Development of Additively Manufactured Cryptographic Structures for Tamper Detection

Francisco Gonzalez-Castillo
Advisor: Dr. Derek Haas
The University of Texas at Austin
fragonz@utexas.edu

Abstract:

Within the nuclear nonproliferation regime, tamper detection ensures nuclear equipment and materials are kept out of the hands of adversaries. Tamper-detection systems (TDS), such as Tamper-indicating devices or enclosures are at the forefront of this effort and usually take the form of seals applied to nuclear material canisters or equipment that leave unambiguous proof of unauthorized access to a container of interest. TDSs are critical for ensuring the compliance and safety of nuclear materials and equipment worldwide. However, there are gaps in tamper-detection standards or "theory" for what characteristics qualify an effective TDS. One plausible avenue for the development of tamper-detection theory is to map the principles of adjacent security research to applications in nonproliferation. Research in developing anti-counterfeiting measures for AM components in medicine and aerospace is a growing subset of research that may apply to similar research in nuclear nonproliferation compliance. Embedding high-security features like physical unclonable functions (PUFs) into AM components is an example of a robust cryptography technique that contains the level of security needed for a critical application like nonproliferation. PUFs leverage inherent entropic properties of components and systems to generate physical cryptography with in-house authentication techniques that are purposefully obfuscated to prevent adversaries from replicating or decrypting them. Applying cryptographic structures to AM components shows great promise in addressing the growing need for versatile and high-security TDSs. Once a tamper-detection theory is in place, designers across the field of tamper-detection can leverage its principles to develop robust and effective TDSs. Correspondingly, the research will also be able to advance into a development stage in which we will work toward integrating tamper-detection theory and additive manufacturing design principles to develop TDSs that realize the benefits of additive manufacturing.