Karlsruhe Institute of Technology

Competence Center for Applied IT Security Technology (KASTEL)

Institute of Theoretical Informatics

Software Protection in Accordance with Kerckhoffs's Principle

Considering the fact that software has an increasing share in value creation, software protection becomes a more and more important branch of IT security. Software protection prevents copying and reverse engineering of software products and hence is a reliable protection against industrial espionage. In addition, it is a basis for tamper-proof software and thus protects the industry of the future from cyber sabotage.

Conventional software protection solutions rely on keeping their mechanisms secret. For hackers who know these methods sufficiently well, it is relatively easy to break the software protection. This violates Kerckhoffs's principle which dictates that the security of an IT system should depend solely on the secrecy of a (short) key and NOT on the secrecy of the security mechanisms. There are methods that guarantee an efficient software protection in accordance with Kerckhoffs's principle. However, these solutions are useless in practice due to the application of extremely complex techniques. Compared with these solutions, it would be less expensive to include for each program a dedicated computer that only runs this software and does not leak the program code. By contrast, Blurry-Box® only uses a small external hardware – the so-called dongle (see illustration).

The Blurry-Box® approach obeys Kerckhoffs's principle and even proves the security of the software protection. This proof is based on a simple premise: The adversary (hacker)

Security Token, Wibu-Systems

does not (completely) know the inner workings of the protected program since otherwise he could just write the program himself, and would not have to break the protection. Based on this assumption, one can prove that a hacker can only gain obvious information about the program: He can input data and receive the corresponding outputs. Knowledge about the security mechanisms does not help him here.

In order to reach this goal, the complexity of the program flow is exploited. Every section of an execution path is split into various parts, each of which is encrypted separately.

The PC requests the key for the required part and decrypts it with the received key. Moreover, the links between sections are computed in the protected RAM of the dongle. By this means, the dongle can monitor the execution order.
This compliance with Kerckhoffs's principle allows for independent analysis and assessment of security. This is a great advantage over all previous solutions whose mechanisms have to be kept secret. Blurry-Box® offers advantages in the protection against industrial espionage and sabotage and leads to excellent market opportunities for systems that are protected through this method.

The first place in the IT Security Contest was reached by the application of Kerckhoffs's principle for software protection (© RUB, Photo: Sadrowski)

Karlsruhe Institute of Technology
Am Fasanengarten 5
76131 Karlsruhe, Germany

Prof. Dr. Jörn Müller-Quade
Institute of Theoretical Informatics
Phone: +49 721 608-44205
E-mail: crypto-info@iti.kit.edu

KASTEL

Zertifikat seit 2010
audit familiengerechte hochschule