COMMSCOPE®

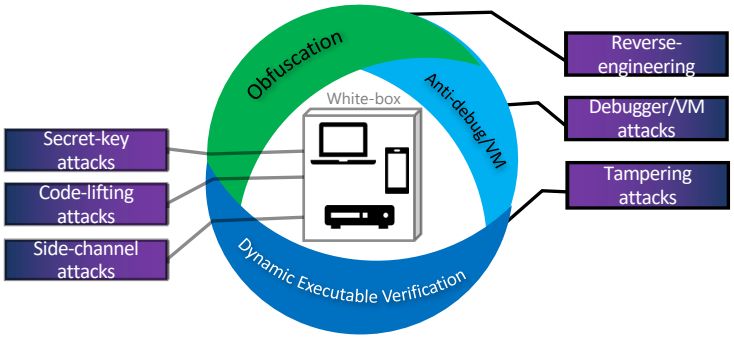
CipherKnight™ & BinaryKnight™ Protection Suite

Secure your software against threats

Why Protect Your Application?

- Application attacks grew by 88% in 2021
- Distributed denial-of-service and injection attacks represent 75% of exposures
- The OWASP top 10 software vulnerabilities increased yearly by 20% in average
- Reverse engineering tools are more sophisticated
- Sensitive data and software exposures are more evident
- User/device credentials leaks are proven to be costly resulting in IP loss
- Cost of "doing nothing" is higher over time!

CipherKnight™ and BinaryKnight™ Protection Suite Snapshot



The Challenge

How to address security gaps created by a growing demand for quickly deployable and securely protected applications?

The Solution

Utilizing a combination of innovative solutions such as white-box cryptography, software obfuscation and code signing, CommScope's suite balances protection and performance while allowing users to design, code and build to suit their needs.

Capability	Open Source	Others	CommScope
White-box node-locking	✗	✗	✓
Data Flow Protection	✗	✗	✓
OpenSSL Engine (TLS/SSL)	✗	✗	✓
Dynamic Verification	✗	✗	✓
Tunable	✗	✓	✓
Protection Audit Report	✗	✓	✓
Binary Object Obfuscation	✗	✓	✓
Cloud-based Obfuscation	✗	✗	✓
Fully Customizable White-box	✓	✗	✓
Java Obfuscation	✓	✓	✗

Modules

CipherKnight™ White-box

Secures software against key-extraction, code-lifting and side-channel attacks; and enables the implementation of standard ciphers such as RSA, AES, and ECC in such a way that no keys or other sensitive data is exposed.

BinaryKnight™ Protect

Provides a further layer of protection against reverse engineering, debugger attachment, and tampering attacks.

www.pki-center.com | pki-center@commscope.com

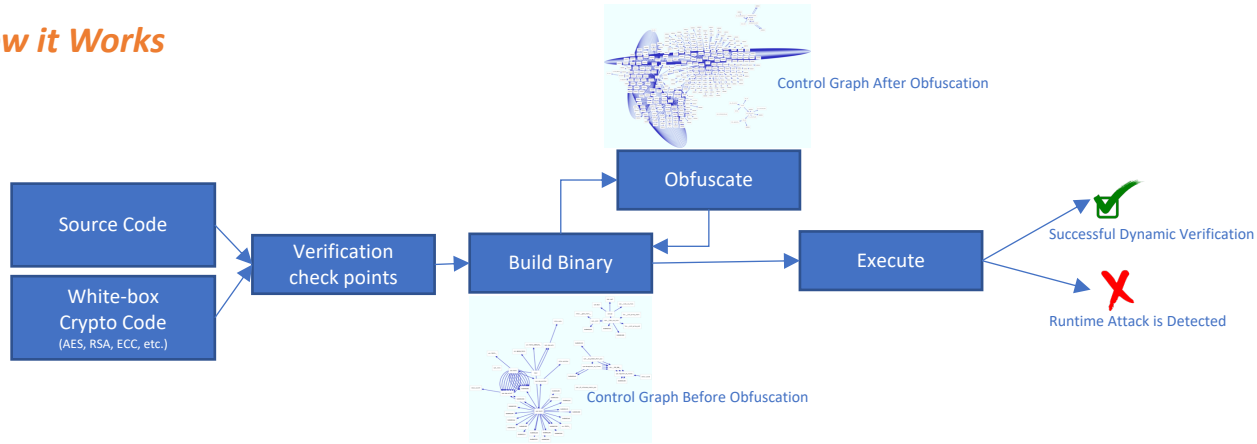
CommScope CipherKnight™ White-Box

Secure	• Static or dynamic white-boxes • Secure chaining • Node-locking
Customizable	• Standard algorithms: AES, RSA, ECC, DH and SHA in white-box • Custom white-boxes with KDFs • Balance security vs. performance
Proven	• Patented Technologies • Peer-reviewed and Audited • Backed by ongoing research
Universal	• Platform independent C++ lib • Usage of White-box APIs • Compatible with OpenSSL

CommScope BinaryKnight™ Protect

Obfuscation	• Resilience against reverse-engineering • Data-flow and Control-flow obfuscation • Fully tunable
Anti-debug Defenses	• Debugger detection and response • Randomized and stealthy • Hard to trace failure location
Dynamic Executable Verification	• Protect against dynamic tampering • Compatible with standard code-signing • Hard to trace default failure actions
Broad Platform Compatibility	• C, C++, ObjC/C++, Swift, JavaScript • Native objects and LLVM-IR bitcode • iOS, Android, Windows, Mac, Linux, Boot code and RTOS support

How it Works



Typical Scenarios

Mobile

Protect your users' data,
secret business logic and protocols

Cloud

Perform cipher operations for user authentication,
authorization, and identity without exposing users' credentials

Software SDK

Secure your middleware
software integrity in runtime

Devices

Utilize software root of trust, device identity, keys and
crypto operations on devices with weak or low security

www.pki-center.com | pki-center@commscope.com