YESsafe AppProtect+

Protect your API keys, certificates, and other fixed app secrets with Secure Application ROM (SAROM)

Created to keep your fixed app secrets safe

Often, your app will have fixed secrets such as certificates or API keys that you need for the security of your app's operation, but you'd rather not have them easily extracted from your app.

Hardcoding app secrets directly into the application assets or source code and potentially relying on obfuscation methods for security, is a common strategy for many app developers. This is however not enough to properly protect your secrets, and hackers can easily retrieve them by reverse engineering.

Hardcoding API keys a vulnerability

According to Gartner, hardcoding API keys or other credentials in web and mobile applications is one of the four most common API vulnerability paths, and the method makes such secrets subject to decompiling attacks.

Did you know?

Mobile health apps leak sensitive data through APIs, a report finds. The 30 apps that were hacked collectively exposed 23 million mobile health users to attacks. Of the 30 apps, 77% contained hardcoded API keys and 7% had hardcoded usernames and passwords.

A unique solution to a difficult challenge

Secure Application ROM (SAROM) offers a simple to use solution to a challenge that is difficult to solve on any mobile platform – protecting specific assets in a published app. It suits a number of use cases where sensitive data must exist in the published app.

Protecting TLS certificates

The TLS protocol aims at providing privacy and data integrity between communicating computer applications. Avoiding a leak of the TLS certificate is important for the integrity of the communication between app and server. SAROM will ensure the integrity and security of TLS certificates in the app by encryption, and therefore also the integrity of your TLS communication.

Protecting API keys

Many apps require the use of private APIs, which are accessed by API keys. To ensure that these are not leaked, they need to be protected against static and dynamic attacks. By encrypting these with SAROM, your API keys are only decrypted when accessed by the application at runtime.

Secure Application ROM (SAROM)

- ✓ Simple to use and easy to integrate
- ✓ Automatic protection of your app assets
- ✓ Suits use-cases where sensitive data must exist in the published app

Protecting specific assets in a published app

Platform-specific functionalities with elements in place to protect the entire app on disk is not a good enough solution. When the app loads, the entire app is decrypted and available in memory – making it possible for an attacker to analyse the app code and extract secrets. Since the encrypted assets are never statically accessible with SAROM, but rather dynamically decrypted when the app needs an asset, the attack scope will be dramatically decreased, making it difficult for attackers to find and retrieve the encrypted secrets.

Shielding and protecting an application with YESsafe AppProtect+ is an automated process easily done with our implementation tool, Shielder. With the SAROM API, your application can dynamically retrieve data which is encrypted by Shielder during Shielding. All data stored using this feature will be encrypted according to the latest standards and recommendations.

The data encrypted in SAROM is encrypted using symmetric keys, which are derived independently by Shielder during Shielding and YESsafe AppProtect+ during runtime to access the data. The encryption keys are derived from a combination of various sources, such as:

- ✓ Customer-specific SAROM seed in YESsafe AppProtect+
- ✓ Customer specified token
- ✓ Data-ID (the key of the key-value data to be stored)

Global Headquarters
Blk 750D Chai Chee Road #08-01
ESR BizPark @ Chai Chee (Lobby 1)
Singapore 469004
☎ +65 6244 3900
✉ enquiry@i-sprint.com

For a complete list of our offices in
China, Hong Kong, Japan, Malaysia,
Thailand & United States, please visit
www.i-sprint.com/contactus