

CLOAKWARE EMBEDDED SECURITY

PROTECT YOUR MULTI-PLATFORM MOBILE AND EMBEDDED APPLICATIONS WITH A SINGLE SET OF PROTECTIONS FROM CLOAKWARE

IMPROVE TIME TO MARKET ON MULTIPLE PLATFORMS

Deploying applications to embedded devices such as smartphones, tablets and specialized hardware such as set-top boxes is rarely limited to one platform. There always seems to be other competing platforms that need your application, as well. Ideally, protecting these applications from reverse-engineering, tampering and data theft should be able to be done once and applied across embedded device deployments.

FLEXIBLE SOFTWARE PROTECTION

Cloakware Embedded Security protects your software from attacks by concealing the digital assets and secrets that are crucial to your business, such as the cryptographic keys embedded in your code. Through its unique set of flexible protection tools, Cloakware Embedded Security allows the application of protection techniques in a platform-independent manner that encourages a single-source approach to application security.

Cloakware Embedded Security makes it easy to write your application security code once and deploy it on almost any embedded platform available.

EFFECTIVE SECURITY

- Defends against reverse engineering and tampering attacks.
- Creates software diversity to protect against scripted attacks
- Makes security inseparable from the software during development—a much more secure approach than those that only wrap the binaries right before shipping.
- Independently audited by customers, academics and ethical hacking service providers.

KEY BENEFITS:

- Effective security – defends against reverse engineering, tampering and scripted attacks
- Inseparable security – baked into the application, not wrapped-on after the fact
- Renewable security – automatable updating of keys, software and security measures
- Automated tools – enable rapid development and deployment of security capabilities
- Flexible Deployment – one set of tools easily adapted to many different embedded platforms using simple per-platform configuration
- Widely-used, proven solution – protecting applications deployed on over a billion PCs and devices

KEY FEATURES:

- Data transformation
- Control transformation
- Key hiding
- White-box cryptography
- Flexible, tuneable technology
- Integrity verification
- Anti-debug
- Secure file encryption
- Multi-platform, flexible deployment

SUPPORTED PLATFORMS:

Hosts (development platforms):

- Windows XP, x86
- Mac OSX 10.5, x86
- Linux 2.6, x86

Targets (deployment platforms):

- Any embedded systems platform with an available c90/c++97-compliant compiler tool chain
- Availability of POSIX-style standard libraries is useful but not required

EASY TO USE

- Integrates directly into your product build process; automated tools enable rapid deployment of security capabilities.
- Highly tuneable for just the right mix of security and performance
- Does not affect program functionality and is invisible to legitimate users.

FLEXIBLE PLATFORM DEPLOYMENT

- Support for compiler-independent source code transformation
- Cloakware security technologies such as White-box cryptography delivered as platform-independent libraries for easy integration
- Platform-configurable application binary protections such as anti-debug and file encryption

BROAD SUPPORT FOR DIVERSE EMBEDDED PLATFORMS

- Platform-independent source code transforms, Cloakware library support and application binary support for almost any ISO C90/ C++97-compliant compiler tool-chain
- Availability of POSIX-style standard libraries is useful but not required.

CLOAKWARE TRANSCODER™

The Transcoder transforms source code into mathematically modified source. Transcoded applications are functionally identical to the originals but are highly resistant to reverse engineering and tampering attacks. Transformations are available for many areas of the application such as program data, control flow, function signatures and bodies, and logic branches. The Transcoder also uniquely links anti-debug, integrity verification and White-box cryptography with code transformations to deliver integrated and layered protection that is far more secure than individual techniques alone.

CLOAKWARE WHITE-BOX CRYPTOGRAPHY

Cloakware's 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 RSA, AES and

ECC are among the most thoroughly studied algorithms, making them particularly vulnerable targets for attacks such as lifting keys from memory. Cloakware's White-box cryptography ensures that critical keying data is not revealed—even during cryptographic operations.

CLOAKWARE INTEGRITY VERIFICATION

Knowing that your code has not been tampered with is a crucial element of establishing security. Cloakware's Integrity Verification resists hacker attempts to modify the original program by creating encrypted vouchers that store a signature of the original application. Using the Integrity Verification run-time library APIs, the integrity of the signed application can be ensured before loading it from disk into memory.

CLOAKWARE DISK FILE ENCRYPTION

Cloakware provides a build-time tool and run-time library API to securely (using Cloakware White-box cryptography) encrypt and decrypt disk files important to your application. These can be application executables, data files, libraries, operating system files, or any other file needing encryption.