

# Understanding The Advantages Of Irdeto's White-Box Cryptography

December 2012

# Table of Contents

1. Executive summary	3
2. Introduction	3
3. The need for white-box cryptography	3
4. What is white-box cryptography?	4
5. Black-box attack	5
6. White-box attack	5
7. The history of white-box cryptography	5
8. Irdeto's white-box advantages	6
9. High performance	6
10. Sized for any application	7
11. Security, diversity an renewability	7
12. What to look for in a white-box solution	7
13. Conclusion	9

# 1. Executive summary

Conventional cryptographic algorithms used to protect software keys and data are ineffective when operating in “white-box” environments, where a hacker has full visibility and control over the executing code. Irdeto’s white-box cryptography patented technology offers many advantages over other cryptography alternatives, including the unique capability of not revealing keys or data while the cryptographic computations are being observed in complete detail, thus ensuring that sensitive data remains secure. When selecting software protection solutions, developers should ensure they understand the capabilities and effectiveness of their alternatives.

## 2. Introduction

In the evolving realm of software security, white-box cryptography is emerging as a key technology to combat hacking and intellectual property (IP ) theft in unsecure or untrusted environments. Software developers seeking to reduce their code’s vulnerability to attack should understand the benefits of white-box cryptography and what to look for when selecting a solution.

## 3. The need for white-box cryptography

Popular trusted ciphers like RSA and AES were not designed to operate in environments where their execution could be observed. In fact, the standard cryptographic model is that communications endpoints and computing platforms are assumed to be trusted. If the target device resides in a hostile environment,

then the cryptographic keys may be directly visible to an attacker. An attacker may be able to monitor the application and extract one or more cryptographic keys embedded or generated by the application. This is a common problem for PCs, set top boxes and other devices where DRM , conditional access or other security sensitive applications are involved. Hackers monitor standard cryptographic API s or memory and simply grab keys when exposed. Two recent examples of successful memory-based key lifting attacks are the AA CS/BackupHDDVD hack that lifts the AA CS keys from memory to enable the BackupHDDVD tool to copy the disc, and the FairUse4WM utility that removes the DRM from protected Windows Media content.

#### THE WHITE-BOX PROBLEM

How to encrypt or decrypt content without directly revealing any portion of the key or data?

White-box cryptography is required when a hacker can observe and/or alter code execution.

## 4. What is white-box cryptography?

In traditional cryptography, a black-box attack describes the situation where the attacker tries to obtain the cryptographic key by knowing the algorithm and monitoring the inputs and outputs, but without the execution being visible. White-box cryptography addresses the much more severe threat model where the attacker can observe everything, can access all aspects of the target system/ application, and may have the black-box knowledge of the crypto algorithm.

## 5. Black-box attack

- Attacker knows algorithm
- Watches inputs and outputs
- Controls input text
- No visibility of execution

## 6. White-box attack

- Attacker can observe everything
- Attacker knows algorithm
- Watches inputs, outputs, intermediate calculations
- Controls input text
- Full visibility into Memory (debuggers and emulators)

## 7. The history of white-box cryptography

Irdeto's technology team coined the term white-box and pioneered its introduction into the market. The patent-pending white-box design has been a key component of Irdeto's software security suite since the WB AES solution was first deployed in 2002, followed by WB RSA in 2005. Since then, it has formed the cornerstone of virtually all Irdeto's customers' software protection architectures. Now in its 5th product generation, Irdeto's white-box cryptography based on Irdeto's technology has successfully withstood academic scrutiny as well as extensive field testing while actively protecting cryptographic keys in well over one billion security applications worldwide.

Taking a closer look at the technology, Irdeto's white-box cryptography remains the only solution on the market to protect the whole cryptographic key at all times, rather than breaking the key up and revealing it only a piece at a time. From a security perspective, this ensures that the protected key remains hidden from hackers and is not susceptible to piecing back together in the clear during the attack process.

## 8. Irdeto's white-box advantages

Irdeto's white-box cryptography technology operates without revealing keys or data while the cryptographic computations are being observed in complete detail. Irdeto's white-box solution is not merely an obfuscation technique, but rather is a white-box attack-secure implementation of standard cryptographic algorithms. The cryptographic libraries enable developers to quickly enhance their applications with the highest level of software security available. Irdeto has developed customized white-box cryptographic library routines for AES , RSA and other ciphers.

## 9. High performance

From a performance perspective, because Irdeto's white-box approach does not require any fragmented computations revealing the key, the performance of the cryptographic functions remains comparable with that of standard cryptographic algorithms. The fully protected Irdeto white-box AES implementation supports High Definition video streams on a variety of platforms, from small, embedded devices to standard PCs.

## 10. Sized for any application

From a size perspective, Irdeto's white-box technology provides customers with a selection of white-box secure algorithms, offering a variety of security, performance and size options to enable deployment on a wide range of platforms—a key benefit for embedded software devices.

## 11. Security, diversity and renewability

Irdeto's white-box technology takes advantage of Diversity technology, allowing customers to easily deploy multiple versions of the white-box implementation. This results in different customers or customer-sets having unique binary instances of both the whitebox implementation as well as fully unique sets of cryptographic tables. This significantly reduces the scope and impact of a compromised key by constraining the breach to a limited subset of the installed base. As a result, a hacker is prevented from creating a single automated tool which can attack the entire installed base. In addition, the limited subset of affected applications can rapidly be renewed with a fresh set of diverse keying material.

## 12. What to look for in a white-box solution

When selecting a white-box cryptography toolkit, software developers should understand the differences between various solutions. The following simple questions can be used to help evaluate the capability and effectiveness of the alternatives.

## WHAT TO LOOK FOR IN A WHITE-BOX SOLUTION

When selecting a white-box cryptography toolkit, software developers should understand the differences between various solutions. The following simple questions can be used to help evaluate the capability and effectiveness of the alternatives.

### DO KEYS OR PARTS OF KEYS EVER SHOW UP IN MEMORY?

With Irdeto's white-box cryptography, keys, in whole or in part, never show up in memory.

### DOES THE SOLUTION SUPPORT SYMMETRIC AND ASYMMETRIC CRYPTOGRAPHY?

Irdeto's white-box cryptography supports both RSA (asymmetric) and AES (symmetric) ciphers.

### CAN THE PERFORMANCE AND SECURITY LEVEL BE TUNED FOR DIFFERENT PLATFORMS?

Irdeto's white-box cryptography can be optimized to perform effectively on any platform up to and including High Definition video protection systems.

### HAVE THE DESIGN AND IMPLEMENTATION BEEN PUBLISHED AND SCRUTINIZED BY THE INTERNATIONAL CRYPTOGRAPHIC COMMUNITY?

Some software security vendors are not willing to have their proprietary cryptographic algorithms reviewed and critiqued by industry experts. In contrast, Irdeto's white-box cryptography based on Irdeto's patented white-box implementation of industry-standard cryptographic algorithms have been publicly documented and validated by cryptography experts world-wide.

## 13. Conclusion

Irdeto's white-box cryptography solutions operate without revealing keys or data while the cryptographic computations are being observed in complete detail. White-box implementations are simple replacements for existing cryptographic functions. The libraries enable designers to quickly add industry-leading software security to their applications.

Irdeto's white-box cryptography is a component within Irdeto's Security Suite, a collection of automated tools that enable developers to protect their application code against reverse engineering, tampering, and automated attacks. Irdeto's security techniques protect applications through data and control flow obfuscation, anti-debug, white-box cryptography, integrity verification and executable encryption. Irdeto's technology integrates into the software build process, embedding application protection directly at the source code level. The tools provide a highly effective, multi-layered, and tunable approach to software protection.

#### REFERENCES

2002 S. Chow, P. Eisen, H. Johnson and P.C. van Oorschot.  
White-box cryptography and an AES implementation. In Proc. 9th  
International Workshop on Selected Areas in Cryptography (SA C  
2002), pages 250-270. Springer LN CS 2595, 2003.

©2012 Irdeto. All Rights Reserved.

This document and the information contained herein is the subject of copyright and intellectual property rights under international convention. All rights reserved. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form by any means, electronic, mechanical or optical, in whole or in part, without the prior written permission of Irdeto. All non-Irdeto company names, product names, and service names mentioned are used for identification purposes only and may be the registered trademarks, trademarks, or service marks of their respective owners. All information is without participation, authorization, or endorsement of the other party.