Why White-Box Cryptography?

Building connected apps with innovative and responsive user experiences requires communicating and maintaining sensitive content. Whether this is account information, functionality updates, levels for a game, or video streams, it is imperative content remains secure—no matter how or where it travels, rests, or is stored. Failing to protect content and communications with users can result in government penalties, fraud, and intellectual property theft—not to mention lost customer trust, brand damage and revenue impact. Today's cybercriminals are exploiting any and all app weaknesses in order to gain financially from stolen customer identities, intellectual property or by gaining access to back office systems.

Encrypting information throughout its lifecycle—in transit, and in app—is key to keeping sensitive data out of the wrong hands. Significant effort has been applied to securing data in transit, from secure transport layers to encrypting data from the source. The weak link in this chain is the endpoint: the app.

The App Is The Weakest Link

Apps utilizing encrypted content use keys to decrypt incoming traffic and encrypt outgoing traffic—operations managed by functions inside the code of the application. If an app's code is reverse engineered, the keys used to encrypt/decrypt content can be discovered and provide a bad actor what they need to decipher encrypted information. Data resident in the app can be compromised along with all communications the app uses to interact with back office systems.

If cipher keys are uncovered, they can be copied, re-distributed, and used maliciously. Detecting misuse of compromised keys is nearly impossible since they will be used through seemingly legitimate traffic. Once compromised, remediating a key breach is time and resource-intensive and will require re-keying and updating every app and process using those keys.

This unsecured threat vector must be remediated, since existing data protection methods were not designed to defend keys from being discovered via reverse engineering or compromised app code.

Arxan White-Box Cryptography

White-Box Cryptography complements existing encryption technologies used to provide strong in-transit protection and is designed to protect encryption/decryption keys stored within an app. Using mathematical techniques. and and transformations, white-box cryptography blends together app code and keys to secure cryptographic operations, so keys cannot be found or extracted from the app to be used elsewhere.

Digital.ai (formerly Arxan) protects sensitive keys and data with a fully-featured white-box cryptography suite that can be used for adding protection to mobile, desktop and server apps. Digital.ai's White-Box Cryptography supports all major ciphers, modes, and key sizes; and, can directly interoperate with other cryptographic packages (such as OpenSSL) and devices in your environment without requiring server-side changes.

In addition to supporting all major algorithms and modes, a version of Arxan White-Box Cryptography protection has been FIPS-certified

to verify that Arxan white-box implementation is compliant with current security standards, and that it produces functionally correct results. White-Box Cryptography is available on iOS, Android, Windows, Mac, and Linux platforms.

Arxan for Android

Digital.ai provides Android Application code protection and threat detection for apps written in Java and Kotlin to protect against reverse engineering and tampering—with a zero-configuration initial setup that does not disrupt continuous integration and continuous development (CI/CD), and DevSEcOPs environments. Arxan App Protection includes threat detection and analytics to help organizations quickly understand the threat posture apps are operating in. Arxan for Android can detect rooted devices, reverse engineering attacks and code tampering.

Arxan for iOS

Arxan delivers protection and threat detection for iOS apps written in all major development languages—with a zero-configuration initial setup that does not disrupt continuous integration and continuous development (CI/CD), and DevSecOPs environments. Arxan App Protection includes threat detection and analytics to help organizations quickly understand the threat posture apps are operating in. Arxan for iOS can detect rooted devices, reverse engineering attacks and code tampering.

Arxan for Desktop & Server

Arxan Application Protection protects apps running across all major desktop and server operating systems—macOS, Windows, Red Hat and Ubuntu, utilizing the most common development languages—without requiring changes to source code to prevent.

Arxan Application Protection includes threat detection and analytics to help organizations quickly understand the threat posture applications are operating in. Arxan for desktop and server can detect reverse engineering attacks and code tampering.

Protecting Apps from the Inside Out

Digital.ai provides comprehensive, app-level security to protect against a range of threats or to enforce enterprise app governance —expanding the corporate perimeter of trust and allowing for easy integration into DevOps processes. Digital.ai provides a broad range of patented security capabilities to protect applications in the wild—such as a dynamic app policy engine, code hardening, obfuscation, white-box cryptography and encryption, and threat analytics.

ABOUT DIGITAL.AI

Digital.ai enables enterprises to focus on outcomes instead of outputs, create greater business value faster, and deliver secure digital experiences their customers trust. The Digital.ai Value Stream Platform seamlessly integrates all the disparate tools and processes across the various value streams, uses data and AI/ML to create connective tissue between them, and provides the real-time, contextual insights required to drive and sustain successful digital transformation. With Digital.ai, enterprises have the visibility they've been seeking to deliver value, drive growth, increase profitability, reduce security risk, and improve customer experience.

Learn more at www.digital.ai