



Cloakware White-box Cryptography

Cryptographic Key Protection by Transformation

KEY FEATURES

- Easy to use tools and library model
- White-box AES, RSA and ECC APIs

KEY BENEFITS

- Secures your software and IP from non-trusted environments.
- Provides secure cryptographic functionality
- Flexible deployment for device manufacturers

SUPPORTED PLATFORMS

- ANSI C and C++ for all major platforms
Linux, Macintosh, Windows, Symbian Embedded devices

Introduction

With Cloakware White-box cryptography, keys, in whole or in part, never show up in memory.

Conventional cryptographic implementations 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. Cloakware White-box 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.

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.

Challenge

Encrypt or decrypt content without directly revealing any portion of the key or data, in a white-box environment.

BLACK BOX ATTACK

- > Attacker knows algorithm
- > Attacker watches inputs and outputs
- > Attacker controls input text
- > Attacker No visibility of execution

WHITE-BOX ATTACK

- > Attacker can observe code execution
- > Attacker knows algorithm
- > Attacker watches inputs, outputs, intermediate calculations
- > Attacker controls input text
- > Attacker full visibility into memory (debuggers and emulators)

ABOUT CLOAKWARE

Cloakware, an Irdeto company and part of the Naspers group, provides innovative, secure, proven software technology solutions that enable customers to protect business and digital assets in enterprise, consumer and government markets. Cloakware's two main product lines include: Cloakware Datacenter Solutions which help organizations meet governance, risk management and compliance (GRC) objectives for privileged password management while ensuring business continuity and the security of mission-critical data and IT infrastructure. Cloakware Consumer Product Solutions protect software and content on PCs, set-top boxes, mobile phones and media players. Protecting more than one billion deployed applications today, Cloakware is the security cornerstone of many of the world's largest, most recognizable and technologically advanced companies. Headquartered in Vienna, VA and Ottawa, Canada, Cloakware has regional sales offices worldwide.

CONTACT INFORMATION

Corporate Headquarters

Cloakware Inc.
8219 Leesburg Pike, Suite 350
Vienna, VA, USA 22182
Tel. +1.703.752.4830

Canada

Cloakware Corporation
84 Hines Road, Suite 300
Ottawa, ON, Canada
K2K 3G3
Tel. +1.613.271.9446

www.cloakware.com

The need for white-box cryptography

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

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.

Cloakware white-box cryptography

Cloakware White-box Cryptography implements standard cryptographic algorithms in a way that hides critical keys in environments where hackers can observe cryptographic operations in complete detail. Popular, trusted ciphers like AES, RSA and ECC are among the most thoroughly studied algorithms, making them particularly vulnerable targets for attacks such as lifting keys from memory. Cloakware White-box Cryptography ensures that critical keying data is not revealed—even during cryptographic operations.

Keying methods supported:

- > Fixed keys (key determined in advance)
- > Dynamic key (key provided during run time)

Cloakware white-box advantages

Cloakware White-box Cryptography operate without revealing keys or data while the cryptographic computations are being observed in complete detail. Cloakware 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. Cloakware has developed customized white-box cryptographic library routines for AES, RSA, ECC and other ciphers.

Conclusion

Cloakware 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.