CS266 Software Reverse Engineering (SRE)

Reversing .NET Intermediate Language (CIL/MSIL)

Teodoro (Ted) Cipresso, teodoro.cipresso@sjsu.edu
Department of Computer Science
San José State University

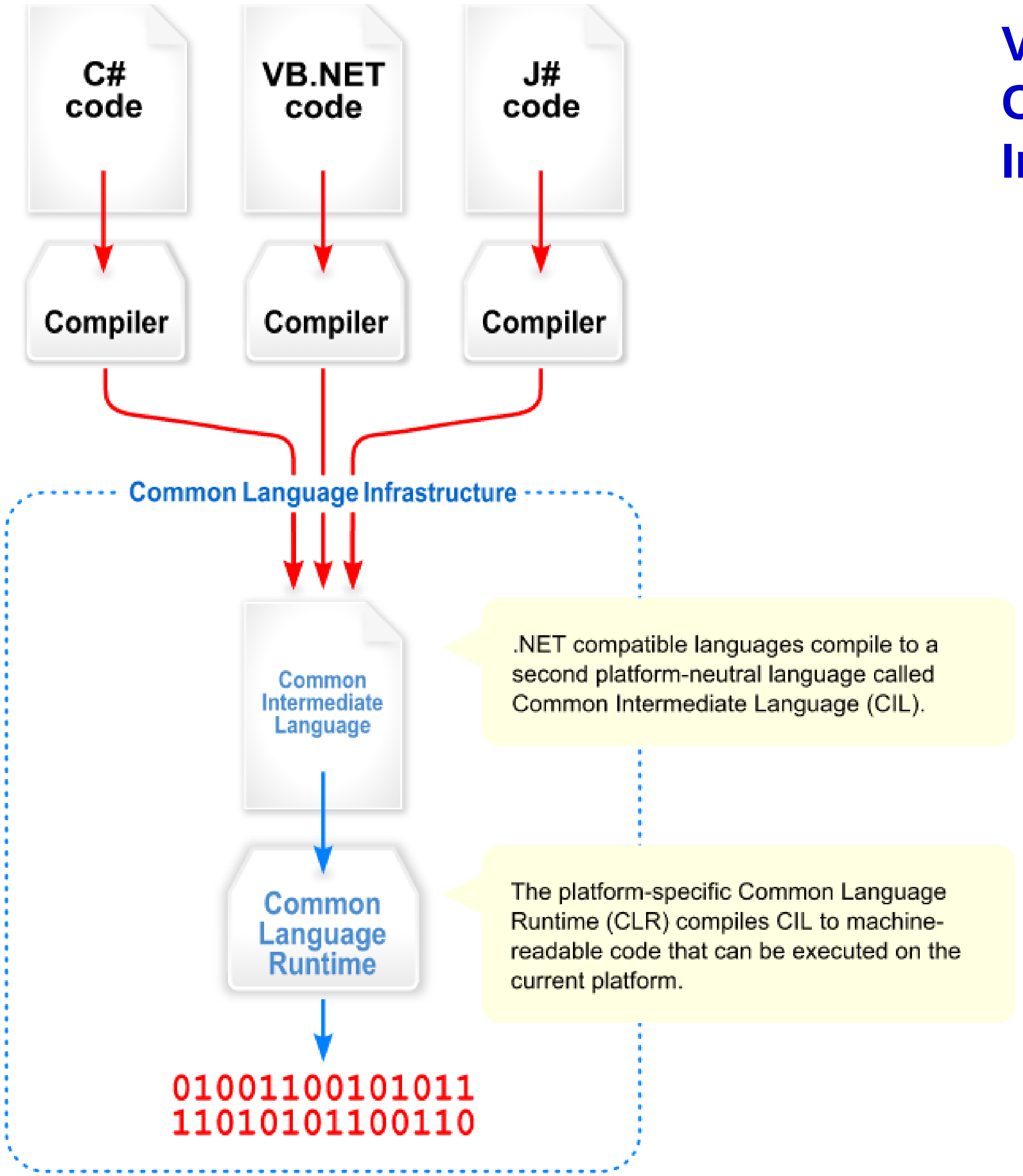
Spring 2015

Reversing .NET Intermediate Language (IL)

.NET CIL Versus Java Bytecode

- When considering compilation, .NET can be compared to Java and the JVM.
  - .NET application code is compiled to Common Intermediate Language (CIL) or Microsoft Common Intermediate Language (MSIL).
    - CIL is the CLI Standard. MSIL is CIL as generated by Microsoft.
  - CIL and MSIL are comparable to Java bytecode.
  - Instead of being being compiled directly to machine code, the .NET Common Language Runtime (CLR) translates CIL to machine code as needed at execution time.
  - Just-in-time compilation increases execution speed while keeping class, function, variable names in the compiled program.

Visual overview of the Common Language Infrastructure (CLI)



.NET compatible languages compile to a second platform-neutral language called Common Intermediate Language (CIL).

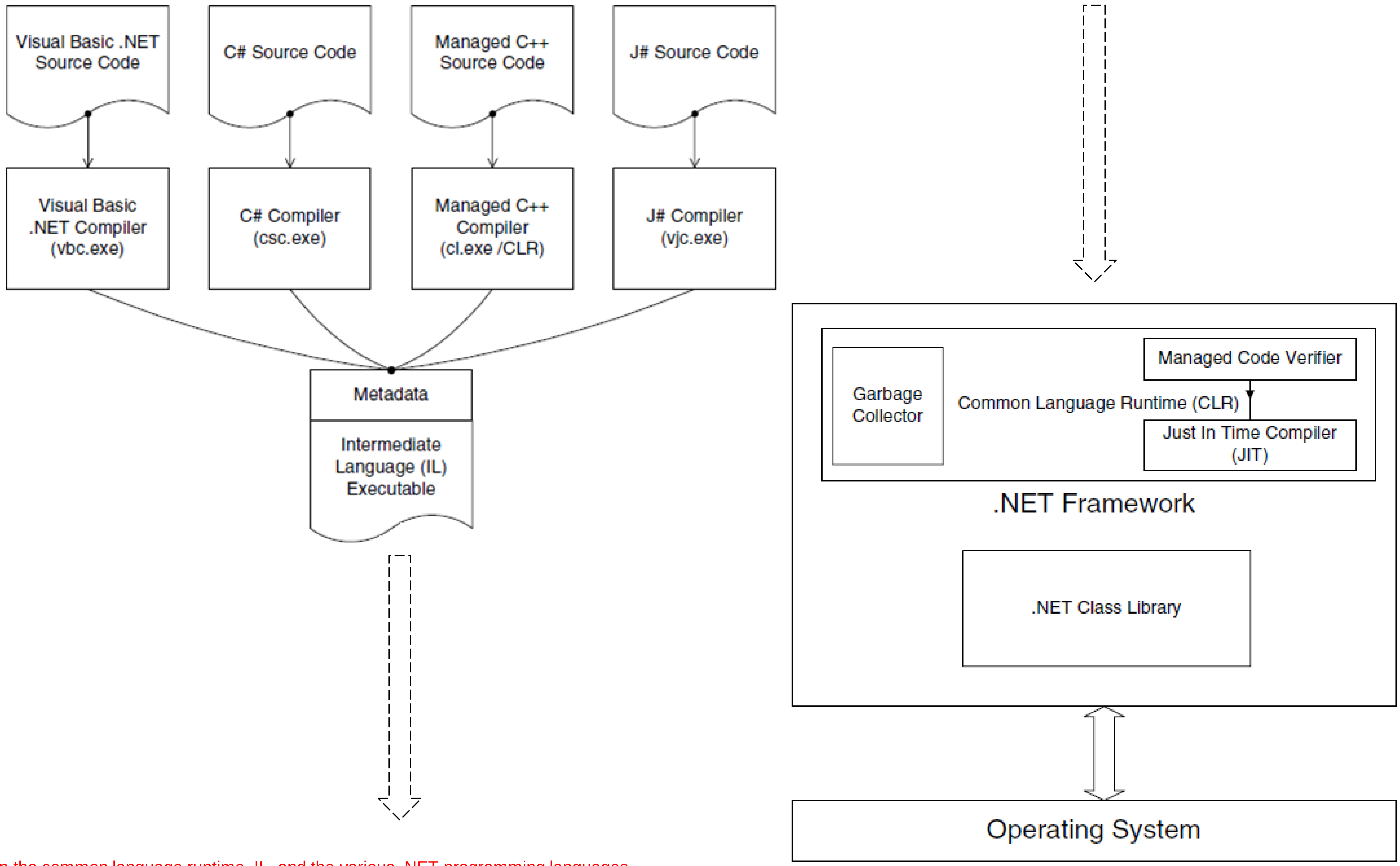
The platform-specific Common Language Runtime (CLR) compiles CIL to machine-readable code that can be executed on the current platform.

Wikipedia contributors. "Common Language Infrastructure." *Wikipedia, The Free Encyclopedia*. Wikipedia, The Free Encyclopedia, 14 Feb. 2015. Web. 20 Apr. 2015

Reversing .NET Intermediate Language (IL)

The .NET Runtime Environment

- The .NET Framework is the execution environment in for .NET programs, and consists of the CLR and the .NET class library.
  - The .NET class library provides .NET programs to access GUI, network, file, and other services to communicate with the outside world.
- A .NET binary module is referred to as an assembly.
  - Assemblies contains a combination of CIL code and associated metadata.
  - Metadata describes the data types, variables, methods signatures, etc..
  - Assemblies are executed by the CLR, which loads the metadata into memory and compiles the CIL to machine code using a JIT compiler.
  - CLR is a VM within the .NET framework that verifies assemblies and provides a safe execution environment.



Visual Basic .NET Source Code

C# Source Code

Managed C++ Source Code

J# Source Code

Visual Basic .NET Compiler (vbc.exe)

C# Compiler (csc.exe)

Managed C++ Compiler (cl.exe /CLR)

J# Compiler (vjc.exe)

Metadata

Intermediate Language (IL) Executable

Garbage Collector

Common Language Runtime (CLR)

Managed Code Verifier

Just In Time Compiler (JIT)

.NET Framework

.NET Class Library

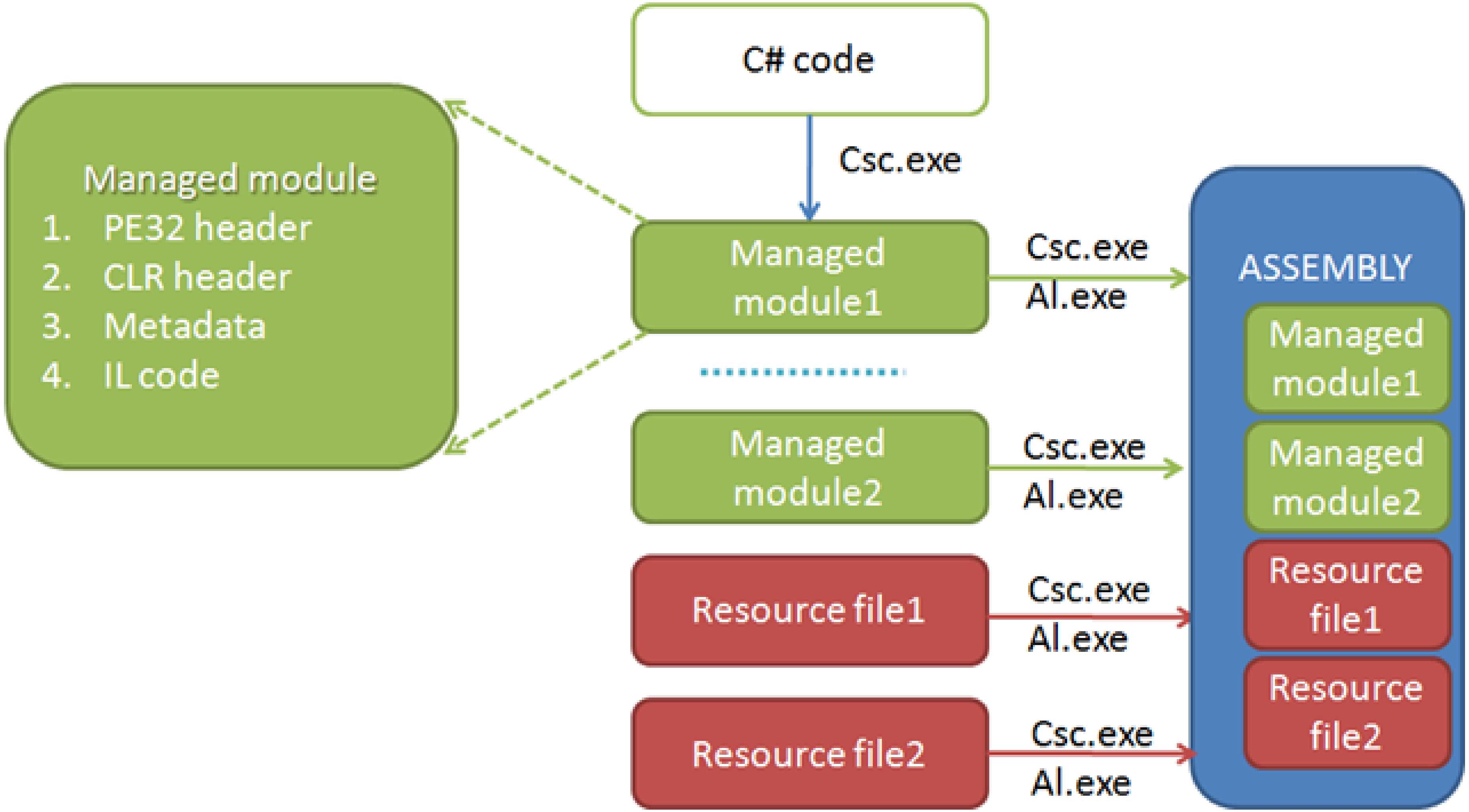
Operating System

Relationship between the common language runtime, IL, and the various .NET programming languages.

Reversing .NET Intermediate Language (IL)

About Managed Code

- Managed code is any code that is verified by the CLR runtime for security, type safety, and memory usage.
- Managed code consists of MSIL code and metadata. The combining of MSIL and metadata is what allows the CLR to actually execute managed code.
- The CLR is always aware of the data types that a program is using.
- In non-managed machine code, memory is accessed using a pointer and offset into memory. The processor has no idea what data structure the memory at a given location represents or whether the address is valid or not.
- Just like non-managed code, every managed code module contains a windows PE header. For managed code, most of the PE header information is ignored.



.NET Foundations – .NET assembly structure

Reversing .NET Intermediate Language (IL)

Some .NET Reversing Tools

- ILSpy (.NET IL browser and decompiler)
  - ILSpy is the open-source .NET assembly browser and decompiler.
  - Red Gate announced free version of .NET Reflector would cease to exist.
- DILE (.NET IL interactive debugger and disassembler)
  - Dotnet IL Editor (DILE) allows disassembling and debugging of .NET applications without source code or .pdb files.
- 9 Rays Spices .NET Decompiler
  - Convert .NET IL to C#, VB.Net, J#, Delphi.Net and managed C++.
  - Not Free. Trial version available.

Reversing .NET Intermediate Language (IL)

Some .NET Reversing Tools

- DUMPBIN (Microsoft COFF Binary File Dumper)
  - Use to examine COFF object files, standard libraries of COFF objects, executable files, and dynamic-link libraries (DLLs).
  - In a Visual studio command prompt, execute the command:
    - **dumpbin /all** assembly_name > output.txt
- Ildasm.exe (IL disassembler)
  - Companion to the IL Assembler (Ilasm.exe). Ildasm.exe takes a Windows PE file that contains IL code and creates suitable input to Ilasm.exe.

End