INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

Université Fédérale Toulouse Midi-Pyrénées

LAAS

Département de Génie Électrique & Informatique

State of the art

Security assessment of connected objects in the Internet of Things

December 4, 2019

Students :

Prénom NOM mail@mail.mail
Prénom NOM mail@mail.mail
Prénom NOM mail@mail.mail
Prénom NOM mail@mail.mail
Prénom NOM mail@mail.mail

Tutors :

Prénom NOM
Prénom NOM
Prénom NOM
Prénom NOM

Keywords: Internet of things ; security ; non-intrusive exploit detection

Abstract :

One of the biggest challenges in the Internet of Things is to be able to secure devices and, therefore, to detect when and how a device is being attacked. In this study, we will investigate the existing research material on intrusion detection systems (IDS) used to detect if a connected object has been compromised. The IDS will use physical measures as well as network monitoring, but, in this study, we will particularly develop the case of physical measures.

Contents

Introduction

In the race of innovation in the Internet of Things, security is often left behind. However, as the Internet of Things is massively developing, the attack possibilities are growing exponentially. Therefore, connected objects are vulnerable to direct attacks towards the objects themselves, but they are also vulnerable to becoming a mean of attack, by becoming part of a botnet. Botnets can then be used to perform large scale attacks such as DDoS.

Many objects in the IoT are vulnerable firstly because of their configuration. Let's take the example of a small business owner wanting to secure his premises. He will likely buy a "plug and play" connected security camera (CCTV) in order to keep an eye on his shop from his home. It is highly probable he will not try to change the basic configuration of the object, such as the passwords.

Unfortunately, these IoT devices often come with weak default username and password (such as "login: admin, password: admin") and therefore are vulnerable to dictionary attacks. We can take as an example the Mirai botnet [1], which scans the Internet looking for IoT devices with default username and password using dictionary attacks over telnet. Once a new vulnerable device has been discovered, the Mirai binary is injected in the device and it joins the Mirai botnet, making it stronger and capable of finding new devices faster. These kinds of botnets are then used to launch bigger attacks such as distributed denial of service (DDoS) on more robust structures.

Thus, one of the biggest challenges in the Internet of Things is to be able to secure devices and, therefore, to detect when and how a device is being attacked. In this study, we will investigate the existing research material on intrusion detection systems (IDS) used to detect if a connected object has been compromised. The IDS will use physical measures as well as network monitoring, but, in this study, we will particularly develop the case of physical measures.

1 IDS based on power monitoring

Most of IoT devices are designed to execute simple functions such as measuring a room's temperature and communicating with other devices. For this reason, there is a limited number of "states" they could be in (i.e. they are not supposed to be executing anything else than their functions). Their power consumption is linked to the code they are running [2], [3] (the side channel of power consumption) which makes it a good indicator to detect if they are running an abnormal code. Moreover, as IoT devices are not supposed to be modified internally and as their power outlets are accessible, power monitoring appears to be a valuable base for IDS.

The Intrusion Detection System based on power monitoring is implemented in at least 2 steps. First step is to collect data about the current and/or voltage during the normal execution of the functions. For the second step, the device is used in a real environment with possible attacks being performed while its current and/or voltage are being monitored. If the obtained values are different than the expected ones, it means that the IoT device is possibly being attacked. This analysis can be done by a machine learning algorithm that has been previously trained with data from normal execution and possibly with data from the device while being attacked.

Several studies have been made about variations or specializations of this system that we are presenting in the following parts.

1.1 Demonstrating the relationship between power consumption and security related attack

In 2018, a study [4] has been made on two IoT devices in order to show the link between attacks on the devices and deviations in power they consumed. A temperature and humidity sensor (that the researchers created) and an IP Camera were used for the experiments as they are representative of the common IoT devices. This study focuses on how the physical data is collected and the link between variations in the data and the device being attacked rather than on developing a system that uses the collected data to detect attacks.

To monitor the supply current, they used a microcontroller on a board with 1 Ohm resistor, two analog inputs and an AC power supply 5V. The analog inputs (used to convert a voltage into a digital value) measured the voltages around the resistor and transmitted them to the microcontroller which was using Ohm's law to compute the power supply current. This setup formed the monitoring device that was connected to the IoT devices through their cylindrical receptacle of 2.1mm.

Their experiments were divided in 2 steps and followed different scenarios. The first step consisted in calculating the average power supply current for a time window of 5 minutes with one sample per millisecond. Then, the second step was the comparison of these averages depending on the scenarios (with or without attacks) to evaluate the deviations in the current. For both devices, two types of profiles were considered: one when the device executed its functions in normal operational conditions and one when a Denial of Service (DoS) attack was performed on the device.

The use case for the temperature and humidity device was measuring the temperature and humidity of a room. For the IP Camera, three different cases were used for the experiments: one when it was streaming video where nothing happened (still image), one where the video consisted of quickly changing images and one when the camera was being moved while streaming video. In the last two scenarios, the IP Camera needed more resources to execute the tasks which means that the power consumed was considerably affected.

The conclusion of these experiments is that deviations in the average current are identified for scenarios where the devices are performing functions that requires important resources or not.

This study shows that for IoT devices, the power supply current is a valuable physical data to monitor in order to detect intrusions. For our project, we will have to create the power monitoring system from scratch which is why this paper is relevant as it provides a detailed setup of their monitoring device.

1.2 Experiments on machine learning techniques to detect malware

WattsUpDoc [2] is a system developed by researchers with the aim of detecting abnormal activities on embedded systems and specifically on medical devices. The paper about this system focuses on using machine learning techniques to draw normal and abnormal patterns of power consumption that can then be used to detect abnormal activities such as malware. IoT devices are embedded systems which enlightens the relevance of this study for our project.

To prove the efficiency of WattsUpDoc, they experimented it on two embedded systems: a pharmaceutical compounder (medical device) and an industrial-control workstation (a Supervisory Control and Data Acquisition (SCADA) device made to control industrial processes). For both devices, they put a 0.1 Ohm sense resistor between the supply power outlet and the device's power outlet. The data was collected thanks to a Data Acquisition Unit (DAQ) that read the voltage on the resistor at a rate of 250kHz.

As their system uses a supervised-learning approach, it requires to be run on the devices without and then with abnormal activity before it can be used on a "real" context. This step is necessary as it enables the system to "learn" how to classify power data as an indicator of a normal activity or not. In order to find the best algorithm for this part, they used 3 different classifiers: 3-nearest neighbors, multilayer perceptron and random forest. They considered eight time-domain features and ten frequency-domain features as well as different sizes of the time window and of the training set with the goal of identifying what setup was the most performant.

After the stage of training the system with the two devices performing their normal functions without being attacked and then while being attacked by malware, they evaluated their system by executing known (i.e. that was used during the training step) or unknown malware on the devices.

WattsUpDoc detected abnormal activity on the medical device and on the SCADA device respectively with 94% and 99% accuracy when malware was known and with 88.5% and 84.9% accuracy when malware was unknown.

As this study relies on several experiments of their system using three machine learning algorithms with different configurations, it can be used as a good base for the analyzing part of our project.

1.3 Recovering executed code to detect malicious modifications

In 2016, a study [3] was published addressing code execution tracking based on power monitoring. Even though it does not focus on IDS, it presents a different approach we could consider for our project.

The aim of the paper is to retrieve the type of executed instructions and at any given time, identify which instruction in code is executed by the microcontroller unit (used in IoT devices). Knowing the code that the microcontroller unit is supposed to execute and what it is really executing enables to detect abnormal behaviors of the device. They used power consumption side channel to track code execution as it is closely linked to the instructions executed but in order to achieve a high accuracy, they developed techniques to extract high quality signals from the power traces (using frequency analysis).

They evaluated their system on a 8051 microcontroller unit running nine different programs. To recover the type of executed instruction, they reached 99.94% accuracy and to identify the executed instruction in a code, they achieved 98.56% accuracy, which are significantly high. Moreover, they proved that their system can detect abnormal activity even when only a single instruction was modified in the code.

With respect to our project, this system has some downsides as it was tested with known code which will not be our case (we will not have any knowledge on the functions' implementation in the IoT devices). However, we can follow the methods they used to extract data from the power measurements and to detect the abnormal behaviors to develop our system.

2 IDS based on electromagnetic emissions

As for every electronic component, IoT devices emit electromagnetic waves when functioning. Thus, an abnormal use of such items can lead to variations in the electromagnetic field surrounding the object, which can be detected. As for the other non intrusive means of detection, it operates without introducing any overheads, adding any hardware support, changing any software, or using any resources on the monitored system itself.

Monitoring with an electromagnetic detection device involves receiving electromagnetic (EM) emanations that are emitted as a side effect of execution on the monitored system. Most of the time, it relies on spikes in the EM spectrum that are produced as a result of periodic activity in the monitored execution.

2.1 One example of an IDS based on radio-frequency emissions

To that end, Bastille Networks Incorporation drafted, in June 2014, a device that can detect such variations [5]. It includes sensors such as radio receivers in order to receive signals within an electromagnetic environment. The electromagnetic signatures are then identified from one or more of the radio frequency signals, enabling to put on feet the representation of a baseline electromagnetic environment, at the radio frequency level.

After such a modelisation has been made, variations of the environment can be detected −using the same method−, processed and analysed. Such method empowers the user of the studied device to monitor anomalies in its functioning: the analysis of those variations are then compared to other validated attack scenarii stored in a database. The operator interface can then serve as a bias to manually check the validity of the algorithm's output.

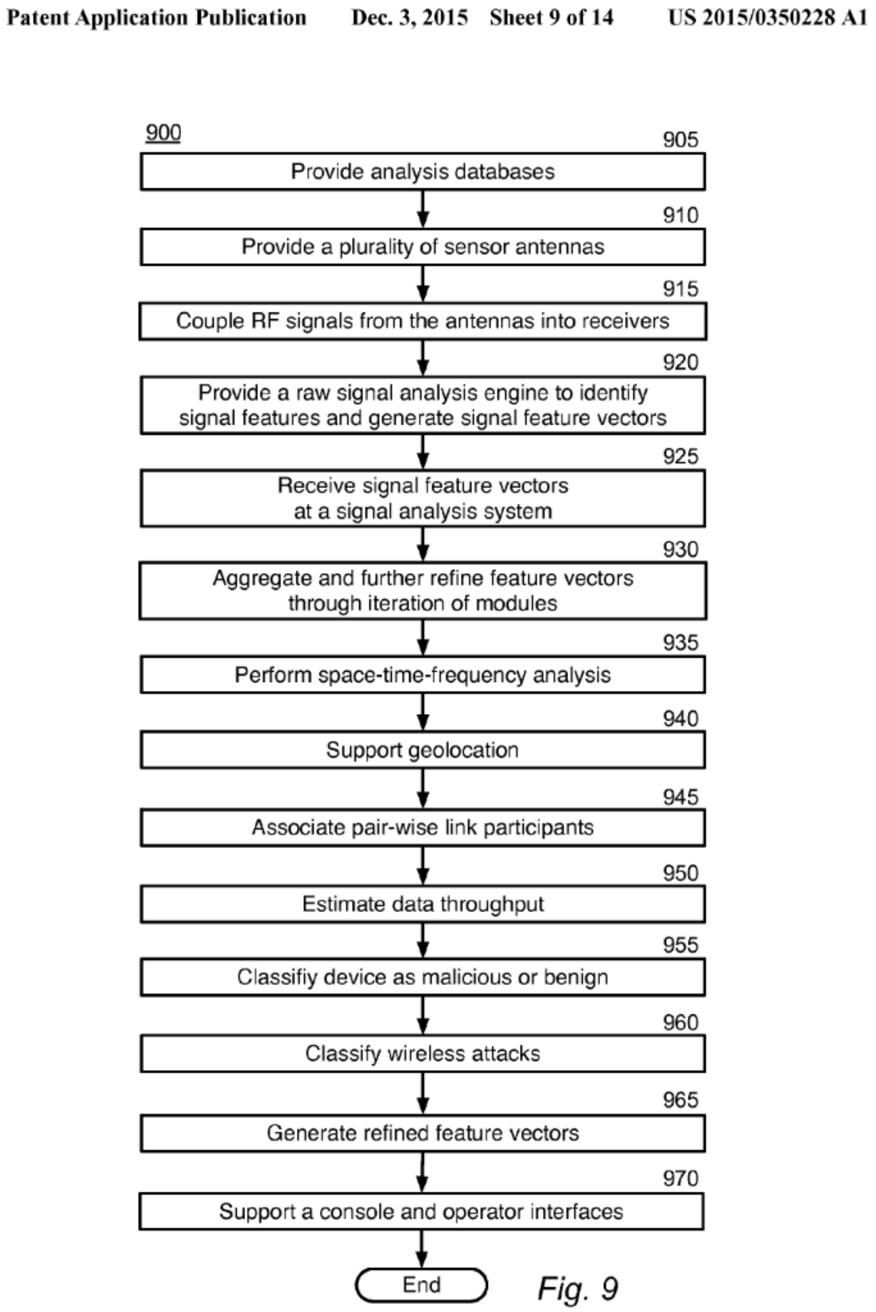
Patent Application Publication Dec. 3, 2015 Sheet 9 of 14 US 2015/0350228 A1
900
905
Provide analysis databases
910
Provide a plurality of sensor antennas
915
Couple RF signals from the antennas into receivers
920
Provide a raw signal analysis engine to identify signal features and generate signal feature vectors
925
Receive signal feature vectors at a signal analysis system
930
Aggregate and further refine feature vectors through iteration of modules
935
Perform space-time-frequency analysis
940
Support geolocation
945
Associate pair-wise link participants
950
Estimate data throughput
955
Classifiy device as malicious or benign
960
Classify wireless attacks
965
Generate refined feature vectors
970
Support a console and operator interfaces
End
Fig. 9

Figure 1: Block flow diagram depicting a method for signal analysis to support electromagnetic signature analysis and threat detection [5]

2.2 Application to EMFI exploits

This electromagnetic mean for exploits detection has already been used for attacks of the EM fault injection (EMFI) type. This kind of attack consists in a highly efficient fault injection, which shows much greater results than many of its counterparts, due to its peculiar capacity to incur local faults into security integrated circuits.

Indeed, a conference paper [6] from Temasek Laboratories and Nanyang Technological University Singapore present with an all digital countermeasure for an on-the-fly detection of the EMFI attempts on targeted silicon chips. In this study, a Hogge Phase Detector was used to sense the frequency turbulences induced by the ongoing EMFI, and a watchdog ring-oscillator enabled to sort out its output.

The fault detection rate of 93.15% of the implemented device proves the efficiency of such a technology and its associated methods.

2.3 Application to hardware trojans

Another paper [7] from CEA-Tech, Telecom ParisTech, Secure-IC and the EMSE present us with a way to detect hardware trojans using electromagnetic detection. A hardware trojan is a subclass of the trojan attack, which consist in hiding malicious content inside code, thus enabling obstructions to the code's function through, for instance, predefinite overrides of fonctions or backdoors in the system. In the case of a hardware trojan, the derivation is made on the chip itself instead of in the software, what causes its detection to be even more complex, as the testing of electronic components admits a far wider margin of mistake than that of code.

As the electromagnetic emission of a piece of hardware depends on its size, the bigger the hardware trojans compared to the size of its original host, the easier detection is. In the case of this study, the researchers managed to reach a minimum 95% standard accuracy - with a false negative rate of 5% - for a hardware trojan of 1.7% of original circuit's size (taking into account the inter-die process variations with a set of FPGA).

2.4 EM-Based Detection of Deviations in Program Execution

Also, the electromagnetic detection of exploits can be used for software exploits, as it was in the study [8] on the system ElectroMagnetic-Based Detection of Deviations in Program Execution (EDDIE). It uses electromagnetic detection to spot anomalies in program execution, such as malware and other code injections.

The device functions with two main phases: learning and monitoring. During its learning period, it does not need any unsane input. Absolutely no characterisation of the infection, or even its effect or its type is needed. Just as the others, the second phase consists in detecting anomalies in the electromagnetic field and analysing them as the results of attacks.

Not needing any background data on the exploit it monitors enables EDDIE to be a powerful and highly versatile tool. It is very suited for security monitoring of embedded and IoT devices. On real IoT objects, it proved to be very accurate, as to spot brief bursts of activity (a few milliseconds) and even the results of the addition of a few lines to existing loops.

3 IDS based on acoustic emissions

Acoustic emissions of computers or electronic devices are a physical signal that can be measured and used in many ways, to check authentication or integrity of the system. Indeed some IDS are based on audio fingerprints and are adapted to some connected objects.

3.1 Audio Fingerprinting

3.1.1 Definition of audio fingerprinting

Comparing an audio signal and linking it to metadata is difficult because of the diversity of audio formats and its high dimensionality, the significant variance of the audio data for perceptually similar content and the huge collection of fingerprints needed for efficient comparison. According to a review [9] about audio fingerprinting, the only way to make such analysis on audio signal is audio fingerprinting. Audio fingerprinting extracts a complex signature of a piece of audio content, i.e. a fingerprint and stores it in the database. To identify an unlabeled audio, its fingerprint is calculated and matched against those stored in the database. Using fingerprints and matching algorithms, distorted versions of a recording can be identified as the same audio content.

3.1.2 Audio fingerprint calculation system requirements

An audio fingerprint can't be a simple hash value, a fingerprinting system has to fulfill some requirements. First it has to be functionally efficient : it can identify an item regardless of the level of compression and distortion or interference in the transmission channel, so it must be robust. It also must be computationally efficient, which means that the cost of the calculation of the fingerprint in terms of resources should not be too high. This cost is related to the size of the fingerprints and the complexity of search and calculation algorithms.

3.1.3 Applications in IDS

An IDS aims to detect an intrusion in the monitored system. For some systems, using acoustic sensors to get audio record from this system during its operation and compare it to a collection of fingerprints can detect a malfunction of the system. This method requires to have first registered an important collection of fingerprints in relation to the normal operation of the system, so the comparison enables detection of a malfunction. The figure below, from the review about audio fingerprints [9], shows how audio fingerprints can test data integrity.

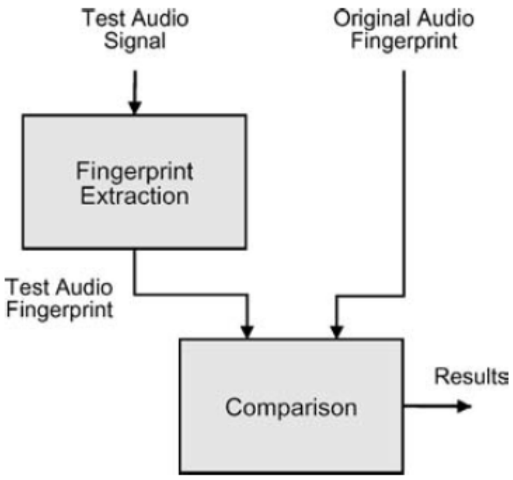

Figure 2: Integrity verification framework [9]

3.2 Example of an IDS using audio fingerprints

3.2.1 System description

A paper [10] describes an IDS aiming to detect a malfunction in a 3D printing process and stop the printing process to compromise objects. This system uses sounds generated by onboard stepper motors to do such detections, by using two algorithms. The first one records sounds and calculates a master audio fingerprint during the printing process, and the second one compares these fingerprints to those stored in a database. The system evaluates in real time the deviation due to tampering and is able to stop the compromised printing process, saving time and preventing material waste.

3.2.2 System limits

a) Detection limits

Detection limits are related to the minimal malicious deviations that can exist in the input file (STL or G-Code commands) of the 3D-printer. The study [10] shows that unit command modification are detected but some modifications of parameters in those commands can be undetected. Furthermore, an audio recording can be altered by the choice of the recording device, its recording position and, in a limited way, background noise. These factors influence the recorded signal and can cause false positive detections.

b) Algorithms limits

The pattern comparison is a frame-by-frame pattern checking, so the algorithm is based on time synchronization. That's why a momentary mismatch that does not break the overall synchronization can cause false positive detections.

Conclusion

In this paper, we presented several recent studies linked with Intrusion Detection Systems based on physical data. Indeed our project is to develop such a system in order to identify, non intrusively, when an IoT device is being attacked. Attacks on IoT devices can be detected by monitoring side channels such as power consumption, electromagnetics and acoustics emissions as we reviewed but also light emissions, temperature, etc...

With regard to power consumption monitoring, three papers were discussed demonstrating the relationship between attacks and current deviations [4], evaluating different variations of machine learning algorithms to efficiently detect malware attacks [3] and explaining a way to extract signals from power consumption traces and use them to identify if unknown code is executed [3].

With respect to electromagnetic emissions monitoring, four different systems were presented: one system using radio frequency signatures to detect threats [5] and three others using other electromagnetic emissions. One system was based on the impacts of electromagnetic emissions on a ring oscillator to identify electromagnetic fault injections [6], one focused on detecting hardware trojans [7] and another one, EDDIE [8], addressing the discovery of abnormal program executions on embedded devices.

In terms of acoustic emissions monitoring, the audio fingerprinting technique was explained (based on a review [9]) as well as its relevance in IDS. We also described an example of its use to detect malfunction in a 3D printer [10] and its limits.

These studies will be useful for our project to design systems to monitor power consumption, electromagnetic and acoustic emissions and to implement machine learning algorithms to analyze all the collected physical data. However, these papers don't cover all the physical side channels that could be used. Other physical data such as light emissions and temperature variations need to be considered.

Indeed, these detection systems are not fully developed yet in IoT devices: they are rather specific to one physical side channel, one system or one type of attacks and are not generic to all kinds of devices. Moreover, they are still at the experimental stage with other studies currently being made. As this subject is of great concern in the field of IoT security, our project aims to contribute in its evolvement, trying to cover the different physical side channels mentioned.

References

[1] M. Antonakaki, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the mirai botnet," in *USENIX Security Symposium*, 2017. [Online]. Available: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf

[2] S. S. Clark, B. Ransford, A. Rahmati, S. Guineau, J. Sorber, W. Xu, and K. Fu, "Wattsupdoc: Power side channels to nonintrusively discover untargeted malware on embedded medical devices," in *Presented as part of the 2013 USENIX Workshop on Health Information Technologies*. Washington, D.C.: USENIX, 2013, p. 11. [Online]. Available: https://www.usenix.org/conference/healthtech13/workshop-program/presentation/Clark

[3] Y. Liu, L. Wei, Z. Zhou, K. Zhang, W. Xu, and Q. Xu, "On Code Execution Tracking via Power Side-Channel," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16*, 2016, pp. 1019–1031. [Online]. Available: https://doi.org/10.1145/2976749.2978299

[4] D. Myridakis, G. Spathoulas, A. Kakarountas, D. Schoinianakisy, and J. Lueken, "Anomaly detection in IoT devices via monitoring of supply current," in *21st Pan-Hellenic Conference*, Sep. 2018, pp. 1–4. [Online]. Available: https://doi.org/10.1109/ICCE-Berlin.2018.8576178

[5] R. J. Baxley and C. J. Rouland, "Electromagnetic threat detection and mitigation in the internet of things," *United States Patent Application Publication*, p. 10, Dec. 2015. [Online]. Available: https://patents.justia.com/patent/20150350228

[6] J. Breier, S. Bhasin, and W. He, "An electromagnetic fault injection sensor using hogge phase-detector," in *2017 18th International Symposium on Quality Electronic Design (ISQED)*, March 2017, pp. 307–312. [Online]. Available: https://doi.org/10.1109/ISQED.2017.7918333

[7] X.-T. Ngo, I. Exurville, S. Bhasin, J.-L. Danger, S. Guilley, Z. Najm, J.-B. Rigaud, and B. Robisson, "Hardware Trojan Detection by Delay and Electromagnetic Measurements," in *Design, Automation and Test in Europe 2015*, Grenoble, France, Mar. 2015. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01240239/file/15_DATE_Trojans.pdf

[8] A. Nazari, N. Sehatbakhsh, M. Alam, A. Zajic, and M. Prvulovic, "Eddie: Em-based detection of deviations in program execution," *ACM SIGARCH Computer Architecture News*, vol. 45, pp. 333–346, Jun. 2017. [Online]. Available: https://doi.org/10.1145/3140659.3080223

[9] P. Cano, E. Batlle, T. Kalker, and J. Haitsma, "A review of audio fingerprinting," *Journal of VLSI signal processing systems for signal, image and video technology*, vol. 41, no. 3, pp. 271–284, Nov 2005. [Online]. Available: https://doi.org/10.1007/s11265-005-4151-3

[10] S. Belikovetsky, Y. Solewicz, M. Yampolskiy, J. Toh, and Y. Elovici, "Detecting Cyber-Physical Attacks in Additive Manufacturing using Digital Audio Signing," May 2017. [Online]. Available: https://arxiv.org/pdf/1705.06454v1.pdf