



CODE PROTECTION

WHITEBOX

verimatrix
DRIVING TRUST

Verimatrix®는 소프트웨어 보안 솔루션의 선도적인 공급업체입니다.
Whitebox는 소프트웨어 암호 보안을 스스로 빌드하고 제어하며 신뢰할 수 있도록 지원합니다.

주요 특징

- 노출된 환경에서 실행될 때에도 민감한 데이터, 키 및 알고리즘을 보호합니다.
- 추가된 종속성이 없기 때문에 어느 곳에도 앱을 간편하게 배포할 수 있습니다.
- 중대한 비즈니스 암호 키에 대한 완전한 통제력을 보유합니다.
- 그래픽 디자이너 툴을 통해 함께 암호 아키텍처를 쉽게 설계하고 생성합니다.
- 모바일 및 IoT 같은 제한된 장치에서도 높은 성능을 발휘합니다.

알고리즘

- AES
- AES-GCM
- Blowfish
- (3)DES
- HMAC
- OMAC
- KDF
- SHA-1, SHA-2
- RSA
- ECC 파생 알고리즘 (ECDSA 포함)Elgamal
- Diffie-Hellman
- HMAC
- OMAC

암호법은 전송 데이터와 저장 데이터의 보안에 유용합니다. 그러나 소프트웨어가 휴대폰이나 IoT 장치 같은 오픈 플랫폼에서 실행되는 경우와 같이, 암호화 연산과 키 자체가 노출된 경우는 어떨까요? 공격자는 암호화 연산을 포함해서 소프트웨어가 하고 있는 모든 것을 볼 수 있습니다.

Whitebox의 장점

Verimatrix의 Whitebox는 자체 소프트웨어 암호 보안을 구축하고 제어하며 신뢰할 수 있도록 지원합니다. Whitebox는 고가의 하드웨어를 추가로 사용할 필요없이 순수한 소프트웨어 환경에서 이렇게 지원합니다.

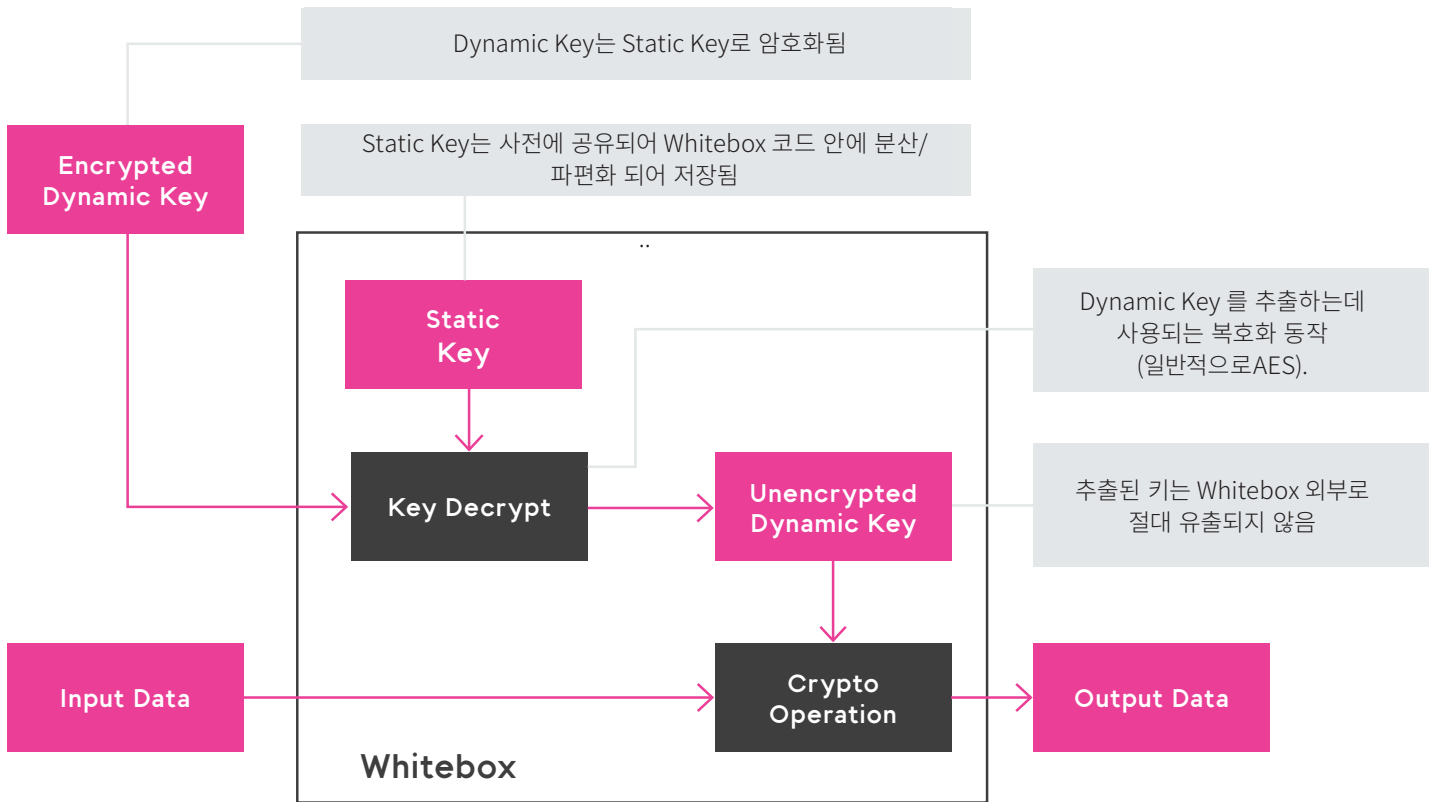
Trusted Execution Environment(TEE)와 같은 비밀을 숨기기 위한 다른 기술은 하드웨어에 대한 종속성을 추가합니다. 비용이 많이 들고 번거로울 수 있는데, 액세스하기 위해 계획을 세워야 하고 비용을 지불해야 하며 장치 별로 다를 수 있습니다. Verimatrix Whitebox는 순수 소프트웨어 기술로 추가적인

프로비저닝 요금 없이, 어느 장치에서나 사용할 수 있습니다.

보호 암호법

데이터를 어플리케이션 내에서 안전하게 지키려면 데이터는 안전한 보안영역내에서 관리되어야 하고 절대로 보안영역을 벗어나지 않아야 합니다. 이는 간단한 소프트웨어 분석으로도 중요데이터를 노출시키는 기존의 구현방식으로는 불가능합니다.

Verimatrix의 Whitebox는 암호화 키를 코드 안으로 분해시키고 알고리즘을 모호하게 하여, 이 보안 영역을 구현합니다. 이렇게 하면 공격자가 알고리즘이 실행되고 있는 장치에 완전히 액세스할 수 있는 경우에도 키와 알고리즘, 데이터를 안전하게 지킬 수 있습니다.



키 제어

전통적인 Whitebox 판매사는 사전 컴파일된 라이브러리를 제공하는데, 이는 판매사가 Whitebox를 “잠금 해제(unlocks)” 하는 키를 소유하고 있다는 뜻입니다. 이들 키는 종종 여러 고객과 공유되는데, 이는 곧, 누군가 다른 사람이 안전하지 않은 어플리케이션을 위험에 처하게 할 수 있다는 뜻입니다. Verimatrix의 Whitebox를 이용하면 자신의 키를 제어할 수 있습니다. Verimatrix는 키를 절대 볼 수 없으며 키는 다른 구현과 절대로 공유될 수 없습니다.

보안을 위한 커스터마이징(Customizing)

Verimatrix는 원하는 경우 단일 구현 내에 있는 여러 알고리즘을 포함해서 자체 Whitebox를 정의할 수 있는 도구를 제공합니다. 오류 없는 암호 아키텍처를 빠르고 쉽게 정의할 수 있도록 당사 고유의 디자이너 툴을 지원합니다.

Custom Whitebox를 정의하여 고유한 Whitebox를 만들 수 있습니다. 이는 분석 및 공격 방법을 공격자가 예측할 수 없게 하고, 동일한 Whitebox를 사용한 다른 어플리케이션에서 얻은 기존 지식을 이용한 공격을 불가능하게 합니다.

유연성을 통한 성능

필요에 맞는 최적의 Whitebox를 정의할 수 있는 능력은 큰 성능 이득을 제공합니다. 알고리즘을 변경하는 것을 통해, 여러 개의 Whitebox를 구현하지 않고도, 복잡한 기능을 쉽게 조작을 수행할 수 있습니다. Verimatrix의 Whitebox는 필요한 성능에 맞게 조정할 수 있고, 고성능 모바일 결제 솔루션부터 소프트웨어 “HSM”까지 모든 것에 사용할 수 있습니다.

모든 Verimatrix 솔루션에 대한 보다 자세한 정보는

www.verimatrix.com에서 확인하십시오.

이 문서에 있는 정보는 법적으로 구속력을 발휘하기 위한 것이 아닙니다. Verimatrix 제품은 Verimatrix의 판매 조건 또는 Verimatrix와 고객이 체결하고 이행하는 계약의 조항에 따라 판매됩니다. © Verimatrix 2019. All Rights Reserved. Verimatrix, Verimatrix 로고와 그 조합 및 기타는 Verimatrix 또는 그 자회사의 등록 ® 상표 또는 상표명입니다.

다른 용어와 제품 이름은 다른 회사의 상표일 수 있습니다. 여기에서 설명한 제품은 관련 데이터시트에 열거된 하나 이상의 특허 및/또는 특허 출원의 보호를 받을 수 있으며, 그러한 문서는 특정 조건 하에서 요청에 따라 제공됩니다. 또한 지역에 따라 추가적 특허 또는 특허 출원이 적용될 수 있습니다.



T : 070.7510.1000

E : softwareprotection@ksmartech.com