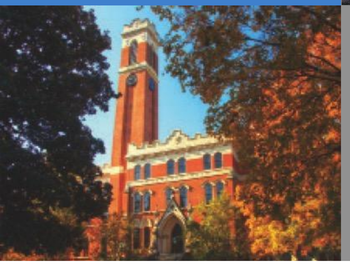


Cyber-Physical System Security and Integrity with Impedance Signatures

Pablo Tarzaga, Jules White, Chris Williams, Jaime Camelio, Logan Sturm, Carlos Olea, Michael Sandborn

Acknowledgement
This work is sponsored by the NSF & DHS under the research award CNS1446303

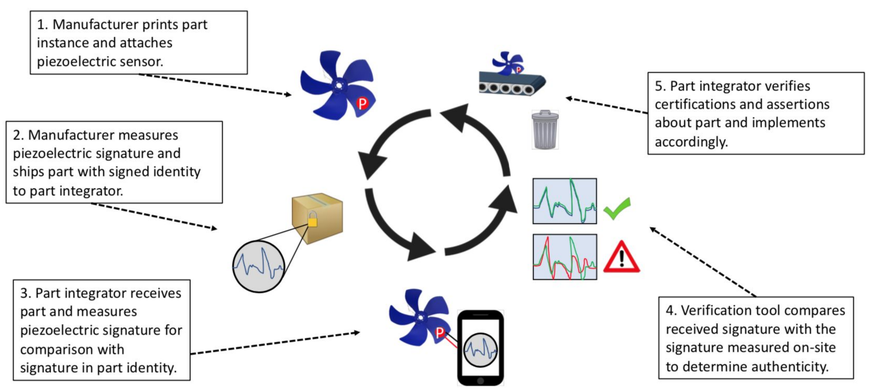
Towards a framework for comprehensive counterfeit detection of additively manufactured parts through unclonable functions as persistent identifiers

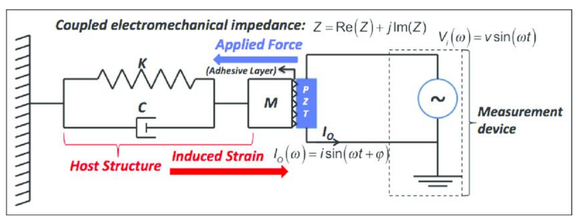
Problem

Counterfeiting will be a $1.82 trillion problem by 2020. Counterfeit parts are known to enter the aerospace supply chain, but the time and place of their entry is unpredictable. ***What measures can be taken to mitigate the counterfeiting problem in additive manufacturing supply chains so attackers can no longer inject flawed parts undetected into a supply chain that produces components for safety-critical systems such as aircraft and industrial equipment***? Is it possible to construct an identification system that leverages intrinsic properties of a manufactured part so that a part can be characterized by properties rooted in its physical makeup and not just an external, affixed identifier? Is it possible to guarantee part authenticity and integrity? How can it be assured that cyber-information really is for a specific part instance?

Solution Approach

Piezoelectric signature- the set of real impedance values (Ohms) of a part in response to a selected set of frequencies that excite the part. This signature is at least dependent on part geometry, structure, size, sensor instance and sensor placement. Additional factors are under investigation. These signatures are a function of the part itself, the sensor attachment, and the location of the sensor on the part.





These signatures can be represented with a binary key that maps impedance value at each frequency step. The size of a given signature depends on the desired matching tolerance and the number of data points in the signature

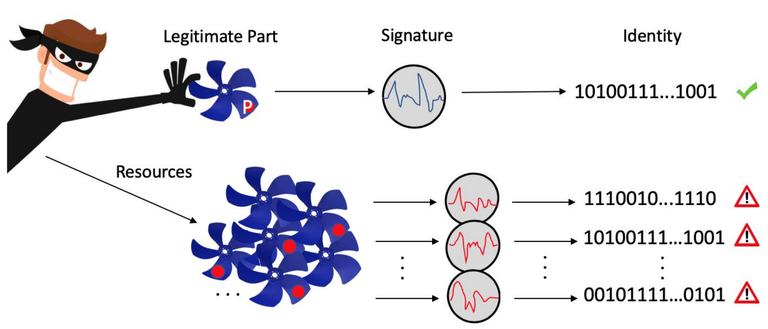
Authenticity - a guarantee that the part was produced in a specific way by the expected manufacturer

Integrity - a guarantee that the part was not maliciously altered along the supply chain

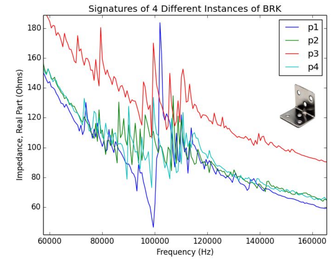
Attack Feasibility

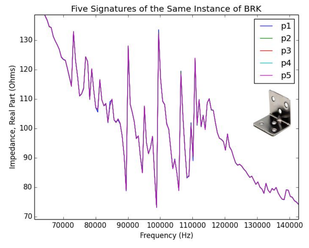
If an impedance identity for a $1 part has ~1600 bits of usable identity. Our current mean and median values for intra-class hamming distance and same instance distance are 1241/1250 and 55/30. Assuming the more conservative pair (mean) and assuming no differences in the counterfeit part are reflected in impedance, an attacker would have to produce ~10^{373} part instances to pass off a *single* counterfeit as legitimate (by producing a signature that falls in the distribution for the same instance). There are ~10^{82} atoms in the universe. In other words, passing off a counterfeit of a $1 part as legitimate would cost more than the combined GDP of every country in the world.

Replicating a part up to its physical specifications does not guarantee the signature of the legitimate part since the identity of the part depends on its physical makeup, the sensor instance attached to it, and the location of the sensor attachment. In theory, an attacker can never replicate a signature of a legitimate part with a counterfeit part, because the counterfeit part won't have the same sensor as the legitimate part. Moreover, relocating the sensor from a legitimate part to a counterfeit part has also been shown to produce a signature different from the original, legitimate part.

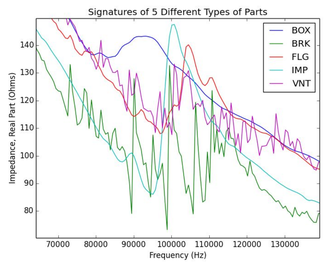


Unclonability and Uniqueness

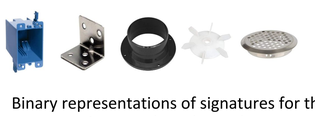


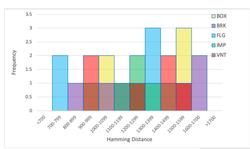


While there is clear variation in signatures of different instances (left), experiments show minimal variation in signatures of the same instance measured on separate occasions (right)

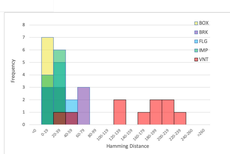


Signatures for each of the 5 different types of parts. These signatures can identify a single part instance and verify part authenticity and integrity by comparing the received signature for a part with a measured signature for that part somewhere in the supply chain. If the signatures do not match at sufficiently many locations, the part is deemed counterfeit.





Binary representations of signatures for the same part instance have been shown to vary by a small fraction of the total length of the signature, indicating these signatures are reproducible. Hamming distances for intra-class (left) and same instance (right) are shown to the right.



Selected Publications

1. Hamilton Turner, Jules White, Brandon Amos, Jaime Camelio, Chris Williams, and Robert Parker. "Bad Parts- Are Our Manufacturing Systems At Risk of Silent Cyber-attacks?" IEEE Security & Privacy (to appear)
2. L. D. Sturm, C. B. Williams, J. Camelio, J. White, and R. Parker, 2014, "Cyberphysical Vulnerabilities in Additive Manufacturing Systems," International Solid Freeform Fabrication Symposium, Austin, TX., August 4-6
3. Jaime Camelio, Lee J Wells, Christopher B Williams, Jules White, Cyber-Physical Security Challenges in Manufacturing Systems, Manufacturing Letters, Volume 2, Number 2, pp. 74-77, 2014
4. Sam Hurd, Carmen Camp, Jules White, Quality Assurance in Additive Manufacturing Through Mobile Computing, The 7th EAI International Conference on Mobile Computing, Applications and Services, Nov 12-13, 2015, Berlin, Germany