2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC) | 978-1-6654-2463-9/21/$31.00 ©2021 IEEE | DOI: 10.1109/COMPSAC51774.2021.00145

Discriminative Pattern Mining for Runtime Security Enforcement of Cyber-Physical Point-of-Care Medical Technology

Fred Love, Jennifer Leopold, Bruce McMillin[1]
Department of Computer Science
Missouri University of Science and Techology
Rolla, MO
{felcm4, leopoldj, ff}@mst.edu

Fei Su
Intel Corporation
Ann Arbor, MI
fei.su@intel.com

***Abstract*— Point-of-care diagnostics are a key technology for various safety-critical applications from providing diagnostics in developing countries lacking adequate medical infrastructure to fight infectious diseases to screening procedures for border protection. Digital microfluidics biochips are an emerging technology that are increasingly being evaluated as a viable platform for rapid diagnosis and point-of-care field deployment. In such a technology, processing errors are inherent. Cyber-physical digital biochips offer higher reliability through the inclusion of automated error recovery mechanisms that can reconfigure operations performed on the electrode array. Recent research has begun to explore security vulnerabilities of digital microfluidic systems. This paper expands previous work that exploits vulnerabilities due to implicit trust in the error recovery mechanism. In this work, a discriminative data mining approach is introduced to identify frequent bioassay operations that can be cyber-physically attested for runtime security protection.**

Keywords—Digital microfluidics, graph mining, point-of-care diagnostics, cyber-physical systems, information flow security

I. INTRODUCTION

Point-of-care (POC) medical technology represents a promising solution for addressing a wide breadth of critical applications including rapid, reliable diagnosis in developing countries commonly afflicted with infectious diseases to protecting neighboring countries from experiencing an outbreak of these diseases [9][15]. In the former case, developing countries are typically scarce in resources and lack fully trained medical staffing and regulation. Due to this deficiency in infrastructure, the availability of POC testing, that brings healthcare closer to the home, is paramount. Additionally, POC and rapid testing medical technology are being explored as an important support for homeland protection. The application has recently gained greater importance with the emergence of the COVID-19 virus. When visual evaluation of symptoms is unreliable and insufficient, providing in-field diagnostics is key for preventing an outbreak that could rapidly become uncontrollable. In response to the COVID-19 outbreak, the research community has promptly evaluated numerous diagnostic platforms that could be quickly and effectively deployed. For example, Abbot Laboratories launched a molecular point-of-care detection device that produced results in as few as five minutes [25]. Such advances are essential in fighting not only the current global pandemic, but also future viral outbreaks.

Microfluidic devices are being demonstrated as effective low-cost diagnostic platforms for both applications. Microfluidics is an interdisciplinary science focusing on the development of devices and systems that process low volumes of fluid for applications such as high throughput DNA sequencing, immunoassays, gene expression analysis, and entire Labs-on-Chip (LOC) platforms. Microfluidic diagnostic technology enables these advances by facilitating the miniaturization and integration of complex biochemical processing through a microfluidic biochip. Recent research has introduced cyber-physical digital microfluidic systems [1] that include error recovery capabilities for increased reliability. In contrast to continuous microfluidics biochips, digital microfluidics systems utilize micro/nano droplets to perform biochemical operations on chip. Cyber-physical digital microfluidic biochip systems tightly couple the biochemical operations, sensing system, control algorithm, and droplet-based biochip. During bioassay execution, the status of a droplet is monitored in real-time to detect operational errors. If an error has occurred, the control algorithm dynamically reconfigures to allow recovery and rescheduling of on-chip operations. During this recovery procedure the droplet that is the source of the error is discarded to prevent the propagation of the error and the operation is repeated. This increased adaptability represents a crucial step towards creating reliable on-chip diagnostics. The work discussed in [1] takes an additional step towards enabling adaptive LOC devices with a novel hardware-assisted approach to error-recovery that utilizes a compact dictionary implemented on a field-programmable gate array (FPGA). The dictionary consists of predetermined actuation sequences needed for error-recovery which are stored

[1] This work was supported in part by a grant from the US National Science Foundation under award CNS-1837472.

978-1-6654-2463-9/21/$31.00 ©2021 IEEE
DOI 10.1109/COMPSAC51774.2021.00145

in memory. Using the proposed finite state machine control, the FPGA can transfer the preloaded actuation sequences to the biochip as required. This error-recovery approach shows promise for handling the highly precise time control of chemical synthesis in flash chemistry, point-of-care field-deployment, and handheld device development. Although within the last decade there has been much research in the development of Cyber-physical digital microfluidic biochips (DMFB), analysis of their security implications and vulnerabilities has only begun as a research topic in recent years. In [16] information flow security threats to the operation of the microfluidics biochip were explored from two perspectives, (1) integrity: an attack can modify control electrodes to corrupt the diagnosis, and (2) privacy: what can a user/operator deduce about the diagnosis. [16] used the novel approach of Multiple Security Domain Nondeducibility (MSDND) and Belief, Information transfer, and Trust logic (BIT) to explore the vulnerabilities of exploiting this error recovery process through implicit trust and creating desirable information flow leakages to protect the system. At the heart of this security methodology introduced in [16] is cyber-physical attestation to verify cyber-physical monitors that form a part of the underlying system infrastructure. This will be discussed in greater detail in a later section.

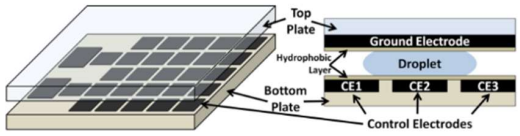
Given the complex nature of bioassay protocol, there are numerous invariant relationships that could be used for cyber-physical security attestation. This inherent complexity presents two research questions concerning the implementation of the independent verifier: (1) How to intelligently determine which biochemical operations are of interest to attest and (2) how to reduce runtime cost of the verifier. This work discusses a solution to both questions using discriminative data mining to identify frequent bioassay operations that can be cyber-physically attested for runtime security protection.

The paper is organized as follows. As background, Sections II-V provides a brief overview of the following topics: cyber-physical digital microfluidics biochips and error-recovery, foundations of cyber-physical system security, related security work, and discriminative subgraph mining. Section VI discusses the problem being addressed and how the discriminative data mining approach is leveraged for the given problem. Section VII discusses the implementation of an independent verifier that relies on discriminative mining for operation selection for attestation. Finally, Section VIII discusses future work and concludes the paper.

II. CYBER-PHYSICAL DIGITAL MICROFLUIDIC BIOCHIPS

Although variations are seen in literature, a common DMFB configuration can be described simply as follows: There is a two-dimensional electrode array with additional built-in resources such as on-chip reservoirs and sensors. The DMFB cell consists of parallel plates with a thin insulator layer coating the electrode surface as seen in Figure 1a. The theory of electrowetting-on-dielectric (EWOD) permits the device to perform a basic set of operations on small picoliter volumes of fluids. EWOD uses the principle of modulating the interfacial tension between the liquid and the dielectric coated electrode. When an electric field is applied in the dielectric layer, a surface imbalance is created and the droplet moves accordingly. The Cyber-physical representation of digital microfluidic system seen in Fig 1b includes the interactions between the primary system components. Frequently, implementations consist of a biochip, single-board computer or FPGA, some peripheral circuitry, and control software running on a computer. The sensing system resident on the biochip provides input to the control algorithm that computes (and recomputes in the event of an error) droplet transport pathways, module placement, and operation schedule. While this approach increases reliability, the computer-in-loop solution may not be optimal for POC deployment [1].To address this shortcoming, a hardware assisted error recovery method has been proposed [1]. This approach uses a finite state machine (FSM) to access a dictionary stored in memory that contains pre-computed actuation sequences to recover from all errors of interest. Since online re-synthesis is not necessary, response time is reduced. Therefore, a portable cyber-physical implementation is possible.

(a)



(b)

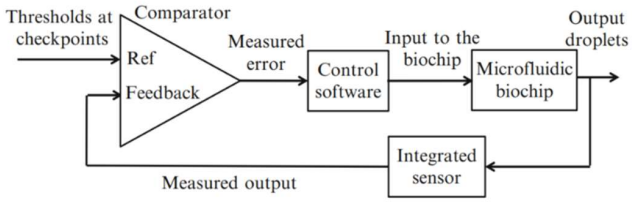


Figure 1: (a) Cross section of digital microfluidic biochip [20] (b) Cyber-physical coupling [1]

Error Recovery in Cyber-Physical Digital Biochips:

The presence of integrated sensors and physical-aware control software enables the composition of cyber-physical digital microfluidic biochips that can monitor operations during runtime. Additionally, cyber-physical digital microfluidic biochips can dynamically adapt to runtime errors and reconfigure in response. Reconfiguration techniques re-compute electrode actuation sequences which produces new module placement, droplet routing, and scheduling to adjust to a previously encountered error:

Recent work has taken an additional step towards enabling adaptive lab-on-chip devices with a novel hardware-assisted approach to error-recovery that utilizes a compact dictionary implemented on a field-programmable gate array (FPGA). The dictionary consists of predetermined actuation sequences needed for error-recovery which are saved and used during bioassay execution. This error recovery dictionary is first

generated in simulation for a given set of errors prior to experimentation and then stored in controller memory [1]. Using the proposed finite state machine control, the FPGA can transfer the preloaded actuation sequences to the biochip as required. This error-recovery approach shows promise for handling the highly precise time control of chemical synthesis in flash chemistry, point-of-care field-deployment, and handheld device development. Figure 2 illustrates the finite state machine control system.

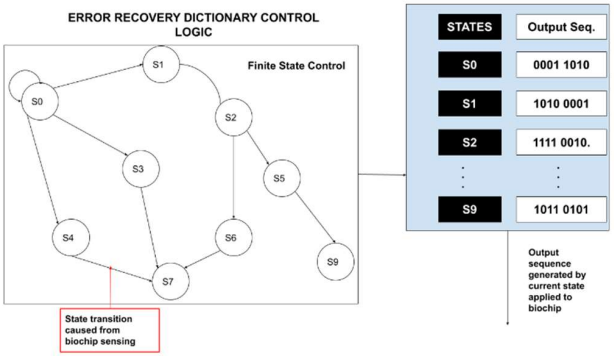


Figure 2: Finite state machine control for hardware-assisted error recovery

The outputs shown saved in memory as shown in Figure 2 are pre-determined recovery actuation sequences that account for all errors of interest that may occur at runtime. If an error is detected, then the system performs a search in the compact dictionary that corresponds to the event that occurred. This dictionary look-up approach to perform re-synthesis has a faster response time than the "computer-in-the-loop" approach that relies on external control application to execute error correction responses. Eliminating the need for control software to execute on-line error recovery also removes the requirement of an external computer and related interfaces. In addition to reducing the latency, this reduction in hardware can increase the overall reliability of the cyber-physical system since each component can be a point-of-failure.

III. CYBER-PHYSICAL SYSTEM SECURITY FOUNDATION

In this section some key concepts are defined to understand the proposed security methodology.

Invariants:

An invariant is a function, quantity, or property that remains unchanged when a specified transformation is applied. An invariant is a logical predicate on a system state that should not change its truth value if satisfied by the system execution. Recently invariants have been used in physical power systems to ensure correct operation [8]. Invariants are well-understood for cyber processes but extending them into the physical domains requires some insight. We can arrive at invariant equations based on the physical, thermal, or chemical properties of the system which can be used as an alternative source of information for a parameter in question.

Attestation:

CPS can become vulnerable to unexpected attacks without physical monitors to verify cyber-physical monitors. Vital areas where an agent trusts a report from another agent should be examined, and where possible, those reports should be verified by physical measurements [4]. CPS attestation is a method of securing a system that exploits the physical system dynamics. This technique uses an independent verifier to continuously monitor invariants to detect whether a component is behaving as expected or driving the system to an unsafe state. [4] emphasizes that the verifier would need to have a physical model of the plant and a model of the control algorithm to be able to identify false sensor or controller signals. As applied to cyber-physical digital microfluidic systems, the verifier would require knowledge of the bioassay protocol, i.e. bioassay sequencing graph, and invariant relationships for attestation. More discussion on attestation and invariants is provided in later sections.

Run-time Information Flow Security Enforcement:

Execution monitoring (EM) enforceability is the approach of monitoring the execution of a program at runtime for security policy violations and terminating this program if a violation has been detected. While this may be adequate for some program properties, it is not applicable to information flow properties (IFP) because they cannot be defined as safety properties as described by the Alpern-Schneider framework [21]. Recently, research has started to explore bridging the gap between existing runtime monitoring schemes and IFP protection. These works have created execution monitoring methodologies that enforce information flow security. In [16] Love *et al* extended these approaches to address potential vulnerabilities in implicit trust in monitors used in POC technology. Intelligent attacks could "hide" behind mechanisms that protect IFP therefore allowing intrusion to go undetected. To counteract this, the proposed independent verifier must induce a beneficial runtime information flow leakage to expose hidden attacks. Although formal definition of the independent verification automata is beyond the scope of this work, later sections will describe how discriminative pattern matching can be used to select which biochemical operations will be paired in this runtime monitor.

IV. RELATED SECURITY WORK

Research investigating the security of DMFB is a new development. [23][24] offer state-of-the art reviews on the challenges facing building secure DMFB systems, current approaches to secure them, and possible research directions. [6] discusses both result manipulation attacks of enzymatic glucose assays and denial-of-service attacks through tampering. [11] investigates DMFB supply chain security vulnerabilities and potential countermeasures. [10] proposes an authentication method that utilizes characteristics of electrodes to generate keys for piracy prevention. [13] focuses on timing attacks and attack site localization using symbolic reasoning. [12]

proposes a method of verifying the accuracy of signals from the online controller that uses a strategically placed droplet test circuit. In [16] a methodology is introduced that primarily focuses on information flow disruption and potential vulnerabilities caused by implicit belief and trust among system components. The outcome of that analysis proposed adopting process-based detection mechanisms that rely on the underlying physical and chemical properties of the bioassay and test to secure the system. This work expands this methodology by utilizing a discriminative subgraph pattern matching approach to select which bioassay operations the independent verifier selects for physical attestation. Such attestation would be used by the verifier for runtime enforcement of a given security policy.

V. FREQUENT SUBGRAPH PATTERN MATCHING

Frequent graph pattern matching is defined as recurring subgraphs found within a collection of graphs or a single, large graph that has an occurrence frequency that surpasses a given threshold. This approach is advantageous when compared to more exhaustive methods that intend to enumerate all subgraphs within a collection. Frequent graph pattern matching focuses on finding high frequency recurrences. These frequent subgraph patterns can be used for various purposes including, but not limited to, characterization, classification, and clustering. These methods have been applied in numerous fields ranging from chemical structure discovery in HIV-screening datasets to the study of protein structural families.

A well-known, frequent pattern matching methodology is discriminative subgraph mining [18][19]. Given two pre-classified graph collections, discriminative frequent pattern matching attempts to find substructures that surpass a defined frequency threshold that contrast the collections. These algorithms, such as LEAP and Top-k LEAP, have been successfully used to compare correct and faulty program executions to pinpoint bugs and provide contextual information useful for root cause analysis. These algorithms model program execution as a software behavior graph that operates with program blocks of code as nodes and calls as edge relationships that describe the flow of execution. LEAP generates the most discriminative subgraph signature, while Top-k LEAP generates a ranked list of k discriminative subgraph signatures which identifies different locations with the program that may contain bugs.

VI. PROBLEM STATEMENT

As initially proposed in [16], the selection of invariants chosen for runtime attestation would rely on domain knowledge or exhaustively attesting all invariants at all time steps. The advantage of the first approach is that domain knowledge could allow evaluating only a subset of operations therefore reducing any unforeseen real-time consequences while still creating the beneficial information flow path needed to protect the system. This disadvantage is that there may be operations or system properties that would be valuable to attest that were not included in the subset. This reasoning leads to the promotion of an exhaustive testing scheme. While the advantage of this approach is clear, all biochemical and system invariants attested, the real-time consequences are unclear at this time. This raises questions such as: can the verifier adequately evaluate all invariants and rapidly respond? With respect to a complete handheld lab-on-chip solution, does the verifier have access to enough memory to hold any required precomputed values that would be needed to attest each invariant? Are there performance limitations that would complicate evaluating all invariants at every time, and in the event of an attack, raise the appropriate alarm?

The focus of this paper is the development of an offline discriminative mining approach to pre-select bioassay operations for cyber-physical attestation. This contribution extends previous work modeling Stuxnet-type attacks on POC technology built around cyber-physical digital microfluidic systems [16]. In [16] the impact of such attacks was evaluated by formulating the following essential questions: Can such an attack be detected while in progress? How can a CPS be protected from the human operator's blind trust in cyber monitoring? If incorrect but reasonable information is used, how will one know? The result of this analysis was a proposed independent verifier that utilized physical invariants of the system and the biochemical process to add a strong layer of protection. In this work, discriminative data mining is explored to intelligently select which bioassay operations will be attested.

DISCRIMINATIVE SUBGRAPH MINING

In [18][19] a discriminative subgraph mining approach was used to identify bug signatures within a program. The graph collection was divided into correct and faulty executions of the program with nodes representing basic code block. This separation of collections allowed the algorithm to identify which portions of the "bad" control flow graphs were more prevalent than the "good". A similar separation between "good" and "bad" executions can be used for bioassays performed on cyber-physical digital microfluidic biochips. With respect to security, this approach will distinguish "under attack" and "attack-free" executions with the goal of identifying the subgraph that is most vulnerable to security attack.

The discriminative subgraph mining algorithm used for this work is described in detail in [18]; the main functionality is briefly summarized here. Let C^+ and C^- represent the sets of graphs for the "good" and "bad" cases, respectively; there must be at least one graph in each such set. First, non-discriminative edges are removed from the graphs in both sets. The algorithm then tries to find a subgraph that is common to all of the "bad" graphs, but not common to all of the "good" graphs. If the algorithm is unable to find such a graph, then the algorithm relaxes the requirement that the subgraph we seek not be present in every "good" graph; instead the subgraph only has to not be present in $\alpha * |C^+|$ of the "good" graphs, where α is a user-specified parameter (our default is $\alpha = 0.5$). If we still fail to find a discriminative subgraph, then the anomaly likely does not involve components that are included in all "bad" cases and not in the "good" cases, but rather involves components that are in "good" cases and not in "bad" cases. Thus, the algorithm

performs the same processing, but reverses the order of the parameters (C^+ and C^-) from the previous execution. If it still fails to find a discriminative subgraph, it again relaxes the requirements and looks for a subgraph that only has to not be present in $\beta * |C^+|$ of the "good" graphs, where β is a user-specified parameter (our default is $\beta = 0.5$).

In terms of analyzing the computational complexity of this algorithm, let $N^+=|C^+|$, $N^-=|C^-|$, E^+ be the total number of edges in C^+, and E^- be the total number of edges in C^-. The task of finding (and removing) non-discriminant edges from the collection of graphs requires $O(E^+ + E^- + N^+ + N^-)$; presumably, N^+ and N^- are much smaller than $E^+ + E^-$, so we can regard this step as $O(E^+ + E^-)$. The process of finding a subgraph that is common to one collection C (either C^+ or C^-), but not the other collection, requires $O(2^N * (2 * N^+ + N^-) * N * (N-1))$ where N is the maximum number of vertices in a graph in collection C. Hence, the overall complexity is exponential, proportional to the size of the largest graph in the entire collection.

When forming a "attack-free" graph collection, it is important to understand that processing errors do occasionally occur during bioassay execution. Error recovery mechanisms are used to address such events and allow the bioassay to complete. The real-time error recovery dictionary described previously accounts for such inherent errors and holds their respective actuation sequences in memory. Since these errors are anticipated, they are not considered under-attack anomalies and their sequence graphs also form part of the "good" collection.

When creating a collection of "bad" graphs, or graphs that represent an under-attack scenario, a result manipulation attack model is currently being considered. This attack model involves the subtle change of bioassay sequence graph that alters the execution of the test. Such an attack could toggle the result leading to a false positive or false negative. This contrast can be seen when comparing a golden execution with an execution under attack as seen in Figure 3 and Figure 4, respectively. Figure 3 shows a golden execution of a bioassay that operates as expected. However, Figure 4 depicts the same assay, but the result has been changed through malicious tampering. In this attack scenario, a sequence of malicious split operations was added to reduce the droplet concentration below the pass/fail threshold. This could lead to a malicious toggling of the diagnostic result.

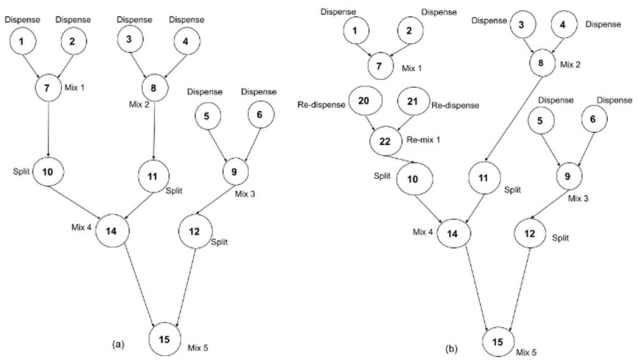


Figure 3: Attack-free bioassay executions (a) without error recovery operation (b) with error recovery operation

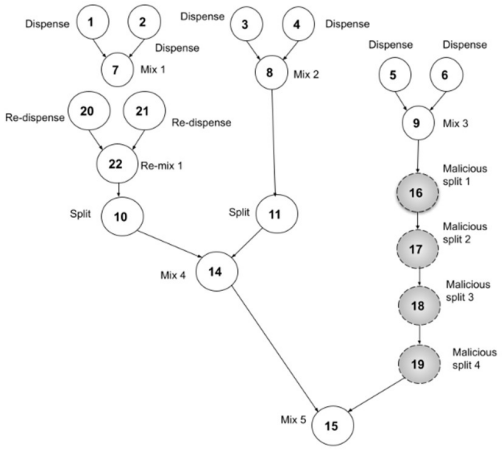


Figure 4: Bioassay execution with error recovery events under results manipulation attack

Figure 4 also includes an inherent error that occurs during operation Mix 1 which requires re-dispensing and re-mixing. Such an error should not be classified as malicious.

Both Figure 3 and 4 were respectively added to "attack-free" and "under attack" collections of graphs representing the same bioassay executions. Both collections included graphs with inherent errors, but only the "under attack" graphs included the malicious split sequence that represent the result manipulation attack model. The discriminative graph mining algorithm implemented in Python successfully identified the malicious bioassay operations as seen in Figure 5:

```
Edges that ALL graphs have in common:  {('11', '13'), ('4', '8'), ('1', '7'), ('6', '9'), ('3', '8'), ('13',
'14'), ('10', '13'), ('5', '9'), ('2', '7'), ('14', '15')}

Looking for discriminative graph in bad graphs...
Comparing a set of 3 graphs to a set of 2 graphs
freq_edges is  {('16', '17'), ('18', '19'), ('9', '16'), ('19', '15'), ('17', '18')}

Here is resulting discriminative graph:
found in bad
('16', '17')
('17', '18')
('18', '19')
('19', '15')
('9', '16')
```

Figure 5: Resulting Discriminative Subgraph

The implementation seen in Figure 5 first finds and removes subgraphs that all graphs have in common. It then finds subgraphs that occur in most of the "under-attack" graphs, but not in the majority of the "attack-free" graphs. The most discriminative substructure is finally reported. The implementation of the discriminative subgraph mining algorithm utilized for this work (which varies slightly from [19]) is described in more detail in [18]. The following section discusses how such offline, pre-processing can be used to identify bioassay operations of interest for cyber-physical attestation at runtime.

Also, it is worth noting that although the current implementation uses NetworkX [22] for offline pre-processing, it easily lends itself to on-device real-time discriminative graph mining since many bioassay graphs contain a relatively small node count, i.e., less than 128 nodes. This approach is currently under investigation.

VII. DISCRIMINATIVE MINING FOR RUNTIME VERIFICATION

To prevent the type of result manipulation attack seen in the previous section, a separate verifier that uses fundamental system properties has been proposed [16]. This verifier processes physical biochemical and system invariants to provide an independent verification of the results as the test is executing. This runtime monitor would allow verification of system dynamics in accordance with both test intent and preservation of the system policy. Figure 6 shows the proposed high-level operation of the independent runtime monitor.

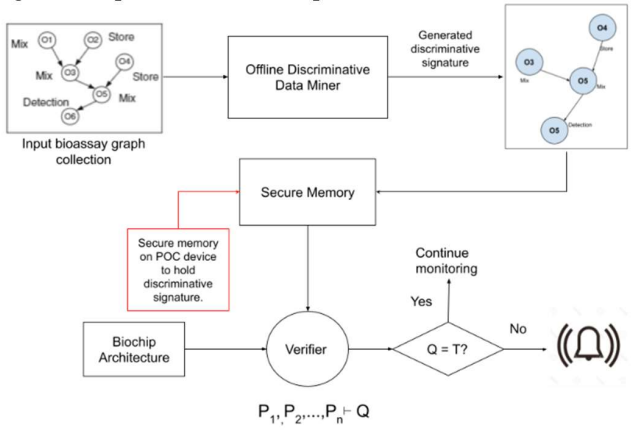


Figure 6: Runtime Execution Monitor

Extending the verifier proposed in [16], this runtime monitor would operate utilizing the following requirements: (1) biochip system architecture, (2) current bioassay under test, (3) physical invariants to be evaluated at runtime, and (4) discriminative subgraph signatures. The first three requirements are well described in [16]. The extended independent verifier would also leverage the precomputed discriminate subgraph signatures to attest only a subset of operations, therefore reducing potential runtime costs.

VIII. SUMMARY AND FUTURE WORK

This paper has described the operation of a runtime execution monitor for DMFB that employs discriminative subgraph mining techniques. Such an approach is promising in cases when an attacker can compromise operation of the system by blinding the system monitor from the actual bioassay operation that is taking place on the DMFB electrode array. Although this work is an extension to past analysis of such attack, the operation of the independent verifier has been further described.

However, there are still many research questions to answer. What are the real-time benefits to the proposed discriminative mining approach to more exhaustive methods? Are their practical implementation limitations? How will future implementations of this discriminative method handle multiple attack models. This group is currently investigating practical implementations with the current objective of developing a verifier and attestation algorithm that will offer "low-impact" security overhead: low-impact to real-time performance for flash chemistry enablement, and low-impact to overall system cost for POC deployment in low-resource settings and for border protection to prevent disease outbreaks.

REFERENCES

[1] Luo, Y., Chakrebarty, K, and Ho, T, Hardware/Software Co-Design and Optimization for Cyber-physical Integration in Digital Microfluidic Biochips, Springer, 2015, DOI= 10.1007/978-3-319-09006-1.

[2] M. Ibrahim and K. Chakrabarty, "Error recovery in digital microfluidics for personalized medicine," 2015 Design, Automation & Test in Europe Conference & Exhibition (DATE), Grenoble, 2015, pp. 247-252. DOI: 10.7873/DATE.2015.1126.

[3] Fair, R.B. Digital microfluidics: is a true lab-on-a-chip possible?. Microfluid Nanofluid 3, 245–281 (2007). https://doi-org.libproxy.mst.edu/10.1007/s10404-007-0161-8.

[4] Gerry Howser and Bruce M. McMillin. A modal model of stuxnet attacks on cyber-physical systems: A matter of trust. In Eighth International Conference on Software Security and Reliability, SERE 2014, San Francisco, California, USA, June 30 - July 2, 2014, pages 225–234, 2014.

[5] C.-J. Liau, "Belief, information acquisition, and trust in multi-agent systems - A modal logic formulation," Artificial Intelligence, vol. 149, no. 1, pp. 31 – 60, 2003.

[6] S. S. Ali, M. Ibrahim, O. Sinanoglu, K. Chakrabarty and R. Karri, "Security Assessment of Cyberphysical Digital Microfluidic Biochips," in IEEE/ACM Transactions on Computational Biology and Bioinformatics, vol. 13, no. 3, pp. 445-458, 1 May-June 2016, DOI: 10.1109/TCBB.2015.2509991.

[7] J. Valente, C. Barreto and A. A. Cárdenas, "Cyber-Physical Systems Attestation," 2014 IEEE International Conference on Distributed Computing in Sensor Systems, 2014, pp. 354-357, DOI: 10.1109/DCOSS.2014.61.

[8] Roth T., McMillin B. (2013) Physical Attestation of Cyber Processes in the Smart Grid. In: Luiijf E., Hartel P. (eds) Critical Information Infrastructures Security. CRITIS 2013. Lecture Notes in Computer Science, vol 8328. Springer, Cham. https://doi-org.libproxy.mst.edu/10.1007/978-3-319-03964-0_9.

[9] R. Peeling and D. Mabey, "Point-of-care tests for diagnosing infections in the developing world,"Clinical Microbiology and Infection , vol. 16,no. 8, pp. 1062–1069, 2010.

[10] Ching-Wei Hsieh, Zipeng Li, Tsung-Yi Ho, "Piracy prevention of digital microfluidic biochips", Design Automation Conference (ASP-DAC)2017 22nd Asia and South Pacific, pp. 512-517, 2017, ISSN 2153-697X.

[11] S. S. Ali, M. Ibrahim, J. Rajendran, O. Sinanoglu and K. Chakrabarty, "Supply-Chain Security of Digital Microfluidic Biochips," in Computer, vol. 49, no. 8, pp. 36-43, Aug. 2016, DOI: 10.1109/MC.2016.224.

[12] S. Basu, S. Saha and I. Pan, "Intrusion Detection in Online Controller of Digital Microfluidic Biochips," 2014 International Conference on Computational Intelligence and Communication Networks, 2014, pp. 1021-1025, doi: 10.1109/CICN.2014.215.

[13] P. Roy and A. Banerjee, "A new approach for root-causing attacks ondigital microfluidic devices," 2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST), Yilan, 2016, pp. 1-6. doi: 10.1109/AsianHOST.2016.7835550.

[14] J. McLean, "Security models and information flow," Proceedings. 1990 IEEE Computer Society Symposium on Research in Security and Privacy, 1990, pp. 180-187, doi: 10.1109/RISP.1990.63849.

[15] Sharma S, Zapatero-Rodríguez J, Estrela P, O'Kennedy R. Point-of-Care Diagnostics in Low Resource Settings: Present Status and Future Role of Microfluidics. Biosensors.2015; 5(3):577-601. 247.

[16] F. Love and B. McMillin, "Breaking Implicit Trust in Point-of-Care Medical Technology: A Cyber-Physical Attestation Approach," 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC),Turin,2017,pp. 242-247, doi: 10.1109/COMPSAC.2017.74.

[17] T. T. Gamage and B. M. McMillin, "EM Enforcing Information Flow Properties using Compensating Events," 2009 42nd Hawaii International Conference on System Sciences, Big Island, HI, 2009, pp. 1-7, doi: 10.1109/HICSS.2009.181.

[18] J.L. Leopold, N.W. Eloe, Jeff Gould, and Eric Willard, "A Visual Debugging Aid Based on Discriminative Graph Mining", Journal of Visual Languages and Sentient Systems (VLSS), vol. 4, December 2018, pp. 1-10.

[19] Hong Cheng, David Lo, Yang Zhou, Xiaoyin Wang, and Xifeng Yan. 2009. Identifying bug signatures using discriminative graph mining. In Proceedings of the Eighteenth International Symposium on Software Testing and Analysis (ISSTA '09). Association for Computing Machinery, New York, NY, USA, 141–15.

[20] Christopher Curtis, Daniel Grissom, and Philip Brisk. 2018. A compiler for cyber-physical digital microfluidic biochips. In Proceedings of the 2018 International Symposium on Code Generation and Optimization (CGO 2018). Association for Computing Machinery, New York, NY, USA, 365–377.

[21] J. McLean, "A general theory of composition for a class of "possibilistic" properties," in IEEE Transactions on Software Engineering, vol. 22, no. 1, pp. 53-67, Jan. 1996, doi: 10.1109/32.481534.

[22] Aric A. Hagberg, Daniel A. Schult and Pieter J. Swart, "Exploring network structure, dynamics, and function using NetworkX", in Proceedings of the 7th Python in Science Conference (SciPy2008), Gäel Varoquaux, Travis Vaught, and Jarrod Millman (Eds), (Pasadena, CA USA), pp. 11–15, Aug 2008.

[23] C. Dong et al., "A Survey of DMFBs Security: State-of-the-Art Attack and Defense," 2020 21st International Symposium on Quality Electronic Design (ISQED), 2020, pp. 14-20, doi: 10.1109/ISQED48828.2020.9137016.

[24] J. Tang, M. Ibrahim, K. Chakrabarty and R. Karri, "Toward Secure and Trustworthy Cyberphysical Microfluidic Biochips," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 38, no. 4, pp. 589-603, April 2019, doi: 10.1109/TCAD.2018.2855132.

[25] A. Vecchione, "NJ adds15 Abbott ID NOW instruments, expanding access to COVID-19 testing," Njbiz, 2020.