Poster: Side-Channel Vulnerabilities Of Cyber-Physical Systems In Biomedical Applications

Sina Faezi
Electrical Engineering and Computer Science
University of California, Irvine
Irvine, U.S.A.
sfaezi@uci.edu

Mohammad Abdullah Al Faruque
Electrical Engineering and Computer Science
University of California, Irvine
Irvine, U.S.A.
alfaruqu@uci.edu

***Abstract*—In recent years, the emergence of automation in biomedical science through Cyber-Physical Systems (CPS) has resulted in tremendous advancements. For instance, 3D printing technologies are revolutionizing medicine by means such as custom-made body parts, while low-cost oligonucleotides synthesized by fully-automated DNA synthesizers are providing solutions for treating a variety of diseases. However, systems with cyber-domain processes and physical-domain components are prone to security breaches like any other computing system. To this end, we present an attack methodology which can be used to steal the sensitive information often used with such machines through unintended emissions of the machine in side-channels such as acoustics. By identifying these type of vulnerabilities, we hope to encourage commercial biomedical equipment manufacturers to strengthen their products' confidentiality.**

***Index Terms*—cyber-physical systems, biomedical, side-channel attack, statistical modeling**

I. Introduction

The computerization revolution has resulted in various new paradigms for biomedical devices: pacemakers regularize heartbeats of patients who suffer from abnormal heart rhythm, 3D printers manufacture personalized body parts, and automated DNA synthesizers fabricate custom DNA sequences with a variety of applications. These innovations are products of the tight integration of cyber and physical components which work together to perform the intended medical procedure and are referred to as cyber-physical systems (CPS).

Countries have implemented regulations to assure the safety of the physical aspect of the systems mentioned above [1], [8] while the computer security community addresses the concerns raised due to the cyber aspect of such systems [9]. However, the integration of cyber and physical components will create a surface for a new set of threats. One of the challenges for securing biomedical CPS is being able to understand these new threats unique to CPS [2].

In a CPS, the computer-based algorithms' executions translate to physical changes in the components of the system. Often, along with the intended physical changes, there are unintentional physical signals emitted in side-channels. For instance, a change in the speed of a motor will also result in the motor generating a different acoustic noise. In biomedical CPS such radiations are usually overlooked in the design phase of the system to reduce complexity. With this intuition, we propose a general attack methodology that can endanger the confidentiality property of many biomedical devices which work with sensitive information.

II. Attack Methodology

As shown in Figure 1, the approach that we use to attack the corresponding biomedical CPS consist of two phases: the training phase and the attack phase. In the training phase, we profile the CPS into a statistical model by providing labels for each emitted signal from the machine, and then in the attack phase, the model predicts the labels (sensitive data) for a given signal. In both phases, we apply signal segmentation and feature extraction to magnify the information carried in the emitted signals. These steps highly depend on the particular biomedical device under attack and the type of the information intended to be stolen. In our attack methodology the attacker can be a disgruntled employee or a visitor who can place a recorder in the close proximity to the target CPS.

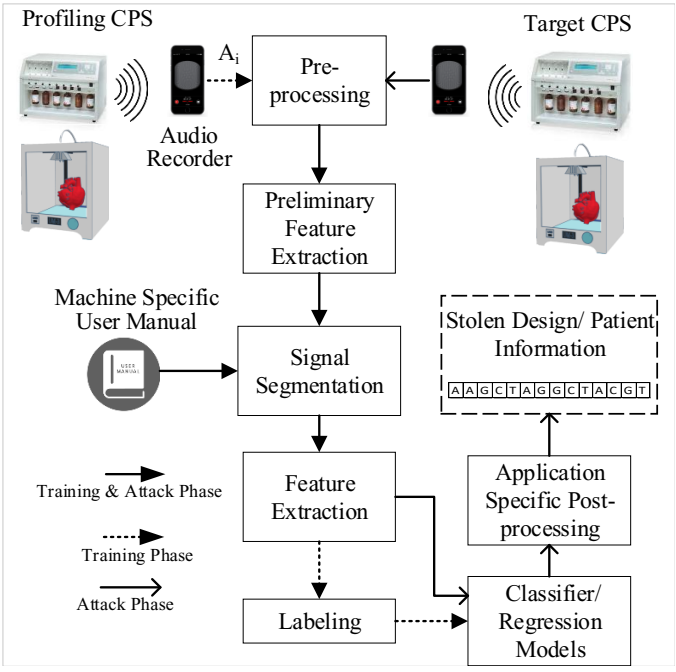
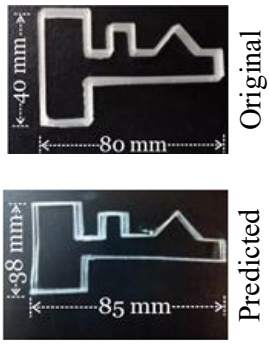


Fig. 1: Side-channel attack methodology on biomedical CPS.

Case #	**Original** Oligonucleotide sequence **Predicted** Oligonucleotide sequence	Sequence Length	Accuracy (%)
1	CGCAA**G**TACTCCTG**C** CGCAA**T**TACTCCTG**A**	15	86.67
2	GGAATAGTAGAAG**AA**TGCTGCACAA**G**CATATGCAGCCTA**T**ACGAACTAGAAGAC**T**ACTGCGAC GGAATAGTAGAAG**CG**TGCTGCACAA**T**CATATGCAGCCTA**C**ACGAACTAGAAGAC**G**ACTGCGAG	63	**90.48**
3	TGGCGACAT**G**ATAACCCGTCGGA**G**GATCCGGG**G**CG**G**G**GG**CACCTC TGGCGACAT**T**ATAACCCGTCGGA**T**GATCCGGG**T**CG**T**G**TT**CACCTC	45	86.67
4	TTTT**T**CGACCGGT**A**T**GA**T**T**CCGCCCGTGACCCAGGACGCTTGCTT TTTT**G**CGACCGGT**C**T**TC**T**G**CCGCCCGTGACCCAGGACGCTTGCTT	45	88.89

The bold colors with larger font size in oligonucleotide sequence represents the misclassified nucleotide bases

(a)



(b)

Fig. 2: Results for reconstructing the test cases: (a) four synthetic DNA sequences; (b) a 3D printed object.

III. Related Publications

The proposed attack methodology has been tailored and applied to two biomedical CPS. In [7] and [3], for the first time, we showed that it is possible to steal the design information of the 3D printed objects via acoustics side-channel emission of the 3D printer. Also, in [6] we further validated the threat of our attack methodology against commercially available DNA synthesizers by predicting the order of bases in the valuable synthesized DNA sequences. Moreover, in [5] and [4] we present a zero-cost countermeasure that can be used in the cyber components of 3D printers so they would leak less information through various types of side-channels such as acoustics, electromagnetic, etc.

IV. Summary of Results

We apply the presented attack to the Printrbot Simple Maker 3D printer and Applied Biosystems 3400 DNA synthesizer. On average, the results of applying the presented attack methodology to the 3D printer show that an attacker can reconstruct a 3D printed object by 92.54% accuracy for the axis prediction and 6.35% error on length prediction for a given object. Also, the results show that the attack methodology can predict the order and type of bases in a synthesized DNA sequence by 88.07% accuracy on average. Figure 2 shows sample stolen information in these two cases. In both scenarios, the sensitive information is considered to be intellectual property (IP). While in the research and development phase, stealing these IPs would result in tremendous financial loses.

By identifying these type of vulnerabilities, we hope to encourage commercial biomedical equipment manufacturers to strengthen their products confidentiality.

Acknowledgment

This research was supported in part by NSF awards CMMI-1739503 and CMMI-1763795. Other researchers involved in this project include Sujit Rokka Chhetri, Arnav Vaibhav Malawade, John Charles Chaput (University of California, Irvine), William Grover and Philip Brisk (University of California, Riverside).

References

[1] *Screening framework guidance for providers of synthetic double-stranded DNA*. US Department of Health and Human Services, 2010.

[2] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, S. Sastry *et al.*, "Challenges for securing cyber physical systems," in *Workshop on future directions in cyber-physical systems security*, vol. 5, no. 1, 2009.

[3] S. R. Chhetri, A. Canedo, and M. A. A. Faruque, "Confidentiality breach through acoustic side-channel in cyber-physical additive manufacturing systems," *ACM Transactions on Cyber-Physical Systems*, vol. 2, no. 1, p. 3, 2018.

[4] S. R. Chhetri, S. Faezi, and M. A. Al Faruque, "Information leakage-aware computer-aided cyber-physical manufacturing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2333–2344, 2018.

[5] S. R. Chhetri, S. Faezi, and M. A. A. Faruque, "Fix the leak!: an information leakage aware secured cyber-physical manufacturing system," in *Proceedings of the Conference on Design, Automation & Test in Europe*. European Design and Automation Association, 2017, pp. 1412–1417.

[6] S. Faezi, S. R. Chhetri, A. V. Malawade, J. C. Chaput, W. Grover, P. Brisk, and M. A. Al Faruque, "Oligo-snoop: A non-invasive side channel attack against dna synthesis machines," in *Network and Distributed System Security Symposium (NDSS)*, 2019.

[7] A. Faruque, M. Abdullah, S. R. Chhetri, A. Canedo, and J. Wan, "Acoustic side-channel attacks on additive manufacturing systems," in *Proceedings of the 7th International Conference on Cyber-Physical Systems*. IEEE Press, 2016, p. 19.

[8] C. Sorenson and M. Drummond, "Improving medical device regulation: the united states and europe in perspective," *The Milbank Quarterly*, vol. 92, no. 1, pp. 114–150, 2014.

[9] P. A. Williams and A. J. Woodward, "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem," *Medical Devices (Auckland, NZ)*, vol. 8, p. 305, 2015.