How do I prevent hackers from decompiling Java class files to reverse engineer my COBOL application?

Question:

How can I secure the code generated by isCOBOL so that it cannot be decompiled? Do you provide a Java code obfuscator? If not, then which one do you recommend and how do I use it with the isCOBOL compiler?

Answer:

The Java bytecode produced by the isCOBOL Compiler is the actual output of the Java Development Kit (JDK) compiler. The isCOBOL Compiler translates COBOL source code to Java source code and then invokes the Java Compiler to compile the Java source code into Java class files (bytecode). There is no way to decompile the bytecode into COBOL source code. There is no COBOL source code embedded in the Java bytecode unless you compile with the -d or -dx switch using 2020R2 and above and don't set "iscobol.debug.embedded_source=false".

A hacker could decompile the bytecode into Java source code. However, this Java source code would be very difficult to understand by someone that did not have access to the original COBOL source code.

An additional degree of protection can be obtained by using one of the many Java bytecode obfuscators available.

For example,

Free and Open Source products such as
http://proguard.sourceforge.net/
http://www.yworks.com/en/products_yguard_about.html

or commercial products such as
http://www.zelix.com/klassmaster/

Veryant Support has experience with and recommends ProGuard http://proguard.sourceforge.net/