2017 IEEE 26th Asian Test Symposium

Security Implications of Cyberphysical Flow-based Microfluidic Biochips

Jack Tang[1], Mohamed Ibrahim[2], Krishnendu Chakrabarty[3], Ramesh Karri[4]
Department of Electrical & Computer Engineering, New York University[1, 4]
Department of Electrical & Computer Engineering, Duke University[2, 3]
jtang@nyu.edu[1], mohamed.s.ibrahim@duke.edu[2], krish@duke.edu[3], rkarri@nyu.edu[4]

***Abstract*—Flow-based microfluidic biochips are revolutionizing biochemical research by automating complex protocols and reducing sample and reagent consumption. Integration of these biochips with sensors, actuators, and intelligent control have compounded these benefits while increasing reliability. And, many flow-based platforms have successfully transitioned to the marketplace, demonstrating their utility through several recent scientific publications. However, these microfluidic technologies and platforms have unintended security and trust implications that threaten their continued success. We survey cyberphysical flow-based microfluidic platforms and perform a security assessment. We then describe an attack on digital polymerase chain reactions and how such attacks undermine research integrity.**

I. Introduction

Flow-based microfluidic biochips are devices that manipulate small volumes of fluid using micro-channels, valves, and pumps [1]. Processing of microliter and sub-microliter fluid volumes bring a number of advantages, such as reduced sample and reagent consumption, increased reaction rates and throughput, portability, and the ability to automate complex protocols [2]. The integration of these biochips with an array of computer controlled sensors and actuators form a cyberphysical system, and has proven benefits in terms of fault-tolerance and reliability. A number of flow-based technologies have successfully made the transition from academic proof-of-concepts to commercially available products. Unfortunately, the continued success of these platforms may be undermined by security and trust issues. Recently described attacks on digital microfluidic biochips (DMFBs) show that subtle attacks with disastrous consequences can be achieved. Flow-based microfluidics operate on different principles than DMFBs, but could potentially suffer from the same—or even unique—security issues. To date, the security and trustworthiness of flow-based microfluidics have not been explored. We address the need for a comprehensive evaluation of these issues with the following contributions:

1) *High-level Security Assessment*. We discuss the flow-based microfluidic biochip design flow, the various actors, and their motivations for attack.
2) *Threat Modeling*. We enumerate attack surfaces present in a typical flow-based biochip platform and describe the expected capabilities of attackers based on where in the design flow they reside.
3) *dPCR Attack Study*. We describe how commercial microfluidic systems used for digital polymerase chain reaction (dPCR) can be compromised and its negative impact on research integrity.

The rest of the paper proceeds as follows. Section II describes the structure and operation of flow-based microfluidics. Section III gives an overview of the design flow and how this structure translates into security and trust vulnerabilities, as well as threat models and attack surfaces. Section IV describes an attack on dPCR with experimental evidence, and discusses the practical implications for research integrity and medical diagnostics. We conclude in Section VI.

II. Background

Security issues in microfluidic systems are only beginning to be explored. The literature only describes attacks and defenses specifically for DMFBs. Distributed supply chains potentially leave open several security and trust issues [3]. Subtle result-manipulation attacks can be achieved by tampering with the actuation sequences which control DMFBs [4]. Randomized checkpoints can leverage error recovery hardware for tampering detection [5], [6]. Fluidic encryption enables protocol designers to protect their intellectual property (IP) [7]. Attacks can be localized by analyzing error logs against those produced by a golden model [8]. A digital rights management scheme based on physical unclonable functions can help protect against IP piracy [9].

Alternate microfluidic design paradigms may have some overlapping security issues. For instance, cyberphysical integration can be performed similarly for both DMFBs and flow-based biochips, and therefore will present similar attack surfaces. However, the physical characteristics and controllability of these devices may differ drastically, leading to unique attacks and defenses.

A. Flow-based Microfluidics

Early flow-based microfluidic devices were fabricated using silicon and glass substrates, borrowing techniques from the semiconductor industry [10]. Later, materials such as polydimethylsiloxane (PDMS) became popular due to the ability

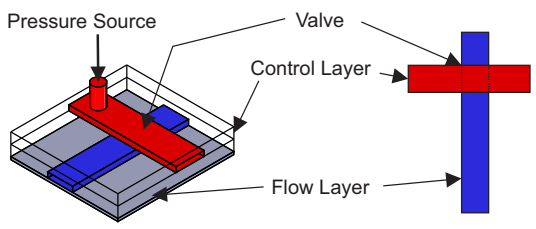

Fig. 1. Flow-based biochip schematic diagram. Fluids in the flow layer are controlled by deflections of valves located at crossings with the control layer.

2377-5386/17 $31.00 © 2017 IEEE
DOI 10.1109/ATS.2017.32

to rapidly fabricate prototypes and integrate microvalves at high density [1]. Fig. 1 illustrates the typical construction of a flow-based biochip. Two elastomer layers are fabricated with channels and bonded together. One layer is comprised of flow channels for the manipulation of samples and reagents. Flow is induced by pumps connected at the end of each fluid reservoir. The next layer comprises a network of control channels, which are connected to external pressure sources. Activation of the pressure sources cause a deflection where the control and flow channels intersect, forming a valve. Consequently, the movement of the fluid in the flow channel is interrupted. The fluid valves and channels can be arranged into more complex networks to allow high-throughput processing and parametric studies [11], [12]. For instance, M input samples can be tested against N different reagents, for a total of $M \times N$ unique reactions. The design of these flow control networks can be automated to allow complex protocols and the targeting of design optimizations such as pin-count minimization [13].

B. Self-Contained Microfluidic Systems

Microfluidic systems can take on a wide array of form factors. Technologies that are early in development often require external laboratory equipment to function properly, limiting their application as true lab-on-chip platforms. Devices that do not have this limitation are *self-contained*, and can be classified according to their actuation mechanism [14].

1) *Passive* self-contained microfluidic systems use mechanisms such as capillary flow and colorimetric detection to provide functionality that does not depend on any external support. Paper microfluidics and home pregnancy tests are examples of passive microfluidics.
2) *Hand-powered* systems require human action to provide the driving force, whether through pressing a syringe, pipetting, or squeezing blister packs.
3) *Active* systems use electronics, sensors, actuators, pumps and control valves to automate the processing of fluids.

Practical systems may have hybrid characteristics; for instance, many commercial systems still rely on humans to pipette the samples and reagents into a cartridge, which is then loaded into an automated processing unit. This paper focuses on security and trust issues in active systems. The integration of computation, sensors and actuators mean that active systems are also cyberphysical systems and thus pose potential security threats and opportunities.

III. High-Level Security Assessment

The design of a flow-based microfluidic biochip platform generally proceeds along the steps illustrated in Fig. 2. The design is centered around a *biochip designer*, who is responsible for integrating various intellectual property blocks to create a functional microfluidic platform. The main required IP block is the biochemical protocol, which is designed by the *biocoder*. The biocoder will specify the samples and reagents to be used in the protocol, along with instructions on how to mix and dilute fluids. These instructions can be provided in a high-level language such as *Biocoder* [15], which has found utility in digital microfluidics that are reconfigurable by nature. The biocoder is analogous to an IP vendor in IC design flows. The hardware vendor provides information on manufacturing capabilities, such as design rules for etching channels, valves, and pumps and fluids that can safely be manipulated on the platform. The hardware vendor fulfills the same role as the foundry in an IC design flow, and may distribute a process design kit to aid the biochip designer. These three parties may or may not be vertically integrated. It is expected that as microfluidic technologies advance, that horizontal integration will be adopted [3]. This presents the possibility of security threats. After the design is synthesized, it is sent to the *foundry* for fabrication, a *tester* for validation, and then finally the *end user*. Once the device has exceeded its useful lifetime, must be collected for *recycling and disposal*.

A. Attack Outcomes

As a consequence of this design flow and the typical construction of a microfluidic platform described in Section II, many types of attacks are possible. We can broadly classify attacks according to their outcome as follows:

1) *Design Theft* is an attack that compromises the IP used to fabricate a microfluidic device. Once stolen, the designs can be used to flood the market with counterfeit devices. The biochemical assay protocol can also be considered to be part of the IP. The fact that microfluidic biochips are often transparent means that the protocol is easily observed and stolen.
2) *Reading Forgery* is an alteration of a sensor reading. Sensors are used to monitor for the progression of an assay, or to determine some property of a final fluid product. This data is often leveraged for medical studies using techniques like statistical analysis and machine learning. Alteration of sensor data has serious implications for patient care, research integrity, and environmental monitoring.
3) *Information Leakage* is the unauthorized dissemination of private or sensitive data. Many microfluidic systems are intended to be deployed in medical diagnostic settings, so sensitive patient data has to be correctly handled. Malware and hardware Trojans [16] could potentially intercept this data.

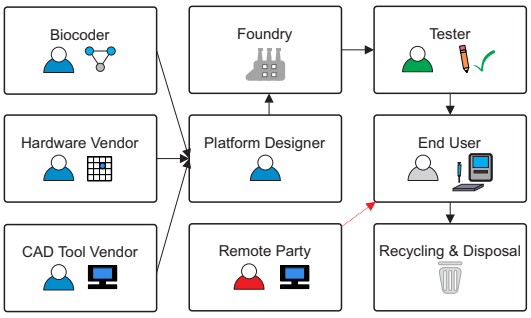

Fig. 2. Design information is synthesized by the platform designer, and forwarded to the foundry and tester before the final product is released to the end user. Used biochips must be recycled or disposed of properly. Remote parties may tamper with platforms once deployed using network interfaces on the platform.

4) *Denial-of-Service* (DoS) violates the availability of a system. This attack has become a common occurrence for internet users. In the context of a cyberphysical system, DoS has the potential to cause costly damage to hardware, samples, and reagents [4].
5) *Modification of Functionality* forces a device to perform in an unspecified manner. This can include subtle modifications such as downgrading of performance and more severe attacks that force execution of an unspecified assay.

B. Motivations

Human motivations for compromising cyberphysical systems are varied and difficult to predict; however, based on the large body of evidence in related fields, we can enumerate a few common motivations that are expected to drive the previously discussed attacks.

1) *Financial gain*. This motivates all the IP attacks. Evidence for counterfeiting, overbuilding, and reverse engineering abound in IC fabrication. Ransomware, identity theft, and sale of user data may drive other attacks.
2) *Revenge*. Disgruntled employees have been behind some of the more high-profile security breaches in recent years [17]. These attackers are embedded within an organization, and once wronged, leverage their access and knowledge to devastating effect.
3) *Politics*. The appearance of the Stuxnet worm in 2010 caused a reevaluation of the true magnitude of state-sponsored, politically-motivated cyber threats [18]. As such, cyberphysical system designers would do well to consider strong adversaries motivated to steal trade secrets or cause physical, psychological, or financial harm.
4) *Personal gain*. Researchers under pressure to publish may be tempted to fabricate data. Given the increasing effectiveness of methods used to detect spurious data, rogue researchers may be tempted to seek out more sophisticated fraud techniques.

C. Threat Models

Following the conventions of [19], we make a distinction between technical and operational abilities of an attacker. Technical abilities describe the knowledge an attacker has about how the microfluidic platform works and their capability to extract this information based on experimentation. Operational capabilities describe the method by which an attacker can carry out the attack. For instance, I/O ports on a microfluidic platform can be leveraged to inject malicious code, while an IP attack assumes that the attacker has access to a foundry. Note that our notions of security and trust are more general than those described in [19] since we consider IP-based attacks. We describe potential threat models for researchers to consider, organized by attacker location.

1) *Manufacturing-level* threat models are a result of the untrusted supply chain. As shown in Fig. 2, biochip platform designers must work with and integrate components from various vendors. These vendors may be located overseas, and multiple vendors may be used simultaneously. These parties would likely be interested in carrying out IP-related attacks, and should be assumed to have considerable technical and operational capabilities since they are provided with critical design information.
2) *Field-level* threats occur once the microfluidic platform is deployed and operational. Adversaries may include malicious end users who wish to modify the functionality of a device, and remote parties who are interested in the compromise of data or physical resources. These adversaries may have strong technical capabilities, especially remote parties as they may be located anywhere in the world and could be sponsored by nation-states. Their operational capabilities are more limited, as their ability to attack are dictated by the hardware and software attack surfaces available to them.

TABLE I. EXAMPLE ATTACK SURFACES

Attack Surface	Examples
Indirect physical access	USB, FireWire, Ethernet, Serial port, Flash reader
Direct physical access	Optical inspection, valve tampering, electronics tampering
Wireless access	Wifi, ZigBee, Bluetooth, GPS
Design documentation	Mechanical drawings, Gerber, GDSII, bioassay protocol
Standard inferfaces	Touchscreen, PC controller, biochip cartridge
Side-channel	Electromagnetic, power

D. Attack Surfaces

An attack surface is a potential entry point for carrying out an attack. We have identified the following attack surfaces. Examples of these attack surfaces are summarized in Table I.

1) *Indirect physical access*. These include ports for the purposes of downloading firmware, uploading data, diagnostics and maintenance. Many microfluidic platforms are designed around standard, off-the-shelf embedded computers and have a variety of physical ports exposed, such as USB and Ethernet jacks.
2) *Direct physical access*. This includes physical tampering attacks. The goal of many microfluidic device designers is to create a truly portable, self-contained lab-on-a-chip. While this has many practical benefits, it makes the platform physically vulnerable. For instance, a device deployed in remote locations for environmental monitoring would be easily tampered with; sensor signals could be sniffed or spoofed.
3) *Wireless access*. Wireless interfaces are increasingly being designed into platforms for convenience, especially for applications with smartphone integration. This presents an opportunity for attackers within close proximity, but not necessarily in possession, of a microfluidic platform.
4) *Design documentation*. The information used to fabricate a microfluidics platform may consist of schematics for circuitry, protocols for a biochemical assay, or layouts for a biochip. When presented in its raw form, design documentation is easily abused for overbuilding attacks.

5) *Standard interfaces*. A device may readily give up its secrets if merely asked to perform its intended duties. For example, an attacker may attempt to reverse engineer a protocol by carefully designing a set of fluids that can indicate the order of mixing.
6) *Side-channels*. Side-channel analysis is effective for breaking unsecured hardware implementations of cryptography algorithms [20]. Cyberphysical systems may present unique side channels, since physical phenomenon other than electricity and magnetism are utilized.

IV. Undermining Digital Polymerase Chain Reaction

Digital polymerase chain reaction (dPCR) is a relatively new method for quantifying and amplifying nucleic acids in a DNA sample [21], [22]. This method differs from traditional PCR techniques in that the sample must be split into multiple small volume reaction chambers. dPCR offers numerous strengths such as tolerance against inhibitors, lack of standard curves, and the ability to provide absolute, rather than relative, quantification [23]. In this section, we describe the concepts behind dPCR and how a commercial microfluidic platform designed for dPCR can be compromised such that the distribution of target DNA among the biochip chambers is biased. Since the dPCR reactions and valve actuations occur inside of a benchtop device, the end user would be oblivious to the attack unless the biochip were screened and analyzed for statistical anomalies—defeating the purpose of benchtop automation entirely. We then discuss the implications for copy number variation studies and research integrity in general.

A. dPCR Background

The operating principle of dPCR is based on randomly partitioning the DNA sample into multiple small reaction chambers (Fig. 3). These reaction chambers can be physically realized in an array (chip-based dPCR), or can be generated by encapsulating the samples in droplets generated in an oil emulsion (droplet dPCR). The PCR reaction is carried out on all of the partitions to amplify the target DNA sequence, and is then read out by a fluorescence detector. The proportion of positive to negative reactions can be used to calculate the number of target DNA sequences in the sample. The idea is that the random partitioning of samples will follow a Poisson distribution, and the estimated number of target DNA molecules ($\hat{M}$) can be calculated as

$$\hat{M} = -\ln(1 - \hat{H}/C) \quad (1)$$

where $\hat{H}$ is the observed number of positive chambers and C is the total number of chambers [24]. The measurement of the positive chambers is subject to uncertainty from sources such as inconsistent chamber volumes and non-random distribution of molecules, which has so far limited the deployment of dPCR for diagnostic applications [25].

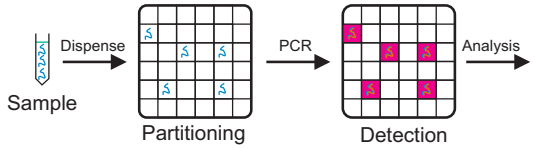

Fig. 3. Digital PCR works based on the random partitioning of a sample into a large number of reaction chambers. The concentration of the target DNA is estimated based on the observed positive reactions.

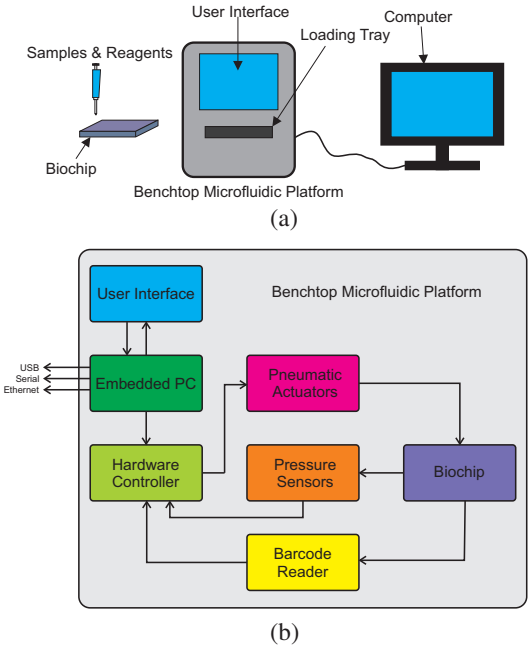

Fig. 4. (a) Commercial microfluidic platforms are offered as bench-top instruments with reloadable trays. (b) Typical construction consists of an embedded PC connected to an array of pneumatic actuators, pressure sensors, and possibly a barcode reader for automating setup and data collection. Connectivity is provided for advanced data collection capabilities, firmware updates, or reprogramming.

Microfluidic technologies have lent themselves to dPCR methods, enabling applications such as studies on copy number variation and drug metabolism [24]. These devices are currently marketed for research use only, with diagnostic applications expected to occur only after the technology matures further [23], [25].

B. Attacks on Commercial Microfluidic Platforms

Fig. 4 illustrates the typical construction of a commercial chip-based dPCR microfluidic platform. A disposable chip contains the reaction chambers with inlets for samples and reagents. The chip is loaded into the platform which contains an array of sensors, actuators, and an embedded computer. The computer controls the on-chip valves to create the multiple small reaction chambers, and then cycles the temperature to carry out PCR reactions. Integrated fluorescence detectors send the result of the experiment to the embedded computer, which then either outputs the data to an integrated display or saves it to file. The microfluidic platform workflow automates many processes that were formerly conducted manually. As such, user error drops precipitously. *However, implicit in this operational protocol is trust that the devices will conduct the experiment with integrity, as the end user is not involved in any steps between the sample preparation and the final readout.*

If an attacker is able to tamper with the actuation of the

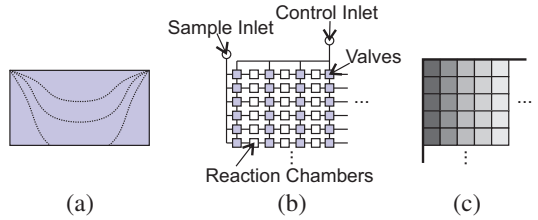

Fig. 5. (a) Cross-section of a valve showing some possible deflections. Valve opening response is linear with pressure. (b) A DNA sample must be randomly partitioned through a grid arrangement of reaction chambers separated by valves. (c) Partial closure of the flow valves would increase the difficulty for fluids to flow to later stages. We represent this schematically as a greyscale gradient across the biochip. Chambers closer to the input are more likely to contain target DNA, indicated by a darker shading.

microfluidic biochip, the distribution of DNA samples may be biased or the PCR reaction may be inhibited, leading to incorrect estimates of the true target DNA concentration. We studied a commercially available microfluidic platform and found that its structure closely matched that described in Fig. 4(b). The USB, serial, and ethernet ports present an open attack surface. If these ports are unsecured, an attacker could load malicious software. We found that this particular platform used an off-the-shelf embedded single-board computer, with the custom software loaded onto a removable CompactFlash (CF) card. A platform that is physically vulnerable could be compromised simply by replacing the CF card with a malicious one. Alternately a remote party could leverage the network connectivity to assume control of the computer.

Once the controller is compromised, an attacker would be able to induce partial failure in the pneumatic actuators. The control signals could be varied to either shorten the priming time, or output a control signal with an intermediate value. The opening of elastomer valves responds linearly to pressure variations for the majority of their operating range [1] (Fig. 5(a)). Therefore, the flow rate of sample into all the reaction chambers would be disrupted and the assumption of a Poisson process with fixed parameters would be violated.

C. Experimental Results

We demonstrate the results of an attack through a large-scale simulation study. A dPCR experiment can be simulated by randomly assigning M molecules into $C \times K$ reaction chambers, distributed over K number of panels. That is, for each molecule, we select one of the reaction chambers with uniform probability and assign the molecule. We then form the estimate of the true molecule concentration based on the observed number of positive reaction chambers $\hat{H}$; in this simulation, we assume the detection works perfectly. If we use the parameters provided in [24] for theory verification, we have $M = 400$, $C = 765$, and $K = 70000$. Fig. 6(a) shows a histogram of the observed $\hat{H}$ over all the K panels. To model a dPCR under a flow restriction attack, we assume that the chambers are arranged as 45 rows by 17 columns in the same structure shown in Fig. 5(b). We also assume that when under attack, the flow of the fluid is restricted through the columns, and some reaction sites will be more likely to contain target molecules. We model this by biasing the reaction chambers such that chambers closer to the inlet are more likely to contain sample than those farther away (Fig. 5(c)). We used a linear biased pmf $p(x) = 1/9 - (6.536 \times 10^{-3})x$ where $x \in \{0, ..., 16\}$ indexes the columns. Fig. 6(b) shows a histogram of the results. We see that an attacker can change the mean detected number of molecules by 5.96%, with just a slight linear bias in the experiment. Thus, an attack can nudge the results to yield a false estimate.

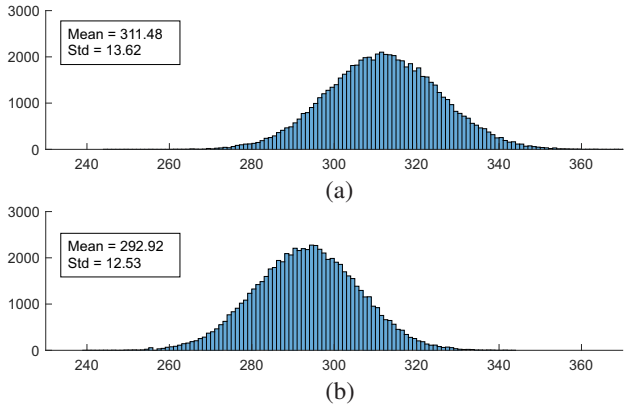

Fig. 6. (a) Histogram of observed positive chambers $\hat{H}$ from simulated standard dPCR experiment. (b) Histogram of $\hat{H}$ when valve actuation is attacked. Thus, a linear bias on the probability that molecules can flow along the biochip causes a shift in the estimate of molecules $\hat{M}$.

D. Implications for Copy Number Variations

Copy number variations (CNVs) are differences in the number of structural repeats in sections of the genome [26], [27], [28]. The sensitive and accurate detection capabilities of technologies such as dPCR have enabled the study of CNVs, promising insight into the role these small variations play in genomic diseases such as autism and Crohn's disease. An attacker who compromises the microfluidic platform used to carry out dPCR would be able to influence the number of positive reactions, and thus influence the copy number ratios calculated in disease studies. Without the correct copy numbers, positive associations between these genome variations and diseases cannot be made. Worse yet, incorrect associations may be generated. Spurious associations will preclude the development of any potential treatments.

V. Discussion

An attacker may be motivated to tamper with research equipment rather than completely fabricating data in an attempt to provide more convincing evidence that the experiments were actually carried out. Attacks on research instrumentation threatens to nullify recent efforts made to increase the quality and reproducibility of research. Specifically within dPCR, it has been noted that many researchers are not even aware of the basic methods and pitfalls of the technique—the Minimum Information for Publication of Quantitative Digital PCR Experiments (digital MIQE) guidelines were published in 2013 specifically to address these issues [29]. However, a researcher could fully comply with the standard and still release unreproducible results. Consequently, time and funding must be wasted in identifying these spurious results.

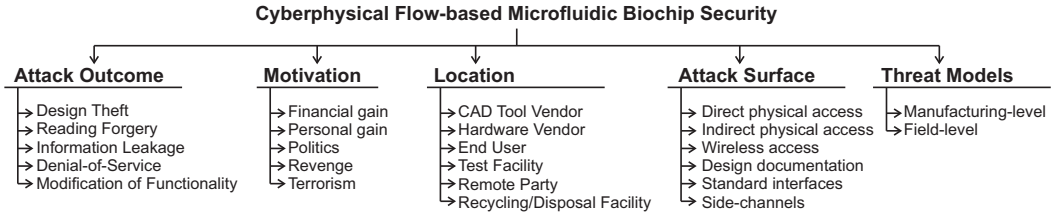

Fig. 7. Taxonomy of cyberphysical flow-based microfluidic biochip attacks and threats.

Occasionally, scientists or lab technicians are motivated to fabricate data for financial gain or bolstering their publication record. Besides blemishing the scientific literature, these violations of research integrity can have a real impact on everyday citizens. In 2011, the Food and Drug Administration found that a drug research company had essentially fabricated data over a span of years [30]. This data was used to win approval for drugs, nearly 100 of which had been placed on the market. And despite these revelations, many of these drugs in question remain on the market in the interest of the drug makers involved. If the instrumentation used to carry out these tests had featured secure and trustworthy microfluidic technologies, perhaps the situation could have been avoided entirely.

Currently, dPCR is only used within research settings due to the cost and resource requirements of the equipment involved. It is expected that dPCR microfluidics technology will mature such that it will be an attractive platform for diagnostic applications. In this case, the potential security implications of an attack on the dPCR platform could threaten the well-being of patients. An attacker could influence the decision making of a healthcare provider by skewing the diagnostic results in such a way that it is within the realm of possibility.

VI. Conclusion

We have provided an overview of flow-based biochips and their security and trust implications. While several factors, such as low complexity, application-specific design, and single use, seem to point to a lack of interesting security threats, we have shown the opposite to be true. The unique properties of flow-based biochips give rise to unique threats and as such will require a concerted effort from the research community to address them. We summarize the taxonomy in Fig. 7. We hope that the work presented here will inspire research into secure and trustworthy microfluidic systems, especially since standards have yet to be imposed upon the industry.

Acknowledgment

This research is supported in part by ARO grant number W911NF-17-1-0320.

References

[1] M. A. Unger *et al.*, "Monolithic microfabricated valves and pumps by multilayer soft lithography," *Science*, vol. 288, no. 5463, pp. 113–116, 2000.

[2] T. M. Squires and S. R. Quake, "Microfluidics: Fluid physics at the nanoliter scale," *Rev. Mod. Phys.*, vol. 77, no. 3, p. 977, 2005.

[3] S. S. Ali *et al.*, "Supply-chain security of digital microfluidic biochips," *Computer*, vol. 49, no. 8, pp. 36–43, 2016.

[4] ——, "Security assessment of cyberphysical digital microfluidic biochips," *IEEE/ACM Trans. Comput. Biol. Bioinform.*, vol. 13, no. 3, pp. 445–458, 2016.

[5] J. Tang *et al.*, "Securing digital microfluidic biochips by randomizing checkpoints," in *Proc. IEEE Int. Test Conf.*, Fort Worth, TX, Nov. 2016, pp. 1–8.

[6] ——, "Secure randomized checkpointing for digital microfluidic biochips," *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.*, in press.

[7] S. S. Ali *et al.*, "Microfluidic encryption of on-chip biochemical assays," in *Proc. Biomed. Circuits Syst. Conf.*, Shanghai, China, Oct. 2016, pp. 152–155.

[8] P. Roy and A. Banerjee, "A new approach for root-causing attacks on digital microfluidic devices," in *Proc. IEEE Asian Hardware-Oriented Security Trust Symp.*, Yilan, Taiwan, Dec. 2016, pp. 1–6.

[9] C.-W. Hsieh, Z. Li, and T.-Y. Ho, "Piracy prevention of digital microfluidic biochips," in *Proc. Asia South Pacific Des. Autom. Conf.*, Chiba, Japan, Jan. 2017, pp. 512–517.

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

[11] J. Melin and S. R. Quake, "Microfluidic large-scale integration: the evolution of design rules for biological automation," *Annu. Rev. Biophys. Biomol. Struct.*, vol. 36, pp. 213–231, 2007.

[12] T. Thorsen, S. J. Maerkl, and S. R. Quake, "Microfluidic large-scale integration," *Science*, vol. 298, no. 5593, pp. 580–584, 2002.

[13] K. Hu *et al.*, "Control-layer routing and control-pin minimization for flow-based microfluidic biochips," *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.*, vol. 36, no. 1, pp. 55–68, 2017.

[14] M. Boyd-Moss *et al.*, "Self-contained microfluidic systems: a review," *Lab. Chip*, vol. 16, no. 17, pp. 3177–3192, 2016.

[15] V. Ananthanarayanan and W. Thies, "Biocoder: a programming language for standardizing and automating biology protocols," *Journal of Biological Engineering*, vol. 4, no. 1, p. 1, 2010.

[16] M. Rostami, F. Koushanfar, and R. Karri, "A primer on hardware security: models, methods, and metrics," *Proc. IEEE*, vol. 102, no. 8, pp. 1283–1295, 2014.

[17] A. Cardenas *et al.*, "Challenges for securing cyber physical systems," in *Proc. Workshop Future Dir. Cyber-physical Syst. Security*, 2009, p. 5.

[18] R. Langner, "Stuxnet: dissecting a cyberwarfare weapon," *IEEE Security Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[19] S. Checkoway *et al.*, "Comprehensive experimental analyses of automotive attack surfaces." in *Proc. USENIX Security Symp.*, San Francisco, CA, Aug. 2011, pp. 77–92.

[20] D. Agrawal *et al.*, "The EM side-channel(s)," in *Proc. Int. Workshop Cryptographic Hardware Embedded Syst.* Springer, 2002, pp. 29–45.

[21] B. Vogelstein and K. W. Kinzler, "Digital PCR," *Proc. National Academy Sci.*, vol. 96, no. 16, pp. 9236–9241, 1999.

[22] P. Sykes *et al.*, "Quantitation of targets for PCR by use of limiting dilution," *Biotechniques*, vol. 13, no. 3, pp. 444–449, 1992.

[23] M. Baker, "Digital PCR hits its stride," *Nat. Methods*, vol. 9, no. 6, pp. 541–544, 2012.

[24] S. Dube, J. Qin, and R. Ramakrishnan, "Mathematical analysis of copy number variation in a DNA sample using digital PCR on a nanofluidic device," *PLoS One*, vol. 3, no. 8, p. e2876, 2008.

[25] J. F. Huggett, S. Cowen, and C. A. Foy, "Considerations for digital PCR as an accurate molecular diagnostic tool," *Clin. Chem.*, vol. 61, no. 1, pp. 79–88, 2015.

[26] M. Zarrei *et al.*, "A copy number variation map of the human genome," *Nat. Rev. Genet.*, vol. 16, no. 3, p. 172, 2015.

[27] A. J. Lafrate *et al.*, "Detection of large-scale variation in the human genome," *Nat. Genet.*, vol. 36, no. 9, p. 949, 2004.

[28] J. Sebat *et al.*, "Large-scale copy number polymorphism in the human genome," *Science*, vol. 305, no. 5683, pp. 525–528, 2004.

[29] J. F. Huggett *et al.*, "The digital MIQE guidelines: minimum information for publication of quantitative digital PCR experiments," *Clin. Chem.*, vol. 59, no. 6, pp. 892–902, 2013.

[30] R. Garver and C. Seife. (2013, Apr.) FDA Let Drugs Approved on Fraudulent Research Stay on the Market. [Online]. Available: https://www.propublica.org/article/fda-let-drugs-approved-on-fraudulent-research-stay-on-the-market