Internet of Things

Technology, Communications and Computing

More information about this series at http://www.springer.com/series/11636

Rajat Subhra Chakraborty
Jimson Mathew · Athanasios V. Vasilakos
Editors

Security and Fault Tolerance in Internet of Things

Springer

Editors
Rajat Subhra Chakraborty
Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur
Kharagpur, West Bengal, India

Jimson Mathew
Department of Computer Science and Engineering
Indian Institute of Technology Patna
Patna, Bihar, India

Athanasios V. Vasilakos
Department of Computer Science, Electrical and Space Engineering
Luleå University of Technology
Skellefteå, Sweden

ISSN 2199-1073 ISSN 2199-1081 (electronic)
Internet of Things
ISBN 978-3-030-02806-0 ISBN 978-3-030-02807-7 (eBook)
https://doi.org/10.1007/978-3-030-02807-7

Library of Congress Control Number: 2018958936

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The aim of this book is to cover various aspects of security, privacy and reliability in Internet of things (IoT) and cyber-physical system design, analysis and testing. Security is a prime design objective in current computing system design, including embedded systems, cyber-physical systems and the IoT devices. Over the years, various techniques have been proposed highlighting security and fault-tolerant system design, analysis and testing. Since cyber-physical systems are typically resource-constrained, these techniques are usually developed keeping the low energy and/or low-power availability into perspective. However, due to continued device miniaturization and technology scaling, reliability in the presence of ever-increasing number of faults is emerging as a design challenge, and more importantly, new security threats have emerged. This is because incorporating security, fault tolerance for reliability with low-energy or low-power consumption are conflicting design objectives. From IoT security to design robustness and big data processing, this monograph offers a potpourri of different methodologies on this rapidly expanding frontier of the new technology, with chapters written by leading international industry practitioners and academic researchers. It is intended that the readers receive both these perspectives, which is important for such cutting-edge technical topics of discourse.

Chapter "Security and Trust Verification of IoT SoCs" looks at the trustworthiness of System-on-Chips (SoCs). In order to ensure the security of IoT devices, it is crucial to guarantee the trustworthiness of SoCs, because advances in modern VLSI miniaturization technologies imply more and more functionality are being packed into complex SoCs than ever before. Verifying the trust in SoCs is a major challenge due to their long and globally distributed supply chain. Malicious components can be inserted in different stages of the design cycle. These malicious functionalities work as a backdoor to severely affect the security of the design by giving control of the system to adversaries. The threat creates a critical need for designing new validation approaches that are capable of identifying hidden Hardware Trojan Horses (HTHs). Existing validation techniques cannot efficiently activate and detect HTHs since Trojans are designed to be passive most of the time and usually triggered using very rare events. For example, if an adversary wants to

hide a HTH in register-transfer level (RTL) designs, rare branches in the control flow would be an ideal choice to host Trojans. To tackle this issue, the authors introduce a Trojan activation technique that utilizes an effective combination of symbolic simulation as well as concrete execution to identify Trojans that are hidden under rare branches and assignments. The technique is scalable as it considers one path at a time instead of considering the whole design. It uses *Satisfiability Modulo Theories* (SMT) solvers to satisfactorily solve the path constraints in order to generate a valid test to explore a new path in the design. The exploration continues until all of the rare branches in the design are activated in the search for hidden Trojans.

Chapter "Low Cost Dual-Phase Watermark for Protecting CE Devices in IoT Framework" presents a novel low-cost dual-phase watermarking methodology during high-level synthesis (HLS) for hardware intellectual property (IP) protection. Robust vendor signature is embedded in two subsequent phases of high-level synthesis to form an integrated watermark. A dual-phase watermarking methodology that embeds a multivariable double-phase watermarking during high-level synthesis for application-specific IPs, while incurring zero delay and register overhead as well as minimal hardware overhead, is presented. The dual-phase watermarking approach yields average reduction of embedding cost of 6% (which includes average area reduction of 7% and average latency reduction of 4%) when compared to two recent HLS-based watermarking approaches for application-specific IPs. Additionally, the approach also achieves stronger proof of authorship compared to two recent HLS-based watermarking approaches.

Chapter "Secure Multicast Communication Techniques for IoT" discusses multicast security approaches mainly based on extending the DTLS protocol and its drawbacks. Also included are the major requirements of secure group communication and different secure multicast communication techniques emphasizing an interesting and effective approach called S-CPABE, based on attribute-based encryption (ABE).

Chapter "An Adaptable System-on-Chip Security Architecture for Internet of Things Applications" addresses emerging threats and security design constraints of architectures catering to IoT and automotive applications and their subsequent limitations. Then, it presents a novel, flexible and adaptable SoC security architecture that efficiently implements diverse security policies. The architecture and associated CAD flow enable "hardware patching", i.e., hardware security policy engines that can be seamlessly and securely upgraded infield to address unanticipated attacks or new security requirements. The chapter describes the implementation of (1) a centralized Reconfigurable Security Policy Engine (RSPE); (2) smart security wrappers and (3) Design-for-Debug (DfD) infrastructure interface as the building blocks of the architecture. The proposed framework provides a systematic approach to represent and synthesize diverse security policies. Through extensive analysis using representative SoC model, it is demonstrated that the proposed framework provides a high level of adaptability with minimal energy and performance overhead. Consequently, the architecture is highly suitable for devices operating under a tight boundary of energy and performance.

Homomorphic encryption constitutes a powerful cryptographic method that enables data aggregation in distributed applications over large datasets, such as storage of data on cloud, electronic voting, electronic wallets, secure auctions, lotteries and secret sharing. At the same time, as attack trends move towards the lower levels of the computation stack and new threats continue to emerge, the lack of trust in contemporary computing paradigms keeps increasing. Since homomorphic encryption helps preserve the confidentiality of sensitive information, it offers a powerful countermeasure against contemporary and future privacy threats, while allowing meaningful processing even though the data remains unreadable. Nevertheless, when homomorphic primitives are mapped to hardware circuits to improve performance, they become vulnerable to random faults and soft errors, since homomorphic operations are malleable by construction and do not provide any explicit assurance towards data integrity. Chapter "Lightweight Fault Tolerance for Secure Aggregation of Homomorphic Data" presents a fault tolerance methodology that protects homomorphic aggregation circuits through concurrent detection of random errors in homomorphic ALUs and encrypted values stored in the memory. The proposed approach establishes the theoretical foundations to extend residue numbering to additive homomorphic operations, which enables lightweight fault detection with detection rates of more than 99.98% for ALU operations and 100% for single bit-flips and clustered faults in memory values. Using an efficient modular reduction algorithm, the method incurs a runtime overhead between 3.6 and 8% and a small area cost.

In Chapter "An Approach to Integrating Security and Fault Tolerance Mechanisms into the Military IoT" the authors look at security and dependability of IoT implementation in military applications. This is an approach for integrating security techniques on the access layer and the fault-tolerant techniques at sensor nodes. Presented solutions for securing the military IoT network ensure strong node authentication within network clusters and securing data transmissions between sensor nodes (SN) and gateways with the use of COTS IoT platforms equipped with TPM modules. Fault diagnosis is based on the comparison method within network clusters. An experimental network called SFTN is also explored to demonstrate the approach.

Physically unclonable function (PUF) circuits are very promising lightweight hardware security primitives, which depend on manufacturing process variations, act as fingerprint generators of electronic devices such as integrated circuits (ICs). PUF circuits can be used as alternatives to computationally expensive cryptographic algorithms and protocols and are extremely suitable for application domains such as IoTs. However, they are vulnerable to injected faults that can help an adversary to launch sophisticated computational attacks on them, revealing secret information that can impact system security. Chapter "Fault-Tolerant Implementations of Physically Unclonable Functions on FPGA" describes fault-tolerant implementations of PUF circuits on FPGAs, through fault detection and fault recovery.

Chapter "Fault Tolerance in 3D-ICs" discusses fault tolerance in three-dimensional IC (3D ICs). Systems based on emerging technologies like Internet of things and beyond von Neumann architectures can be produced in large scale

only if they are resilient-aware, cost-effective and secure. The resilient and cost-effective solutions can be achieved by incorporating fault tolerance techniques at the architectural level of the system design is one of the plausible solutions. The choice of various fault tolerance techniques gives the designers a freedom to incorporate these in the early stage of the design and in turn leading to high yield and reliable architectures. Three-dimensional ICs with through-silicon via (TSV) is one of the emerging technologies consisting of vertical interlayer communication instead of long horizontal wires, results in the reduction of interconnect length and thus can improve the system performance. However, reliability and yield are major concerns that hinder resilient and cost-effective solutions for 3D-IC design. These can be addressed by incorporation of fault tolerance techniques.

Online detection of cyber-attacks on IoT devices is usually extremely challenging due to limited battery and computational resources available in these devices. An alternate approach is to shrink the attack surface in order to reduce the threat of attack. This would require that the device undergo more stringent security tests before deployment. Formal verification is a promising tool that can be used to not only detect potential vulnerabilities but also provide guarantees of security. Chapter "Formal Verification for Security in IoT Devices" reviews several security issues that plague IoT devices such as functional correctness of implementations, programming bugs, side-channel analysis and HTHs. In each of these cases, the chapter discusses state-of-the-art techniques that use formal verification tools to detect the vulnerability much before the device is deployed.

In Chapter "SENSE: Sketching Framework for Big Data Acceleration on Low Power Embedded Cores", the authors address the ever-growing IoT-based big data processing and cognitive computing on mobile and battery-operated devices. Big data processing on low-power embedded cores is challenging due to their limited communication bandwidth and on-chip storage. Additionally, IoT and cloud-based computing demand low overhead security kernel to avoid data breaches. In this chapter, authors present, "LESS", lightweight encryption using scalable sketching techniques for data reduction and encryption. LESS is a heterogeneous framework which consists of three important kernels: (1) a sketching module for data reduction; (2) an accelerator for efficient sketch recovery using scalable and parallel reconstruction architecture and (3) a host processor to perform postprocessing. LESS framework can reduce data up to 67% with 3.81 dB signal-to-reconstruction error rate (SRER). One of the critical challenges in big data processing on embedded hardware platforms is to reconstruct the sketched data in real-time with stringent constraints on error bounds and hardware resources. The authors also explore orthogonal matching pursuit (OMP) algorithm for sketch data recovery and demonstrate performance of LESS framework on face identification application.

We hope this monograph would be valuable to researchers and practitioners alike, not only as a collection of pointers to cutting-edge research in this exciting field, but also as a resource that would encourage the readers to explore newer techniques on their own. Cyber-physical systems and IoTs promise to revolutionize

our lives, but before their promise is fulfilled, many open problems in the context of their security and reliability need satisfactory solutions. It is our sincere wish that this book acts a small step towards that goal.

Kharagpur, India — Rajat Subhra Chakraborty
Patna, India — Jimson Mathew
Skellefteå, Sweden — Athanasios V. Vasilakos
August 2018

Contents