SOFTWARE PROTECTION

WHITEBOX

verimatrix
DRIVING TRUST

Verimatrix® is the leading provider of software security solutions. Whitebox enables you to build, control and trust your own software crypto-security.

Key features

- Protect sensitive data, keys and algorithms even when running in exposed environments.
- No added dependences so apps can easily be deployed anywhere.
- Retain full control of business-critical crypto keys.
- Flexible to meet application architecture and security needs.
- High performance, even on restricted devices such as Mobile and IoT.

Algorithms

- AES
- AES-GCM
- Blowfish
- (3)DES
- HMAC
- OMAC
- KDF
- SHA-1, SHA-2
- RSA
- ECC-derived algorithms, including ECDSA
- Elgamal
- Diffie-Hellman
- HMAC
- OMAC

When applications run in an exposed environment, an attacker can see everything the app is doing – including any secrets within it. Cryptography is used to hide those secrets but if the crypto is exposed, then so are the secrets. Verimatrix's whitebox technology can hide those secrets.

Other technologies to hide secrets, such as TEE, add a dependency on hardware. This can be costly – developers need to pay for access; and is limiting – not all devices will have the required hardware. Verimatrix's pure software approach means that an application can support any device and there are no provisioning fees. According to Gartner, this is achieved without compromising security.

Verimatrix gives our customers unprecedented control and flexibility. By providing our customers with tools to generate their own whiteboxes, we give them flexibly to define and implement the software architectures they need. While being able to generate the whiteboxes themselves means our customers are the only entity that has control over the keys that unlock the whiteboxes.

Protect Cryptography

To keep data safe within your application, it needs to be managed within **a secure cryptographic boundary** – never leaving that boundary in the clear. This is not possible with standard cryptographic implementations that expose their secrets under simple software analysis.

Verimatrix's Whitebox achieves this secure boundary by dissolving the cryptographic keys into the code and obscuring the algorithms. **This keeps the keys, algorithms and data safe** – even when the attacker has complete access to the device on which the algorithms are executing.

Keep Control of Your Keys

Traditional Whitebox vendors provide **a pre-compiled library** - meaning that it is the vendor who owns the key that "unlocks" the Whitebox. These keys are often shared with multiple customers, meaning some else's insecure application can put yours at risk. With Verimatrix's Whitebox, you are in control of your own keys. Verimatrix never sees them and they can never be shared by other Whitebox implementations.

Customising for Security

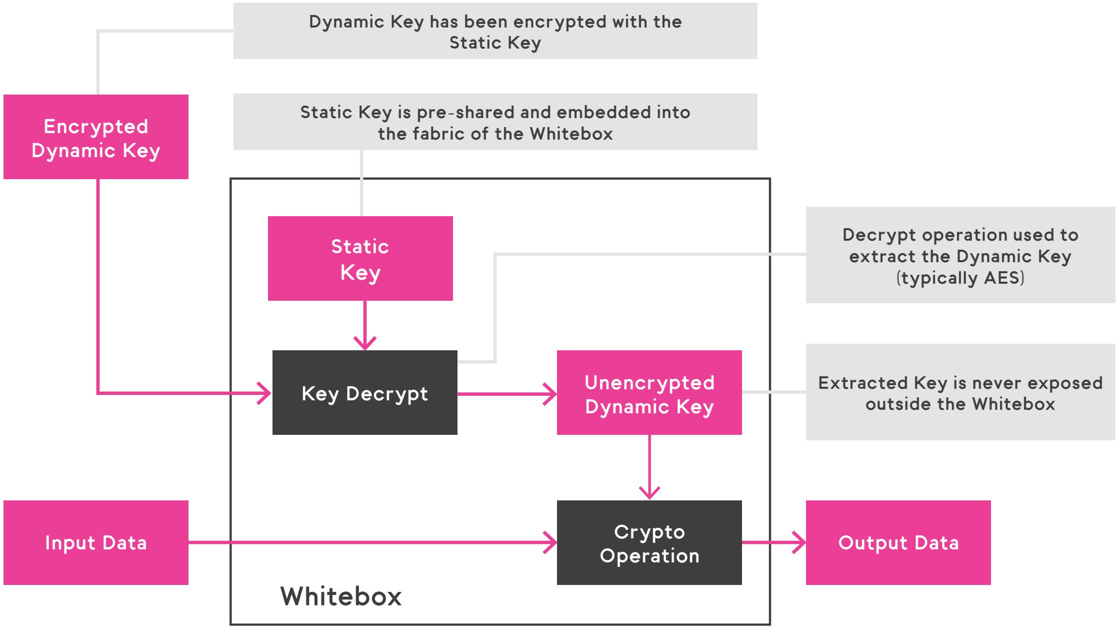
Verimatrix provides a toolkit that allows you **to define your own Whiteboxes**, including multiple algorithms within a single Whitebox if desired.

Being able to define a custom Whitebox ensures it is unique to you. **This stops attackers** anticipating how to analyse and attack your Whitebox. It also ensures they cannot use existing knowledge from other applications that have received the same Whitebox from the vendor.

Performance through Flexibility

Being able to define the optimum Whitebox for your needs **brings massive performance gains**. By chaining algorithms within a single Whitebox, complex operations can be performed without the need to jump between multiple Whiteboxes.

Also, Verimatrix's Whitebox is tuneable to meet your required performance. It is used in everything from high performance Mobile Payment solutions to software "HSMs".


Dynamic Key has been encrypted with the Static Key
Static Key is pre-shared and embedded into the fabric of the Whitebox
Encrypted Dynamic Key
Static Key
Decrypt operation used to extract the Dynamic Key (typically AES)
Key Decrypt
Unencrypted Dynamic Key
Extracted Key is never exposed outside the Whitebox
Input Data
Crypto Operation
Output Data
Whitebox

For further details on all of Verimatrix's security solutions, visit www.verimatrix.com

verimatrix
DRIVING TRUST