Aalto University

Dissertation press release 29.05.2020

White-Box Cryptography for Mobile Payment Applications and more

Title of the dissertation

On the Foundations of White-Box Cryptography

Contents of the dissertation

White-box cryptography has been embraced by the payment industry as a method for increasing the security of mobile payment applications. The aim is to protect an application from an adversary in the form of malware who might gain access to the implementation code of the application and might be in control of its execution environment. Here, white-box cryptography should stop the adversary from misusing the application or extracting sensitive information from it. Although widely deployed for commercial purposes, white-box cryptography has received less attention from the scientific community.

The goal of this dissertation is to provide clarity and motivation towards the foundational studies of white-box cryptography, its security goals, its feasibility and the vulnerability of real-life implementations to popular attack strategies. The work presents formal definitions capturing central security properties for white-box programs when used for protecting mobile payment applications. One example is the property of hardware-binding, which states that a white-box program should only be functional when used in combination with a specific hardware device. The work proposes to focus on this property and also explains how hardware-binding can be achieved, providing theoretical feasibility results.

This dissertation also studies the success of popular attack methodologies on real-life white-box implementations, such as the differential computation analysis, analyzing the reasons why this attack is able to break a large class of implementations. The analyses let conclude that popular design frameworks for white-box cryptography do not provide the desired security, and also give insights on how the security of such implementations can be increased.

Field of the dissertation

Mathematics, Computer Science, Cryptography

Doctoral candidate

Estuardo Alpirez Bock, M.Sc.

Time of the defence

12.06.2020 at 16:00

Place of the defence

Held remotely via Zoom: https://aalto.zoom.us/j/65850868700

Opponent

Dr. Pascal Paillier, CryptoExperts, France

Custos

Professor Chris Brzuska, Aalto University School of Science, Department of Mathematics and Systems Analysis

Electronic dissertation

http://urn.fi/URN:ISBN:978-952-60-3922-0

Doctoral candidate’s contact information

Estuardo Alpírez Bock, estuardo.alpirezbock@aalto.fi