Secure and Trustworthy Cyberphysical Microfluidic Biochips

Jack Tang • Mohamed Ibrahim
Krishnendu Chakrabarty • Ramesh Karri

Secure and Trustworthy Cyberphysical Microfluidic Biochips

A practical guide to cutting-edge design techniques for implementing secure and trustworthy cyberphysical microfluidic biochips

Springer

Jack Tang
New York University
Brooklyn, NY, USA

Mohamed Ibrahim
Intel (United States)
Santa Clara, CA, USA

Krishnendu Chakrabarty
Department of ECE
Duke University
Durham, NC, USA

Ramesh Karri
New York University
Brooklyn, NY, USA

ISBN 978-3-030-18162-8 ISBN 978-3-030-18163-5 (eBook)
https://doi.org/10.1007/978-3-030-18163-5

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

To Amy and Simone,
for showing me what truly matters.
— Jack Tang

Preface

Security, trust, and privacy issues arising out of the mass adoption of modern technologies are now commonplace. The rate at which these issues have gone from afterthought to frequently appearing front page news is disconcerting. Interestingly, even though security is now a marketing buzzword, the actual adoption and implementation of security measures in certain industries is still inadequate. When the Internet-of-Things (IoT) movement began to take shape during the 2000s, numerous articles on the security of these highly connected, resource-constrained devices were published. Despite this knowledge, IoT manufacturers proceeded to develop insecure devices due to either cost, time, lack of interest, or poor management decisions. The success of the Mirai botnet in 2017, which leveraged insecure password defaults to take over devices such as DVRs and webcams, is a case in point.

This book concerns the security and trust of cyberphysical microfluidic biochips (CPMBs), with emphasis on the analysis and design of hardware that is robust against tampering. We argue that it is the responsibility of a system designer to anticipate security issues, and we demonstrate this through the development of several hardware-based countermeasures. The work in this book is not reactionary—it is not a series of Band-Aid fixes for systems designed without security implications in mind, which is essentially the practice used by Internet-based services and devices today. Instead, this work is completely anticipatory in nature, building from the ground up with performance under malicious activity as a key design metric.

Security and trust is a broad and sometimes difficult-to-define topic of academic inquiry. This book's definition of security and trust is inspired to a large extent from the field of hardware security, which has historically been understood to refer to semiconductor devices, processes, and their manufacturing models. It includes a large body of work on intellectual property (IP) protection schemes, driven by the interests of large semiconductor and media companies. But it also includes attacks and countermeasures that more directly affect the end user as well as interesting

new physical primitives such as physical unclonable functions (PUFs). The field has roots in the VLSI design-for-test community and often utilizes the same tools such as Boolean satisfiability, automatic test program generation (ATPG), and integer linear programming (ILP).

Another commonality hardware security shares with DfT is that of intense initial resistance from industry. The concept of a scan chain was at one point considered to be unnecessary overhead that could be better used for implementing functionality but eventually gained widespread adoption. Similarly, the concept of using a scan chain for attacks and having to design a secure scan chain was met skepticism. As such, security researchers often face a catch-22 when developing any new work. This book takes the stance that it is better to anticipate security threats rather than wait for them to appear. To that end, this book features three design techniques for the prevention, detection, and mitigation of actuation tampering attacks on CPMBs.

For prevention, we present the concept of a tamper-resistant pin-constrained digital microfluidic biochip (DMFB), which manipulates fluids in discrete droplets on a grid of patterned electrodes. The most straightforward implementation of a DMFB brings out each electrode to a pin which is then connected to driver circuitry. To overcome the high pin count, pin-constrained DMFBs short compatible electrodes to the same pin. This trades off the pin count for a reduction in freedom of droplet movement and forms the basis of the tamper resistance property, which we then optimize for using graph theory and integer linear programming.

We then propose a randomized checkpoint system for the purposes of detecting an actuation tampering attack. Practical DMFBs are often integrated with sensors for the purpose of monitoring the progression of assays since they are prone to many failure modes. Due to cost and resource constraints, these sensing systems are limited in the number of locations on the biochip that can be monitored. By randomizing the inspection of electrodes in time and space, we accommodate these constraints while making it probabilistically difficult for an attack to evade detection.

Finally, we develop a design framework for tamper-mitigating microfluidic routing fabrics. Such reconfigurable primitives are attractive to end users for their convenience, but they also present an opportunity for an attacker to force the biochip into an unintended state. This book describes a method for analysis and synthesis of routing fabrics that probabilistically mitigate fault injection-based tampering attacks.

The work featured in this book fits into the broader context of hardware security as a new subfield, which we call *cyberphysical microfluidic biochip security* or CPMB security. The implementation of CPMB security measures shares many similarities with those used in other cyberphysical systems and electronic devices, but the key differentiator is that we leverage unique microfluidic aspects of these systems wherever possible. The authors hope that this book functions as a resource and inspiration for the designers of next-generation microfluidic systems.

The authors acknowledge the financial support received from the Army Research Office under grant number W911NF-17-1-0320, the National Science Foundation under grant CNS-1833624, the NYU Center for Cyber Security, and the NYU-AD Center for Cyber Security.

Brooklyn, NY, USA — Jack Tang
Santa Clara, CA, USA — Mohamed Ibrahim
Durham, NC, USA — Krishnendu Chakrabarty
Brooklyn, NY, USA — Ramesh Karri

Contents