VERIMATRIX WHITEBOX

verimatrix DRIVING TRUST

Verimatrix 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 dependencies, so apps can easily be deployed anywhere
- Retain full control of business-critical crypto keys
- Easily design and create your crypto architectures with our graphical designer
- 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

Cryptography helps to secure data in transit and at rest. But what if the cryptographic operations and keys themselves are exposed? That is exactly what happens when software is executing on an open platform like a mobile phone or IOT device – an attacker can see everything the software is doing including any cryptographic operation.

WhiteBox Advantage

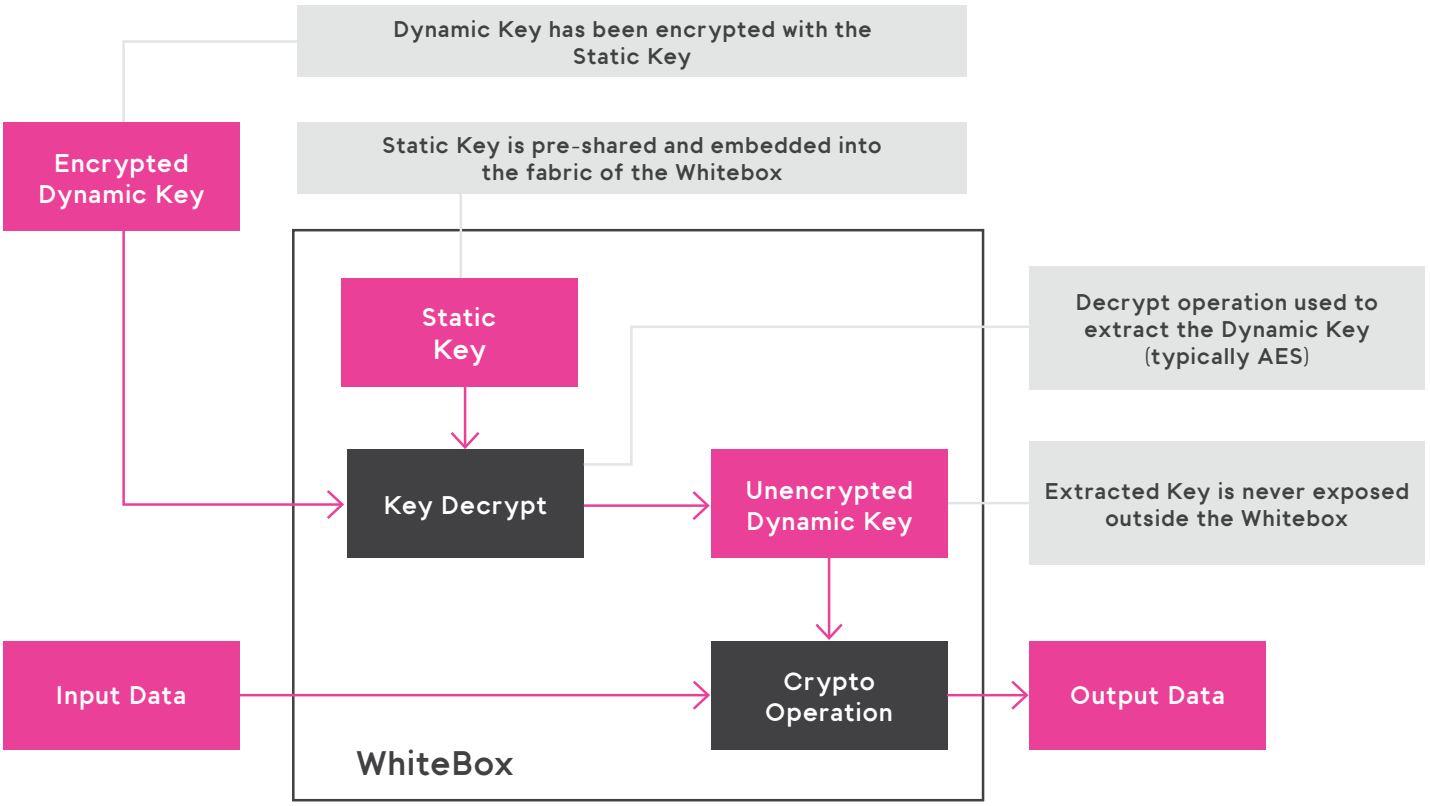
Verimatrix's WhiteBox enables you to build, control and trust your own software crypto-security. It does this in a pure software environment, without the need for expensive and resistive hardware.

Other technologies to hide secrets, such as trusted execution environment (TEE), add a dependency on hardware. This can be costly and cumbersome – access needs to be arranged and paid for, this can vary from device to device. Verimatrix's pure software approach means that an application can support any device, with no provisioning fees.

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 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.



Control 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 implementations.

Customizing for Security

Verimatrix provides the tools that allows you to define your own WhiteBoxes, including multiple algorithms within a single implementation if desired. Our unique graphical designer allows you to quickly and easily define your error-free crypto architecture.

Being able to define a custom WhiteBox ensures it is unique to you. This keeps attackers from anticipating how to analyze and attack. 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, complex operations can be performed without the need to jump between multiple implementations. Verimatrix's WhiteBox is also tunable to meet your required performance. It is used in everything from high-performance Mobile Payment solutions to software "HSMs."

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

verimatrix™
DRIVING TRUST