The rapid adoption of mobile devices has led to an active growing market in the mobile application ecosystem, pushing enterprises and organisations towards a strategic take on mobile application development to reach a larger audience internally and publicly. Having a more centralised control over their applications, they are able to roll out updates and patches as a mass as opposed to traditional web browsers. Whilst having standard built-in security features to protect us from cybercrimes, our mobile devices are simply not designed for strong security.

Developers are aware of integrating standard security processes to the app development. However, it is often observed that the security aspects are de-prioritized over new features to maintain speed of development and to stay ahead of the competition. Moreover, implementing in a strong, trusted encryption platform can be challenging, depending on the interface and the point of implementation, unless done by a domain expert.

V-OS App Protection is a globally certified product at the highest level of security, secured with industry-leading, military grade V-OS Virtual Secure Element, ensuring app integrity when deployed, and safeguarding user privacy even if the device is lost or compromised.

With defences in place such as binary code morphing, anti-reverse engineering, trojan, tampering and malware detection, you can be sure that your end users’ devices are always protected from attackers while they carry out important transactions on your applications.
SECURE CRYPTOGRAPHIC FUNCTIONS FOR BOTH DATA-AT-REST AND DATA-IN-USE

Attackers have the ability to dump the at-rest and in-memory contents of your application which allows them to extract not only the function calling sequences and business logic of your app but also enables them to extract the user secrets you hold in the memory for authentication and identification purposes. All keys used by V-OS App Protection are also masked so that they do not appear in plaintext while at rest. By using Secure File IO APIs provided with V-OS App Protection, you can store your end user’s critical personal information securely within V-OS and be assured that it stays protected while in use and at rest.

ABOUT V-KEY

V-Key is an internationally-acclaimed software-based digital security company, headquartered in Singapore. V-Key’s pioneering technology powers ultra-high-security solutions on premise and Cloud-based, for digital identity management, user authentication and authorization, IoT, as well as electronic payments for major banks, payment gateways, and government agencies.

V-Key is the inventor of V-OS, the world’s first virtual secure element to be FIPS 140-2 validated (US NIST), Common Criteria EAL3+ certified and accredited by the Infocomm Media Development Authority of Singapore (IMDA). V-OS has been the subject of multiple rigorous penetration tests and has been stress-tested by e-commerce players, government agencies, regulatory bodies and financial services companies.

PRODUCT FEATURES

RUNTIME APPLICATION SELF-PROTECTION (RASP) BUILT IN

There are many methods that attackers can use to tamper with your application at runtime. The built in RASP capabilities in V-OS App Protection makes your app resilient against such attack scenarios by preventing attackers from using emulators, debuggers, code injection or tracing tools and hooking frameworks.

DEVICE AND FILE SYSTEM INTEGRITY CHECKS

Any kind of modification/tampering done to the device at its file system level to gain escalated privileges on the device not intended by the device manufacturer or operating system is considered as a compromise of device and its file system integrity. Jailbreaking or rooting is one such process. Carrying out sensitive transactions on an app running on a compromised device can result in an attacker stealing critical personal information associated with the end user. V-OS App Protection uses a mix of malware, function and file signatures related matching and verifications to assess whether its integrity is comprised.

SECURE CRYPTOGRAPHIC FUNCTIONS FOR BOTH DATA-AT-REST AND DATA-IN-USE

Attackers have the ability to dump the at-rest and in-memory contents of your application which allows them to extract not only the function calling sequences and business logic of your app but also enables them to extract the user secrets you hold in the memory for authentication and identification purposes. All keys used by V-OS App Protection are also masked so that they do not appear in plaintext while at rest. By using Secure File IO APIs provided with V-OS App Protection, you can store your end user’s critical personal information securely within V-OS and be assured that it stays protected while in use and at rest.

APP INTEGRITY CHECKS AGAINST TAMPERING

Mobile applications can be tampered through the process of reverse engineering, as obfuscation of the source code is not comprehensive, allowing easy modification of application binaries and resigning. V-OS App Protection verifies the integrity of an app through a multi-step process. Anauthentic signature is first packaged in the embedded profile that is used. This file is then encrypted with a customer specific key that is stored within V-Key’s patented virtual secure element - V-OS. At runtime, the app’s signature is compared against the authentic signature to check it’s integrity.

NETWORK INTEGRITY CHECKS AGAINST MAN-IN-THE-MIDDLE (MITM) ATTACKS ON DATA-IN-TRANSIT

MITM attack is a form of active eavesdropping in which the attacker makes independent connections between two victims and relays messages between them. The most direct form of attack is an attempt to intercept HTTPS traffic by using a custom certificate. V-OS App Protection provides alternative means to verify SSL certificate of the server. The server certificates are stored in an embedded file that is encrypted with a customer specific key that is protected within V-Key’s patented V-OS. These signatures are extracted at runtime and verified whenever a HTTPS connection for the particular domain is requested, thus preventing MITM attacks.

V-Key is an internationally-acclaimed software-based digital security company, headquartered in Singapore. V-Key’s pioneering technology powers ultra-high-security solutions on premise and Cloud-based, for digital identity management, user authentication and authorization, IoT, as well as electronic payments for major banks, payment gateways, and government agencies.

V-Key is the inventor of V-OS, the world’s first virtual secure element to be FIPS 140-2 validated (US NIST), Common Criteria EAL3+ certified and accredited by the Infocomm Media Development Authority of Singapore (IMDA). V-OS has been the subject of multiple rigorous penetration tests and has been stress-tested by e-commerce players, government agencies, regulatory bodies and financial services companies.
SECURE ANTI-KEYLOGGER KEYBOARD

Keylogging is the activity of recording the keys struck on a keyboard such that the person using the keyboard is unaware about the fact that their actions are being observed. It can be done through injecting malicious software on user’s phone or the use of third party keyboards. V-OS App Protection has a secure keyboard implementation which cannot be hooked or snooped upon by Keylogger malwares or rootkits thereby allowing you accept sensitive inputs like one time password etc from your end users on your apps without worries.

OVERLAY AND SCREEN MIRRORING PROTECTION

Overlays can be used in phishing attacks to trick the user into entering critical personal information and capturing it, or in tap-jacking attacks that trick the user into performing undesired actions. Attackers can also exploit vulnerabilities present in 3rd party screen recording apps to capture sensitive information from your app. V-OS App Protection overlay and screen mirroring protection addresses these attacks by employing various overlay detection techniques.

EMULATOR AND HOOKING DETECTION

Hooking is a term for a range of code modification/tampering techniques that are used to change the behaviour of the original code running sequence by inserting instructions into the code segment at runtime. V-OS App Protection employs various anti-debugging and anti-hooking checks that are scattered throughout various layers within V-Key's patented V-OS which makes it practically impossible for any attacker to turn these checks off.

SERVERLESS OPTION AVAILABLE

One can opt for V-OS App Protection solution suite with various server side options mainly- on-premise/on-your-cloud/on-V-OS-cloud/server -less depending on one’s budget, security, time to go live and compliance needs. With V-OS Cloud, you can enjoy a high performance secure cloud environment allowing you to cut down your go live time and significant savings in server purchase and maintenance costs.

WHAT IS V-OS?

Internationally patented, V-OS uses advanced cryptographic and cybersecurity protections to comply with standards previously reserved only for expensive hardware solutions. Today, V-OS secures millions of users around the world. V-OS enables digital leaders to create powerful customer experiences that combine high security and delightful convenience. V-OS integrates seamlessly with biometrics, PKI-based technology, out-of-band authentication, making delightful user experiences possible while being uncompromisingly secure.

PRODUCT FEATURES

SMS HIJACKING PROTECTION

Most end users tap on “install/allow” when apps require access to Messages/ SMS of the device without caring much about the list of permissions requested. V-OS App Protection for Android uses the malware scan approach to detect various SMS stealer malwares. Besides alerting your app at run time upon detection of such malwares, configured actions such as quit app, disable app etc. can be set-up to ensure SMS stealing prevention and detection gets kicked in upon launching of the app by the end user.
V-OS App Protection is a robust solution secure by anti-fraud and anti-malware. The dashboard provides a number of policy controls that the administrator can use:

- SSL pinning and multi-layered authentication for server APIs
- Real time application threats monitoring
- Over the air updatable threat response behaviour of mobile apps
- Threat details with context into triggers, location and type
- Integrable with external analytics systems
- Configurable UI login options with on-premise AD systems

The screenshot above shows real time application threats monitoring as well as threat details with context into triggers, location and type.