Epona
Application Protection by Quarkslab

Release July 2019

Paris, France - July 4 2019

Quarkslab, the leading information security R&D, consulting and software company in Europe, announced today the release of Epona Application Protection v1.5, its advanced application shielding solution for mobile, desktop and embedded software.

Epona Application Protection protects software and firmware against attacks that seek to obtain cryptographic signing and encryption keys, exfiltrate encrypted data itself, lift proprietary algorithm implementations, or compromise other high-valued assets present on software that runs on unmanaged devices. It also allows organizations to detect when a protected application is running on a potentially hostile environment such as a tampered or otherwise unsanctioned device, and to enforce protection measures according to the developers' policy.

Quarkslab's unique combination of in-depth knowledge of offensive and defensive information security, coupled with its compiler engineering and program analysis expertise crystallized in a comprehensive application protection solution built to meet the requirements of customer organizations in the Banking, Mobile Payments, Media and Entertainment, Automotive, Defense, Aerospace, and Healthcare markets.

Epona Application Protection is based on the industrial-strength, widely adopted LLVM compiler infrastructure maintained and extensively tested by the world's top technology organizations, resulting in seamless integration with the most common software development environments and toolchains.

The full set of capabilities includes:

- State-of-the-art obfuscation techniques agnostic of the application's programming language and target platform, thus the same protection mechanisms can be used on all supported platforms and with software written in any of the supported languages. This guarantees a similar level of protection and robustness against manual and automated reverse engineering for software running on any of the supported platforms.
- Integrity protection to prevent modification of the application code or tampering with the application's sensitive data.
- Runtime Application Self-Protection (RASP) capabilities to prevent and detect tampering of the application's runtime environment such as jailbreaking, rooting, debugging, and dynamic instrumentation (*hooking*).
- Static and dynamic whitebox cryptography implementations of standard ciphers.
- Fine-grained controls that let customer organizations optimize the performance vs. security trade-off according to their needs and policies.

«The release of Epona Application Protecion v1.5 is the result of an effort of many person-years developing an answer to our customer's most challenging question: How do I protect my code and data on an unmanaged device, under the control of a potential attacker ? We believe we now have a robust, comprehensive and affordable response to address that question» said Iván Arce, CTO of Quarkslab.

What's new in Epona Application Protection v1.5

- A new Control Flow Graph obfuscation, in addition to CFG Flattening.
- Improved use of Opaque Predicates.
- Improved instruction-level obfuscation.
- Fine grained control of obfuscations to achieve binary runtime performance and size optimizations.
- Android NDK 18b and 19b support.
- Obfuscations that require threading support can now be used on ARM.
- The *epona-report* tools can now be used to check properties of the protected app's final binary.
- A static and dynamic whitebox implementation using Epona compiler.
- An advanced whitebox implementation library.

Epona Application Protection v1.5 supports software written in C, C++, and Objective-C for iOS, Android, OS X, Windows, and Linux on 32 or 64 bits x86 and ARM and it is available now from Quarkslab.

For more information visit https://epona.quarkslab.com or contact us at sales@quarkslab.com or @quarkslab on Twitter.

About Quarkslab

Quarkslab is a French company specializing in information security R&D, consulting and software development. Our expertise is in combining offensive and defensive security to help organizations adopt a new security posture: Force the attackers, not the defender, to adapt constantly. Through our consulting services as well as our software we provide tailored solutions to organizations, helping them to protect their assets, sensitive data, and users against increasingly sophisticated attacks.

Contact

13 rue Saint-Ambroise - 75010 Paris - FRANCE

+33 (0)1 58 30 81 51
contact@quarkslab.com

https://www.quarkslab.com
https://www.quarkslab.com/blog

@quarkslab on Twitter and LinkedIn