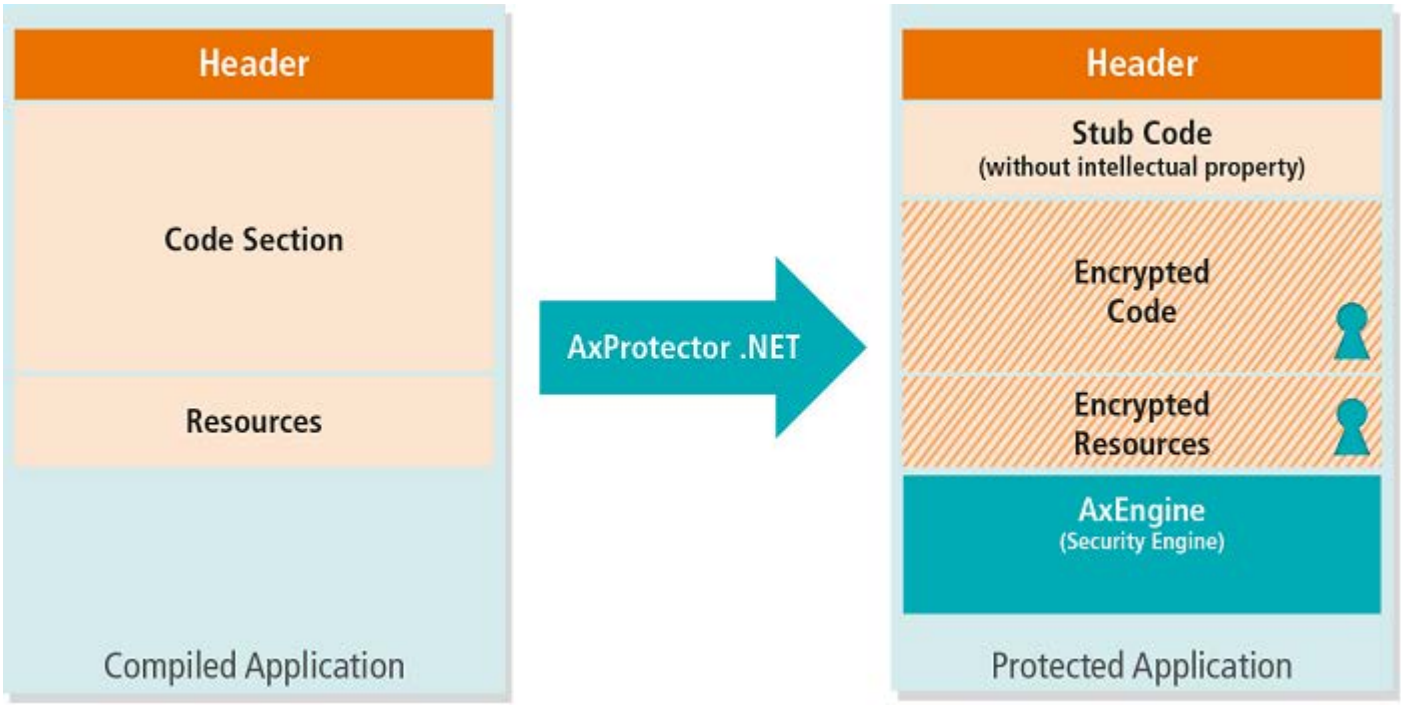
This article was posted on 01/02/2018

Blurry Box software security scheme makes code theft more expensive than development

Using a combination of seven different methods, the Blurry Box scheme foils hackers at every turn

Software can be a significant part of product development, but that investment is often altogether too easy to steal through simple copying. Yet preventing such copying can be difficult, especially when a product is out in the field, where it is subject to physical as well as cyberattacks. The Blurry Box scheme foils such attacks with a combination of methods that include encryption, creation of variants, and traps.



There are both hardware and software elements to Blurry Box. The software includes both a conversion tool and a runtime security engine. Developers take their compiled application code and incorporate AxProtector in a post-build process. The protector encrypts the code and incorporates the AxEngine security wrapper, which provides runtime software decryption as well as other security monitoring. This software works with a hardware dongle that contains both the encryption keys and a state machine that tracks code execution.

In addition to encrypting application code, the protector tool creates multiple callable variants of code functions. Executing the resulting code requires the security wrapper to send a function call and its parameters to the dongle, which determines which variant is to be executed. The dongle selects the variant based on the parameters sent, so not all function calls use the same variant. Furthermore, some of these variants are traps, which, if executed, will cause the hardware dongle to lock out further software access. Thus, an attacker cannot determine which parametric combinations are valid and which are decoys without trying all of the possible parameter combinations, and such an attempt would trigger a trap to prevent further attempts.

Other protection elements include a monitoring state machine that can identify the proper ordering of function calls and a decryption delay timer that is triggered when function calls occur too quickly. Both help add to the time and complexity of any piracy attempts.

Learn more about Wibu-Systems

By Richard Quinnell