Principle of .NET Autoprotection

A twostage protection approach is used for the automatic protection of .NET assemblies with each stage performing its own tasks in the overall process:

- MSIL code symbol obfuscation
- Transfer of a portion of MSIL-code into a protected storage

This concept permits a significant increase in the overall level of .NET protection, since the widely distributed .NET reverse engineering tools (ildasm, reflector.net, etc.) become useless.

It is predicated upon the fact that most of .NET assembly’s code is stored in the protected native container, which in turn is protected by both pseudocode (software) and the dongle’s functionality (hardware solution).

When MSIL code previously encrypted by a hardware algorithm is called, the dongle itself is addressed first for decryption purpose and only after the execution of code begins.