intertrust®

Application Shielding for Mobile Financial Services

Protecting your applications from reverse engineering and tampering

Product Brief

Secure Systems

Financial applications are a target

The proliferation of mobile banking and other mobile financial services applications has made banks a popular target for attacks. The rewards to be gained from reverse engineering financial services applications can be great. APIs and keys can be exposed, giving hackers an easy way to access back end systems.

The consequences from compromised or hacked systems are huge, and it's not just about financial loss—damage to an organization's reputation or exposure to liability can cause far greater harm.

A hacker's first method of attack is often to decompile or reverse engineer an application. They do this to understand how the application works, and to identify methods to circumvent business logic that the developers may have included. If the application is well structured and follows a clear flow, this makes their life easier. In addition, they try to gain access to encryption keys so they can access customer data, or provide authentication to host services.

Delivering comprehensive application shielding

The Intertrust whiteCryption suite of products give developers powerful ways to protect their applications, and the sensitive data stored inside those applications from attack.

whiteCryption Code Protection™ is a solution that a developer can use to protect their applications. It gets integrated into the build chain and uses a number of advanced techniques to protect the application.

Before applying any protection mechanisms, the tool analyzes your code and supplies recommendations for how to best protect the application. It then hardens your application at the source code level, embedding checks and advanced protection mechanisms into the application.

whiteCryption Code Protection™ enables developers to proactively protect their applications. The code protection is integrated into the build chain with a number of advanced techniques to prevent reverse engineering and tampering.

whiteCryption Secure Key Box™ is a simple to deploy white-box cryptography library that provides a secure implementation of cryptographic algorithms and keeps keys and other secrets protected at all times, during use, and when at rest.

Business benefits

Proven techniques
Intertrust solutions have been successfully applied to millions of devices to mitigate software attack risks, including many wallets and banking solutions.

Wide platform support
Our software tools support most operating systems, CPU architectures, and programming languages.

Brand protection
Build your brand and prevent loss of reputation by protecting your endpoints and managing risk with application shielding.

Global support services
Our distributed development and support teams cover the Americas, EMEA, and Asia-Pacific.

Cost efficiency
Integrating with Intertrust security products is faster, cheaper, and more secure than developing your own software security infrastructure.

Protecting today's mobile financial services

Mobile point-of-sale
The new generations of mobile point of sale (mPos) solutions remove the need for expensive hardware devices. The interim solutions, starting to be deployed now still utilise an external hardware device to read the card, but the PIN entry is performed on the phone UI. This solution is called PIN on COTS. However, the end goal is to remove the need for hardware altogether and to deploy solutions where the card is read through the phone's NFC interface and the PIN is entered on the screen UI. Obviously to move to a solution without any dedicated secure hardware adds an element of risk, and this is where white-box cryptography and application-level security provide protection.

Cloud-based payments
Cloud-based payment solutions enable Android phones to perform payments through standard contactless PoS terminals. The specifications were created by the major payment schemes to remove the requirement to use any hardware-backed security like secure elements, SIMS or TEEs, thus simplifying the deployment model for these solutions, and enabling scalability.

However, as the hardware-based security requirements were removed, the solutions require white-box cryptography and software anti-tamper mechanisms to be used to protect the keys from being extracted and preventing applications from being modified.

Mobile banking
Mobile banking solutions have been increasing in functionality over the past few years, and in most cases offer a fully featured service. With the addition of the capability to do things like setup new payees, comes an added level of risk. The bank must be able to trust that the application is genuine and have a high level of confidence that the user is the one they claim to be. Enabling strong protection of keys and guarding the application logic from reverse engineering and tampering is essential, and is the minimum any organization should do to protect their applications.

whiteCryption Code Protection and Secure Key Box solutions are easy for developers to use, integrate seamlessly into their existing build systems, and deliver the highest level of application shielding that is available for any device.

If you want to understand how to protect your applications, please contact the Intertrust team at:
information@intertrust.com

Features

Obfuscation
Makes the code appear obscure while keeping functionality the same.

Integrity protection
Prevents attackers from making any modifications to the application.

White-box cryptography
Provides strong protection for cryptographic keys.

Anti-debugging
Enables the application to identify the presence of a debugger.

Jailbreak and rooting detection
Prevents the application from running on jailbroken and rooted devices.

Diversification
Ensures every protected application is different.

Customizable defense actions
Enables custom callback functions when threats are detected.

intertrust®

Building trust for the connected world.

Learn more at: intertrust.com
Contact us at: +1 408 616 1600

Intertrust Technologies Corporation
920 Stewart Drive, Sunnyvale, CA 94085

DS_SS_OR19