CYBERCRYPT A1

CYBERCRYPT.

Efficient In-App Protection to Safeguard Applications

Application security is instrumental to the livelihood of many business models, e.g., in banking, gaming, content disribution, and industry. It can be mobile, desktop, embedded or even backend applications that need protection of the underlying assets such as secrets, credentials, intellectual property, algorithms, business logic, licensing, etc.

Yet, popular off-the-shelf offerings often fall short of the practical requirements.

Firstly, being generic, they allow for automated attacks. Secondly, they often come with an unacceptable performance overhead. Furthermore, being non-specfic to the application by their nature, they may be difficult to apply correctly in all cases.

CYBERCRYPT A1 is an in-app protection solution for elevated security and efficiency with regular updates.

A1's customization greatly complicates real-world attacks by limiting the exposure and minimizes performace losses by fitting A1 to the app's exact needs.

Regular updates make sure that A1 is state-of-the-art at all times: CYBERCRYPT's team is closely following the attacker scene and making adjustments to A1 ahead of time.

CYBERCRYPT A1 integrates with development toolchains and applications in form of binary libraries and compiler plugins.

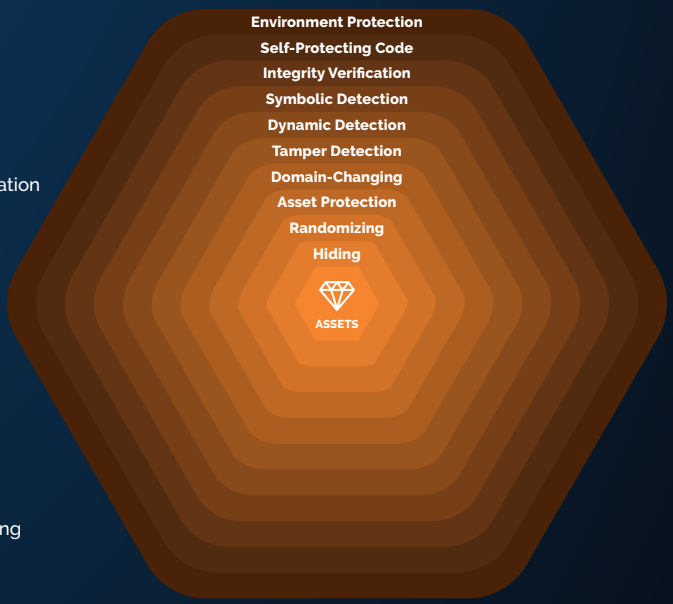
CFG transformations
- control-flow flattening
- bogus control flow

Indirection-increasing transformations
- on-the-fly unscrambling of data
- run-time instruction fetch target calculation

Asset encryption
- just-in-time decryption
- integrity checks and authentication

Code compartmentalization hiding
- breaking up the code structure
- function and instruction scattering

Code randomization
- compiler idioms avoidance
- randomization of ABI/parameter shuffling



Dynamic analysis framework detection
- anti-debugging & anti-emulation
- anti-dynamic binary instrumentation

Symbolic analysis framework detection
- mixed Boolean-arithmetic expressions
- symbolic pointer dereferencing

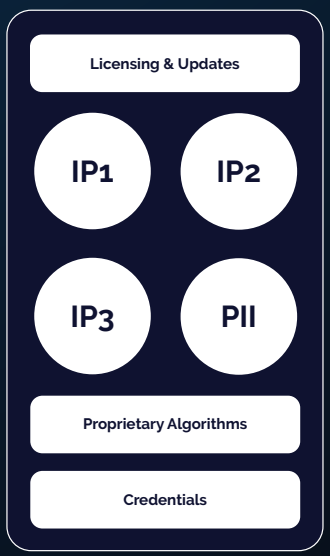
Tamper detection
- checking for program modifications
- detection of cracking attempts

Split-personality execution
- silent activation of program's paths
- stealth obfuscation of execution

Domain-changing transformations
- trigger condition trapdoors using hashing
- variable representation changing

CYBERCRYPT A1 has numerous protective mechanisms to thwart modern attack techniques of dynamic, static and symbolic analysis

BEFORE: App without protection



AFTER: App with CYBERCRYPT A1 protection