techniques and propose a data-flow based decentralized device swarm attestation scheme: the first complete and efficient swarm attestation approach that takes care of both static and runtime attestations, assuring that swarm members execute the correct and unmodified program, and checks if they are exposed to runtime attacks. We describe a full prototype implementation and evaluate the performance using OP-TEE, which is ARM TrustZone based open-source implementation of TEE (Trusted Execution Environment). We also assess performance and analyze security for large swarms and show that the proposed approach is very effective and robust against various attacks.

सार

एंबेडेड डिवाइस व्यापक हैं और सुरक्षा और मिशन क्रिटिकल में उपयोग की जाने वाली प्रणालियों के निर्माण के लिए महत्वपूर्ण हैं इंटरनेट ऑफ थिंग्स (IoT) एप्लिकेशन, स्मार्ट ग्रिड से लेकर रोबोटिक्स सिस्टम और प्रोसेस तक नियंत्रण प्रणाली। इस तरह के सिस्टम बड़ी संख्या में स्मार्ट मोबाइल और परस्पर जुड़े हुए होते हैं डिवाइस (यानी, डिवाइस स्वार)। इस प्रकार, एक अच्छा सत्यापन तंत्र होना अनिवार्य है जो डिवाइस को स्केल करता है और सहयोगी सदस्य डिवाइसों के बीच विश्वास स्थापित करता है। आजकल, हमलों का पता लगाने के लिए एक व्यवहार्य तकनीक के रूप में रिमोट सत्यापन (आरए) का उपयोग किया जा रहा है साइबर-फिजिकल सिस्टम (CPS) और इंटरनेट ऑफ थिंग्स (IoT) डिवाइस। इस सुरक्षा सेवा की आवश्यकता है अनुप्रमाणन-संबंधित कोड को संग्रहीत करने के लिए एक सुरक्षित मेमोरी और के लिए कुंजी और आइसोलेशन गारंटी पर हस्ताक्षर करना सत्यापन कोड का निष्पादन। इस तरह का न्यूनतम हार्डवेयर समर्थन विभिन्न द्वारा प्रदान किया जाता है सुरक्षित और व्यावहारिक एम्बेडेड सिस्टम के लिए अत्याधुनिक आर्किटेक्चर दूरस्थ सत्यापन जैसे स्मार्ट, ट्रस्टलाइट, एआरएम ट्रस्टज़ोन के सुरक्षा एक्सटेंशन इत्यादि। वर्तमान अत्याधुनिक झुंड सत्यापन तकनीकों की प्रमुख सीमाएँ हैं: एकल (केंद्रीय) होना सत्यापनकर्ता विफलता का एकल बिंदु बनाता है, डिवाइस के झुंड के लिए मापनीयता की कमी, वे नहीं करते हैं उपकरण गतिशीलता का समर्थन करते हैं, वे केवल मैलवेयर की उपस्थिति का पता लगाने पर ध्यान केंद्रित करते हैं, और वे हैं सभी स्थिर, यानी, वे केवल रैंडम-एक्सेस में लोड किए गए बाइनरी कोड की प्रामाणिकता की जांच करते हैं मेमोरी (रैम)। इस शोध प्रबंध में, हम उपकरणों के झुंड के लिए एक नया विकेन्द्रीकृत सत्यापन दृष्टिकोण प्रस्तुत करते हैं। में झुंड सत्यापन को कुशल बनाने और प्रमुख सुरक्षा मुद्दे को संबोधित करने की रोशनी, हमारी तकनीक सत्यापनकर्ता (सत्यापन) कर्तव्यों को झुंड के सदस्यों तक फैलाता है। यह विकेंद्रीकृत है, इसमें कोई एकल नहीं है विफलता का बिंदु, और नोड्स से समझौता होने के बाद बदलती टोपोलॉजी को संभाल सकता है। पहुंच नोड समझौता/विफलता के लिए सिस्टम लचीलापन का आश्वासन देता है जबकि केवल निष्पादित करने वाले उपकरणों की गारंटी देता है

वास्तविक कोड समूह का हिस्सा बना रहता है। हम रन-टाइम के प्रदर्शन माप का संचालन करते हैं, ट्रस्टलाइट एम्बेडेड सिस्टम पर आधारित संचार, गणना, स्मृति और ऊर्जा OMNeT++ सिमुलेशन वातावरण में वास्तुकला। हम दिखाते हैं कि हमारा दृष्टिकोण बहुत है विभिन्न हमलों के खिलाफ प्रभावी और मजबूत। हम एक उपन्यास विकेन्द्रीकृत, आत्मनिर्भर, और पुन: विन्यास योग्य सत्यापन योजना भी प्रस्तुत करते हैं कि SMM ऑपरेटिंग मोड में निष्पादित होता है, जो x86 CPU के साथ निर्मित IoT उपकरणों में उपलब्ध है। बाद में सफल सत्यापन, हमारा दृष्टिकोण एक विश्वसनीय ग्राफ उत्पन्न करता है जिस पर संदेश आदान-प्रदान भरोसा करते हैं।

यह नोड समझौता/विफलता के लिए लचीला है और अतिरिक्त हार्डवेयर आवश्यकताओं की आवश्यकता नहीं है। हम वास्तविक-विश्व एम्बेडेड (साइबर-भौतिक) अनुप्रयोगों का उपयोग करके प्रदर्शन का मूल्यांकन करें और प्रदर्शित करें कि निष्पादन उपरि नगण्य है। हम सुरक्षा का भी विश्लेषण करते हैं। इसके अलावा, हम डिवाइस से समझौता करने के बाद झुंड के सदस्यों को कीटाणुरहित करने के मुद्दे से भी निपटते हैं। इस संबंध में, हम एप्लिकेशन सॉफ़्टवेयर के भ्रष्टाचार का पता लगाने के लिए एक विधि और प्रणाली पेश करते हैं एक IoT नोड पर और स्वयं अपने पड़ोसियों का उपयोग करके स्वयं को सुधारता है। यह विकेन्द्रीकृत तंत्र रोकता है स्व-प्रसारित मैलवेयर का प्रसार और IoT पर एप्लिकेशन कोड अपडेट करने के लिए भी इसका उपयोग किया जा सकता है उपकरण। हम ट्रस्टलाइट के एम्बेडेड सिस्टम सुरक्षा आर्किटेक्चर का उपयोग करके प्रदर्शन का आकलन करते हैं OMNet++ सिमुलेटर में। परिणाम बताते हैं कि हमारा दृष्टिकोण हजारों . तक है डिवाइस, पूरे नेटवर्क के गारंटीकृत अपडेट को सुनिश्चित करता है, और 95% नोड्स को पुनर्प्राप्त कर सकता है आंतरिक और बाहरी प्रसार मॉडल दोनों में 10 मिनट में। इसके अलावा, हम स्मृति का मूल्यांकन करते हैं और संचार लागत और दिखाते हैं कि यह दृष्टिकोण कुशल है और बहुत कम उपरि खर्च करता है। इसके अतिरिक्त, हम रनटाइम सत्यापन तकनीकों पर हाल के प्रयासों की जांच करते हैं और डेटा प्रवाह का प्रस्ताव करते हैं आधारित विकेन्द्रीकृत उपकरण झुंड सत्यापन योजना: पहला पूर्ण और कुशल झुंड सत्यापन दृष्टिकोण जो स्थिर और रनटाइम सत्यापन दोनों का ध्यान रखता है, उस झुंड को आश्वस्त करता है सदस्य सही और असंशोधित प्रोग्राम को निष्पादित करते हैं, और जांचते हैं कि क्या वे रनटाइम के संपर्क में हैं हमले। हम एक पूर्ण प्रोटोटाइप कार्यान्वयन का वर्णन करते हैं और OPTEE का उपयोग करके प्रदर्शन का मूल्यांकन करते हैं, जो टीईई (विश्वसनीय निष्पादन) का एआरएम ट्रस्टजोन आधारित ओपन-सोर्स कार्यान्वयन है पर्यावरण)। हम प्रदर्शन का आकलन भी करते हैं और बड़े झुंडों के लिए सुरक्षा का विश्लेषण करते हैं और दिखाते हैं कि विभिन्न हमलों के खिलाफ प्रस्तावित दृष्टिकोण बहुत प्रभावी और मजबूत है।

Contents

List of Figures

List of Tables

List of Acronyms

AMD	Advanced Micro Devices
ARM	Advanced RISC Machines
BC	Blockchain
BIOS	Basic Input Output System
BFS	Breadth First Search
CPS	Cyber-Physical Systems
CPU	Central Processing Unit
DFS	Depth First Search
DOP	Data-oriented Programming
DRAM	Dynamic Random Access Memory
DRTM	Dynamic Root of Trust for Measurement
DDoS	Distributed Denial-of-Service
DoS	Denial-of-Service
EA-MPU	Execution-Aware Memory Protection Unit
ECDSA	Elliptic Curve Digital Signature Algorithm
EPC	Enclave Page Cache
EPCM	Enclave Page Cache Map
GPIO	General-Purpose Input/Output
GPU	Graphics Processing Unit
HMAC	Hash-based Message Authentication Code
HR	High Resource
IDT	Interrupt Descriptor Table
IoT	Internet of Things
IIoT	Industrial Internet of Things
IRQ	Interrupt Request
I/O APIC	Input/Output Advanced Programmable Interrupt Controller
LR	Low Resource
MAC	Message Authentication Code
ML	Machine Learning
MPU	Memory Protection Unit

NS-3	Network Simulator Tool-3
OS	Operating System
PC	Program Counter
PPT	Probabilistic Polynomial-Time
QoSA	Quality of Swarm Attestation
RA	Remote Attestation
RAM	Random Access Memory
RISC	Reduced Instruction Set Computer
ROP	Return-Oriented Programming
RSM	Resume
SGX	Software Guard Extensions
SHA-1	Secure Hash Algorithm-1
SMI	System Management Interrupt
SMRAM	System Management Random Access Memory
SoC	System on a Chip
SPOF	Single Point of Failure
TEE	Trusted Execution Environment
TLS	Transport Layer Security
SMM	System Management Mode
UAV	Unmanned Aerial Vehicles
VERMAC	Verify Message Authentication Code