Attacks and Countermeasures for Digital Microfluidic Biochips

Extended Abstract

Navajit Singh Baban[1], Prithwish Basu Roy[2], Pauline John[1], Azhar Zam[1,2], Sukanta Bhattacharjee[3], Yong-Ak Song[1,2], Ramesh Karri[2], and Krishnendu Chakrabarty[4]

[1] New York University Abu Dhabi, Division of Engineering
[2] New York University, Tandon School of Engineering
[3] Indian Institute of Technology Guwahati, Department of Computer Science and Engineering
[4] Arizona State University, School of Electrical, Computer and Energy Engineering
{nsb359, pb2718, pj2266, az2832, rafael.song, rkarri}@nyu.edu,
sukantab@iitg.ac.in, krishnendu.chakrabarty@asu.edu

Abstract. Digital Microfluidic Biochips (DMFBs) precisely control droplets on an electrode array, making them vital for healthcare. However, they are vulnerable to numerous security threats, including structural modifications during the design phase, material vulnerabilities in manufacturing, and code-level cyber-physical attacks. These risks encompass microstructural changes, chemical tampering, and manipulation of bioprotocols. This study experimentally demonstrates these attacks on a commercial DMFB and proposes using the optical coherence tomography (OCT) technique as a countermeasure to detect structural and material anomalies, along with hash-based techniques for code-level defense.

Keywords: Digital Microfluidic Biochips · Cyber-physical Security · Optical Coherence Tomography · Plasma· Hash· Droplet

1 Introduction

Digital Microfluidic Biochips (DMFBs) use electrowetting-on-dielectric (EWOD) technology for precise droplet control, enabling bioprotocols—automated sequences of chemical or biological tasks designed for precise and efficient biochemical analyses [1]. However, DMFBs face security threats across various stages, including stealthy structural modifications during design, such as micro-level alterations to electrode or dielectric thickness [2]; material vulnerabilities like chemical degradation during manufacturing [3]; and bioprotocol code alterations, which can lead to faulty diagnostics and denial of service (DoS) [4]. Using benchtop techniques, we demonstrate material-level plasma-induced surface wettability attacks and code-level electric arc attacks caused by droplets engulfing high-voltage lines. As countermeasures, we propose OCT-based techniques for detecting structural and material threats, along with hash function-based code-level security measures to safeguard DMFBs.

2 Background and Threat Model

The complex supply chain of DMFBs, combined with high market demand, creates opportunities for cyber-physical attacks to jeopardize patient safety [2]. Attackers may include disgruntled employees, industrial saboteurs, third-party insiders, or opportunistic actors, motivated by personal grievances or illicit monetary gains [3]. Fig. 1 presents a threat model outlining potential attack stages across the DMFB supply chain, from design to customer delivery [3]. In the design phase, attackers may stealthily modify structural aspects, like electrode thickness or dielectric layers, which evade detection in standard quality checks [4]. During manufacturing, attackers may introduce harmful chemicals into critical material components or alter machine parameters, compromising the reliability of DMFBs [3]. After quality control, tampering with components or modifying bioprotocol can cause system failures, inaccurate diagnostics, or denial of service (DoS).

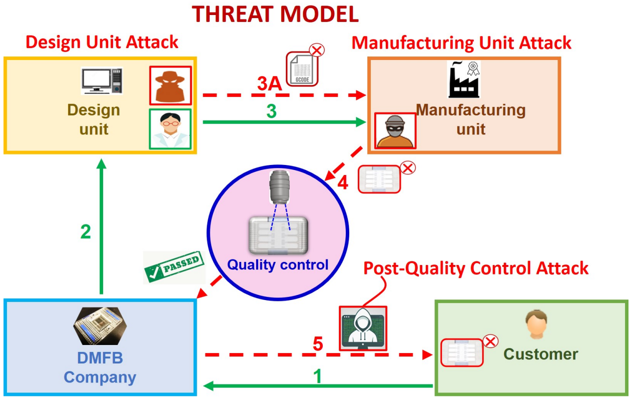

Fig. 1. Threat model for DMFBs.

3 Methodology

This work demonstrates two attack vectors: plasma attacks at the material level, altering wettability and disrupting droplet behavior, and code-level electric arc attacks, triggering deliberate short circuits.

3.1 Plasma Attacks

Employing benchtop techniques, we performed a plasma attack on a commercial DMFB by directing oxygen plasma from a plasma gun (Fig. 2a) onto a 4 mm^2 region of the DMFB's top plate for 5 seconds. This treatment effectively etched the superhydrophobic layer, compromising surface wettability and subsequently altering droplet shape and dynamics.

3.2 Electric Arc attacks

Open-source DMFB code allows attackers to modify the user interface (UI), keeping the device at a hardcoded high voltage even when a lower voltage is selected [5]. We executed this by setting one electrode to a lower voltage and another to a higher one, causing the droplet to move toward the high-voltage electrode, resulting in an electric arc.

4 Results

Fig. 2 illustrates material-level plasma attacks and code-level-induced electric arc attacks on DMFBs, along with proposed OCT-based countermeasures. Plasma attacks (Fig. 2b) alter surface wettability, impacting droplet shape and movement, while electric arc attacks (Fig. 2c and Fig. 2d) use high voltage to force and engulf droplets into adjacent lines, resulting in short circuits. Plasma attacks can be introduced both during manufacturing and after quality control, subtly altering surface properties and disrupting droplet manipulation. In contrast, electric arc attacks can be launched by malicious code modifications that display an intended voltage on the user interface, while a higher voltage is applied at the physical level, causing droplets to engulf high-voltage lines and induce short circuits.

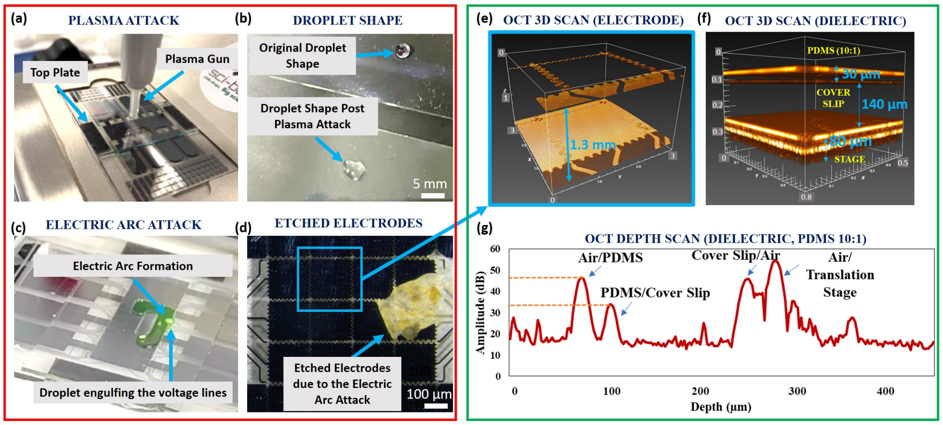

Fig. 2. Attacks and countermeasures for DMFBs: Plasma attacks (a, b) and electric arc attacks (c, d) on DMFBs (red border), alongside OCT-based countermeasures for microstructural (e, f) and material-level (g) detection (green border), highlighting its noninvasive, layer-by-layer detection capability with high resolution down to a few micrometers.

5 Countermeasures

To prevent code-level cyber-physical attacks on DMFBs, we propose verifying each execution by comparing the hash of a trusted reference executable with that of the current version upon each execution [5]. DMFBs face numerous threats, especially from structural and material levels [6]. To counter them, we propose OCT-based measures that use low-coherence light source to capture interference signals, creating high-resolution 3D images [7]. We conducted an OCT scan on the commercial DMFB, precisely identifying subsurface thicknesses (Fig. 2e: combined dielectric and electrode thickness, 1.3 mm) and (Fig. 2f: polydimethylsiloxane (PDMS) thickness, 30 µm). Moreover, using PDMS (10:1 curing ratio), we demonstrate that material irregularities can be detected through depth-specific signal variations, including peak locations and distances between them (Fig. 2g). We conducted an OCT test on PDMS samples with a 30:1 curing ratio, revealing signals that were significantly different from those of the 10:1 standard. A similar approach could be adopted to detecting material anomalies in DMFBs.

6 Conclusion

We demonstrated plasma and electric arc attacks on DMFBs and proposed OCT- and hash-based countermeasures to address structural, material, and code-level vulnerabilities, enhancing DMFB security.

References

1. Baban, N., Zhou, J., Elkhoury, K., Bhattacharjee, S., Sanjairaj, V., Gupta, N., Song, Y.A., Chakrabarty, K., Karri, R.: Biotrojans: viscoelastic microvalve-based attacks in flow-based microfluidic biochips and their countermeasures. Scientific Reports **14** (08 2024). https://doi.org/10.1038/s41598-024-70703-0
2. Baban, N.S., Zhou, J., Bhattacharya, S., Chatterjee, U., Bhattacharjee, S., Vijayavenkataraman, S., Song, Y.A., Mukhopadhyay, D., Chakrabarty, K., Karri, R.: Physically unclonable fingerprints for authentication. In: International Conference on Applied Cryptography and Network Security. pp. 235–239. Springer (2024)
3. Baban, N.S., Saha, S., Jancheska, S., Singh, I., Khapli, S., Khobdabayev, M., Kim, J., Bhattacharjee, S., Song, Y.A., Chakrabarty, K., Karri, R.: Material-level countermeasures for securing microfluidic biochips. Lab Chip **23**, 4213–4231 (2023). https://doi.org/10.1039/D3LC00335C
4. Baban, N.S., Saha, S., Orozaliev, A., Kim, J., Bhattacharjee, S., Song, Y.A., Karri, R., Chakrabarty, K.: Structural attacks and defenses for flow-based microfluidic biochips. IEEE Transactions on Biomedical Circuits and Systems **16**(6), 1261–1275 (2022). https://doi.org/10.1109/TBCAS.2022.3220758
5. Belikovetsky, S., Yampolskiy, M., Toh, J., Gatlin, J., Elovici, Y.: dr0wned-cyber-physical attack with additive manufacturing. In: USENIX Workshop on Offensive Technologies (WOOT) (2017)
6. Mohammed, S., Bhattacharjee, S., Song, Y.A., Chakrabarty, K., Karri, R.: Security of Biochip Cyberphysical Systems. Springer (2022)
7. Zam, A., Dsouza, R., Subhash, H., O'Connell, M., Enfield, J., Larin, K., Leahy, M.: Feasibility of correlation mapping optical coherence tomography (cmoct) for anti-spoof sub-surface fingerprinting. Journal of Biophotonics **6**(9), 663–667 (Sep 2013). https://doi.org/10.1002/jbio.201200231