System to secure cryptographic keys and codes for data protection

July 25 2017, by Chris Blake

IBM today announced that its engineers have been granted a patent on an approach for utilizing the inherent structure of a printed circuit board (PCB) to protect cryptographic keys and codes in a manner that is designed to be highly tamper-resistant. The patented system does not require extensive use of resin or other materials to encase a module or package containing keys and codes, thereby providing the opportunity for significant improvement in manufacturing yield, as well as a decrease in repairs needed in the field due to package reliability. The invention could help protect keys and codes that encrypt data stored on any platform whether your data is in the cloud or an enterprise storage system.

Protecting cryptographic keys and codes that are used to encrypt and decrypt data is fundamental to effective information security. When cryptographic keys and codes are stored on modules within an electronic device, preventing physical tampering or access to those modules is important to help prevent the keys and codes from being compromised.

IBM was granted U.S. Patent 8,938,627: Multilayer securing structure and method thereof for the protection of cryptographic keys and code for this invention.

Traditional approaches to prevent tampering have typically involved encasing or "potting" modules in a plastic or epoxy-like resin. While these approaches have been generally effective in preventing tampering, other problems such as the deformation and warping of circuit boards on

which encased modules reside during resin curing continue to be challenges during manufacturing.

"At IBM, there are teams engaged in inventing and innovation on data protection and security which are fundamental cornerstones of our global digital future. We had this in mind when creating this innovation." said Stefano Oggioni, Engineering Manager, IBM Systems and co-inventor on the patent.

IBM's patented approach uses circuitry on layers of a PCB or other laminated structure to encode the cryptographic keys and codes. Additional layers of the PCB or laminate structure, which are added above and below the layers containing the keys and codes, act as physical access barriers. The circuitry protecting the keys and codes can be placed in random patterns or locations within the PCB or laminate structure to prevent access or discovery. The circuitry in the approach is also comprised of materials which are undetectable via X-ray inspection or acoustic microscopy thereby further enhancing the security of the keys and codes.

IBM has been working in this area for decades, and last week announced IBM Z, the next generation of the world's most powerful transaction system, capable of running more than 12 billion encrypted transactions per day. The patented system is part of the pipeline of technologies reflected in the design of IBM Z and other IBM Systems.

More information: patft.uspto.gov/netacgi/nph-Pa … patentnumber=8938627

Provided by IBM