Microfluidic Trojan Design in Flow-based Biochips

Mohammed Shayan
New York University
mos283@nyu.edu

Sukanta Bhattacharjee
IIT Guwahati
sukantab@iitg.ac

Yong-Ak Song
NYU Abu Dhabi
rafael.song@nyu.edu

Krishnendu Chakrabarty
Duke University
krish@duke.edu

Ramesk Karri
New York University
rkarri@nyu.edu

***Abstract*—Microfluidic technologies find application in various safety-critical fields such as medical diagnostics, drug research, and cell analysis. Recent work has focused on security threats to microfluidic-based cyberphysical systems and defenses. So far the threat analysis has been limited to the cases of tampering with control software/hardware, which is common to most cyberphysical control systems in general; in a sense, such an approach is not exclusive to microfluidics. In this paper, we present a stealthy attack paradigm that uses characteristics exclusive to the microfluidic devices - a *microfluidic trojan*. The proposed trojan payload is a valve whose height has been perturbed to vary its pressure response. This trojan can be triggered in multiple ways based on time or specific operations. These triggers can occur naturally in a bioassay or added into the controlling software. We showcase the trojan application in carrying out practical attacks - contamination, parameter-tampering and denial-of-service - on a real-life bioassay implementation. Further, we present guidelines to launch stealthy attacks and to counter them.**

***Index Terms*—microfluidic, trojans, fluid flow, valves, security**

I. Introduction

Microfluidic technology enables biochemical reactions on a miniaturized platform called lab-on-a-chip or a biochip. A biochip minimizes reagent and sample consumption, reaction time, and associated cost [1]. Further, biochips can be integrated with a controller, actuators, sensors, and network, making it a cyberphysical system (CPS). Due to these advantages, they find application in medical diagnostic, drug development, and genomics.

The continuous flow-based microfluidic biochip (CFMB) is a two-layered device. At the intersection of the two layers - flow and control layer, a 'valve' is formed (Fig. 1(a)) that can be controlled by an external pressure source [2]. When the valve is pressurized, the flexible membrane of the control layer deflects deep into the flow layer blocking the fluid flow (Fig. 1(b)). Such fluid control enables microfluidic operations such as dispensing, mixing, and splitting. These, in turn, can be used to build more complex biochemical protocols [3].

The current biochip market is estimated to be 5.7 billion U.S. dollars and is expected to grow to 12.3 billion U.S. dollars by 2022 [4]. This is corroborated by the increase in investments [5], and high-valued acquisitions [6] of microfluidic companies. Microfluidic products have been deployed in: 1) Personalized drug identification out of thousands of available options, which is not plausible using traditional lab methods [7]. 2) Diagnosis of common diseases in remote locations such as refugee camps where there is no access to traditional labs [8]. 3) Diagnosis of common diseases in newborn babies where the test-sample is very scarce [9]. In light of these developments, there is no doubt that microfluidics has revolutionized various biomedical fields.

This research is supported in part by the Army Research Office under grant number W911NF-17-1-0320, NSF Award numbers CNS-1526405, CNS-1833622 and CNS-1833624, NYU Center for Cyber Security (CCS), and CCS-Abu Dhabi.

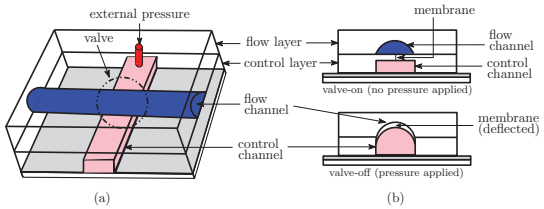

Fig. 1. Schematic of a two-layer microfluidic device: (a) top view and (b) cross-sectional view of valve states.

The current production of biochips is low-volume and customized. However, as the microfluidic market grows, high-volume production of programmable devices will be required to meet the market demand. We know from the Integrated Circuit (IC) market experience that this is enabled by a horizontal supply chain, wherein third-party computer-aided design (CAD) software, microfluidic design libraries, and manufacturing facilities could be used. This unfortunately opens the door for supply chain attacks such as overproduction, trojan insertion, and intellectual property (IP) theft [10]. Successful scaling of the microfluidic market requires that these security concerns be addressed. The fact that biochips are often targeted for security-critical application only further emphasizes the need to address these concerns.

Accordingly, security in microfluidics has been an important focus of the research community. Previous work has focused on network-based tampering of controlling software, and controller-based trojan attacks [11]–[13]. In other words, researchers focused on attacks that are common to all cyberphysical systems. In this work, we showcase a microfluidic trojan design, which is exclusive to microfluidics technology. This is the first such attempt and is focused on CFMBs. Our contributions include:

- Design of a microfluidic trojan - a new attack paradigm - using multi-height valves.
- Various attack strategies of payload insertion and triggering mechanisms.
- An analysis of the different types of pneumatic interfaces, one-to-one mapping and control-logic-based mapping, on triggering the trojans.
- Application of the trojan in launching attacks such as contamination, parametric, and denial-of-service (DoS).
- Guidelines that the attacker and the defender can use to sharpen their attacks and strengthen their defenses.

The paper is organized as follows: Section II describes the basics of CFMB fabrication, pneumatic interfaces, and related work. Section III describes the threat model and the microfluidic trojan design. In Section IV, we launch several

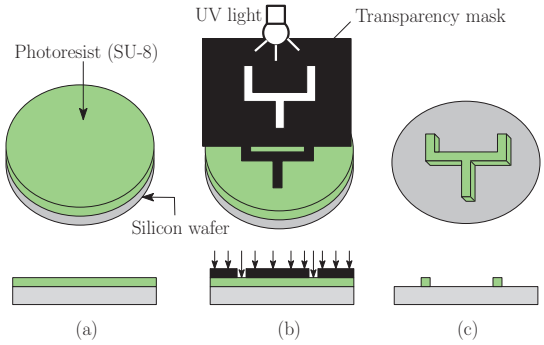

Fig. 2. CFMB fabrication steps (cross section view): (a) Spin coating negative photoresist on a silicon wafer. (b) Exposing to UV light through a transparency mask. (c) Washing of the unattached photoresist film from the wafer.

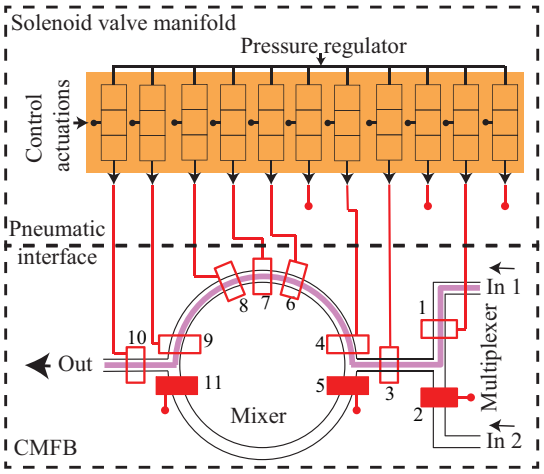

Fig. 3. A schematic of the one-to-one mapping between CFMB valves and external solenoid valves.

attacks using the microfluidic trojan. We demonstrate these attacks on a real-life bioassay implementation in Section IV-A. In Section V, plausible guidelines for and against trojan attacks are laid out. Finally, Section VI concludes the paper.

II. Background

In this section, we describe the fabrication process of the continuous-flow microfluidic biochips (CFMBs), pneumatic interface, and the recent works on microfluidic security.

A. Continuous-Flow-Microfluidic Biochips

A CFMB consists of two layers of permanently etched microchannels called the flow and the control layer. The microchannel patterns for individual layers are transferred to the silicon wafer using a photolithography process. In this process, a negative photo-resist (e.g., SU-8) is spin-coated to the desired thickness on the silicon wafer (Fig. 2(a)). Then, the wafer is exposed to the UV light through a transparency mask (Fig. 2(b)). The exposed part of the photo-resist to the UV become cross-linked. The unexposed photo-resist film remains soluble and is washed to transfer the desired pattern on the silicon wafer (Fig. 2(c)).

Soft lithography is used to transfer flow and control channel patterns from the silicon wafers to the PDMS. After the two PDMS layers are cast separately, they are aligned and bonded irreversibly. At the intersection of the two layers, a 'valve' is formed (see Fig. 1(a)). A pressurized valve closes the flow layer by deflecting the flexible membrane of the control layer deep into the flow layer (see Fig. 1(b)). The amount of pressure needed to open or close a valve is determined by the membrane thickness in the valve region [14].

B. Pneumatic Interface

The CFMB valves are controlled using a pneumatic pressure source connected through solenoid valves. The solenoid valves are electrically actuated to toggle between high pressure and low pressure. The implementation of a bioassay on a CFMB requires transforming each assay into a sequence of fluidic operations. These operations are then mapped to a sequence of electrical actuations. These actuations open (close) the solenoid valves, which in turn close (open) the microfluidic valves on the CFMB. This regulates the flow of fluid as required to realize fluidic operations. The pneumatic interface connects the CFMB valves to the external solenoid valves. The interface connection can be a direct one-to-one map or a control-logic-based-based mapping. In a one-to-one map, each CFMB valve is connected to an external solenoid valve. We explain this more in Example 1.

Example 1: Consider a sample preparation biochip shown in Fig. 3. The CFMB has a mixer and multiplexer that selects from two fluid inlets. It consists of eleven valves. Each valve is connected to a solenoid valve array, i.e., eleven solenoid valves. These solenoid valves are part of a manifold(s) and can be individually actuated through a microcontroller to pressurize or depressurize the CFMB valves.

To reduce the number of external pressure source controlled by solenoid valves, the control-logic-based interface is used. Such an interface has a core input pressure which is connected to a CFMB valve selected through an on-chip control logic, as shown in Fig. 4. The control logic creates control patterns that specify which CFMB valve gets connected to core input to update its pressure state. When a given valve is not selected, it latches (remembers) its state, which then needs to be refreshed periodically. The core input and control logic select lines are driven by individual solenoid valves.

Example 2: Consider the sample preparation biochip described in Example 1. The eleven CFMB valves can be controlled by on-chip control logic, as shown in Fig. 4. The pressure state of a valve is changed by applying appropriate control patterns to the solenoid valves at the control ports. To close the valve 10 in Fig. 4, the control pattern needs to be $abcd$ = "1111" and core input needs to be '1', where '1' denotes high pressure and '0' denotes low pressure. Similarly, the control pattern needs to be $abcd$ = "1001" and core input state be '0' to open the valve 1 in Fig. 4. The interface requires $2 \times \lceil \log_2 11 \rceil = 8$ control ports and one core input port, i.e., total nine solenoid valves as compared to eleven in Example 1.

C. Related Prior Work

Previous work has shown that biochips are susceptible to operational attacks such as denial-of-service and result manipulation [15]. IP security threats in the supply chain due to the distributed design flow include overbuilding, reverse engineering, and counterfeiting [10], [15]. One of the early countermeasures for tamper detection used randomized checkpoints [13]. Even with these measures, an attacker can

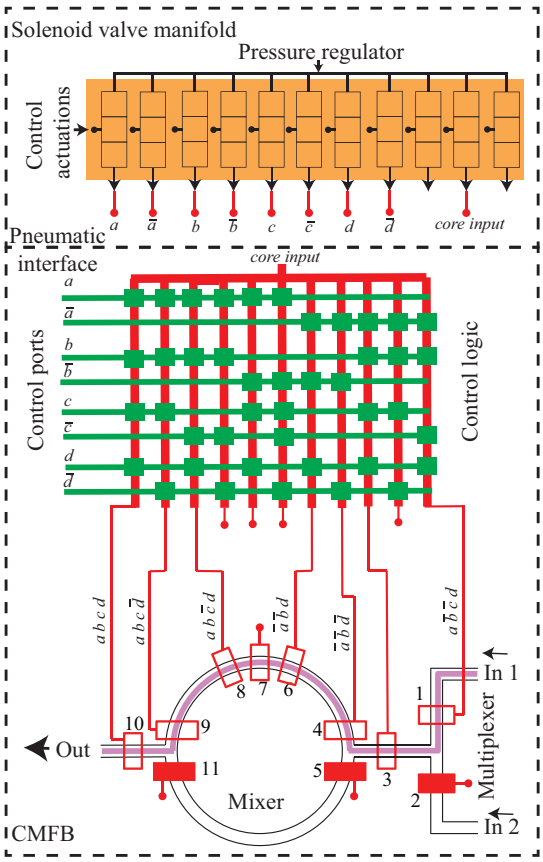

Fig. 4. A schematic of the control-logic-based interface.

escape detection with some probability. A micro-electrode-dot-array (MEDA) platform with fine-grained integrated sensor modules offers strong proof of security [16]. The security solutions for digital microfluidics cannot be readily applied to CFMBs due to the inherent differences in the technologies. A threat model for CFMBs is discussed in [11]. Hardware-tampering attacks that target microfluidic routing fabrics were presented in [17]. Software-programmable flow-based biochips have been shown to be susceptible to attacks such as fluid swapping, contaminating, and aging [12]. The defense against such attacks is limited by sensor coverage [12]. Machine-learning techniques can be used to maximize the accuracy of attack detection from incomplete sensor coverage [12]. However, all previous work considers tampering of hardware and/or software, which is similar in most computing systems. Hence, these methods have a key shortcoming in that they do not consider the specifics related to the microfluidic platforms. In previous work, we used dummy valves to obfuscate the bioassay implementation [18]. In this work, we use multi-height valve to deploy trojans in the flow-based biochips.

III. Microfluidic Trojan Design

In this section, we outline the threat model and describe the microfluidic trojan design.

A. Threat Model

Consider a biochip developer who outsources the fabrication of the biochip to an untrusted foundry. A rogue element in the foundry tampers with the biochip design to insert a trojan. The objective of the attacker could be to bring disrepute to the biochip developer [19]. The attacker has access to the design files through which he/she could identify the biochip components. However, the attacker has a constraint that the biochip needs to pass the post-manufacturing fault testing. We assume that the test of the biochip is performed by a trusted actor. The trojan trigger can occur naturally in a bioassay implementation or the control software can be modified remotely to trigger the trojan, as shown in Fig. 5.

B. Microfluidic Trojan

A trojan is defined as a malicious modification of the design. It can be divided into two components - trigger and payload. The basic idea of a microfluidic trojan is to use a multi-height (thinner) valve as a trojan payload, which begins to leak when the valve pressure drops due to activity on the other valves. We explain the design through the following two concepts:

1) Design of a multi-height valve: An attacker can maliciously lower the height of the control channel, as shown in Fig. 6. This results in a thicker membrane which requires a higher pressure to operate (close/open) compared to the normal membrane. When it is operated at a lower pressure, the valve does not close/open completely [2], [20]. For example, the work in [20] shows that a $34\,\mu\text{m}$ membrane valve requires a minimum pressure of 12 psi to operate, whereas a $28\,\mu\text{m}$ membrane requires a minimum pressure of 8 psi to operate. Such valve misbehavior can hamper biochip functioning. The proposed microfluidic trojan payload is designed based on this phenomenon.

2) Draining of valve pressure: The proposed microfluidic trojan is triggered in two ways - operation-based or time-based. The valve state can be closed (opened) when the pressure at the valve is high (low). The valve pressure is controlled through the pneumatic interface. The pressure source is connected to multiple valves through a solenoid valve manifold. If the valves associated with a manifold close/open at a high frequency, the pressure at the source drops. This is analogous to draining of voltage at a battery when a large current is drawn from it. This is referred to as an *operation-based trigger*.

In the case of the control logic interface, the pressure source is connected to the valve selected through the control logic. Recall that such valves latch their states and need a periodic refresh. However, as the membrane height increases, it requires more frequent refresh, else the valve pressure drops [21]. Suppose the normal valves need to be refreshed at rate T to retain their valve state. Due to its thicker membrane, the payload valve will need a frequent refresh rate τ ($\tau < T$). If the refresh rate (t) is in the range $T > t > \tau$, the payload valve can be triggered after τ time. This is referred to as a *time-based trigger*.

C. Attack Model

Payload — A rogue element in the foundry inserts the trojan by identifying one or more valves suitable for the attack objectives. The attacker increases the valve (trojan-payload) membrane height to the maximum extent that allows the device to pass the post-manufacturing test. When the biochip is deployed in operation, the trojan can be triggered by either time-based or operation-based draining of the pressure source.

Trigger — The trigger conditions can occur naturally in a bioassay that has been synthesized for high throughput

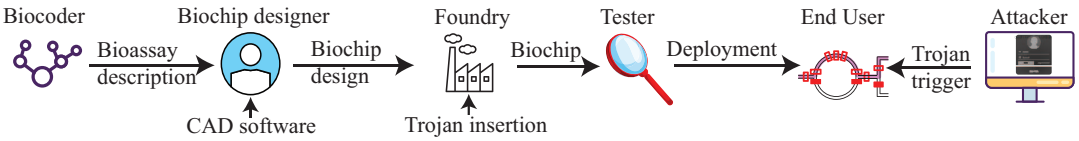

Fig. 5. Biochip design supply chain and threat model for the microfluidic-trojan-based attack.

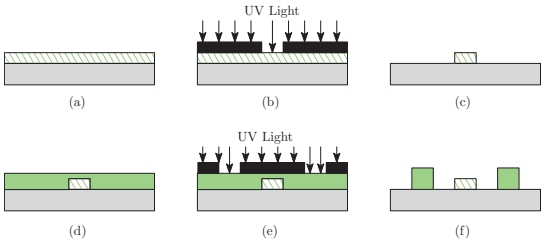

Fig. 6. Fabrication of multi-height structure: a cross-sectional view of (a) spin coating with photoresist (b) UV exposure (c) washing of uncured photoresist (d) spin coating with photoresist (e) UV exposure (f) washing.

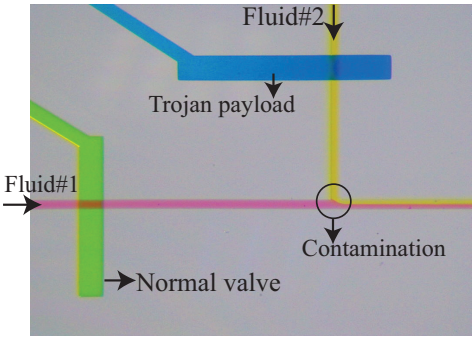

Fig. 7. Snapshot of the microfluidic chip fabricated at our lab with a multi-height valve as trojan payload. The payload leaks fluid#2 and contaminate fluid#1, when triggered.

(tighter refresh cycles) and lower overhead (multiple valves share a pressure source). The trojan gets activated for a very short time, causing an intermittent fault. Current testing and functional methods are not designed for detecting intermittent faults [2], [22]. Therefore, it is unlikely that the designer considers the change in timing and pressure behavior of the valve. Alternatively, the attacker can gain access to the controller through network access and induce one of the two trigger conditions. The attacker can insert time-based trigger by elongating/skipping the refresh steps of the payload valves. Further, the attacker can insert extra actuations to toggle dormant valves and drain the pressure source. This leads to an operation-based trigger.

Novelty — The microfluidic trojan attack is stealthy because: 1) There is no visible change in the payload valve, so the online sensor-based monitoring cannot detect it [12]. 2) If the trigger occurs naturally, then the attacker need not gain network access. This makes it easier for the attacker. 3) In the case of network-based software modification, the dormant valves are unlikely to be monitored as their state does not change the bioassay. In fact, previous work has shown that the monitoring of non-dormant valves increases the probability of detection of any assay tampering [12]. This way the attacker can escape detection by both post-manufacturing test and online-monitoring.

IV. Microfluidic Trojan-based Attacks

Using the steps described in the previous section, we fabricated a multi-height valve as trojan payload, as shown in Fig. 7. We maintained the pressure that allowed normal valves to work correctly. However, for the same pressure, the payload did not close, which lead to contamination of fluids, as shown in Fig. 7. Using such trojan various attacks can be realized such as contamination, parametric, and denial-of-service attacks.

1) Contamination attack: The fluid can be contaminated by unspecified mixing. Here, the valve that isolates two fluids is the trojan payload, which leaks when it is triggered. This leads to contamination of fluids that the valve (payload) was meant to isolate (Fig. 7).

2) Parametric attack: An assay implementation requires fine-tuning of various parameters such as mixing time, incubation time, and concentration ratio. Any deviation from these parameters results in variations in the assay results [10]. Using the microfluidic trojan, malicious alteration of mixing accuracy can be achieved. Here, the peristaltic valves are the trojan payload. When these are triggered, the peristaltic pumping pressure drops, leading to insufficient mixing.

3) Denial-of-service: The above two attacks lead to subtle variations in the end results. This may not raise an alarm and the user will trust the result. However, tampering with the implementation can also lead to no result or an untrustworthy result. This would lead to a denial-of-service attack [13]. For example, if an expected reagent is not dispensed in a chemiluminescence reaction, then the final color will not be as expected and the results will be discarded.

A. Case Study: Chromatin Immunoprecipitation (ChIP)

Chromatin immunoprecipitation (ChIP) is used for interrogating proteinDNA interactions in the cell [23]. By using this technique, specific proteins are purified along with the DNA they bind to. After that, the DNA is isolated, identified, and quantified to determine the binding site of the protein on the genome. AutoChIP is a microfluidic implementation of the ChIP that performs the following two-step: 1) Cell lysis and DNA fragmentation are performed on the sample cells through a series of mixing operations. 2) The resulting fluid is divided equally into four rings (Ring-A - Ring-D) to perform Immunoprecipitation. These rings are preloaded with anti-body functionalized beads, as shown in Fig. 8(a). We describe the microfluidic implementation of the ChIP [23]:

1) Preprocessed sample cells are loaded into the mixer Ring-1 through the inlet 1 of the multiplexer (Fig. 8(b)).
2) NP40 buffer is pushed from the inlet 2 into Ring-1 between valves P2 and P3 by keeping them closed. Next, cells are mixed with the NP40 buffer for 10 min.

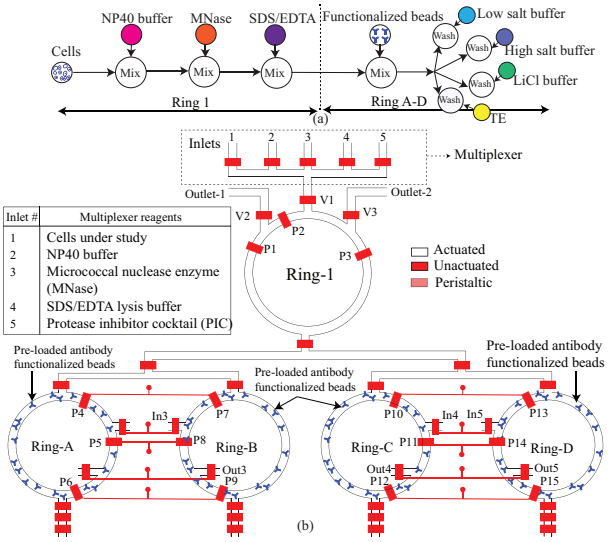

Fig. 8. (a) ChIP bioassay description. (b) AutoChIP implementation platform.

3) Next, similarly, micrococcal nuclease enzyme (MNase) is loaded into Ring 1 from inlet 3 and mixed for 10 min.
4) The process for loading is repeated for SDS/EDTA lysis buffer from the inlet 4 and mixed for 5 min.
5) The resultant cellular material is equally divided among Rings A-D by flowing protease inhibitor cocktail (PIC) from the inlet 5 by dead-end priming.
6) After that the contents of each of the four rings (A-D) is washed with four different buffers for 90 s (Fig. 8(a)).
7) The washed beads are then moved to micro-centrifuge tubes for qPCR analysis.

Interface AutoChIP has in total 54 valves; these can be controlled by 44 solenoid valves (one-to-one mapping scheme), because five valves of Ring A (C) and B (D) share the same input control, as shown in Fig. 8(b). The same can also be controlled using control logic-based mapping, which requires $2 \times \lceil \log_2 44 \rceil = 12$ control ports and one core-input port, i.e., total 13 ports instead of 44. We demonstrate the practicality of launching contamination, parametric, and DoS attacks on the AutoChIP by considering both one-to-one or control-logic-based pneumatic interface.

1) Contamination attack: During cell lysis, the mixing operations require the loading of measured quantities of reagents. MNase reagent that performs DNA digestion into fragments is loaded from inlet 3. SDS/EDTA lysis that is loaded in the next step stops the DNA digestion by inhibiting MNase. An attacker can insert a trojan payload at the multiplexer inlet 4. The payload when triggered leaks to contaminate MNase reagent, as shown in Fig. 9(a). During loading, the peristaltic valves corresponding to the Ring A-D are dormant (Fig. 9(a)). The attacker can insert extra actuations to toggle these dormant valves. This drains the source and momentary triggers the payload at inlet 4 of the multiplexer.

In control logic-based interface, the attacker has more opportunities to trigger a trojan. The multiplexer valves are opened only during the load operation. The multiplexer valve payload can be triggered (time-based) if the refresh cycle is not frequent enough. Additionally, if the control logic valves and multiplexer valves correspond to the same manifold and pressure source, then the attacker can insert malicious (dummy) actuations on the control ports that either select an invalid pattern or a dormant valve. This drains the source and momentary triggers the multiplexer valve payload.

2) Parametric attack: Active mixing is achieved by actuating three valves in a sequence for peristaltic pumping. The attacker can insert the microfluidic trojan payload at these peristaltic valves to tamper with the efficiency of mix operation — a parametric attack. The triggering of the trojan reduces the pressure on the mixing fluid, thereby reducing the rotation speed of the fluid in the rotary mixer. Insufficient mixing prevents washing of the unbounded proteins in Ring A-D, which leads to wrong results, as shown in Fig. 9(b). Mix operations in Ring A-D are executed in parallel. The increased activity on the shared manifold drains the pressure source. This leads to the operation-based triggering of the peristaltic valves in Ring A (Fig. 9(b)).

During the mix operation in ring A-D, the valves at the Ring 1 are dormant. Their state (close/open) does not influence the bioassay as the path through these valves is closed downstream, as shown in Fig. 9(b). An attacker could insert extra actuations to toggle these dormant valves. This drains the source and consequently trigger the peristaltic valve payload in Ring A. In the case of control logic-based interface, apart from these possibilities, malicious actuations on the control logic can trigger the peristaltic valve payload.

3) Denial-of-service attack: The cellular material from Ring 1 is flushed into Ring A - D by flowing PIC from the inlet 5 of the multiplexer. This divides the number of cells equally to Ring A-D. These rings are dead-end-filled, i.e., no outlet is opened. An attacker can insert a payload at the outlet to eject the cellular material during the flushing, as shown in Fig. 9(c). This leads to loss of soluble DNA and failure of subsequent analysis — a denial-of-service. The trigger can be time-based or spurious actuations on control ports, in the case of the control-logic-based interface. Similarly, DoS attack is also possible through a trojan payload in the control logic. A leaky control valve leads to undesirable patterns at the control logic. This leads to wrong valves being controlled, which in turn can hinder the microfluidic operation such as dispensing, mixing, and transporting.

V. Guidelines

In this section, we describe guidelines that the attacker and defender can use to sharpen attacks and strengthen defenses.

A. Attack Guidelines

The objective of the attacker is to maximize damage while minimizing the probability of detection. This is best achieved by subtly tampering with the valve height such that it passes the post-fabrication test [2]. A larger variation increases the chance of detection if, during the test phase, the pressure source is drained. For the time-based trigger, the attacker can choose the valves that are part of multiplexer, waste outlet or metering circuit [24]. These valves do not change their state for a longer duration, hence are less likely to be frequently refreshed. The control-logic-based pneumatic interface provides a choice of multiple control patterns to control a given valve [25]. The attacker can select a control pattern that maximizes the activity at the pressure source.

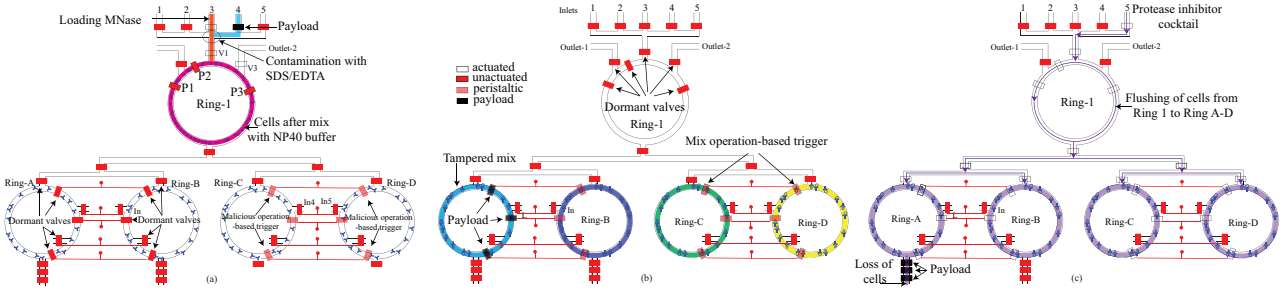

Fig. 9. (a) Contamination attack during loading of MNase: Inlet 4 valve is the payload triggered by malicious operations on the dormant valves of Ring A-D. (b) Parameter tamper attack during wash operation: peristaltic valve in Ring A is the payload triggered by natural mix operations in Ring C and D. (c) Denial-of-service attack during flushing of cellular material from Ring 1 to Ring A-D: the output valves are payload time-triggered due to lack of refresh.

B. Defense Guidelines & Future Work

So far we have described the threat to biochip integrity from bad actors in the supply chain. We hope our work will motivate the exploration of secure practices in the microfluidic industry. Towards this end, we suggest that the first line of defense against microfluidic trojan be a trojan-aware test plan. The current state-of-the-art testing of CFMBs does not include testing of the pressure profile of the valve [2]. The test can include testing of valves for minimum and maximum pressure analogous to the analog IC testing. For the control-logic-based pneumatic interface, the valve states are latched for a certain duration [21]. This latch timing behavior needs to be verified in the test plan similar to an IC delay test.

Recall that the draining of the pressure source is used as a trigger. The trigger is feasible when the payload valve shares the solenoid manifold with either high activity operation valves or dormant valves, as shown in the case study (Section IV). On the one hand, the payload in Ring A is triggered in Fig. 9(b) because the peristaltic valves that are active at the same time shared a manifold. On the other hand, the payload in multiplexer inlet 4 is triggered in Fig. 9(a) because it shared the manifold with inactive or dormant valves of Ring A-D. This allowed the attacker to insert malicious (dummy) actuations on these valves. The biochip defender can avoid such trigger by careful clubbing valves with different manifolds based on their activity. We plan to develop this strategy as future work.

VI. Conclusion

We have proposed a design of microfluidic trojan that uses valve pressure behavior to launch a stealthy attack. We showcase how subtle changes in the membrane thickness can be exploited to insert a trojan in the CFMBs. The trojan can be triggered in various conditions based on time or high activity operations, which can occur naturally or could be inserted by control software modification. We showcase that the trojan can be used to carry out attacks such as contamination, parameter-tampering, and denial-of-service attacks. We also lay down guidelines for the future work towards secure biochips.

References

[1] G. M. Whitesides, "The origins and the future of microfluidics," *Nature*, vol. 442, no. 7101, pp. 368–373, 2006.

[2] K. Hu *et al.*, "Testing of flow-based microfluidic biochips: Fault modeling, test generation, and experimental demonstration," *IEEE Trans. on CAD*, vol. 33, no. 10, pp. 1463–1475, 2014.

[3] R. B. Fair, "Digital microfluidics: is a true lab-on-a-chip possible?" *Microfluid Nanofluid*, vol. 3, no. 3, pp. 245–281, 2007.

[4] (2019) Zion market research. [Online]. Available: https://www.globenewswire.com/news-release/2019/04/17/1805498/0/en/Global-Microfluidics-Market-Will-Surpass-USD-12-380-Million-By-2025-Zion-Market-Research.html

[5] (2019) 10x Genomics. [Online]. Available: https://www.10xgenomics.com/news/10x-genomics-lands-new-financing

[6] (2018) Illumina-press release. [Online]. Available: https://www.illumina.com/company/news-center/press-releases/press-release-details.html?newsid=1840193

[7] (2016) A high throughput screening system to identify actionable treatments for cancer patients. [Online]. Available: https://biosero.com/wp-content/uploads/2016/10/a_high_throughput_screening_system_to_identify_actionable_treatments_etc_npm.pdf

[8] R. Fobel, C. Fobel, and A. R. Wheeler, "DropBot: An open-source digital microfluidic control system with precise control of electrostatic driving force and instantaneous drop velocity measurement," *Applied Physics Letters*, vol. 102, no. 19, p. 193513, 2013.

[9] (2016) FDA advisors back approval of baebies seeker analyzer for newborns. [Online]. Available: http://baebies.com/fda-advisors-back-approval-baebies-seeker-analyzer-newborns

[10] M. Shayan *et al.*, "Bio-protocol watermarking on digital microfluidic biochips," *IEEE Trans. Information Forensics Security*, vol. 14, no. 11, pp. 2901–2915, 2019.

[11] J. Tang *et al.*, "Security implications of cyberphysical flow-based microfluidic biochips," in *Proc. ATS*, 2017, pp. 115–120.

[12] M. Shayan *et al.*, "Toward secure microfluidic fully programmable valve array biochips," *IEEE Trans. on VLSI*, 2019 (to appear).

[13] J. Tang *et al.*, "Secure randomized checkpointing for digital microfluidic biochips," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 37, no. 6, pp. 1119–1132, 2018.

[14] S. Chung *et al.*, "Multi-height micro structures in poly (dimethyl siloxane) lab-on-a-chip," *Microsyst. Technol.*, vol. 10, no. 2, pp. 81–88, 2004.

[15] S. S. Ali *et al.*, "Microfluidic encryption of on-chip biochemical assays," in *Proc. BioCAS*, 2016, pp. 152–155.

[16] S. Mohammed *et al.*, "Security assessment of micro-electrode-dot-array biochips," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, 2018 (to appear).

[17] J. Tang *et al.*, "Analysis and design of tamper-mitigating microfluidic routing fabrics," *IEEE Trans. on CAD*, 2019 (to appear).

[18] S. Mohammed *et al.*, "Desieve the attacker: Thwarting ip theft in sieve-valve-based biochips," in *Proc. DATE*, 2019, pp. 210 – 215.

[19] U.S. Secret Service *et al.*, "2011 cybersecurity watch survey: How bad is the insider threat?" 2011. [Online]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a589979.pdf

[20] A. Lau *et al.*, "Dynamics of microvalve operations in integrated microfluidics," *Micromachines*, vol. 5, no. 1, p. 5065, Feb 2014. [Online]. Available: http://dx.doi.org/10.3390/mi5010050

[21] W. H. Grover *et al.*, "Development and multiplexed control of latching pneumatic valves using microfluidic logical structures," *Lab Chip*, vol. 6, pp. 623–631, 2006.

[22] C. Liu *et al.*, "Testing microfluidic fully programmable valve arrays (FPVAs)," in *Proc. DATE*, 2017, pp. 91–96.

[23] A. R. Wu *et al.*, "Automated microfluidic chromatin immunoprecipitation from 2,000 cells," *Lab Chip*, vol. 9, pp. 1365–1370, 2009.

[24] I. E. Araci and S. R. Quake, "Microfluidic very large scale integration (mVLSI) with integrated micromechanical valves," *Lab Chip*, vol. 12, pp. 2803–2806, 2012.

[25] Y. Zhu *et al.*, "Multi-channel and fault-tolerant control multiplexing for flow-based microfluidic biochips," in *Proc. ICCAD*, 2018, pp. 1–8.