2021 NSF CYBER-PHYSICAL SYSTEMS PRINCIPAL INVESTIGATORS' MEETING

CPS: TTP Option: Medium: Collaborative Research: Cyber-Physical System Integrity and Security with Impedance Signatures

Vanderbilt/ Virginia Tech / Tennessee Tech

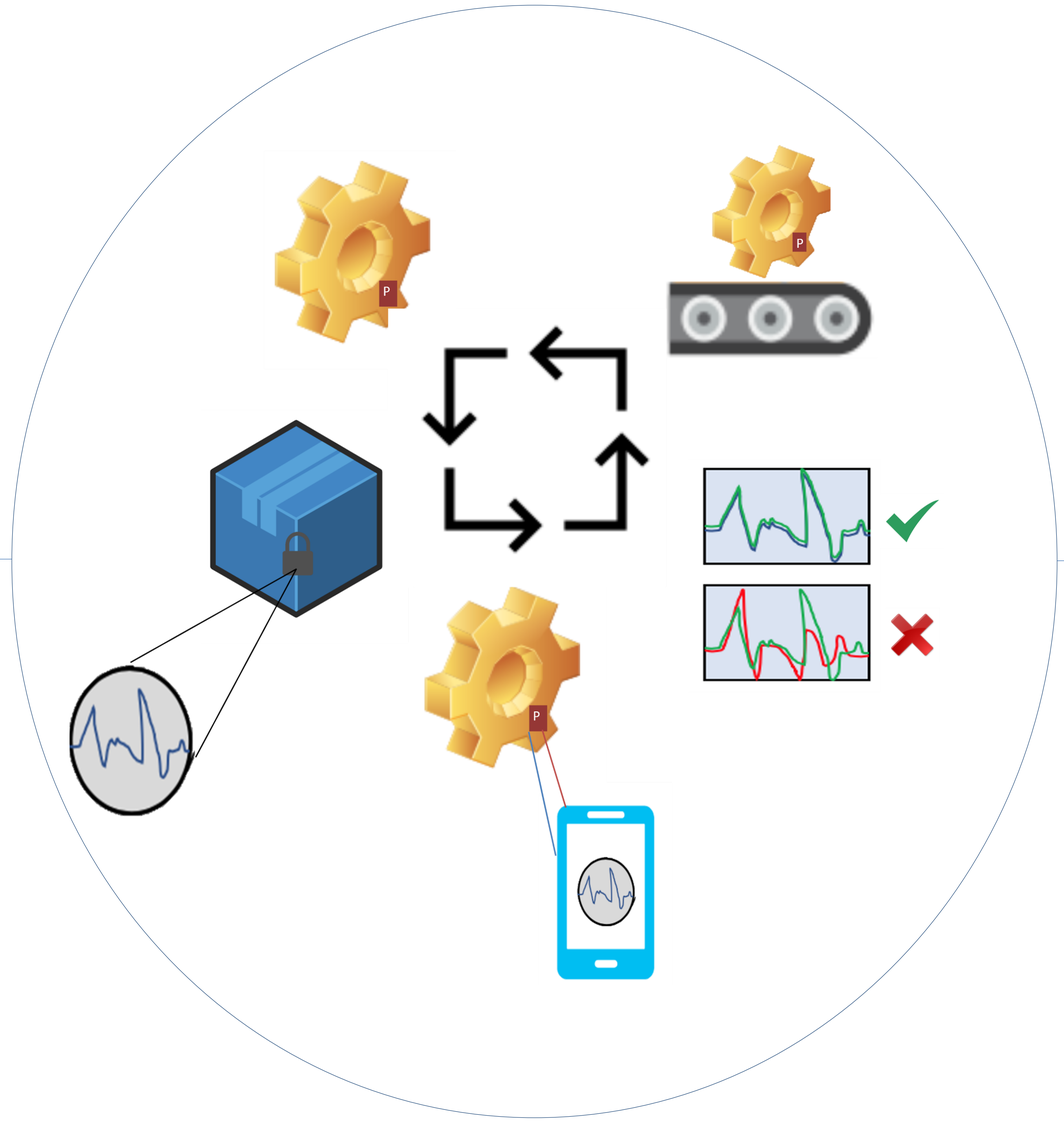
Challenge:

- Preserving integrity of Cyber-physical Systems (CPSs) in a distributed supply-chain.
- Ensuring that parts and the associated data is untampered.
- Advance fundamental understanding that provides the necessary knowledge to avoid counterfeiting and other CPS associated threats, while being able to uniquely identify part instances.
- Finding a solution to counterfeiting, which is a rampant issue with significant financial and safety consequences for domains including medicine, manufacturing, and consumer goods.

Solution:

- Leverage the electromechanical impedance of a part for advancing an unclonable identity.
- Uniquely identify each part using its impedance signature, which is inherent to each part instance owing to its unique physical characteristics and material properties.
- Link cyber and physical information in order to assert that a received part is the authentic instance of the expected part.

Award #: 1931931
Award date: October 1, 2019
Collaborators: VU, VT, TTU
Contact: jules.white@vanderbilt.edu



Tracking a component throughout a supply network: the physical measurement uniquely identifies the part and is asserted to match a ground truth identity until the part reaches the intended consumer.

Scientific Impact:

- Linking cyber information to physically unclonable parameters can establish a robust CPS infrastructure.
- This CPS infrastructure would be less vulnerable to counterfeiting, tampering and false certification than existing solutions.
- Introduce a new paradigm for part identification by requiring a measured identity to match an accepted identity instead of asserting a match between shallow identifiers (barcodes or serial numbers).

Broader Impact:

- Will enhance security and safety of CPSs systems in light of current counterfeiting threats.
- Will impact industries that rely on intricate supply chains and have difficulty in tracking the parts in circulation.
- Will educate current and future workforce about importance of CPS security and the consequences of cross-domain vulnerabilities.
- The proposed approach promotes a new paradigm of security for CPSs where physical properties are encoded into a digital identity to parallel CPS interactions between cyber-space and physical space.