SAND2013-7380C

Perspectives on Security

Dr. Samuel Mulder

Sandia National Laboratories

September 2013

Program Understanding

- Understanding a program is easiest at the source code level.
- When was the last time you read a good program?

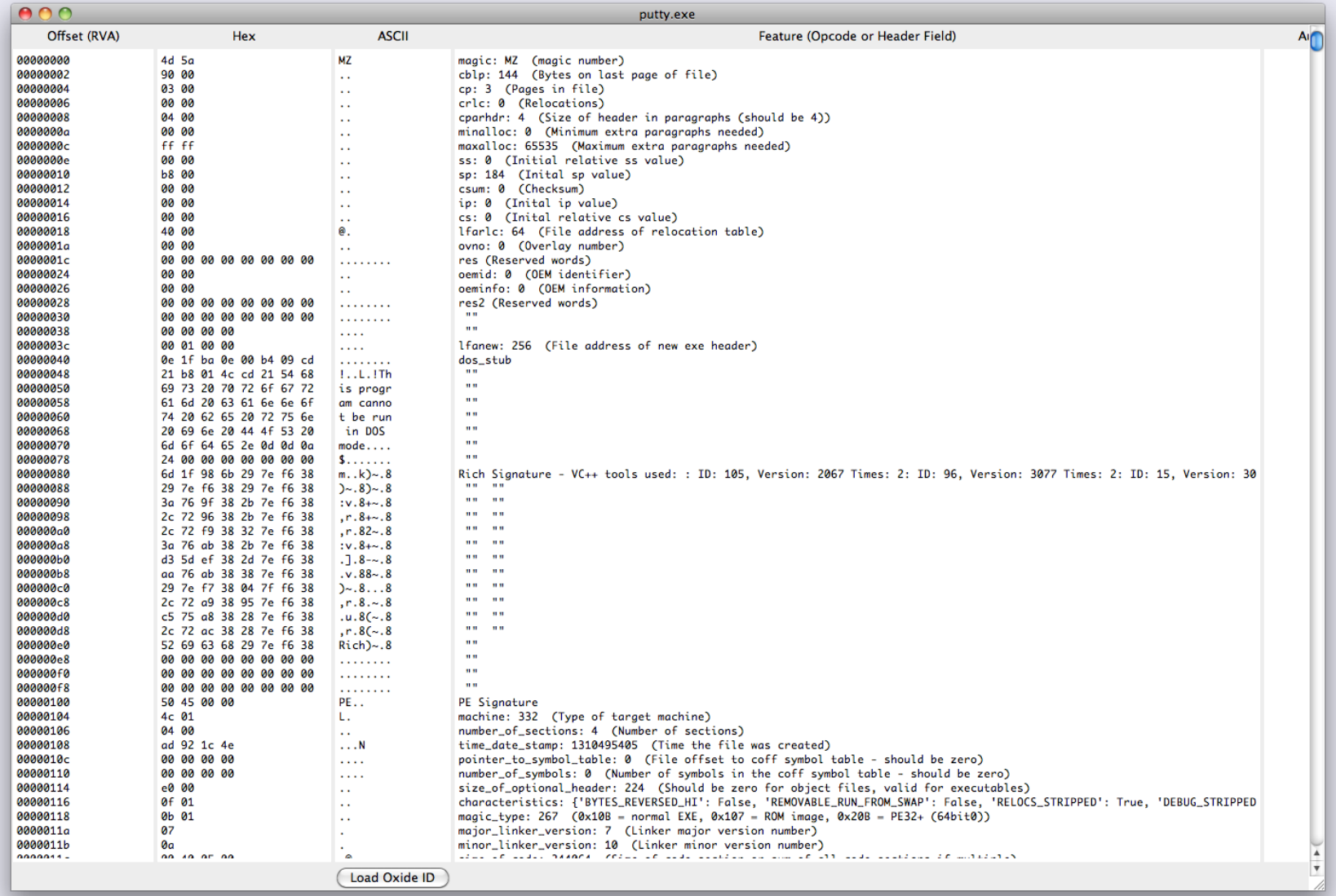
How closely does the program you wrote match what gets run?

- Language transformation
- Compiler optimization
- Libraries and system calls

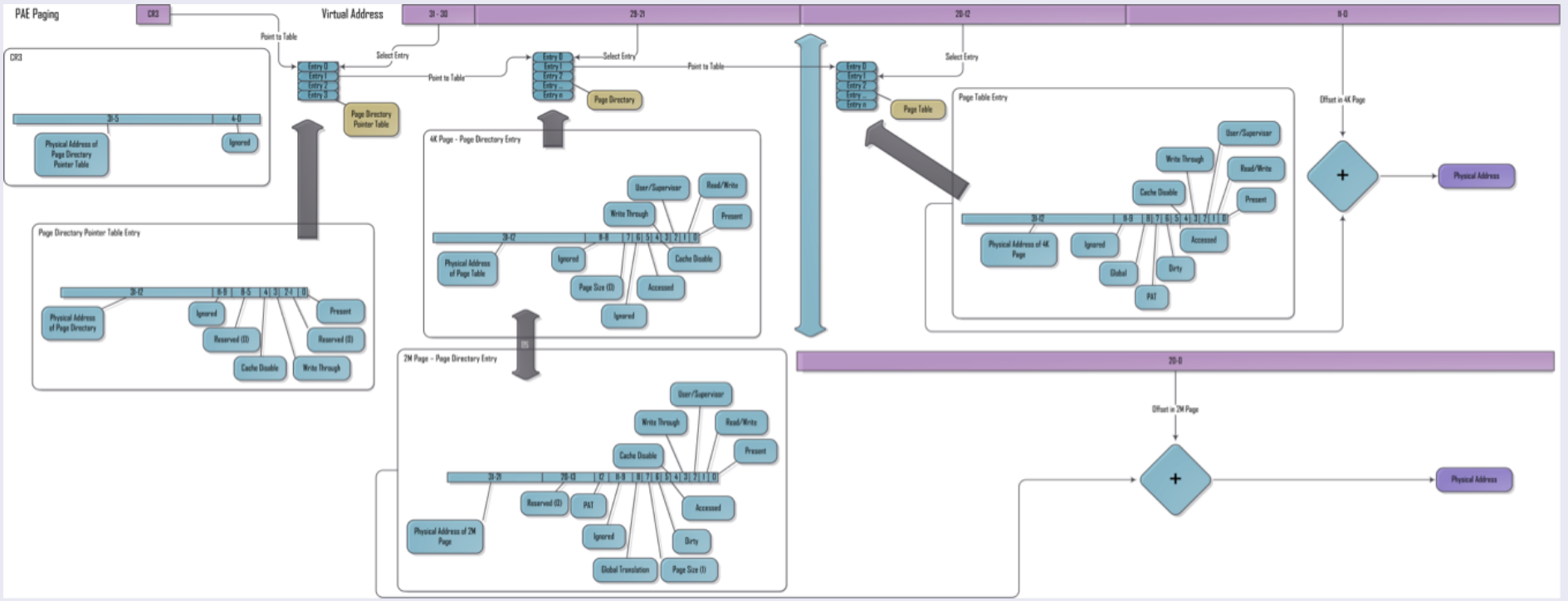
To really know what gets executed, we must look at the binary image.

- Disassembly is undecidable.
- Program features like switch statements, inheritance, object-oriented programming all translate into code/data mingling.
- Libraries and system calls bring in new code.

The system loader interprets the PE header.



The system loader loads a program into virtual memory.



Programs are like onions...

- The user assumes the application works
- The application assumes the DLLs work
- The DLLs assume the OS works
- The OS assumes the BIOS works
- The BIOS assumes the hardware design works
- The hardware design assumes the physics work

How can we know anything?

- Radical Skepticism?
- Security researchers have to be epistemologists.
- Most of the interesting stuff lies in between layers of abstraction.

Complexity is the enemy of my enemy?

- Which is easier to understand - a Windows executable or a custom embedded system?
- Absolute Knowledge vs. Known Unknowns vs. Unknown Unknowns.

Good vs. Evil

- I just need to find the 'evil bit'.
- Everywhere I look there is badness.

Badness != violating the security properties of the OS

With user level access, a bad guy can:

- Steal all my money
- Steal all my information
- Impersonate me
- Alienate my friends
- Implicate me in criminal activity

With kernel level access, a bad guy can:

- Install a device driver?

Assessing Risk

- Cyber security vs. Physical security.
- Progress is based on accepted risk.

What to do?

- We are accepting more risk on a daily basis, at an alarming rate.
- That will not change.
- We must rise to the challenge.

An effective mindset...

- Effectiveness requires deep humility...
- and amazing hubris.
- Breadth vs. Depth
- A unique adversarial problem space
- A willingness to tackle hard problems