

CLOAKWARE DESKTOP SECURITY

PROTECT YOUR PC APPLICATIONS—AND BRAND REPUTATION—FROM DAMAGE BY HACKERS

YOUR SOFTWARE PROTECTION

Today's PC platforms are more open to attack than ever before. Tools that assist hackers are easily available on the Internet and online communities promote a sharing of techniques. Threats to software security include reverse engineering, tampering and copying—all of which threaten the integrity of your digital assets and can adversely affect your business model for monetizing those assets. You need a security strategy that can keep you ahead of the threats and the technology to implement that strategy.

AUTOMATED SOFTWARE PROTECTION

Cloakware Desktop 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. It lets you deploy your applications safely on untrusted PCs. Cloakware Desktop Security is a set of automated developer tools that apply security technologies for data and control flow transformations, anti-debug, White-box cryptography, and executable encryption.

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
- Easy Deployment – support for all of today's popular desktop platforms
- 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 application loading and encryption

SUPPORTED PLATFORMS:

- Microsoft Windows XP, Vista, Windows 7 – 32-bit and 64-bit
- Mac OSX 10.4 (PPC & x86), 10.5 (PPC, x86-32bit and x86-64bit), 10.6 (x86-32bit and x86-64bit)
- Linux/x86 kernel 2.6 – 32-bit and 64-bit

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.

COMPLETE DESKTOP PLATFORM SUPPORT

- Microsoft Windows support for XP and above, both 32-bit and 64-bit application
- Mac OSX 10.4, 10.5 and 10.6 support including x86-32bit, x86-64bit and PPC platforms.
- Linux x86-32bit and x86-64-bit support

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. The Integrity Verification run-time library uses the voucher to detect tampering of the application. Integrity verification can also ensure the authenticity of externally-signed modules that interact with the application, including components of the operating system. Integrity Verification continuously verifies signed components "in memory" to ensure that they are integral at all times. If integrity is compromised, developer-configured failure paths and anti-tamper actions are taken.

CLOAKWARE PROGRAM ENCRYPTION AND SECURE LOADER

The final step to application security is encrypting the application executable to prevent static analysis. Cloakware's Secure Loader provides a range of options for encrypting the executable, and then, at runtime decrypting it directly into a memory location.