EnsureIT® for Android on ARM

Software protection for Native Code Based Android Applications

Protect your Android Applications from Attack

Android is rapidly being adopted by many industries, with digital media at the forefront. Consumer devices including smartphones, mobile/portable tablets, set top boxes, etc. are increasingly being used and accessed by Android applications. Additionally, the ARM® Partnership spans a wide and diverse set of applications and markets such as mobile, home, embedded & enterprise. As these markets continue to experience explosive growth in both the number and type of devices, and as global deployment of embedded systems on ARM® continues, the importance of securing Android applications against tampering, reverse-engineering, counterfeiting and piracy attacks becomes paramount. Software protection is needed to ensure business models, intellectual property (IP), and digital rights management (DRM) requirements.

Arxan’s Automated Security

Arxan’s EnsureIT for Android on ARM delivers automated software protection that is durable and easy to deploy. EnsureIT features defend, detect and react capability by deploying various Guards directly into the software code for ARM processors.

The EnsureIT toolkit consists of an application programming interface (API) and two utilities. The utilities, finalizer and asmproc, are used to complete the protection process after the GuardSpec® is applied to the program. The GuardSpec contains specific commands to implement a unique protection scheme per application which leverages obfuscation, checksum, damage, debugger detection and repair security Guards. In concert, this layered protection of diverse Guard types provides control, trust and tamper-resistance for the application.

Arxan Protects
- Brand
- Revenue
- Data
- Code Integrity
- Intellectual Property

Arxan Prevents
- Malware Injection
- Tampering with Security Controls / Sensitive Functions
- Reverse-Engineering
- Unauthorized Access and Fraud
- IP Theft and Piracy

Android apps are vulnerable to:

Hacker Toolkits designed to:
- reverse-engineer
- disassemble
- debug

Limited security components of Android Market & download sites
Open-source nature of Android apps
EnsureIT® for Android on ARM

Core Feature and Benefits of EnsureIT

- Tunable security for mobile platforms and their application offerings
- Layered network of protections, with no single point of failure
- Self-heal in the event of an attack by restoring protections
- Requires no changes to source code
- Support for a broad range of emulators and devices

Durable, Automated Software Protection: Defend, Detect, React

Arxan protects critical functions of an application through patented Guard technology. Guards are tiny security units which protect the application and each other in three ways:

- Defend against reverse engineering, tampering and any manner of theft
- Detect an attempted attack on the application code, or on another Guard
- React in standard ways such as safely exiting - or user-specified ways, such as phoning home.

Arsenal of Guards

EnsureIT leverages thousands of guard instances, of many types, to comprehensively safeguard your software applications against tampering, piracy and any manner of theft.

<table>
<thead>
<tr>
<th>Class of Defense</th>
<th>Guard Type</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEFEND</td>
<td>Obfuscation</td>
<td>Transforms program instructions into code that is difficult to disassemble and understand, but has the same functionality as the original.</td>
</tr>
<tr>
<td></td>
<td>String Encryption</td>
<td>Encrypts string literals and decryption at run-time.</td>
</tr>
<tr>
<td>DETECT</td>
<td>Debugger Detection</td>
<td>Detects whether the program is executing in a debugging environment.</td>
</tr>
<tr>
<td></td>
<td>Checksum</td>
<td>Detects whether a program has been modified by computing a checksum within a specified range.</td>
</tr>
<tr>
<td></td>
<td>Damage</td>
<td>Damages a specified range at runtime with random bytes or user-specified bytes.</td>
</tr>
<tr>
<td></td>
<td>Root Detection</td>
<td>Detects whether the mobile device on which the application is running is a rooted device.</td>
</tr>
<tr>
<td></td>
<td>Hook Detection</td>
<td>Detects whether an attacker has overridden a called function that resides in a system library or within the application.</td>
</tr>
<tr>
<td>REACT</td>
<td>Repair</td>
<td>Self-heals any damaged or tampered code/data</td>
</tr>
</tbody>
</table>

EnsureIT® Specifications

<table>
<thead>
<tr>
<th>Supported Languages</th>
<th>C, C++</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported Compilers</td>
<td>Latest Clang versions</td>
</tr>
<tr>
<td>Supported Host Platforms</td>
<td>Ubuntu, Mac OS X, Windows</td>
</tr>
<tr>
<td>Supported Android Platforms</td>
<td>Various Android Versions</td>
</tr>
<tr>
<td>Supported NDK platforms</td>
<td>Latest Versions</td>
</tr>
</tbody>
</table>

www.arxan.com | info@arxan.com | +1. 301.968.4290