HOW CAN SECURE SOFTWARE PROTECTION WITH A PUBLIC METHOD WORK?

BlurryBox®: Software Protection by Kerckhoffs‘s Principle

BlurryBox® is an innovative procedure for software protection with provable security features. The procedure was developed in cooperation between the FZI, KIT and WiBu-Systems AG and was the winner of the German Prize for IT-Security. The demonstrator illustrates its principles and functionality in a playful way. The possible applications of BlurryBox® range from the protection of traditional software to the protection of industrial plants.

“The security of a cryptographic procedure shall be only dependent on the secrecy of the key but not on the secrecy of the procedure.“

This rule called Kerckhoffs’s principle is the basis for all modern encryption methods. When this rule is followed, none of the applications protected by this procedure can be threatened solely due to the fact that the procedure has become known. However, this principle has not been established yet in the field of software protection. The effectiveness of all common methods relies on their secrecy.

BlurryBox® is the first software protection procedure whose security relies on the secrecy of a key. For that, BlurryBox® takes advantage of the inherent complexity of the software to be protected. The more complex the software is, the more effective is the protection. BlurryBox® splits up the software to be protected into many small parts and decrypts them only when necessary. The decryption can be only carried out by a secure hardware component whose key cannot be read. An attacker who seeks to copy protected software has no other choice than to use all different parts of the programme in order to make sure that all parts of the programme are decrypted – if the protected code is complex enough, this is virtually impossible.

The demonstrator shown at CeBIT allows the visitors to comprehend the functionality of the BlurryBox® procedure in a playful way. For that purpose, the visitors can play a simple game that is protected by BlurryBox®. At the same time, they can attack the copy protection while watching the game run.

The fields of application of BlurryBox® are almost unlimited: whether copy protection of office software, the protection of motor controls or the protection of integrated systems in industrial plants. BlurryBox® is applicable to almost all systems with complex software and provides formally provable software protection according to Kerckhoffs’s principle.

CONTACT PERSON

Matthias Huber | mhuber@fzi.de | Phone +49 721 9654-666

ABOUT THE FZI

The FZI Research Center for Information Technology at the Karlsruhe Institute of Technology is a non-profit institution for applied research in information technology and technology transfer. Its task is to provide businesses and public institutions with the latest research findings in information technology. For more information visit: www.fzi.de