Journal of Manufacturing Systems 59 (2021) 27–41

Contents lists available at ScienceDirect

Journal of Manufacturing Systems

journal homepage: www.elsevier.com/locate/jmansys

Technical Paper

Towards secure cyber-physical information association for parts

Michael Sandborn [a,*], Carlos Olea [a], Jules White [a], Chris Williams [b], Pablo A. Tarazaga [b], Logan Sturm [b], Mohammad Albakri [b], Charles Tenney [b]

[a] Department of Computer Science, Vanderbilt University, Nashville, TN 37212, United States
[b] Department of Mechanical Engineering, Virginia Tech, Blacksburg, VA 24060, United States

ARTICLE INFO

Keywords:
Cyber-physical system security
Manufacturing security
Counterfeit detection
Supply chain security
Real-time verification
Distributed supply chains

ABSTRACT

Counterfeiting is a significant problem for safety-critical systems, since cyber-information, such as a quality control certification, may be passed off with a flawed counterfeit part. Safety-critical systems, such as planes, are at risk because cyber-information cannot be provably tied to a specific physical part instance (e.g., impeller). This paper presents promising initial work showing that using piezoelectric sensors to measure impedance identities of parts may serve as a physically unclonable function that can produce unclonable part instance identities. When one of these impedance identities is combined with cyber-information and signed using existing public key infrastructure approaches, it creates a provable binding of cyber-information to a specific part instance. Our initial results from experimentation with traditionally and additively manufactured parts indicate that it will be extremely expensive and improbable for an attacker to counterfeit a part that replicates the impedance signature of a legitimate part.

1. Introduction

Safety-critical cyber-physical systems (CPSs) [1], such as automobiles, planes, and heavy equipment rely on complex distributed supply chains that source parts from manufacturers across the world. For example, the production of over two thirds of the physical parts in the Boeing 787 were outsourced to third-parties [2]. A fundamental problem that these systems must contend with is ensuring the integrity of both the cyber components and physical parts that they receive through their supply chain. Because of the separation between the manufacturer and the consumer of the part, there are immense challenges in ensuring that physical parts arrive from the desired source and are not modified or swapped for inferior copies in transit. The Global Brand Counterfeiting Report for 2018–2020 estimates that the total amount of counterfeiting globally will reach 1.82 Trillion USD by the year 2020 [3]. Counterfeiting is a major concern to the aerospace and automotive supply chains as it poses not only risk of intellectual property theft (i.e., unlicensed copies of parts entering the black market) but also risk of system failure and loss of life due to the accidental use of poor quality fake parts. The U.S. Department of Homeland Security reported that the number and value of seizures of counterfeit automotive parts increased by 83% and 66% respectively between 2015 and 2016 [4]. The Aerospace Industries Association stated in a 2011 report that "though we know counterfeit parts enter the aerospace supply chain, the time and place of their entry is unpredictable" [5].

Cyber-physical systems relate the properties and dynamics of the physical parts in the system (e.g., jet engine turbines) with the cyber components (e.g., engine control algorithms). Tampering with either the cyber components or the physical parts of these systems introduces significant cyber-physical security risk, i.e. adverse effects in physical space manifested by exploiting vulnerabilities in cyber components of the system. While we have existing cyber-security techniques, such as roots of trust and signing chains, to help ensure software integrity, we lack roots of trust and signing chains that can guarantee the source of the physical parts and the information associated with them. There are a number of threats that a CPS built using parts from a distributed supply chain must contend with in order to maintain the integrity of the whole system:

- Counterfeiting: Malicious facilities can produce illegitimate copies of parts that appear correct at a surface level, but exhibit different performance characteristics [6]
- IP Theft: Both physical parts and their digital twins can be intercepted in the supply chain and digital thread, respectively, for unlicensed reproduction [6]

* Corresponding author.
E-mail addresses: jules.white@vanderbilt.edu (J. White), cbwill@vt.edu (C. Williams), cbwill@vt.edu (C. Tenney).

https://doi.org/10.1016/j.jmsy.2021.01.003
Received 6 October 2020; Received in revised form 7 January 2021; Accepted 8 January 2021
Available online 5 February 2021

- Part Tampering: Parts can be modified en route to their destination [7]
- False Certification: Parts can be sold with fake attestations regarding the legality, testing, or other aspects of the part [8]

All of these are attack vectors through which malicious actors may compromise quality control procedures for parts. The proposed method improves the integrity of quality certifications for manufactured parts in supply chains, thereby reducing the likelihood of attacks resulting in the use of counterfeit parts in CPSs. A severe risk of current practice is that it is difficult to provably link cyber-information, such as a CT scan for quality control of a part [9], to the specific physical part instance for which it was created. For example, a manufacturer can send a 3D printed fuel injector for a jet engine to be CT scanned for integrity and a digital certification of the part can be created to be sent to the purchaser of the part. An attacker who has the CT scan or other certification data for an authentic part can simply produce a counterfeit part, clone any physical identifiers (e.g., serial numbers, etc.), and claim that the authentic certification data is for the cloned part. In reality, the counterfeit part may have significant manufacturing flaws that create safety risks. However, the consumer of the counterfeit part instance will believe it is safe when provided the CT-scan for the real part instance. There is a clear need to provably tie the cyber-information to a specific part instance to mitigate this vulnerability.

Isn't this just a quality control problem? Manufacturers can and do use quality control checks to ensure that physical parts meet many different types of technical specifications. However, these procedures are not securely linked to each part instance's cyber data (e.g., certifications), and for many types of complex parts, the quality control checks are extremely expensive and cannot detect all types of defects. Defective or counterfeit parts can also be slipped into a supply-chain after quality control has been performed. In addition, the integrators of the complex systems (e.g., Boeing, Northrop Grumman, Ford) often rely on the Tier 1 suppliers to perform these quality checks and assume security in a part's transit through the supply chain. Many lower tier suppliers are much less stringent in determining the origin and authenticity of parts. Each station along a supply chain introduces an additional point in which a malicious part could be injected. Contrast this with the cyber world where we use hashes and signatures to guarantee the integrity of data after transmission – we don't execute and functionally test software components at each network hop to see if their underlying bits have been tampered with.

Solution Approach → Signed Physically Unclonable Identities. This paper introduces initial work on a possible physically unclonable identity and method to provably link cyber-information to specific part instances. The approach is based on using (i) a physical measurement technique (electromechanical impedance) to provide parts with an unclonable physical identity and (ii) Public Key Infrastructure (PKI) approaches to sign impedance measurements and provably bind cyber-information to specific part instances. We call the overall approach Signed Physically Unclonable iDentities (SPUDs).

The key research contributions of this paper are:

- Each individual part *instance* can be uniquely identified by its impedance identity (which is unique to each part instance due to inherent variation in the manufacturing process, the sensor, and the sensor configuration) without reliance on a printed or physical serial number.
- The origin of parts can be verified by checking if the impedance identity for a part has been signed by the private key of the expected source of the part.
- Counterfeits or unauthorized productions of the part can be detected by measuring an impedance identity and comparing it against the set of signed/licensed impedance identities for valid part instances.
- **Cyber-information can be provably tied to a specific physical part instance's unique and unclonable impedance identity using cryptographic techniques**.
- Initial experimental results show that the approach provides defenders a significant cost advantage over attackers when trying to ensure that cyber-information is tied to a specific physical part instance.

The remainder of this paper is organized as follows: Section 2 compares SPUDs to related work; Section 3 outlines the SPUD approach; Section 4 presents results from experiments testing the SPUD hypotheses; Section 5 presents a taxonomy of cybersecurity hazards and defenses for SPUDs; Section 6 discusses future work and open research questions regarding SPUDs; and Section 7 provides concluding remarks.

2. Related work

Physically unclonable functions [10–12] have been investigated for circuits to provide a foundational building block for security. A Physically Unclonable Function (PUF) uses physical characteristics of the circuit's manifestation to generate unique keys or other security primitives. There is ongoing work to understand how unclonable the functions are. The physically unclonable identities in this paper are a form of physically unclonable function targeting identification of physical parts (e.g., rotors, screws, impellers, etc.) as opposed to creating security primitives for circuits. Future work may show that impedance identities could be helpful in creating physically unclonable functions for circuits or that techniques from this domain could be used to improve SPUDs. A key difference between PUFs and SPUDs is that unlike the Challenge-Response Pairs (CRPs) of a PUF, which are expected to be fixed input and output values for the lifecycle of the circuit, the impedance identity of a SPUD is subject to slight variation between multiple measurements for the same part instance. This variation is related to several factors including the physical condition of the part, properties of the attached sensor, and measurement environment conditions. In this work we propose a method to attribute impedance identities with minimal variation tolerance to uniquely identify a single part instance.

Fuzzy Extractors [13–15] are functions that take a possibly noisy physical measurement and reliably produce a key that can be matched for security purposes. For example, fuzzy extractors for biometrics have been studied to reliably create keys using inherently noisy biological measurements. Continued development and analysis of SPUDs will require application of fuzzy extractor research to impedance identity representation and matching algorithms. The paper presents an initial identity matching representation and algorithm, but we expect that significant improvements in design and analysis can be made with insights from fuzzy extractor research. An important distinction from fuzzy extractors is that the identities do not need to serve as encryption keys, they just need to have a low enough probability of being physically replicated that they become expensive to counterfeit. Future work will explore how impedance identities vary across many measurements for a single part instance as well as additional methods to approximately match SPUDs to accommodate noisy measurements while preserving SPUD uniqueness for individual part instances. Fuzzy extractors and approximate hashing techniques are promising directions to address these issues.

Part Identifiers have been investigated to prevent counterfeiting both from a physical and cyber perspective. Vehicle identification numbers [16], engraved serial numbers, and holographic stickers [17] are all examples of physical countermeasures that have been developed. [18] proposes impedance-based analysis for part authentication and detection of defects such as internal voids. Some work has looked at permanently attaching RFID tags to parts in a way that the tag cannot be removed without destroying it [19,20]. The SPUD approach is similar, but relies on a physically unclonable function as opposed to the security

of the physical attachment mechanism. Attachment mechanism security is similar to past physical security mechanisms and does not rely on physically unclonable functions. Others have looked at manufacturing unique attributes into additively manufactured parts [21]. However, these unique attributes inserted into the layers of an additively manufactured part instance are still clonable if they are observed correctly, as opposed to impedance identities, which are not clonable. SPUDs can also be used in conjunction with existing physical countermeasures, such as holographic stickers. The core motivation for SPUDs is that manufactured parts are currently labeled and identified according to a shallow identification scheme e.g., a bar code or serial number intended to designate a single part instance. These identifiers can be easily removed or cloned by a malicious entity to indicate that a counterfeit part is authentic. SPUDs serve as deep identifiers for individual part instances, capturing both the physical characteristics of a part instance as well as inherent variation in material properties of the attached piezoelectric sensor instance.

Blockchain in Manufacturing [22] discusses the use of digital twins combined with Blockchain for effective manufacturing service collaboration and data sharing. [23] proposes a data management method using Blockchain to ensure the integrity of product information and transparent collaboration between multiple parties in a manufacturing network. [24] presents the use of Blockchain combined with PUFs from Integrated Circuits (ICs) to track and detect counterfeit ICs in supply chains. Blockchain is an information exchange framework that helps guarantee the integrity of information through consensus and trust mechanisms. Combining a framework such as Blockchain with a physically derived identity (PUFs or SPUDs) allows a powerful way to ensure the authenticity of physical objects across manufacturing supply networks. An information exchange framework helps guarantee the integrity of information as well as sender and receiver identities in the cyber domain, while the physical identity helps guarantee the quality of parts as they are transported across a supply chain. In this work, we discuss Public Key Infrastructure (PKI), a provably secure, widely used information exchange framework to combine with SPUDs as one approach to address counterfeit part detection. Future work will include evaluation of other frameworks such as Blockchain and similar methods.

3. Signed physically unclonable identities

SPUDs rely on the ability to generate a unique identity for nearly every rigid physical part instance on the planet without relying on a physical or printed identifier. We believe the identity of the part instance is based on a physically unclonable function [10–12] and makes production of another part with the same identity hard or cost prohibitive (or impossible – but this needs further research). Similar approaches have been investigated in physically unclonable functions, which build security in circuits by using physical characteristics that are unclonable to produce security primitives. Throughout the paper, we use the term physically unclonable identity, which is the output read from the physically unclonable function, and we compare SPUDs with physically unclonable functions in Section 2. This paper presents initial results showing that impedance identities can be used for this unclonable identity – although we acknowledge the community as a whole needs to do additional work to fully explore the potential of these identities. The results indicate that, at a minimum, SPUDs will make counterfeiting a part instance with an existing part instance's identity much more expensive. An overview of the proposed method is shown in Fig. 1.

A key insight is that once a part's identity cannot be forged, the identity can be incorporated into traditional signed messages. These messages can carry critical cyber-information regarding parts, such as certifications from manufacturers, IP holders, or testing facilities. Because the messages are signed and carry the unclonable identity of a part, information and the sources of that information can be provably tied to a specific part instance. Finally, detection of counterfeits and verification of cyber-information attached to parts can be performed using well understood Public Key Infrastructure (PKI) techniques.

3.1. Measuring part impedance identities

The insight for this proposed cyber-physical integrity system came from challenges in our prior research in manufacturing cyber-security. Past work has explored the use of electromechanical impedance measurements as a means to detect and identify additive manufacturing (AM) defects and cyber-attacks [25,26]. A vibration-based damage identification technique, impedance measurements have laid the foundation for impedance-based Structural Health Monitoring (SHM) as a promising, non-intrusive, highly-sensitive solution for real-time damage assessment [27]. In its most practical form, impedance-based SHM employs piezoelectric (e.g. lead zirconate titanate, PZT) wafers as collocated sensors and actuators to simultaneously excite the structure of interest and measure its response [28]. A PZT wafer is first attached to the part under test, as shown on the left of Fig. 2. Due to the coupled electromechanical characteristics of piezoelectric materials, the electrical impedance of the PZT wafer is related to the mechanical impedance of the host structure, as depicted on the right of Fig. 2. The figure shows a representative experimental setup with schematics of the instrumentation of the part under test and a single degree of freedom representation that approximates the response near any individual resonance.

The electromechanical impedance of the PZT wafer, as a function of frequency ω, can be expressed as [28]:

$$Z(\omega) = \left[i\omega \frac{\mathrm{bl}}{h} \left(\frac{d_{13}^2}{s_{11}^E} \left(\frac{tan(\mathrm{kl})}{\mathrm{kl}} \left(\frac{Z_{\mathrm{PZT}}}{Z_{\mathrm{PZT}} + Z_{\mathrm{ST}}} \right) - 1 \right) + \varepsilon_{33}^{\sigma} \right) \right]^{-1}$$

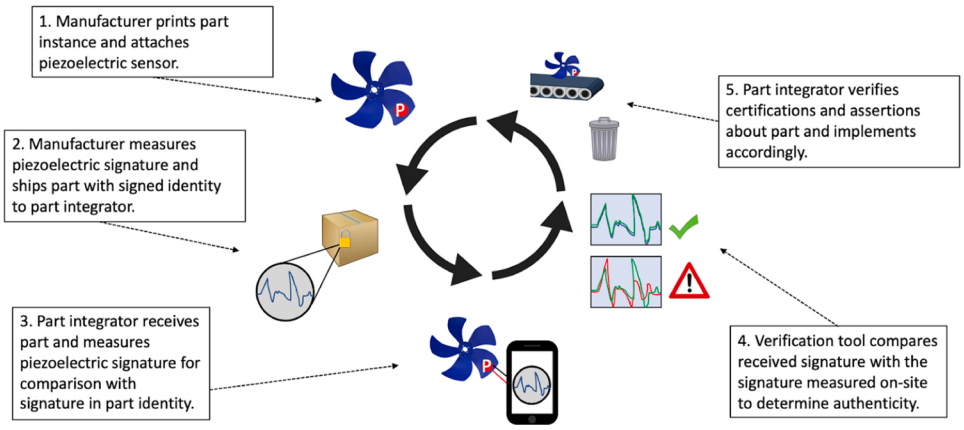

Fig. 1. Signed physically unclonable identities overview.

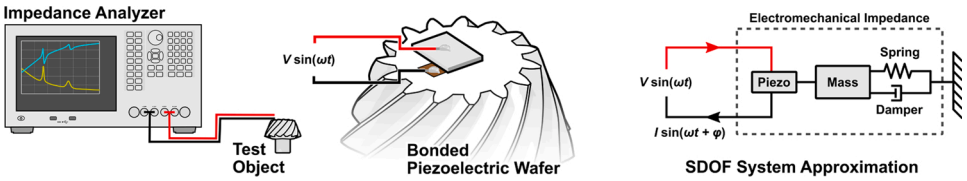

Fig. 2. Physical measurement of impedance identities.

where Z_{PZT} is the piezoelectric transducer short circuit impedance, $Z_{ST} = f(m,k,\zeta)$ is the mechanical impedance of the part under test. d_{13} is the piezoelectric coupling coefficient, s_{11}^E is the mechanical compliance of the piezoelectric material measured at zero electric field, $\varepsilon_{33}^{-\sigma}$ is the materials permittivity measured at zero stress. $k = \omega(\varrho s_{11}^E)^{1/2}$ is the wave number, ϱ is the density of the piezoelectric material, b, h, $2l$ are the piezoelectric patch width, thickness and length, respectively. Thus, the fundamental characteristics of the part under test, such as its mass (m), stiffness (k), and damping (ζ), can be inferred from the easily measured electrical impedance of the PZT wafer.

The fundamental basis of this technique is that the presence of damage (i.e., physical change) in a part will alter the inherent mass, stiffness and damping characteristics of the structure, which in turn will be reflected in the measured dynamic response. Impedance-based SHM has been successfully applied to detect damage in numerous civil, aerospace, and mechanical components and structures, including composite structures [29], wind turbine blades [30], and space structures [31].

Prior work on manufacturing cyber-physical security has explored cyber-physical approaches to use manufacturing side-channels, such as vibration, acoustics, and network traffic, to detect cyber-attacks [32–34, 26,35–37]. Piezoelectric impedance monitoring is a promising technique that works for detecting malicious changes to parts as it is responsive to small changes/defects in fabricated parts. Past work has hypothesized that, by comparing the impedance identity of a known, defect-free part against that of subsequently fabricated copies, a manufacturer would be able to detect defects from process variation and malicious cyber-attack. Researchers have explored the adaptation of this SHM technique as a both a post-process non-destructive evaluation tool [25] and as an in-situ side channel measurement technique [26]. However, the use of impedance measurements as a comparative evaluation technique across different components is inherently limited, as there exists variation in the signatures from individual parts produced with the exact same processes and part specification.

3.2. An unclonable cyber-physical identity with impedance identities

If the CPS system integrator could know without question the real identity of a part, they could (i) check its origin and (ii) access the related digital thread data that has been accumulated throughout its lifecycle (e.g., certifications, IP licensing, etc.). The naive approach to solving this identity problem is to simply apply a serial number to the part itself. The manufacturer then provides a database of authorized part serial numbers that the part can be checked against. For example, the part's serial number can be engraved into the part during machining/molding, 3D printed directly onto its surface, or painted on as the last step in manufacturing. However, the serial numbers can be easily cloned and applied to illegitimate parts, so that they match up against a legitimate entry in a part database. Engraved/embossed identifiers can be cloned via 3D scanning and/or removed through destructive means. The $1.82 Trillion in estimated global counterfeiting by 2020 speaks to the limitations of current approaches.

With the SPUD approach, the impedance signature of the sensor-part coupled system is tied intrinsically to its physical state. If either the sensor, the part, or the attachment of the sensor is altered, the identity of the part will change. More formally, attaching the piezoelectric sensor to the part creates an unclonable identity of the form:

$$I(p_i, s_j, a_k, \omega_m, \omega_n) = \begin{bmatrix} Z(\omega_m) \\ Z(\omega_{m+b}) \\ \vdots \\ Z(\omega_n) \end{bmatrix} \quad (1)$$

where:

- I - is the impedance identity of a part that is a physically unclonable function of the part, piezoelectric sensor, sensor attachment, and frequency range that impedance is measured at
- p_i - is the unique part instance
- s_j - is the unique piezoelectric sensor instance
- a_k - is the unique attachment of the piezoelectric sensor to the part
- b - is the frequency step size
- ω_m - is the lower bound frequency that impedance is measured at
- ω_n - is the upper bound frequency that impedance is measured at

The physically unclonable identity, I, is produced by attaching a piezoelectric sensor to a physical part instance (e.g., gluing the sensor to the part instance). The physically unclonable identity is based on the unique impedance characteristics produced by the combination of the part p_i, the piezoelectric sensor s_j, and the attachment of the sensor a_k. The identity is read by activating the sensor and measuring impedance across the frequencies $\omega_m \ldots \omega_n$. The identity of the part is the measured impedance at each frequency in the target frequency range.

The $< p_i, s_j, a_k >$ triple values cannot be engineered to clone a piezoelectric identity function. I then provides a means for producing unclonable part identity functions that are intrinsic to the part, sensor, and precise attachment of the sensor to the part. At manufacturing time, the $< p_i, s_j, a_k >$ triple can be produced by attaching a piezoelectric sensor to a part, which then produces an unclonable identity for the part. Our initial results, presented in Section 4, indicate that changing either the part instance, sensor instance, or attachment (e.g., placement, gluing, etc.) fundamentally changes the triple and creates a different set of impedance characteristics across the measured frequencies (changes the identity). The current cost of piezoelectric sensors in small volumes is on the order of $1 and the impedance analyzer needed to read signatures can range from $100 for a custom Arduino-based device to $20,000+ for a high-end commercial analyzer. The analyzer cost is fixed and only a single analyzer is needed to read signatures for multiple parts. However, the added sensor cost will limit application to domains where the added per-part cost is not cost-prohibitive and the added security is necessary.

3.3. Cyber-physical information association and provenance

How do we protect against an attacker counterfeiting a part, copying a serial number from a legitimate part, and claiming that it has a specific certification that was really generated for the legitimate part instance? We borrow a technique used in securing digital communications, Public Key Infrastructure (PKI), as an example to illustrate the use of the impedance identity with an existing information exchange framework with demonstrated security. The open problem with physical parts is that there is no verifiable connection between messages signed with a private key and a physical part. Consider the serial number of a part.

Though the cyber channel can be secure – the serial number can be sent as a signed message – the physical channel is not: an attacker can remove, alter, or replicate the serial number. There is no way to verify the link between a physical serial number and its signed message. This weakness on the physical side creates a low-cost attack point. By combining PKI with the impedance identity, information about the physical part is guaranteed by the impedance identity and the identities of the communicating parties as well as the integrity of the exchanged information is guaranteed by PKI.

The SPUD approach uses PKI to allow IP owners, certifiers, customs agencies, and others to verify the identity of a manufactured part. Producers of information about a specific physical part instance can first measure its impedance identity, then produce a signed message containing its identifier and other properties of interest. Signed messages can then travel with the part to verify its specific properties. The signed messages carry the physically unclonable impedance identity of the part instance and hence can be provably connected back to the specific physical part instance held by the receiver of the message. Any holder of the physical part instance can measure the unclonable impedance identity and then compare it to the identity contained in the signed message received with the physical part instance. For example, the IP holder of the design of a part can sign the impedance identity to prove that the production of the part was authorized and properly licensed. A certifier can test a part instance and sign the combination of the impedance identity and digital data to bind the certification to the specific physical part instance. We use the formal notation described in [38] to explain the protocol. The part holder, A, uses their private key, K_A^{-1}, to sign the part identity and generate a message that can be sent to an entity, B, along with the physical part, to verify properties of the physical part:

$$A \rightarrow B : \{C, I(p_i, s_j, a_k, \omega_m, \omega_n), O\}K_A^{-1} \tag{2}$$

where:

- A – is the certifier that will assert a property of the part p_i
- B – is a receiver of a physical part that needs to verify its integrity and information about it
- C – is the set of cyber-information being asserted by A (e.g., licensed, certified, etc.)
- $I(p_i, s_j, a_k, \omega_m, \omega_n)$ – is the unclonable identity of a part
- O – other parameters required for the signature and impedance identity matching
- K_A^{-1} is the private key for A

The signed assertion messages are produced by the different entities involved in attaching cyber-information to the part instance. For example, the manufacturer may not be the IP holder. The unclonable signatures can be produced in the manufacturing facility and sent to the IP holder for signature. The IP holder then sends back the signed assertion messages for each part instance indicating that they were licensed for production.

The signed assertion messages can be transmitted with the part (e.g., by including them in the packaging) or via the typical central database approach. However, the central database is not required in the approach. An entity, B, that wants to verify that cyber-information, C, was asserted by entity A for a specific physical part instance, p_i, uses the public key, K_A, of entity A, to verify that A is the source of the message, that the cyber-information in the message matches C, and that the impedance identity measured from the physical part matches the signature in the message. Additional parameters, O, can be included in the message and may include physical measurement parameters for obtaining the impedance identity, calibrating equipment, timestamping, nonces, etc.

The SPUD approach compares impedance identities of a particular part instance collected at different points in time. For example, if a part is certified and then an attacker drills a hole in the part, the assertion should no longer hold for the part. Modifying the physical properties of the part (e.g., drilling a hole and changing its geometry) will impact the impedance identity. If the part consumer receives a part, obtains its impedance identity, and it does not sufficiently match the signed impedance identity, then the part was tampered with at some point and hence its attached assertions should no longer match the part. This ability to detect tampering has important ramifications. There is the potential that an attacker could tamper with a part after a signed assertion (e.g., certification) is generated for the part. Our hypothesis is that tampering with the part will be detectable to a very fine level of detail. Prior work has shown that it is possible to detect physical part changes as small as 1mm with comparative impedance measurements [25]. This detection resolution has been limited due to the noise caused by using multiple sensors/parts and not attempting to repeatedly measure the signature of a single part instance and detect deviations. However, we believe that using the SPUD approach, where the goal is to uniquely identify individual part instances rather than perform quality control on classes of parts, we can identify changes at a much smaller granularity.

3.4. Matching impedance identities

A fundamental component of SPUDs is transmitting and matching impedance identities. We provide an initial representation and matching algorithm. We believe that there will be many possible signature representations and matching algorithms that could be used with SPUDs based on prior work from Fuzzy Extractors [13], ranging from approximate hashing to approaches based on mean squared deviation. A simple configurable matching algorithm is shown in Listing 1 and used to produce a simple cost model in the following section.

Listing 1. Identity Matching Algorithm

```
1  MsIdentity = [...] % measured impedance identity
2                     % of part instance
3  SdIdentity = [...] % target impedance identity in
4                     % signed msg
5  Tolerances = [...] % allowed impedance variation
6                     % from signed msg
7
8  for i=0; i < length(MsIdentity); i++
9    diff = abs(MsIdentity[i] - SdIdentity[i])
10   if diff > Tolerances[i]
11     return NO_MATCH
12
13 return MATCH
```

The impedance identity is transmitted as a vector of impedance values measured at each of the target frequencies, as shown in Line 3. The i_{th} element in the vector represents the impedance value of the i_{th} frequency. The minimum, maximum, and frequency step sizes are also transmitted in the message. The message also includes an allowed matching tolerance for the impedance value at each frequency, as shown on Line 5. The impedance value for the physical part being assessed is measured from the part at the specified frequencies and frequency step size to produce a vector as shown on Line 1. The algorithm performs a component by component comparison of the impedance vector values from the message and what was actually measured on Lines 8–11. If the absolute value of the difference between the impedance value from the signed message and the actual measured impedance value differ by more than the specified tolerance for the frequency, the impedance identity matching fails.

The algorithm relies on transmitting both the impedance identity and a set of allowed matching tolerances for the impedance values at each frequency. These tolerances can be set on a per-part instance basis and adjust for material or other variations, such as temperature and fixturing, that may introduce noise in repeated measurements. Section 4 provides example values for these tolerances derived from physical experiments and discusses the impact of noise on matching. Moreover, the tolerances may be adjusted on the fly as manufacturers produce greater numbers of a part and learn more about variations in the impedance

identities specific to the part's geometry, process, sensors, etc.

3.5. Attack cost model

Currently, the cost to produce a counterfeit part is often lower than to produce a legitimate part, since the counterfeiter may not adhere to legal, licensing, labor, quality, or other standards of a legitimate manufacturer. The key advantage of a SPUD is that it correlates with geometry and microstructural properties of a part that determine quality and performance. To produce a counterfeit part that replicates the impedance identity of a legitimate part, the counterfeiter needs to at least produce a part that is equivalent in quality to the legitimate part.

Are impedance identities truly unique and how expensive would it be to potentially replicate one? Can a counterfeiter manufacture a part instance that produces a collision with the impedance identity of an existing part? **An important note is that guessing to find a collision fundamentally requires manufacturing a physical part.** Each guess requires real manufacturing work that is much more expensive than the traditional guessing done when attempting to find hash collisions.

Regardless of the approach, the impedance identity matching algorithm needs to be robust to noise but still provide a significant cost advantage to a defender. In particular, any algorithm must consistently match impedance identities over time as a part is handled, shipped, etc. Let:

$$I_{t_0}^{p_i} = I(p_i, s_j, a_k, \omega_m, \omega_n) \tag{3}$$

be the impedance identity of part, p_i, measured at time t_0. Assume that an algorithm will match all signatures that differ by at most α. We will assess algorithms based on their ability to guarantee that all impedance identities measured up to a future point in time, t_i, also match (or provide reasonable long-term stability):

$$\forall t_i \in T(|I_{t_i}^{p_i} - I_{t_0}^{p_i}| < \alpha) \tag{4}$$

Noise is inherent in these types of physical measurements and all signature matching approaches will need to minimize α for the same part. The value of α corresponds to the fidelity that impedance identities can be stably matched over time and directly influences the cost for an attacker to try and produce a counterfeit part that replicates the signature:

$$\mathrm{AC} = \frac{\mathrm{Cost}_{p_i}}{P(|I_{t_i}^{p_k} - I_{t_i}^{p_j}| < \alpha)} \tag{5}$$

The cost, AC, for an attacker to produce a counterfeit physical part, p_k, that replicates a signature for a valid part, p_j, will inherently be based on the cost to produce a physical instance of the part, Cost_{p_i}, divided by the probability that part instance will match the target impedance identity, $P(|I_{t_i}^{p_k} - I_{t_i}^{p_j}| < \alpha)$. The hypothesis is that as α shrinks, the attacker will have to make more and more physical instances of the part to successfully produce a single instance that collides with the target impedance identity of an existing legitimate part. If the attacker has a perfect process and analysis, they can produce parts for roughly identical costs to legitimate parts (leaving aside other manufacturing advantages). We are unaware of any two parts that have ever been produced with identical impedance identities.

An important ramification of the approach is that to generate a counterfeit part that produces a collision with the impedance identity of a legitimate part, you must produce a physical copy that is similar in quality and performance – otherwise the geometry and microstructure of the physical part will produce a different impedance identity. This has the ramification that security is immediately improved simply by: 1) ensuring that any counterfeit parts will be similar in cost to produce as the defender's parts and 2) the quality of the counterfeits will need to be high in order to collide with a signature for a legitimate good part. First, to have any possibility of a signature collision, the material, process, and geometrical properties of the part, all of which determine the quality of the part, must be identical or near identical to a legitimate part. This relationship between quality and impedance identity was part of our and others' prior work. Counterfeiters cannot get away with producing poor quality parts and hope to collide with a legitimate impedance identity as quality failures will inherently move their signatures into different parts of the impedance identity address space from legitimate good parts (see Section 3.6).

3.6. Address space size and collision probability

A question that impacts the cost, AC, to produce a counterfeit part that replicates an existing signature is how large the "address space" is for the impedance identities that are generated. There are two components to this question: 1) how many part instances could theoretically have completely unique impedance identities given what we know about impedance identity behavior and 2) how likely is a random impedance identity collision in this address space. The larger the address space and the less likely a random collision is, the smaller the denominator in Eq. (5) will be and the more expensive attacks will be.

For an address space of size N, if k addresses are randomly generated, the probability of a collision is approximated by [39,40]:

$$1 - e^{\frac{-k(k-1)}{2^{N+1}}} \tag{6}$$

The number of bits in the address is N and the number of randomly generated addresses is k. For a 32-bit address space, there is a roughly 50% probability of a collision when $k = 77163$ [40]. However, if the addresses are not generated randomly, the probability of a collision may be higher or lower. If the addresses are biased to a small slice of the address space, then collisions will be more probable.

The impedance identity is not designed to be used as a cryptographic key and may be guessable. However, manufacturing a part to match a known impedance identity is beyond the current state of knowledge in manufacturing. Therefore, any attack using the current state of knowledge in manufacturing will be based on producing random collisions.

An estimate on the **upper bound** of the address space size for the impedance identity of the i_{th} part is given by:

$$\Omega = \frac{|\omega_n - \omega_m|}{\delta\omega} \tag{7}$$

$$N_i = \sum_{j=0}^{\Omega} \left(\left\lfloor \log(\sigma_k^j \beta_k^j U_i^j - \sigma_k^j \beta_k^j L_i^j) \right\rfloor - \alpha_i^j \right) \tag{8}$$

where:

- N_i – is the total number of usable bits in an impedance identity of an instance of the i^{th} part
- Ω – is the number of frequencies the signature is measured across and hence the number of impedance data points in the signature
- ω_m – is the minimum frequency of measurement
- ω_n – is the maximum frequency of measurement
- L_i^j, U_i^j – are the minimum and maximum impedance value at the j^{th} frequency for the i^{th} part
- β_k^j – is the measurement bias of the k_{th} piezoelectric wafer at the j^{th} frequency
- σ_k^j – is the measurement bias of the k_{th} piezoelectric wafer's a attachment to p_i at the j^{th} frequency
- α^j – is the loss of usable bits in a data point due to observed noise in repeated measurements of impedance (e.g., ±0.2 Ohm)
- $\delta\omega$ – is the step size that is used when incrementing frequencies

This estimate is only the *upper bound and not the actual address space size*. This estimate provides a simple test to determine if a part is unsuitable for a SPUD-based approach. If the upper bound on the address space size is too low for a given part design, then it is not worth using a

SPUD. If the part passes the upper bound test, empirical measurements are required to estimate the actual probability of an identity collision based on observed variation in impedance identities. We describe this analysis for several parts in Section 4.

An impedance identity of a part is made up of Ω data points, each containing some number of bits. Although each data point in an impedance value could have a potentially large range of values, those values will tend to fall into a much smaller range for a given part geometry, material, and process combination. That is, the shapes of impedance identities for the same part design and material will be similar at a macro level, limiting the range of values that any individual data point can take. As shown in Eq. (8), the number of bits in each data point at a given frequency is a log of the difference of the minimum and maximum impedance value that the the part can have at a given frequency minus the tolerance that individual data points can be matched within (some bits are lost due to inherent measurement noise). Since the specific piezoelectric wafer and its precise attachment (e.g., position, type/amount of glue, etc.) all impact the signature, coefficients are introduced to model the bias that these items introduce into the impedance measurements (β_k^j and σ_k^j).

As shown in Eqs. (7)–(8), the defender can control the size of the address space by adapting part geometry, material, piezoelectric wafer, wafer attachment, or the frequency range used. For the moment, we will assume that geometry and material are fixed, although this need not be the case. A simple technique that the defender can use to increase the size of the address space is to measure impedance across a wider range of frequencies. Particularly at higher frequency ranges, impedance identities are more distinct. Second, the defender can randomize the exact positioning or attachment of the piezoelectric wafer which creates noticeable changes in the impedance identity. Third, the defender can use piezoelectric wafers with highly variable qualities. All of these methods of manipulating the address space map directly back to the definition of an impedance identity function given by $I(p_i, s_j, a_k, \omega_m, \omega_n)$.

An impedance identity can then be represented by a concatenation of bits corresponding to each data point across Ω. A collision then would require identities of distinct part instances of the same model to have every investigated data point with an identical impedance– a condition that we hypothesize is sufficiently rare even for a large supply of the same part. The probability of this is further decreased with a greater number of data points, and a tighter bound for α^j at each point on the signature.

Assuming that a part can be interrogated at $\Omega = 400$ frequencies, each frequency produces an impedance value that differs by 36 Ohms (we ignore sensor/attachment bias for simplicity), the noise causes a loss of 1 bit of information, then the upper bound on the number of bits in each impedance identity will be:

$$N_i = \sum_{j=0}^{400} \left\lfloor \log_2(36) - 1 \right\rfloor = 1600 \tag{9}$$

Assuming that the manufacturer of legitimate parts produces 1,000,000 copies of the part and the upper bound on the address space mirrored the actual bound on total impedance identities, an attacker would have a probability of generating a random part with a colliding impedance identity of:

$$1 - e^{\frac{-1000000(999999)}{2^{1601}}} \approx \frac{1.12}{10^{470}} \tag{10}$$

Up to this point, we have assumed geometry is constant. Another strategy that will disperse these signatures is to randomly attach another structur to the part instance or alter the sensor attachment. These types of changes will alter the original signature in a non-deterministic way and creates a dynamic address space for impedance identities to further reduce the possibility of a signature collision. Fig. 3 demonstrates one of these methods. A piezoelectric wafer was moved from the base plate of the impeller to one of the 6 fins for additional measurements. This relocation resulted in a signature with similar characteristics as the others, but a different range of impedance values.

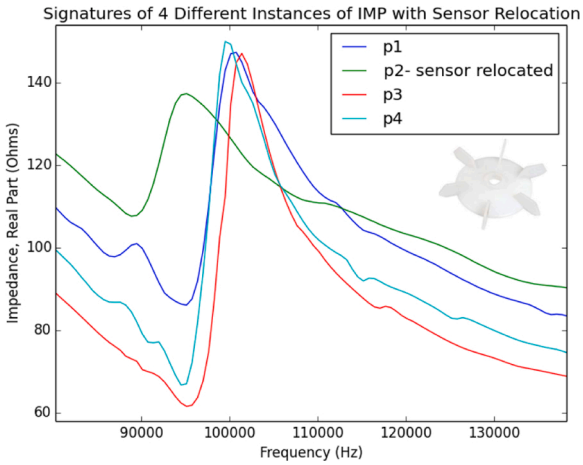

Fig. 3. Signatures for four part instances, one with sensor relocation.

3.7. Empirical measurement of part impedance identity variation

Although the upper bound on the impedance identity address space size for a part is helpful, the actual impedance identities may be distributed in different ways within the address space. The distribution of impedance identities for an arbitrary geometry, material, etc. is not feasible to predict and experimentation is required to derive actual distributions. Rather than calculating the probability of a collision solely based on an upper bound, a manufacturer can continuously update a collision probability based on comparing the Hamming distances of all parts produced to a given date.

As a manufacturer produces each part instance, they will measure its impedance identity and add it to a database of all part instance impedance identities. At any point in time, the manufacturer (or IP holder) can pair-wise compare the Hamming distance of each impedance identity to create an estimated probability mass function (PMF) for the impedance identities of the parts. Each pair-wise Hamming distance computation shows the "distance" between the impedance identities of two instances of the same part. The PMF shows the likelihood that the Hamming distance between two part instances' impedance identities, $I_{t_i}^{p_k}$, $I_{t_i}^{p_j}$, will be exactly a given value. The PMF can also be used to calculate the probability of two random parts being within a given Hamming distance from each other (e.g., within a collision threshold) and estimate a value for $P(|I_{t_i}^{p_k} - I_{t_i}^{p_j}| < \alpha)$. That is, the manufacturer can use empirical data to estimate the probability of two part instances having a Hamming distance close enough to generate a collision in impedance identity matching.

Similarly, the manufacturer can calculate the Hamming distances between repeated measurements of impedance identities for the same part instance. Using this data, the PMF for Hamming distances of repeated measurements of the same part can be built to model noise in the impedance identity. This PMF of the impedance identity measurement noise is likely to be useful in development of more advanced matching algorithms. Section 4 calculates the PMFs of the Hamming distances between different instances of the same part type and repeated measurements of the same part instance.

3.8. Impedance identity unpredictability

It is our conjecture that, given the number of sources of variance – in the manufacturing process, the raw material, the impedance sensor and its configuration – it is infeasible to produce a new physical part that replicates the impedance identity of an existing part to an arbitrary

degree of accuracy.

The difficulty stems from the fact that predictive numerical simulations at high frequency are prohibitively computationally expensive. In the case of finite element modeling, the cost of each element is low, but the number of elements required to produce an accurate dynamic model grows quickly with frequency. Alternative approaches, such as spectral element modeling, accept greatly increased per-element computational cost in order to create a model where high-frequency simulation is no more expensive than low-frequency simulation. However, the use of spectral element models quickly becomes intractable when the required number of elements is high (i.e. when the geometry is complex). Because the effect of small geometrical changes on the impedance identity is magnified at higher frequencies, geometrical accuracy requirements for the model grow with frequency, so the number of spectral elements required for an accurate model effectively increases with frequency as well. These challenges suggest that the task of creating a false impedance signature from a digital part model can be made arbitrarily difficult by increasing the frequency range of interest. Further, these difficulties are compounded when attempting the inverse problem: predicting the geometry that will produce a known impedance identity. The high computational cost of simply solving for the response of the part, along with the very large number of parameters that impact the impedance identity of a given part (which includes material and geometric characteristics of the part itself, the piezoelectric wafer, and the adhesive bonding layer), makes the task of reverse-engineering a part to match an existing impedance identity extremely difficult even in the case of relatively low frequency and simple part geometry [41].

4. Empirical results

4.1. Hypothesis 1: Each instrumented part has a unique impedance identity

Our hypothesis is that impedance identities are unique to individual parts, even among a set of parts with the same nominal geometry, nominal material properties, and manufacturing process.

Experimental Setup. To test the first hypothesis about the uniqueness of impedance identities, we collected a sample set of both additively and traditionally manufactured parts. The parts that we tested included: (1) a 3D-printed impeller for a fuel pump (additive), (2) galvanized steel screws (traditional), (3) plastic electrical housing boxes (”BOX”, traditional), (4) aluminum brackets (”BRK”, traditional), (5) plastic flanges (”FLG”, traditional), (6) plastic impellers (”IMP”, traditional), (7) aluminum vent fittings (”VNT”, traditional) and (8) steel lug nuts (”LUG”, traditional) as shown in Fig. 4. Identities for each of parts 3–7 were measured in 5 groups, with each group containing a total of 5 impedance identities, 1 for each part instance, for a total of 5 measured impedance identities per part instance and 25 measured impedance identities per part type. For part 8, the impedance identities of 20 instances were measured 5 times each. These measurements comprise the data studied for assessing identity variation. The parts were left to rest for approximately 150 s between subsequent measurements of the same instance to provide roughly uniform time spacing (connect, measure, write data, disconnect, repeat). A single impedance identity measurement consists of five sweeps over the designated frequency range, averaging impedance values on each successive sweep. To measure a single impedance identity of 500 datapoints requires approximately 5 s. Sine excitation was used in these experiments with a 1V peak-to-peak signal to excite the host structure.

All of the traditionally manufactured parts were procured from a hardware supply store. This means that all of these parts went through the quality control checks that are used in industrial manufacturing settings – these parts were not manufactured in a lab. The data from these parts is representative of real-world industrial scale production of physical parts.

For the additively manufactured parts, three part instances were produced using each of two processes. One set of three parts was produced through material jetting, where a photosensitive resin is deposited and then cured with UV light in layers. A Stratasys Connex 350 system was used to fabricate these parts from their VeroWhitePlus material. A second set of three parts was produced through an extrusion process by a Stratasys Fortus 400mc system in one of their proprietary nylon materials. Both of these processes are common in industry.

The impedance identity of each part instance was measured 5 times. For all part instances of the same part type, we did a pair-wise comparison of the identities to compute the Hamming distance between the impedance identities of different part instances. Using the data from these calculations, we plotted the probability mass function of the Hamming distances for different instances of the same part type.

Results. As discussed in prior sections, the impedance identity of a part is determined by its geometry and material properties. Thus, we expect that the highly distinct parts considered here should have highly distinct impedance identities as well. In Fig. 5 this expectation is borne out. The next question is whether part instances of the same nominal geometry and material properties have distinct impedance identities as well.

As shown in Fig. 6, multiple instances of the same part type have distinguishable impedance identities even with sensors of the same type, specification, and attachment on each part instance. The impedance identities of different instances of the same part had Hamming distances that were roughly centered around 600 or more bits apart as shown in Fig. 7. Although the number of part instances and materials examined is small, the initial results appear promising that the likelihood of a random impedance identity collision would be low for the tested parts.

In order to establish that there exists sufficient variation to distinguish specimens that are extremely similar from a quality control perspective, an additional test was performed on a suite of traditionally manufactured specimens that were selected and instrumented to be as close to identical as possible. From a total of 20 nominally identical $\frac{3}{4}-10$ hex nuts, a group of five hex nuts were selected wherein the mass of any individual varied no more than 0.1% from the average of the five. The five specimens were then instrumented in the same manner and their impedance identities were measured over the range of 10-100 kHz (Fig. 8). Despite the fact that the signature of each specimen is in

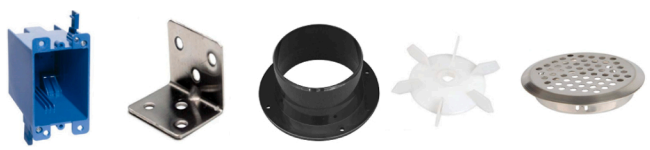

Fig. 4. Traditionally manufactured parts (box, bracket, flange, impeller, vent).

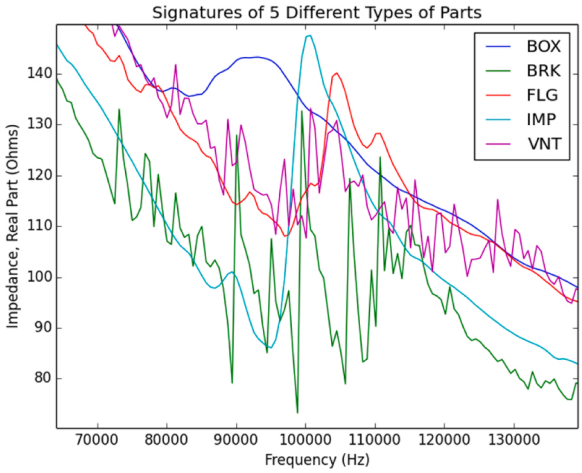

Fig. 5. Identities of all tested part types.

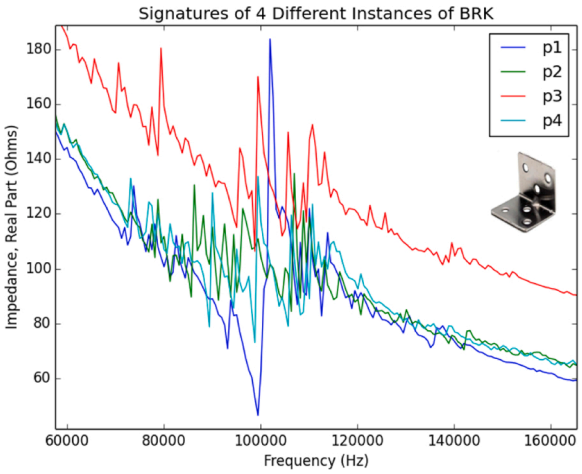

Fig. 6. Identities of multiple part instances.

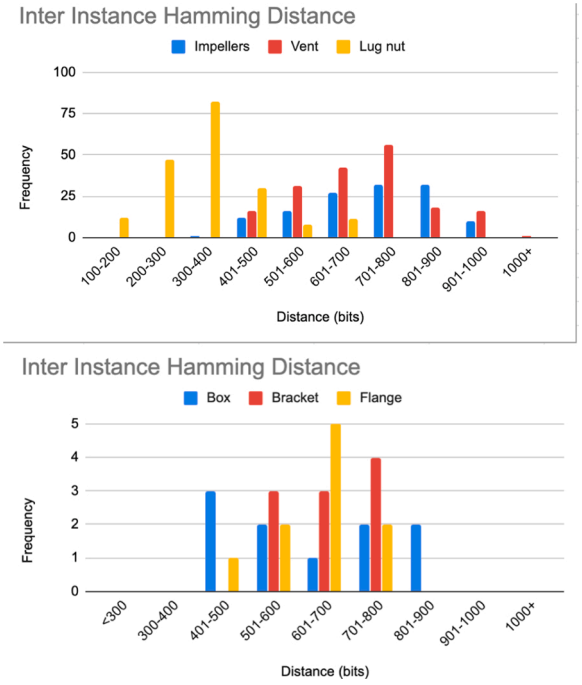

Fig. 7. Hamming distances between impedance identities of different instances of the same part type.

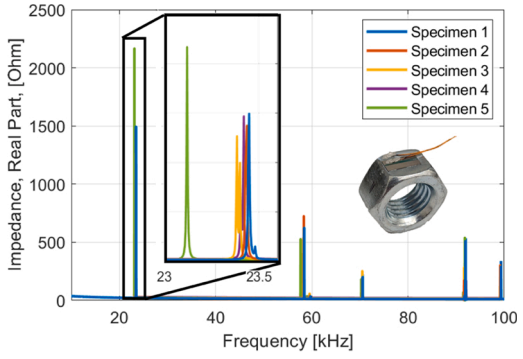

Fig. 8. Impedance identities of the five-specimen ensemble.

qualitative agreement with the others, close inspection reveals that each specimen's peak lies at a distinct frequency.

The distinct features of a part type's impedance identity depend on the geometry and material of the part, while the actual impedance values designate the specific instance of the part type, because of variations in both instrumentation and fabrication.

In other words, the characteristic shape of the impedance identity is shared between parts with a common nominal geometry and material, but minor part-to-part variations and the precise characteristics of the sensor attachment make the impedance identity unique to a specific instrumented part. To reproduce this identity, then, requires that a part and sensor pair remain attached throughout the supply chain to be remeasured as needed until a part is deemed fit for integration into a larger system.

4.2. *Hypothesis 2: Impedance identities are stable over time*

Our hypothesis is that impedance identities are stable across repeated measurements to within a tolerance α that is reliably distinguishable from other part instances. That is, we believe that the variation between repeated measurements of the same part does not introduce so much noise that an impedance identity collision is likely. As with any physical experimentation, the results to test this hypothesis are promising, but still require additional research to prove conclusively.

Experimental setup. The same data set produced by the additively and traditionally manufactured parts was used to test the hypothesis. As opposed to the first experiment, the pair-wise Hamming distances of repeated measurements of the same part instance were used to estimate the probability mass function of Hamming distance.

Results. The Hamming distances of repeated measurements of the same part instance are shown in Fig. 9. In contrast to the approximately 600 bit average Hamming distance between impedance identities of different instances, repeated measurements of the same part instance show a Hamming distance of roughly 10–20 bits, further supporting the idea that a part instance can be reliably identified over time even within a large batch of other instances of the same part type.

Figs. 10 and 11show the variation between impedance values on

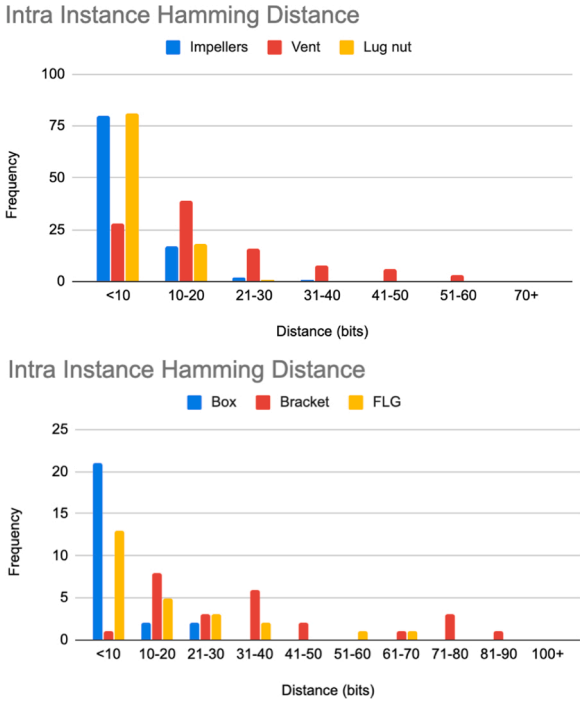

Fig. 9. Hamming distances between repeated measurement of impedance identities of the same part instance.

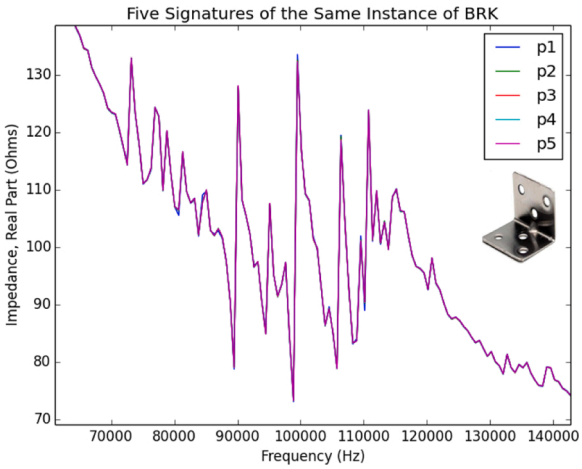

Fig. 10. Repeated impedance identity measurements of one part instance.

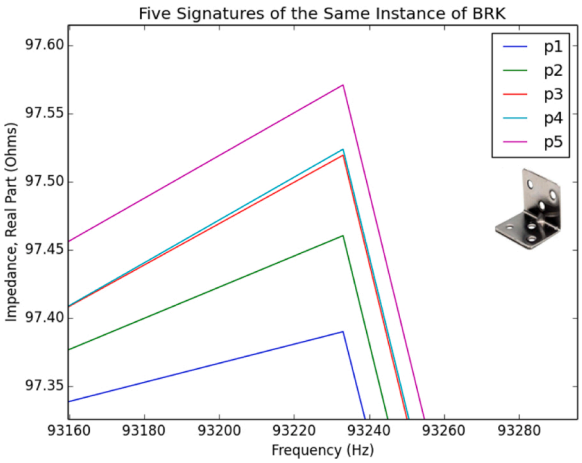

Fig. 11. Zoomed detail of repeated measurements of one part instance's identity.

different measurements of the same bracket (BRK) part instance. Across all of the measurements of the same part instance, identities are replicable at every frequency to within tenths of an Ohm. In contrast, for different instances of the BRK part, variation in impedance values typically approached 20–40 Ohms at many frequency steps.

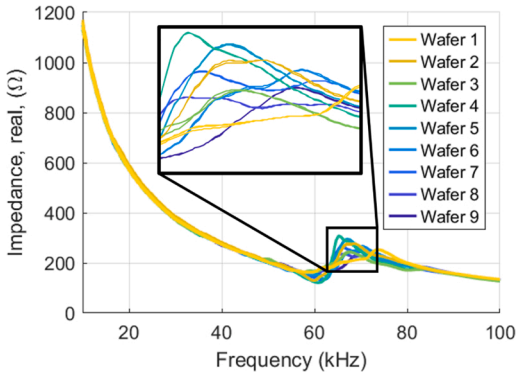

Fig. 12. Impedance identities of nine piezoelectric wafers.

4.3. Hypothesis 3: Piezoelectric wafers introduce random noise aiding identity uniqueness

Our hypothesis is that even when nominally identical piezoelectric wafers are measured alone, without an attached part, the impedance identities are distinguishable and create the bias σ_k^j. In Fig. 12, we show the impedance identities collected from each of nine unmounted piezoelectric wafers. All were nominally identical: cut from the same parent wafer and have the same dimensions, instrumentation, and measurement conditions. It can be seen that, though all wafers follow the same general trend, each wafer produces a distinct identity. Furthermore, the inset of Fig. 12 shows the consistency of repeated measurements of each piezoelectric wafer.

The frequency at which the piezoelectric wafer is actuated also affects the distinctiveness of the impedance identity as shown in Fig. 13. As the frequency of excitation increases, the impedance identity becomes more distinct when compared between two nominally identical $\frac{3}{4}-10$ hex nut specimens. And as in Fig. 10, repeated measurements of the impedance identity of the same specimen remain consistent, even as the specimen is disconnected from the analyzer, handled, and reconnected.

These results are important in that they indicate that each individual piezoelectric wafer will introduce random noise into an impedance identity. These results support the hypothesis that the unclonable identity function, $I(p_i, s_j, a_k, \omega_m, \omega_n)$, is influenced by the piezoelectric wafer and its mounting on a part. Moreover, as shown in the results, the selection of frequencies $\omega_m \ldots \omega_n$ impacts the variation seen in the impedance identity. More research is needed to definitively verify this for a wider range of geometries, materials, and other parameters, but the results are extremely promising and support the belief that impedance identities are unclonable.

5. Impedance identities and cybersecurity

As cyber attacks increase in complexity and frequency, resources must be allocated to monitoring and prevention of counterfeits within manufacturing networks. [42] surveys the security of current manufacturing systems and discusses known attacks on manufacturing infrastructure and corresponding mitigation strategies. The intersectional model of system security is explored by [43] as a framework for vulnerability assessment in manufacturing systems. In the following subsections, possible vulnerable entry points for the proposed impedance identity method are discussed.

5.1. Impedance identity parameters

We hypothesize that the following parameters should be considered when examining the ways in which a malicious entity might capture an impedance identity or otherwise compromise the specifications of an authentic part instance. For an attacker to successfully forge or steal an impedance identity, some or all of the following data about a part must be obtained by the attacker:

1) Piezoelectric material used
2) Sensor uncertainty
3) Sensor adhesion process
4) Sensor location on part
5) Comprehensive geometry of part
6) Material makeup of part
7) Manufacturing process to produce part
8) Excitation frequency range
9) Impedance analyzer configuration

The information provided by these parameters could enable an attacker to misguide counterfeit detection logic, causing a counterfeit

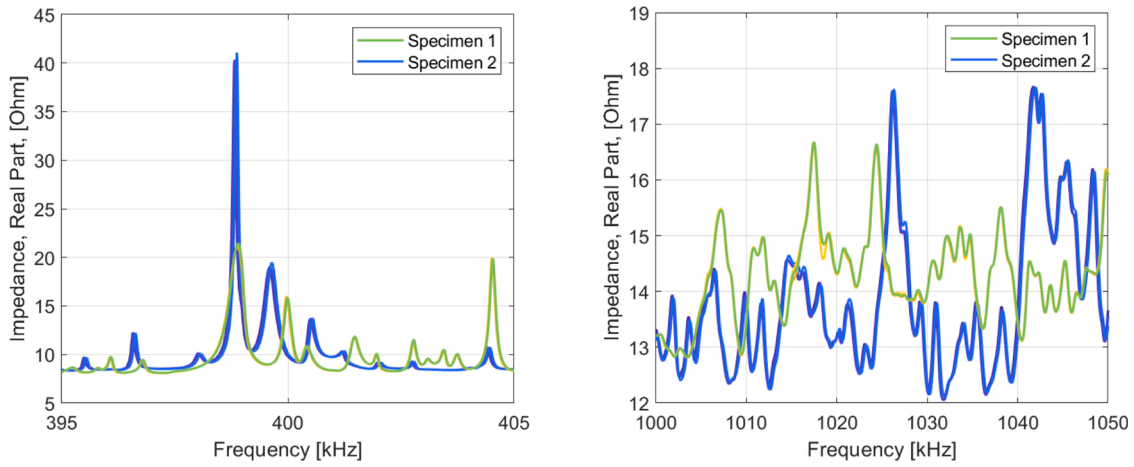

Fig. 13. Measurements of impedance identity at higher frequencies for two part instances.

part to remain in a production supply chain undetected.

5.2. Attacker motivation and threat landscape

The following attacker motivations are considered: (1) A financially motivated attacker, incentivized to swap authentic parts with illegitimate ones along a supply chain to sell the authentic parts; (2) An attacker interested in sabotage of a larger system that persistently manufactures parts of inferior quality in hopes of evading counterfeit detection; (3) An attacker seeking to steal part specifications that may attack the manufacturing network through a vulnerable entry point. Currently, there are no reported instances of complex orchestrated attacks against manufacturing supply chains. There are, however, illicit markets for inferior quality parts including those that may have been previously used but are labeled and sold as new. These markets typically exchange unauthorized or unmarked components such as small electronics and scrap pieces [44].

5.3. Current anti-counterfeiting measures

Companies that integrate manufactured components into safety-critical systems allocate resources to ensure only Original Component Manufacturer ("OCM") parts travel across the supply chain. The ability to authenticate the OCM is currently one of the most effective ways to identify counterfeits [44]. However, as supply chains increase in complexity, so does the difficulty associated with verifying the source of a part [45]. Additional documentation and tracking measures have been implemented to travel with parts and increase the probability of counterfeit detection, but these methods do not evaluate the structural properties of a part to determine fitness for integration into a system. There currently exist several inspection techniques, including passive, destructive, in-situ, and external post-processing evaluation that help determine the quality of a component based on external and internal properties. Examples of these include: X-Ray Fluorescence Spectroscopy, Real-Time Radiography, Destructive Physical Analysis, and Optical Emission Spectroscopy [46]. [47] presents the use of a physical hash of process parameters and toolpaths for additively manufactured parts to detect counterfeits. The impedance identity method uses an impedance analyzer to compare the impedance identity of a part as it moves through a manufacturing network. The impedance analyzer can measure a part's impedance identity to monitor changes in the structural properties of a part, adverse or otherwise. By comparing the impedance identity of a part at different points along a supply chain, both the part manufacturer and part integrator can ensure the integrity of a part and determine whether a part is authentic or should be marked as counterfeit and removed from the supply chain.

5.4. Most common counterfeit parts

The most commonly targeted additively manufactured materials include thermoplastics such as ABS, PLA, and PC, as well as metals such as stainless steel, aluminum, and titanium. These materials are used in a variety of processes to produce components that will comprise safety-critical systems. Commonly counterfeited parts include nuts, bolts, blades, rings, gaskets, fasteners, connecting rods, gearboxes, brake shoes, titanium aerospace parts, and aluminum parts [5]. Moreover, companies are gradually integrating an increasing quantity of mission-critical components into their systems [48–51], and this number is expected to increase as these manufacturing techniques improve. We now outline possible attacks on the impedance identity method as well as risk level, difficulty, and defense strategies for each of them.

5.5. Potential attacks on impedance identities

We consider the following attacks as posing the greatest risk to the impedance identity verification system. We identify assumptions an attacker might make, the requisite information and infrastructure, the relative level of risk, and the costs associated with each of these attacks. **Zero-day and Insider Attacks.** Possible zero-day attacks on the impedance identity method include: (1) backdoors to impedance analyzer software or hardware; (2) backdoors to software components used for identity matching; (3) malicious obtainment of keys or artifacts used by parties to securely exchange part information. We expect that all of these attacks require extensive insider cooperation, internal information leakage, or carefully orchestrated theft or cooperation from analyzer manufacturers. If successful, any of these attacks would destabilize the impedance identity method by allowing an attacker to access impedance identity measurements or analyzer configuration data which could enable impedance identity matching for arbitrary parts. To mitigate the risks associated with (1) involves the meta-problem of securing the production supply chains of impedance analyzers; we acknowledge this vulnerability but do not address it in this work. To minimize the risk of attack through (2) manufacturers should ensure minimal exposure of the identity matching implementation to internal or external networks; for (3) key storage and generation mechanisms for information exchange should be routinely updated or audited. An additional consideration is the network access of the impedance analyzer used to measure impedance identities of parts. Impedance analyzers are not typically manufactured with built-in wireless network capabilities but have Ethernet and USB ports which may be vulnerable to malware exposure by an insider who may directly access the machine. Separation of the analyzer from direct network access (e.g., via a secured interface or protocol between the analyzer and the information

exchange framework) should decrease the likelihood of successful attacks on the impedance analyzer and/or malware propagation through internal networks. The following attack models provide an outline for evaluating threats in terms of risk, cost, and viability.

5.5.1. Network attack

- **Assumptions:** Attacker has identified one or more network vulnerabilities and can distribute a payload into a network undetected
- **Information needed:** escalated privilege network access, I/O access to equipment
- **Risk level:** High
- **Defense:** Offline equipment, network monitoring
- **Attacker Urgency:** Medium
- **Cost:** Time, compute, hardware, payload
- **Type:** Online; Cyber

In a network attack, an attacker seeks to gain an entry point into the part integrator's local network(s) to compromise connected equipment and produce lower quality parts or read authentic part information to produce copies as shown in Fig. 14. Successfully attacking the ground truth of part information or the equipment network allows the attacker to inject part information along with a counterfeit part in order to bypass counterfeit detection logic. Seizure of this information, if undetected, may contribute to a larger, long-term attack including theft of part information or IP, impedance identity parameters, sabotage of impedance analyzing equipment, or production of similar but lower quality parts than were originally produced.

5.5.2. Replay attack

- **Assumptions:** Attacker can store an impedance identity on unobtrusive read-only hardware
- **Information needed:** verified impedance identity of a part, state storage device to read from
- **Risk level:** Low
- **Defense:** Physical inspection of part and sensor, monitor impedance identity for apparent lack of deviation over time
- **Attacker Urgency:** High
- **Cost:** Time, compute, hardware, payload
- **Type:** On/Offline; Cyber

In a replay attack, an attacker obtains an authentic impedance identity and affixes state storage hardware onto a counterfeit part to store this identity. When the counterfeit part with attached storage hardware containing the authentic identity arrives for analysis, the authentic impedance identity stored on the hardware is read by counterfeit detection logic and the actual impedance identity of the counterfeit part is not measured as shown in Fig. 15. Such an attack would require that an attacker compromises the impedance identity of a known authentic part, produces a counterfeit part instance with visibly

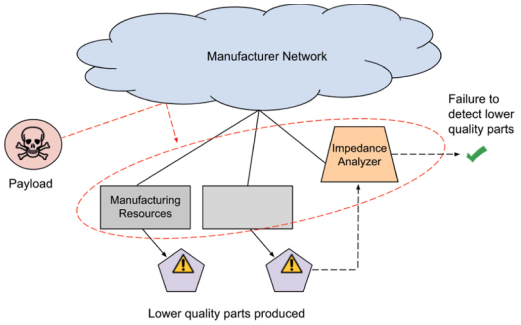

Fig. 14. Network attack.

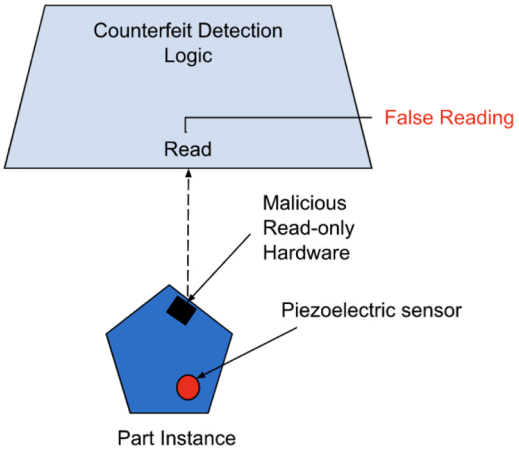

Fig. 15. Replay attack.

acceptable specifications, and then affixes an undetectable state storage device containing the authentic impedance identity of a similar looking part to be read by the impedance analyzer. In theory, this would allow a counterfeit part to move through a supply chain considered an authentic part. However, because of the challenge of affixing an undetectable state storage device, this attack is considered highly difficult, if not impossible.

5.5.3. Brute force attack

- **Assumptions:** Attacker has significant resources to produce an arbitrarily shaped part in large quantities
- **Information needed:** Authentic impedance identity of some part as well as its specifications, type of sensor used, excitation frequency range
- **Risk level:** Low
- **Defense:** Establish a watch list and criteria for investigating highly targeted parts, transparency with OCMs to identify compromised supply chains
- **Attacker Urgency:** Low
- **Cost:** Materials, manufacturing, sensor procurement, feedback to iterate
- **Type:** On/Offline; Physical

In a brute force attack, an attacker seeks to produce arbitrarily many counterfeit parts based on some collection of partial or total information from an authentic part instance until a targeted part instance is successfully counterfeit, i.e. the impedance identity of the counterfeit part is undetectably similar to the authentic version of the targeted part. In other words, the impedance identity of the n^{th} part instance produced by the attacker is considered legitimate by the part integrator's counterfeit detection logic. A key obstacle to this method is that the attacker must manufacture an unknown number of part instances while obtaining actionable feedback from each of the prior parts produced to guide subsequent part specifications, as shown in Fig. 16. The reason for relatively low urgency and risk for a brute force attack is the following: the impedance identity method proposes a way to assign a unique identity to each instance of a given part type. As shown in Section 4, these identities are distinguishable partially because of the configuration of the sensor attachment to a part as well as inherent noise in the sensor material properties as shown in Figs. 6, 8, and 12 . These differences are quantified in this work by the Hamming distance, a similarity metric between the binary representation of two impedance identities. The Hamming distance between two impedance identities is an initial approach to indicate whether a received part is the expected part. To illustrate the difficulty of a brute force attack, consider two different part instances A and B of the same part type, manufactured

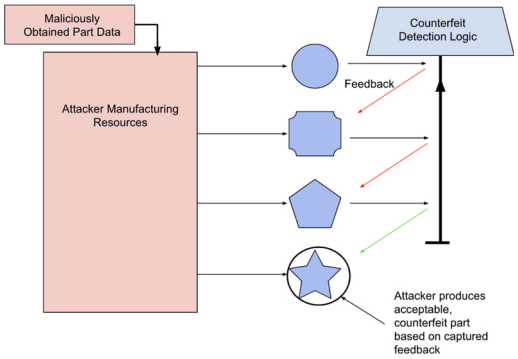

Fig. 16. Brute force attack.

according to the same process and specification, and containing the same sensor type and attachment configuration. Let *A* be the expected, authentic instance and *B* a counterfeit instance. Assume also that *B* is the best possible result of a brute force attack i.e., an attacker has produced a part with nominally and visually identical characteristics. When the impedance identities of the two parts are measured, we expect that the Hamming distances between the received identity (corresponding to *A*) and the measured identities (obtained from measuring the impedance identity of *A* and measuring the impedance identity of *B*) indicate that *A* is in fact the authentic part and that *B* should be flagged as counterfeit despite a nearly identical physical appearance. The difference in Hamming distance between the impedance identities of *A* (authentic) and *B* (counterfeit) is expected to have roughly the same order of magnitude as the difference between *A* (authentic) and *C* (another authentic instance of the same part type as *A* manufactured with the same process and with the same sensor specification and configuration) as shown in Figs. 7 and 9. In other words, the key feature of the impedance identity method is that even though an attacker may be able to produce a part-sensor pair that is visually and nominally identical to an authentic part instance, the attacker will not be able to produce a counterfeit part having both properties of identical visual appearance *and* sufficiently similar impedance identity to the authentic part because, given a sufficient similarity metric, a single part-sensor pair creates an identifier that is attributable to a single part instance and that cannot be replicated or substituted by a different part and sensor pair. This also precludes successful attacks involving interception of an authentic part and replacement with a visually identical but counterfeit part *or* sensor. Thus, we expect successful attacks on the impedance identity method to include those which target the measurement technology (e.g., analyzer) or the identity matching implementation (e.g., Hamming distance comparison) rather than repeated attempts to manufacture nominally identical counterfeit parts. For this reason, we assign greater urgency and risk to attacks aiming to deceive counterfeit detection logic by compromising the impedance analyzer or information exchange framework; we expect the most significant threats to the impedance identity method to arise in the cyber domain rather than the physical. Additional experimental results to further support these claims will be included in future work.

5.5.4. Replacement attack

- **Assumptions:** Attacker has access to genuine used parts and can uninstall them from retired machinery or equipment
- **Information needed:** The types of parts, where and how to sell them, specifications for buyer, authentic impedance identity
- **Risk level:** Medium
- **Defense:** Regularly check and update impedance identities of parts in use and monitor for aberrations, develop strategies to enforce and track the unauthorized sale of used or compromised parts that should remain out of circulation
- **Attacker Urgency:** Medium
- **Cost:** Time to obtain discarded parts and new sensor, resources to identify the specifications of the original part, resources to restore the part to sell
- **Type:** Offline; Physical

In a replacement attack, an attacker, who may have access to used genuine parts, seeks to replace the used genuine parts with counterfeits and resell the genuine used parts as new with a sensor and an authentic impedance identity (see Fig. 17). To prevent this, impedance identities of parts should be regularly updated or removeed from data storage when they are no longer in use. This narrows the opportunity for an attacker to pass off a used authentic part as a new authentic part. In addition, working closely with the OCM will help to enforce resale of used or worn parts and prevent unauthorized removal or replacement of parts.

6. Open questions and future work

Our initial results investigating this approach have showed promise. However, significant additional fundamental cyber-physical research is needed to understand how to design the cyber and physical elements of this approach to create identities that are proven to be physically unclonable but stable enough to be algorithmically identified and used for secure identification and binding of cyber-information. We hope that others will find the results in this paper promising and begin investigations into key questions outlined below.

SPUDs are a new use context for impedance measurements wherein the uniqueness of a part's impedance identity must be verified. There is still much to be learned about the variability in identities across materials, shapes, attachments, etc. to determine the most appropriate cyber-representation of the identities and algorithms for analysis. While the team has performed preliminary experiments to verify that impedance identities are affected by variations in sensor configuration and manufacturing process, a systematic study aimed at quantifying the effects of each of the isolated process parameters has not not been conducted. Such a study is needed in order to (i) further verify the uniqueness of parts' identities; (ii) design appropriate cyber-representations and impedance identity matching algorithms; (iii) estimate the cost required to attack the security measure, and (iv) design guidelines for defenders to maximize the uniqueness of the identity.

Our preliminary research has shown that impedance identities between seemingly identical parts vary such that their identities are individually unique, with Hamming distances of 600 bits or more, despite having identical geometry, material specification, and manufacturing process. In order to ensure uniqueness and unclonability, further research is needed by the community to systematically identify

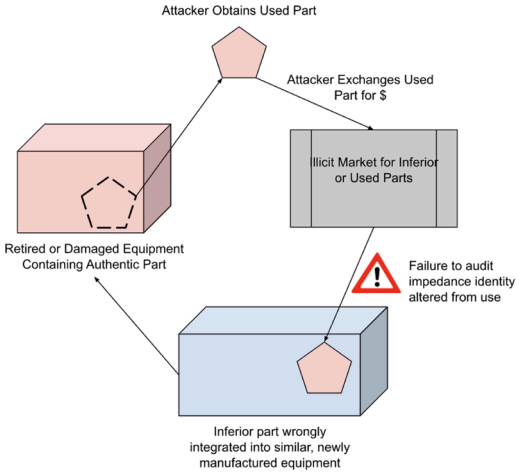

Fig. 17. Used part replacement attack.

the sources of identity variance and quantify their impact on the identity itself. How does the piezoelectric sensor, sensor location, sensor mounting configuration, and the manufacturing process affect a resultant part's impedance identity? This question must be answered in detail to be able to prescribe a methodology for part manufacturing and piezoelectric sensor mounting that will maximize identity variation among identical parts. Where should randomization be injected in the process to maximize a defender's advantage?

It is hypothesized that the variation in the impedance identity across multiple parts of the same geometry is due to a variety of sources throughout the piezoelectric measurement technique that are random and unclonable, including: (1) the crystalline microstructure of each piezoelectric wafer is unique; (2) variations in a sensor's size, (3) mounting configuration, and (4) location on the part can alter the identity; and (5) inherent variations in the manufacturing process can alter part properties that are reflected in the identity. More work is needed to understand how the impedance identity varies based on these manufacturing and instrumentation parameters.

The robustness of impedance measurement to several sources of uncertainty, including ambient temperature, boundary conditions, and measurement equipment, needs to be investigated and countermeasures developed to guarantee that the unique identity of each part will not be masked. For this purpose, impedance identities of parts representing different materials (steel, aluminum, nylon, and PEI resin "ULTEM") and manufacturing processes (CNC milling, powder bed fusion, material extrusion, and material jetting) will need to be researched to understand variations across materials and processes.

More data on identity variation is needed to design robust algorithms that stably match identities over time, yet do not easily admit counterfeit parts or incorrectly associate cyber-information with a part instance. As more data becomes available on the variability and other parameters of identities outlined above, it is expected that there will be significant opportunities to use specific insights in identity randomness to inform identity matching algorithms. Further, differing frequencies, materials, and attachment processes may generate different attack cost models and hence dictate different defensive strategies.

Ensuring the stability of impedance identities after shipping parts as well as in different measurement environments is part of ongoing work. Initial results indicate the impedance identity is stable after shipping of parts and when using different analyzers with similar configurations and under similar conditions (e.g., temperature, humidity). Results from these experiments will be included in future work to demonstrate the viability of the impedance identity method for parts shipped across a supply network.

7. Concluding remarks

Although physical countermeasures (e.g., holographic serial numbers, etc.) have been studied for a long time, counterfeiting is still a global problem that affects safety-critical systems, such as aeronautics. We believe that using piezoelectric sensors to measure the impedance identities of physical parts may serve as a physically unclonable function for determining an intrinsic identity of a part. In comparison to prior work on physically unclonable functions, we focus on the use of these identifiers solely for identification purposes to bind cyber-information to and not as the source of cryptographic material with sufficient entropy for encryption. We also focus on traditional physical parts (e.g., screws, impellers, brackets) as opposed to circuits. Once an impedance identity is measured for a physical part instance, well-established PKI mechanisms can be used to provably bind safety and other cyber-information to a specific part instance.

The novelty of the proposed method is that the physical properties of a part are contained in information (impedance identity) which can be reliably exchanged through existing methods with demonstrated security e.g., PKI. Unlike shallow identifiers such as serial numbers or barcodes, the impedance identity is a deep identifier that indicates the physical quality of a given part instance rather than an arbitrarily assigned label or identifying string. Thus, the impedance identity helps prevent attempts to pass off a counterfeit part instance as authentic. In the cyber domain, the information exchange framework helps guarantee the identity of the sender and receiver of part instance information. Combining these techniques offers a robust solution to detecting counterfeits: the impedance identity secures physical channels (part and sensor pairs shipped across a supply chain) while the information exchange framework secures the cyber channels (information sent and received over a network). The impedance identity guarantees the physical identity of a single part instance and the information exchange framework guarantees sender and receiver identities as well as the integrity of part information. Both of these components are needed to address counterfeiting issues in both cyber and physical domains.

There are no known ways to produce two parts of identical impedance identity using the state of the art knowledge in manufacturing. A key question, then, is how likely it is that an attacker could randomly manufacture a physical part that collided with the impedance identity of a legitimate part. As we showed in our experimental results from both traditional and additively manufactured parts, the likelihood of manufacturing a physical part with a collision appears to be extremely low. When comparing the impedance identities of identically manufactured part instances, we have seen Hamming distances ranging from 500 to 1000 bits or more. Given that colliding with an existing impedance identity requires production of a physical part and that the probability of getting lucky and producing a collision is extremely low, the technique has the potential to give manufacturers and integrators a cost-effective technique to combat false cyber-information being passed on with counterfeit parts.

Although we see significant promise in the SPUD approach, we believe that much further research into many aspects of impedance identities is needed. The work in this paper is preliminary and promising, but a large amount of further work by a community of researchers (e.g., thousands of physical experiments) is needed to further validate the conjectures in the paper. The best formats for representing and matching impedance identities need to be further developed using insights from past work on fuzzy extractors and other topics. Significant physical experimentation is needed across materials, geometries, and processes to understand the physical limitations of the technique. There are many exciting avenues to explore regarding threat models, cost modeling, and defensive countermeasures (e.g., geometry, attachment, and piezoelectric wafer randomization) using SPUDs.

Declaration of Competing Interest

The authors report no declarations of interest.

Acknowledgment

The authors would like to thank the NSF for supporting this work under Award #1931931: Cyber-Physical System Integrity and Security.

References

[1] Lee J, Bagheri B, Kao H-A. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manuf. Lett. 2015;3:18–23.
[2] Tang CS, Zimmerman JD, Nelson JI. Managing new product development and supply chain risks: The boeing 787 case. Supply Chain Forum Int J 2009;10(2):74–86. Taylor & Francis.
[3] ResearchAndMarkets.com. Global brand counterfeiting report 2018-2020. https://www.researchandmarkets.com/reports/4438394/globalbrand-counterfeiting-report-2018.
[4] Murray F. Top counterfeiting risks manufacturers face in 2016. https://www.manufacturingindustryadvisor.com/top-counterfeitingrisks-manufacturers-face-in-2016.
[5] A.I.A. of America. A special report, counterfeit parts: increasing awareness and developing countermeasures. http://www.aiaaerospace.org/wp-content/uploads/2016/05/counterfeit-web11.pdf.
[6] Kliewe D, Kühn A, Dumitrescu R, Gausemeier J. Challenges in anti-counterfeiting of cyber-physical systems. Int J Soc Behav Educ Econ Manage Eng 2015;9:1732–9.

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

[8] Lee I, Sokolsky O, Chen S, Hatcliff J, Jee E, Kim B, et al. Challenges and research directions in medical cyber-physical systems. Proc IEEE 2012;100(1):75–90.

[9] Andreu J-P, Rinnhofer A. Modeling of internal defects in logs for value optimization based on industrial CT scanning. In: Fifth international conference on image processing and scanning of wood; 2003. p. 23–6.

[10] Helfmeier C, Boit C, Nedospasov D, Seifert J-P. Cloning physically unclonable functions. In: 2013 IEEE international symposium on hardware-oriented security and trust (HOST); 2013. p. 1–6.

[11] Maes R, Verbauwhede I. Physically unclonable functions: A study on the state of the art and future research directions. Towards hardware-intrinsic security. Springer; 2010. p. 3–37.

[12] Suh GE, Devadas S. Physical unclonable functions for device authentication and secret key generation. In: 2007 44th ACM/IEEE design automation conference; 2007. p. 9–14.

[13] Dodis Y, Reyzin L, Smith A. Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. In: International conference on the theory and applications of cryptographic techniques; 2004. p. 523–40.

[14] Boyen X. Reusable cryptographic fuzzy extractors. In: Proceedings of the 11th ACM conference on Computer and communications security; 2004. p. 82–91.

[15] Buhan I, Doumen J, Hartel P, Veldhuis R. Fuzzy extractors for continuous distributions. In: Proceedings of the 2nd ACM symposium on information, computer and communications security; 2007. p. 353–5.

[16] Harris PM, Clarke RV. Car chopping, parts marking and the motor vehicle theft law enforcement act of 1984. Sociol Soc Res 1991;75(3):107–16.

[17] Stern B. Warning! Bogus parts have turned up in commercial jets. where's the FAA. Bus Week 1996;90.

[18] Komolafe T, Tian W, Purdy GT, Albakri M, Tarazaga P, Camelio J. Repeatable part authentication using impedance based analysis for side-channel monitoring. J Manuf Syst 2019;51:42–51. Available at: http://www.sciencedirect.com/science/article/pii/S0278612518301997.

[19] Weimerskirch A, Paar C, Wolf M. Cryptographic component identification: enabler for secure vehicles. IEEE vehicular technology conference, vol. 62, no. 2 1999, 2005:1227.

[20] Weimerskirch A, Höper K, Paar C, Wolf M. Component identification: enabler for secure networks of complex systems. Proceedings of applied cryptography an network security 2005 (ACNS 2005) 2005.

[21] Chen F, Luo Y, Tsoutsos NG, Maniatakos M, Shahin K, Gupta N. Embedding tracking codes in additive manufactured parts for product authentication. Adv Eng Mater 2018:1800495.

[22] Tao F, Zhang Y, Cheng Y, Ren J, Wang D, Qi Q, et al. Digital twin and blockchain enhanced smart manufacturing service collaboration and management. J Manuf Syst 2020. Available at: http://www.sciencedirect.com/science/article/pii/S0278612520301953.

[23] Huang S, Wang G, Yan Y, Fang X. Blockchain-based data management for digital twin of product. J Manuf Syst 2020;54:361–71. Available at: http://www.sciencedirect.com/science/article/pii/S0278612520300091.

[24] Aniello L, Halak B, Chai P, Dhall R, Mihalea M, Wilczynski A. Anti-bluff: towards counterfeit mitigation in IC supply chains using blockchain and PUF. Int J Inf Secur 2020;06.

[25] Albakri MI, Sturm LD, Williams CB, Tarazaga PA. Impedance-based non-destructive evaluation of additively manufactured parts. Rapid Prototyp J 2017;23(3):589–601.

[26] Sturm L, Albakri M, Williams CB, Tarazaga P. In-situ detection of build defects in additive manufacturing via impedance based monitoring. Proceedings of the 27th international solid freeform fabrication symposium 2016:1458–78.

[27] Farrar C, Park G, Sohn H, Inman DJ. Overview of piezoelectric impedance-based health monitoring and path forward. Shock Vibr Digest 2003;35(6):451–63.

[28] Liang C, Sun F, Rogers C. Coupled electro-mechanical analysis of adaptive material systems – determination of the actuator power consumption and system energy transfer. J Intell Mater Syst Struct 1997;8(4):335–43.

[29] Annamdas VG, Radhika MA. Electromechanical impedance of piezoelectric transducers for monitoring metallic and non-metallic structures: a review of wired, wireless and energy-harvesting methods. J Intell Mater Syst Struct 2013;24(9):1021–42.

[30] Taylor SG, Farinholt K, Choi M, Jeong H, Jang J, Park G, et al. Incipient crack detection in a composite wind turbine rotor blade. J Intell Mater Syst Struct 2014;25(5):613–20.

[31] Annamdas VGM, Soh CK. Application of electromechanical impedance technique for engineering structures: review and future issues. J Intell Mater Syst Struct 2010;21(1):41–59.

[32] Wells LJ, Camelio JA, Williams CB, White J. Cyberphysical security challenges in manufacturing systems. Manuf Lett 2014;2(2):74–7.

[33] Turner H, White J, Camelio JA, Williams C, Amos B, Parker R. Bad parts: are our manufacturing systems at risk of silent cyberattacks? IEEE Secur Privacy 2015;13(3):40–7.

[34] Sturm L, Williams C, Camelio J, White J, Parker R. Cyberphysical vunerabilities in additive manufacturing systems. Context 2014;7(2014):8.

[35] Strutner SM, Tenney C. Inexpensive verification via electromechanical impedance for additively manufactured parts. SAMPE conference 2018.

[36] Sturm LD, Williams CB, Camelio JA, White J, Parker R. Cyber-physical vulnerabilities in additive manufacturing systems: a case study attack on the. STL file with human subjects. J Manuf Syst 2017;44:154–64.

[37] Pan Y, White J, Schmidt DC, Elhabashy A, Sturm L, Camelio J, et al. Taxonomies for reasoning about cyber-physical attacks in IoT-based manufacturing systems. Int J Interact Multimedia Artif Intell 2017;4(3).

[38] Briais S, Nestmann U. A formal semantics for protocol narrations. In: International symposium on trustworthy global computing; 2005. p. 163–81.

[39] Suzuki K, Tonien D, Kurosawa K, Toyota K. Birthday paradox for multi-collisions. In: International conference on information security and cryptology; 2006. p. 29–40.

[40] Preshing J. Hash collision probabilities. 2011. http://preshing.com/20110504/hash-collision-probabilities.

[41] Albakri MI, Tarazaga PA. Electromechanical impedance-based damage characterization using spectral element method. J Intell Mater Syst Struct 2017;28(1):63–77. https://doi.org/10.1177/1045389X16642534.

[42] Tuptuk N, Hailes S. Security of smart manufacturing systems. J Manuf Syst 2018;47:93–106. Available at: http://www.sciencedirect.com/science/article/pii/S0278612518300463.

[43] DeSmit Z, Elhabashy AE, Wells LJ, Camelio JA. An approach to cyber-physical vulnerability assessment for intelligent manufacturing systems. J Manuf Syst 2017;43:339–51. high Performance Computing and Data Analytics for Cyber Manufacturing. Available online at: http://www.sciencedirect.com/science/article/pii/S027861251730033X.

[44] Counterfeit materials prevention, 2019. Available online at: https://www.lockheedmartin.com/content/dam/lockheedmartin/eo/documents/suppliers/rms/rms-quality-counterfeit.pdf.

[45] Aniello L, Halak B, Chai P, Dhall R, Mihalea M, Wilczynski A. Towards a supply chain management system for counterfeit mitigation using blockchain and PUF. 2019.

[46] Counterfeit parts detection. Available online at: https://www.securingindustry.com/electronicsand-industrial/scientists-embed-anti-fake-features-in-metalparts/s105/a8404/.Xu5NXpNKhTY.

[47] Brandman J, Sturm L, White J, Williams C. A physical hash for preventing and detecting cyber-physical attacks in additive manufacturing systems. J Manuf Syst 2020;56:202–12. Available at: http://www.sciencedirect.com/science/article/pii/S0278612520300789.

[48] SpaceX uses DMLS to 3D print Inconel SuperDraco engine chamber. Available online at: https://additivemanufacturingtoday.com/spacexuses-dmls-to-3d-print-inconel-superdraco-engine-chamber.

[49] Sher D. Tesla shows massive generatively designed part in model Y underbody. 2020 May. Available at: https://www.3dprintingmedia.network/tesla-shows-massivegeneratively-designed-3d-printed-part-in-model-y-underbody/.

[50] Sertoglu K. Tesla fixes model Y HVAC system using 3d printing. 2020 April. Available online at: https://3dprintingindustry.com/news/teslafixes-model-y-hvac-system-using-3d-printing-171017/.

[51] Huskamp C. 3D printing is the future of aerospace defense manufacturing: Jabil. Available online at: https://www.jabil.com/blog/3dprinting-in-aerospace-and-defense-manufacturing.html.