Principles .NET & Java Malware Analysis

Interpreted vs. Compiled

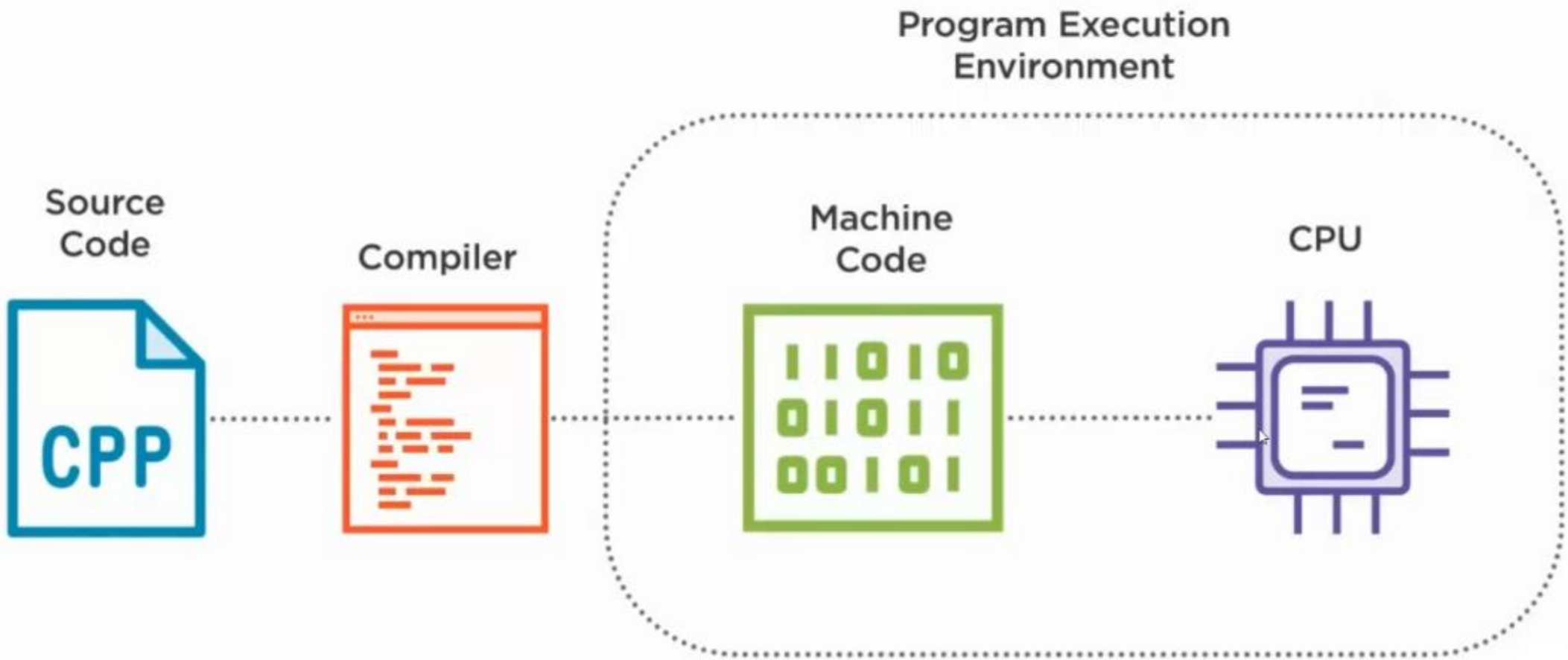
Compiled Languages

Source code is translated into machine code

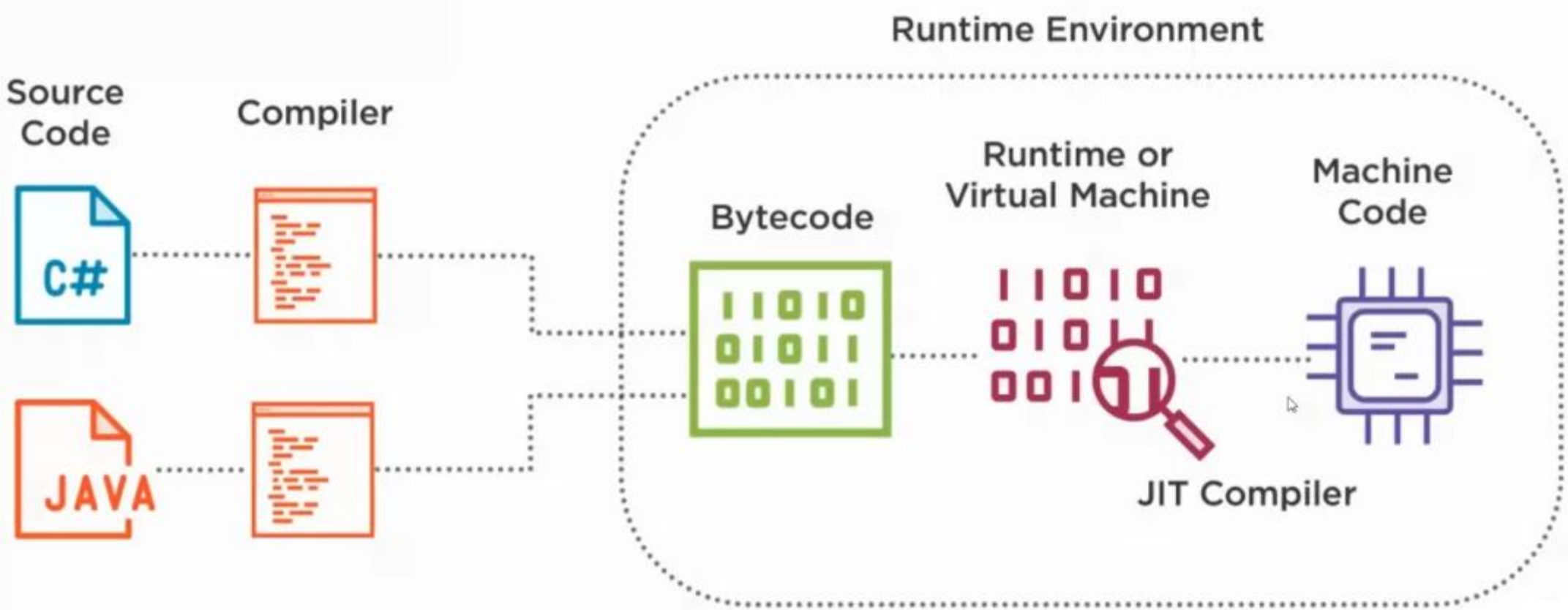
Interpreted Languages

Source code is translated into a bytecode representation

Compiled Languages



Interpreted Languages



Code Obfuscation

- Because .NET and Java ByteCode can be de-compiled back into source code with relative ease, programmers use Code Obfuscation to make it harder to analyse the code after de-compilation.

Obfuscation Comes in Many Forms

String manipulation and/or nonsensical naming is one of the most prevalent ways

Use of encoding or encryption will also be common

Authors will also include unnecessary code to slow down your analysis

Anti-analysis will also be present to disrupt both manual and automated analysis

Nonsensical Naming of Functions/Variables

```
3   public static void E2X2QDArgLHRsFtgsih6u7uWipQxHTrkRE9xMUq5r55q8DEPIt06cx3LNbCuw76BY7LRkF9()
4   {
5       Form2.ao5CrzX1W6();
6       Form2.aC0V5FB();
7       Form2.aOr5gT49Qk();
8       Form2.aivcCiy();
9       Form2.aQ80so9q6DcVP();
10      Form2.arm7Y7UM();
11      Form2.uWipQxHTrkRE9xMUq5r58KCF6hMHBUqXf5zhYYAPuYqL5 =
          Form3.KCF6hMHBUqXf5zhYYAPuYqL4FO0kgXtIziDEHPGG21vvdDfq7J3().Load
          (Form1.Aw0thGO34Z72LsABWmZu6FO0kgXtIziDEHPGG21vvdDfq7J1);
```

String Manipulation

```
private static string dire_c_toryy_ofdelll =
    Environment.GetFolderPath(
    Environment.SpecialFolder.CommonApplicationData) +
    "\\" +
    encc.DecryptStringAES("EAAAAOeHr6QeAnAEeR04Cna7WcCsBCEg
    pGA5pyNBz3e1BNyy",
    Program.msaltpassss);
```

Unnecessary Instructions

```
public static void E2X2QDArgLHRsFtgsih6u7uWipQxHTrkRE9xMUq5r55q8DEPIt06cx3LNbCuw76BY7LRkF9
  ()
{
    Form2.ao5CrzX1W6();
    Form2.aC0V5FB();
    Form2.aOr5gT49Qk();
    Form2.aivcCiy();
    Form2.aQB0so9q6DcVP();
    Form2.arm7Y7UM();
    Form2.uWipQxHTrkRE9xMUq5r58KCF6hMHBUqXf5zhYYAPuYqL5 =
      Form3.KCF6hMHBUqXf5zhYYAPuYqL4FO0kgXtIziDEHPGG21vvdDfq7J3().Load
      (Form1.Aw0thGO34Z72LsABWmZu6FO0kgXtIziDEHPGG21vvdDfq7J1);
}
```

```
public static double ao5CrzX1W6()
{
    return 6038.1;
}
```

Thank you