YESsafe AppProtect+

Run-Time Mobile App Protection

Protect mobile app from cracking + Prevent invasion when application is running + Provide callback API customization

YESsafe AppProtect+ is a security technology that provides real-time mobile app protection. AppProtect+ proactively protects your applications from malicious attacks, even when accessing via a compromised device. It provides callback API and users can invoke callback API to perform the desired functions, such as collecting risk parameters and sending such data back to server.

In comparison with other anti-virus software, AppProtect+ eliminates the need to update any virus database or the presence of internet connection to fulfill app protection requirements. Protection against attacks such as reverse engineering, repackaging and source code modification, AppProtect+ has the ability to respond immediately by taking necessary measurements for real-time attacks, a wholesome protection for mobile apps.

4 Core Functions

Anti-reverse engineering & Anti-tampering

Protect APK from reverse engineering, debugging and cache attack from tools like apktool, dex2jar and JEB. The unique authentication technology stops the APK from running if any APK data tampering is reported.

Anti-theft

Supports data encryption, scan and validate input methods, screenshot blockage and data protection to prevent capturing, hijacking and tampering app's dynamic and statics data.

Anti-debugging

With the use of white-box cryptography, it prevents malicious code injection, block tampering attempts to game apps, HOOK attacks, attack using system accessibility, prevent phishing attacks, transaction hijacking, data modification etc.

Server Management Client

Using callback function, users can call the server API to transmit data collected from mobile terminals to the server. Server administrator can setup policies based on the collected data to manage user accounts and users' access right.

All-Round Protection

- ·Code-Injection
- ·Jailbreak/ Root Detection
- ·Debugger
- ·Screen-Reading
- ·Emulator Execution
- ·Repackaging
- ·Hook Framework Attack
- ·Keylogging
- ·Screenshot
- ·Code Logic Leakage

i-Sprint
Trust without Boundaries

Functions

Source Code Protection
· DEX file obfuscation
· SO file obfuscation

App Integrity Protection
· Authenticate source code, resource file and configuration files
· Exits apps should authentication fail and notify server through callback function

Mobile Environment Detection
Exit apps on rooted/ jailbreak devices and inform server by callback function

Anti-Fraud
· Anti-Phishing
· Code-Injection Prevention
· Prevent Overlay Attack
· Certificate Protection
· Anti Process Injection Attacks

Business logic(source code) protection
· Emulator Detection
· Debugger Detection
· HOOK Detection
· Anti DUMP Debugging
· Prevent Decompile

Data Protection
· Memory Data Protection
· Anti-Screenshot initiated by System
· Anti-Screenshot initiated by User
· Anti-Screen Mirroring
· Anti-Keylogger
· Whitebox Cryptography

Anti-Tampering
· Anti-Repackaging
· Prevent Transaction Attacks
· Prevent Leakage of Login Credential
· AndroidManifest.xml Modification Detection
· Reverse Engineering Prevention
· Resource File Protection

Core Advantage

Integrated with AccessMatrix, YESsafe AppProtect+ responds promptly to any risk detected on the client side. Fulfilling app protection, risk detection and respond actions requirements, providing the complete app protection cycle.

Protection
Prevent Malicious

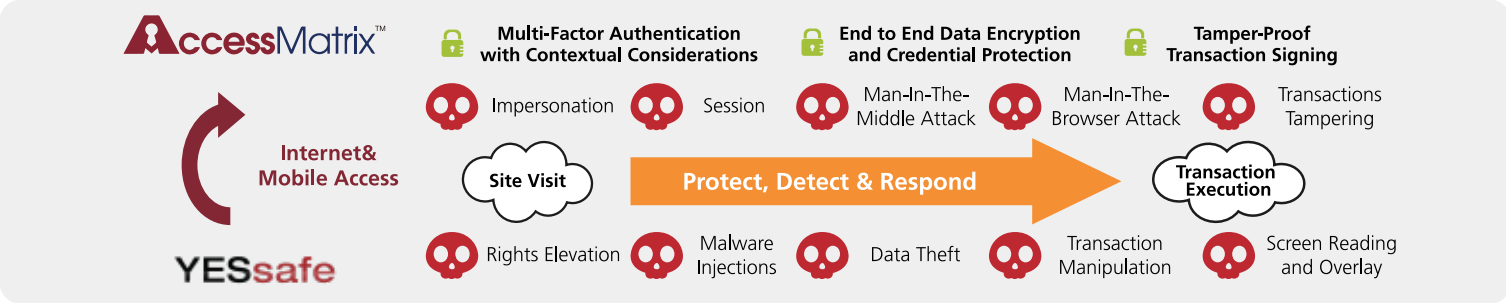
- ✔ Code obfuscation
- ✔ App Binding
- ✔ Repackaging detection
- ✔ App communication
  - › TLS certificate pinning
  - › Client authentication using a client-certificate
  - › Identifying the app/device as an authentication factor
- ✔ Store data encrypted inside the app
- ✔ Binding the data to be encrypted to the device
- ✔ Whitebox cryptography
- ✔ App Management Solution
  - › Trusted binding between a user, an app and the device
  - › Making the app trusted without external security tokens
  - › Registration / activation – securely pair the app / device with the user

Detection
Detect Runtime Attack

- ✔ Ensure app is running in safe environment
  - › Debugger detection
  - › Jailbreak / Root detection
  - › Emulator detection
- ✔ Ensure app is not altered or tampered with (e.g. by malware) at runtime
  - › Checksum
  - › Resource verification
  - › Hook detection

Respond Action
Counter Attack

- ✔ Shutdown (Exit / Fail)
- ✔ Integrity checking
- ✔ Custom reactions
- ✔ Screenshot detection / blocking
- ✔ Anti keylogging
  - › Anti screenreading
- ✔ Alert / reporting
- ✔ Blocking external screens
- ✔ Prevent brute force decryption of sensitive information



Runtime App Self-Protection (RASP)

- AppProtect+ isolates applications from the runtime environment, proactively scans and protects mobile apps against malicious attack, allowing apps to run securely even on rooted/ jailbreak devices. For example, screen reader on Android devices and data theft (e.g. stealing of login credential) from entry through non-reputable third-party keyboard, fulfilling real-time app protection needs.
- The uniqueness of AppProtect+ lies in the ability to detect risks even at the absence of internet connection, different from traditional virus database matching mechanism. AppProtect+ can therefore avoid possible risk cause by desynchronized database.

Core Benefits

Defeats Targeted Attacks

Provides Reliable Apps

Protects Multiple Business Apps

Enables A Secure Mobile Strategy

Protects Software Keys

Quick in Deployment

Meets Strict Compliance Requirements

Similar User Experience

Deployment

- With application source code, users can add the AppProtect+ SDK to the application's development project for integration with the security functions mentioned-above, and implement the SDK callback function that works with the server APIs.
- SDK callback function will not work without the presence of application source code. In this situation, AppProtect+ security functions can only be added by wrapping AppProtect+ into the existing app.

Available for download in both Android and iOS devices.

i-Sprint

About i-Sprint Innovations

i-Sprint Innovations (i-Sprint) established in the year 2000, is a leading provider in Securing Identity and Transactions in the Cyber World that enables individuals, organizations, and societies to build trust and identity assurance for powering productivity gain through digital identity and identity of things (IDoT).

i-Sprint's unique brand of security products, intellectual properties, and patents are designed to exceed regulatory requirements such as global financial services. By incorporating the latest mobility/ biometrics/ cloud/ identification technologies, i-Sprint provides solutions that ensure secure access and protection of data, transaction and assets. i-Sprint delivers trusty, versatile and strong authentication, and identity management platform to secure multiple application delivery environments based on a common security platform.

i-Sprint's digital identity product offerings include adaptive authentication (biometrics, multi-factor authentication and more), single sign-on services, end-to-end encryption (E2EE) authentication and data protection for transaction data and to secure access to the web, mobile, and cloud-based applications. i-Sprint's IDoT product offerings provide the next-gen anti-counterfeiting, track and trace, and interactive consumer engagement that aims to help business in building consumer trust, improve brand protection, personalize consumer engagement and provide business intelligence.

i-Sprint's clients include leading global and regional financial service institutions, government agencies, telecommunications, public utilities, manufacturing, healthcare, education, multi-national corporations and others. Currently, i-Sprint has a direct presence and active authorized partners across Singapore, China, Hong Kong, Taiwan, Malaysia, Thailand, Japan and the United States.

Global Headquarter
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

20211011