
SPQR

Dynamic Binary Instrumentation

Avoid malware evasion during analysis

By f_palmaro

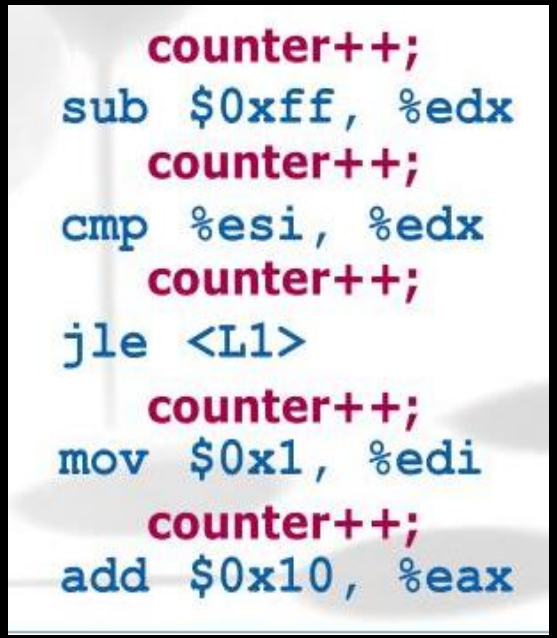
Dynamic Binary Instrumentation

Malware Evasion

BluePill

Dynamic Binary Instrumentation

A program analysis technique used to understand the behavior of a binary application at run time through the injection of instrumentation code. Such code executes as part of the normal instruction stream after being injected in the program.



DBI Framework

Pin is a software system that performs Dynamic Binary Instrumentation (DBI) of application. It allows a user to place instrumentation for calls to analysis code in arbitrary positions in the executable.

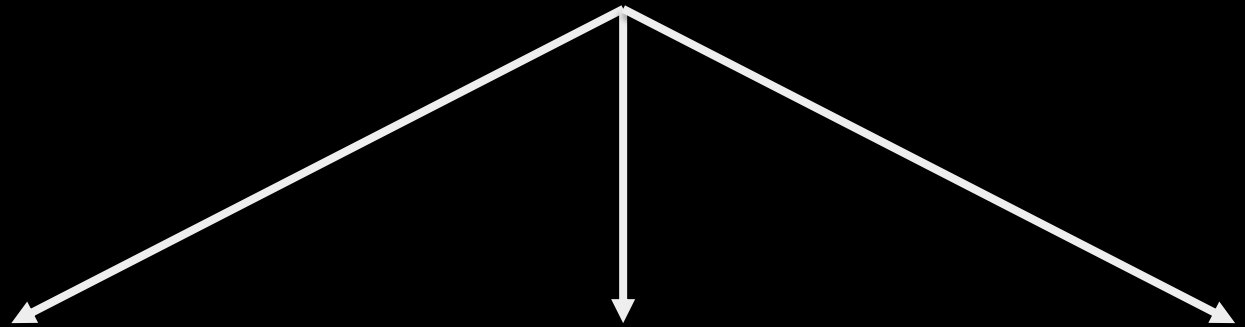
DBI Framework

Pin & Pintools:

- Pin – The intrumentation engine –> JIT for x86
- PinTool – The instrumentation program -> pintool.dll

DBI Framework

PinTools register hooks on events in the program



Instrumentation routines

called only on the first time something happens

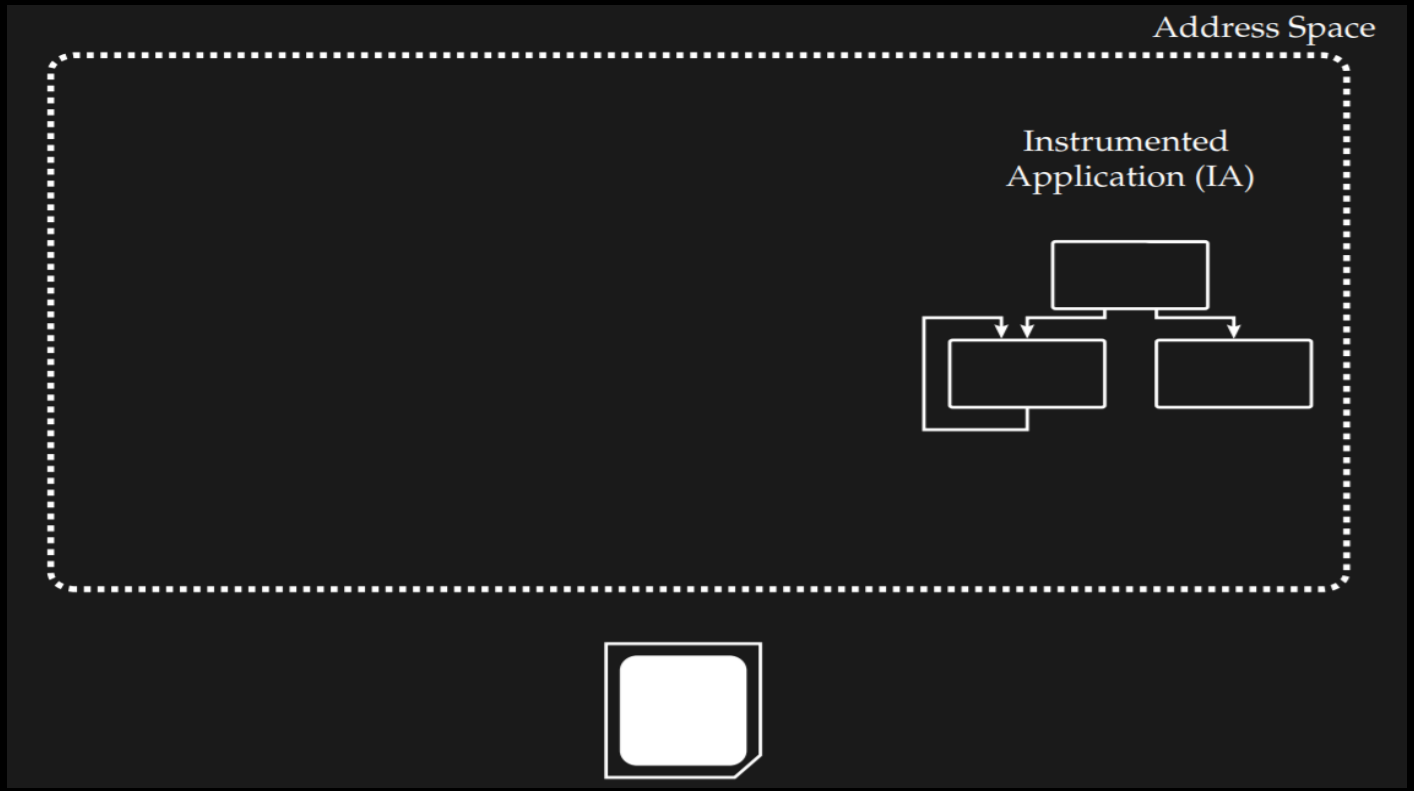
Analysis routines

called every time this object is reached

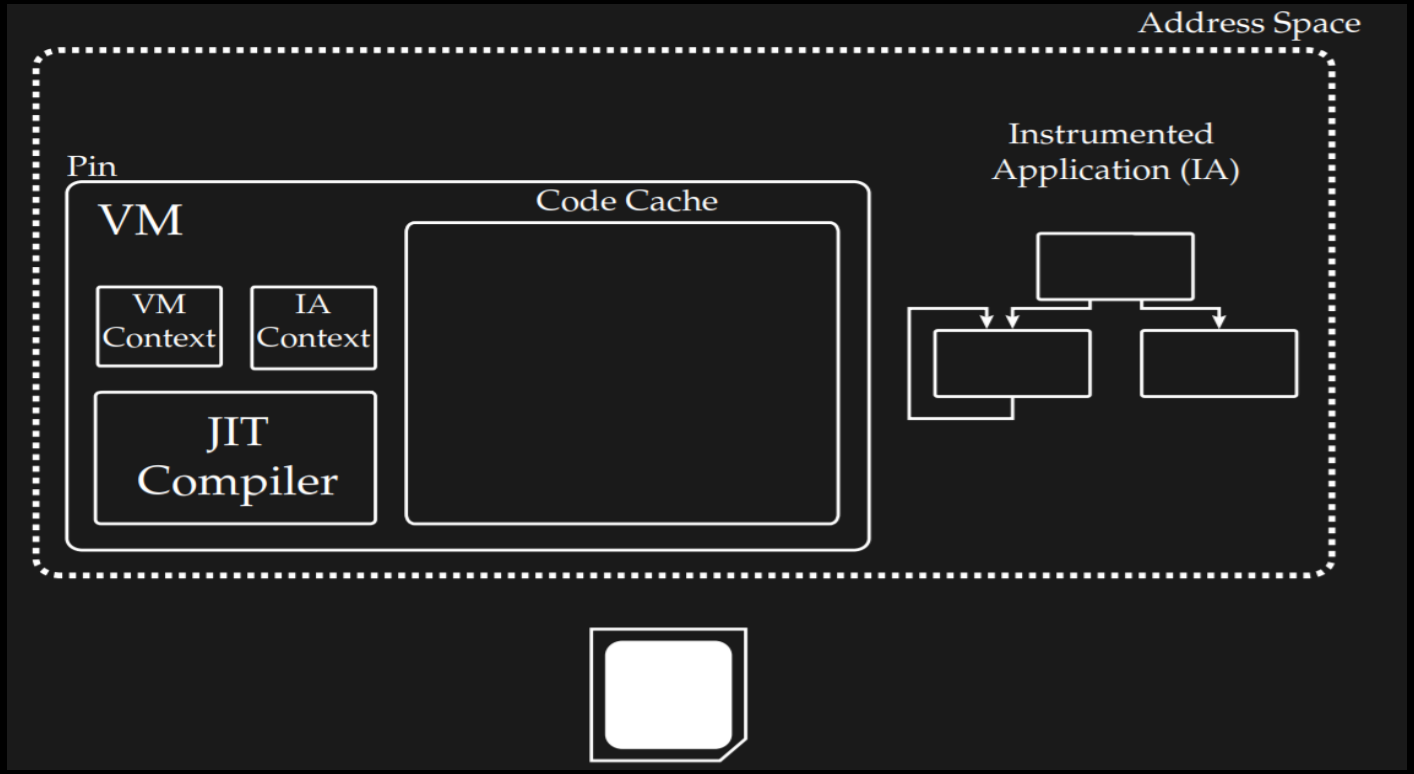
Callbacks

called whenever a certain event happens

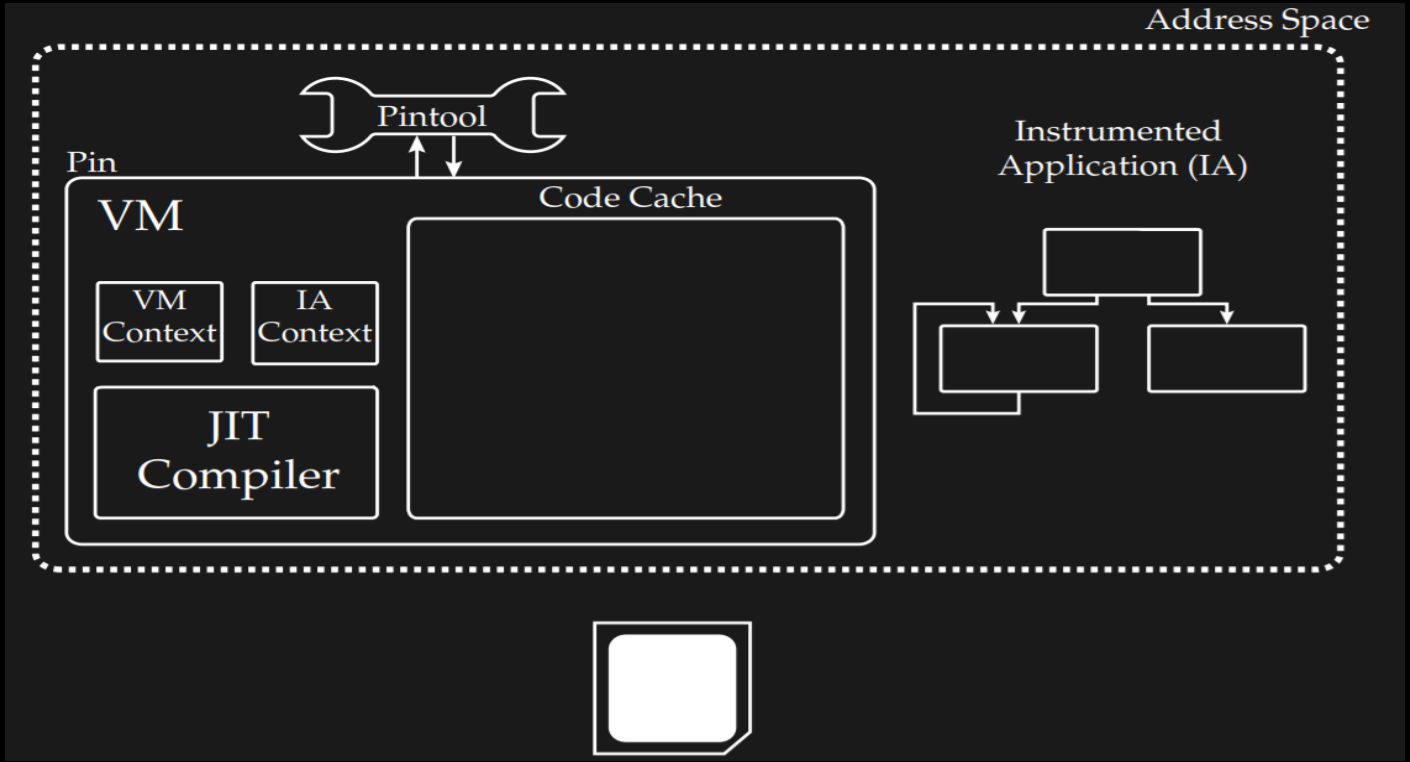
Dynamic Binary Instrumentation



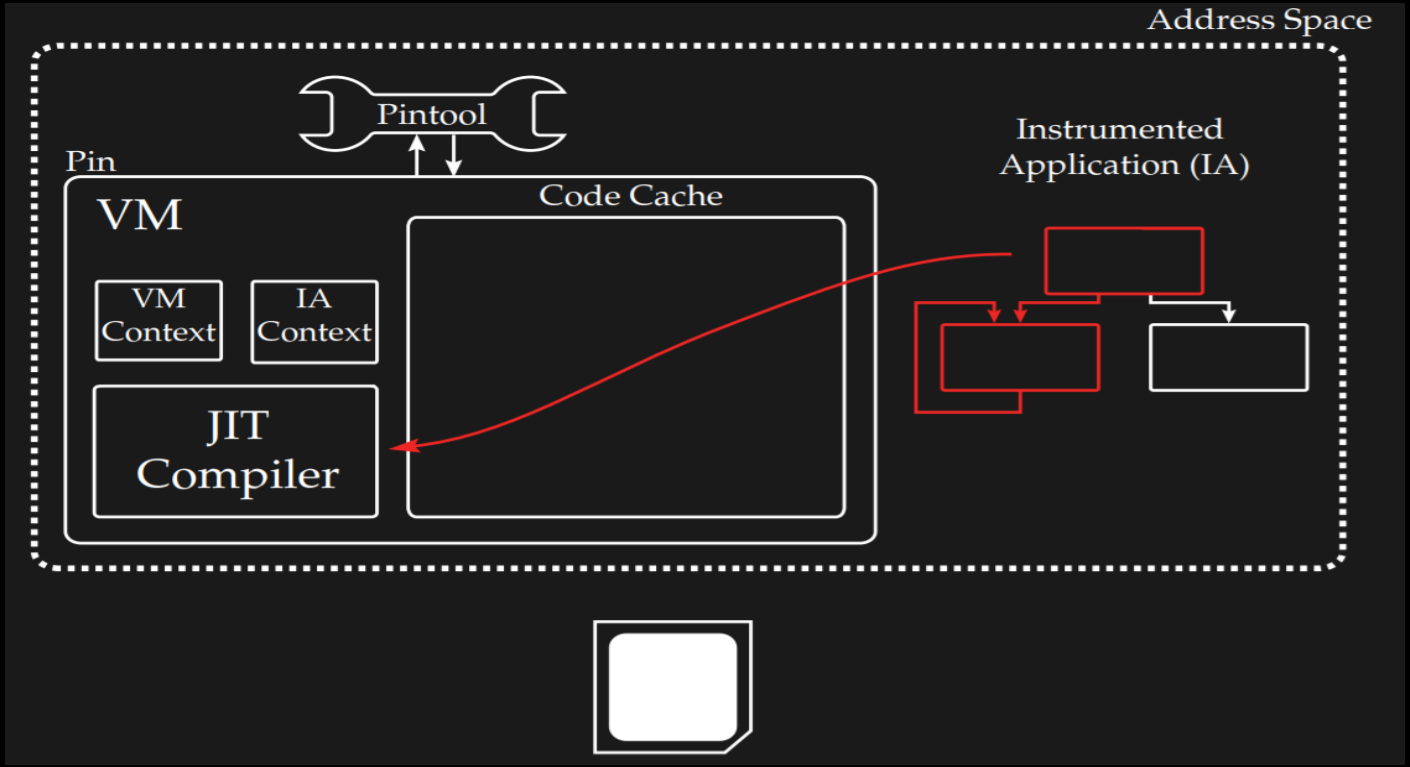
Dynamic Binary Instrumentation



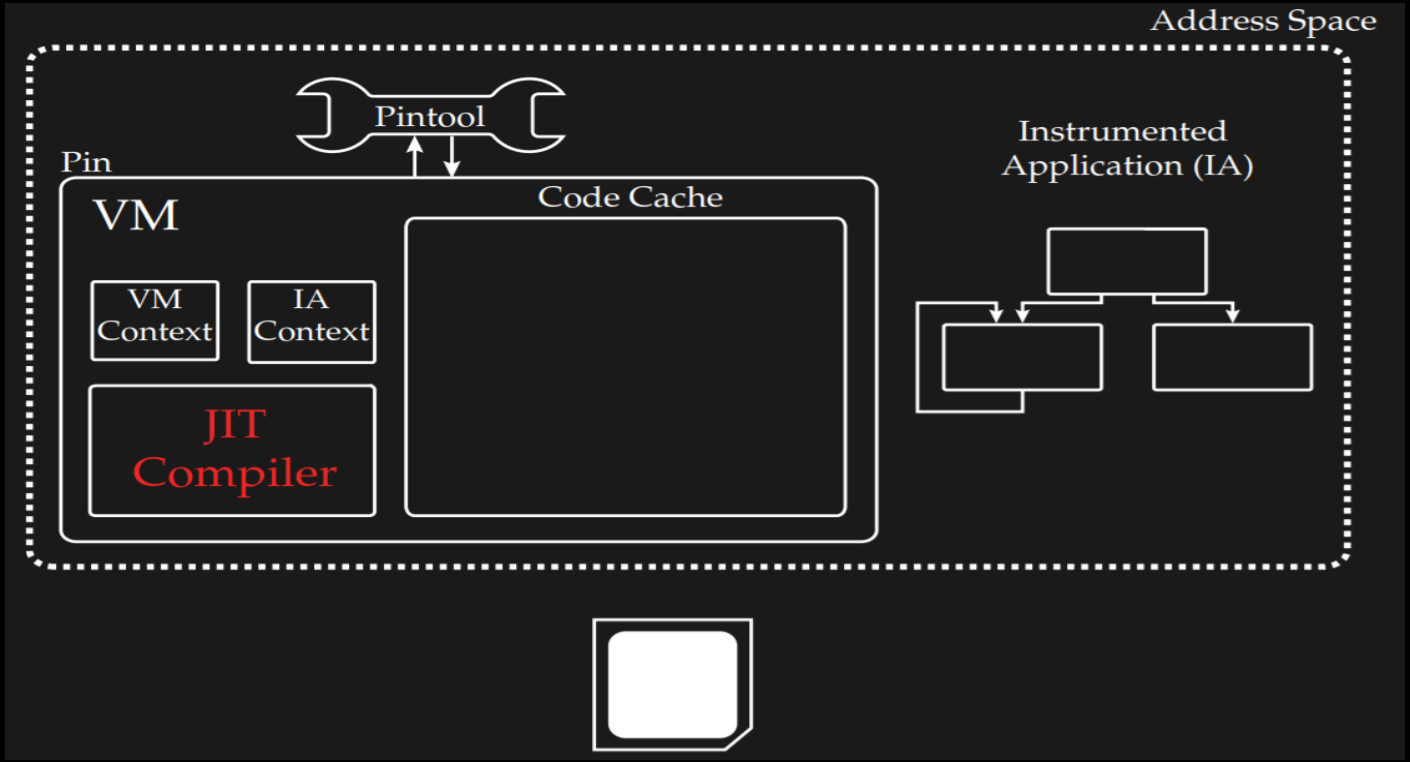
Dynamic Binary Instrumentation



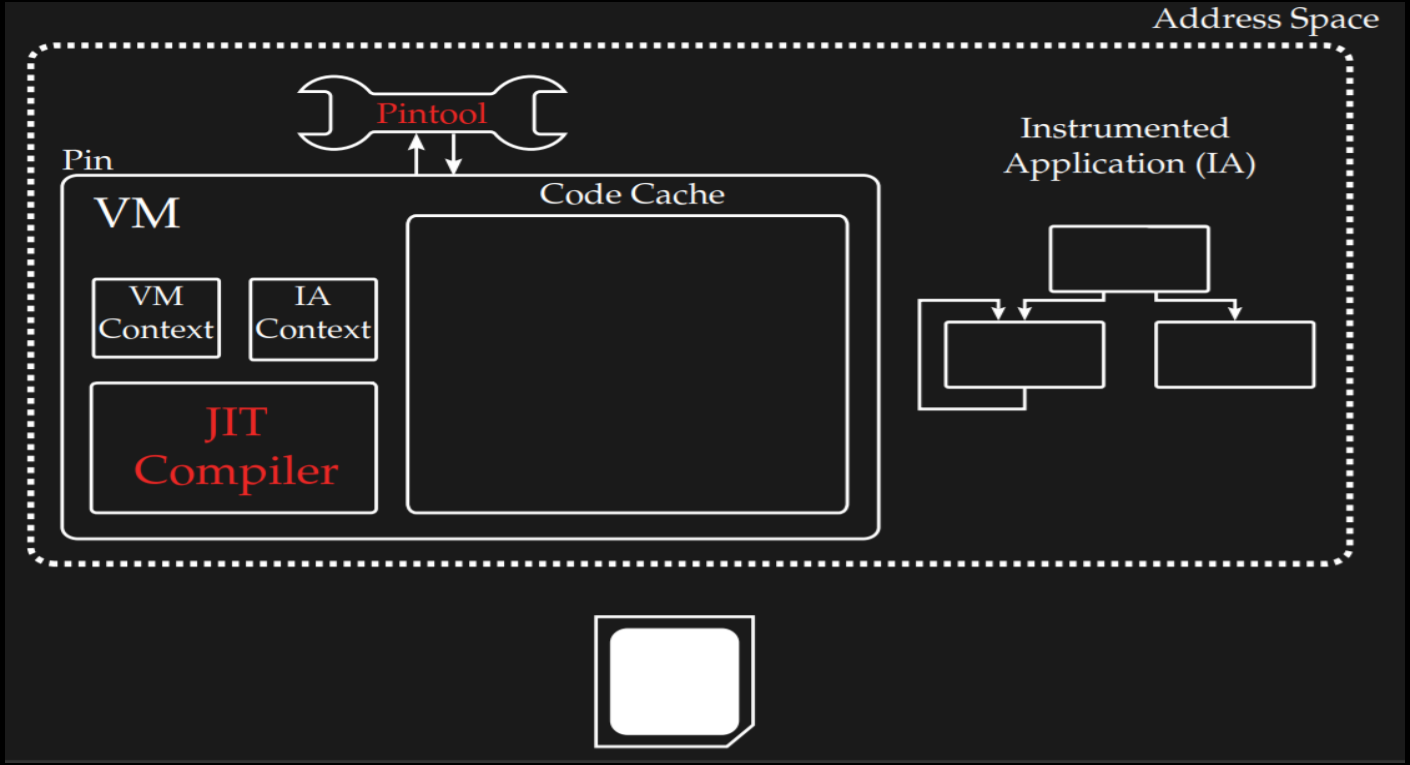
Dynamic Binary Instrumentation



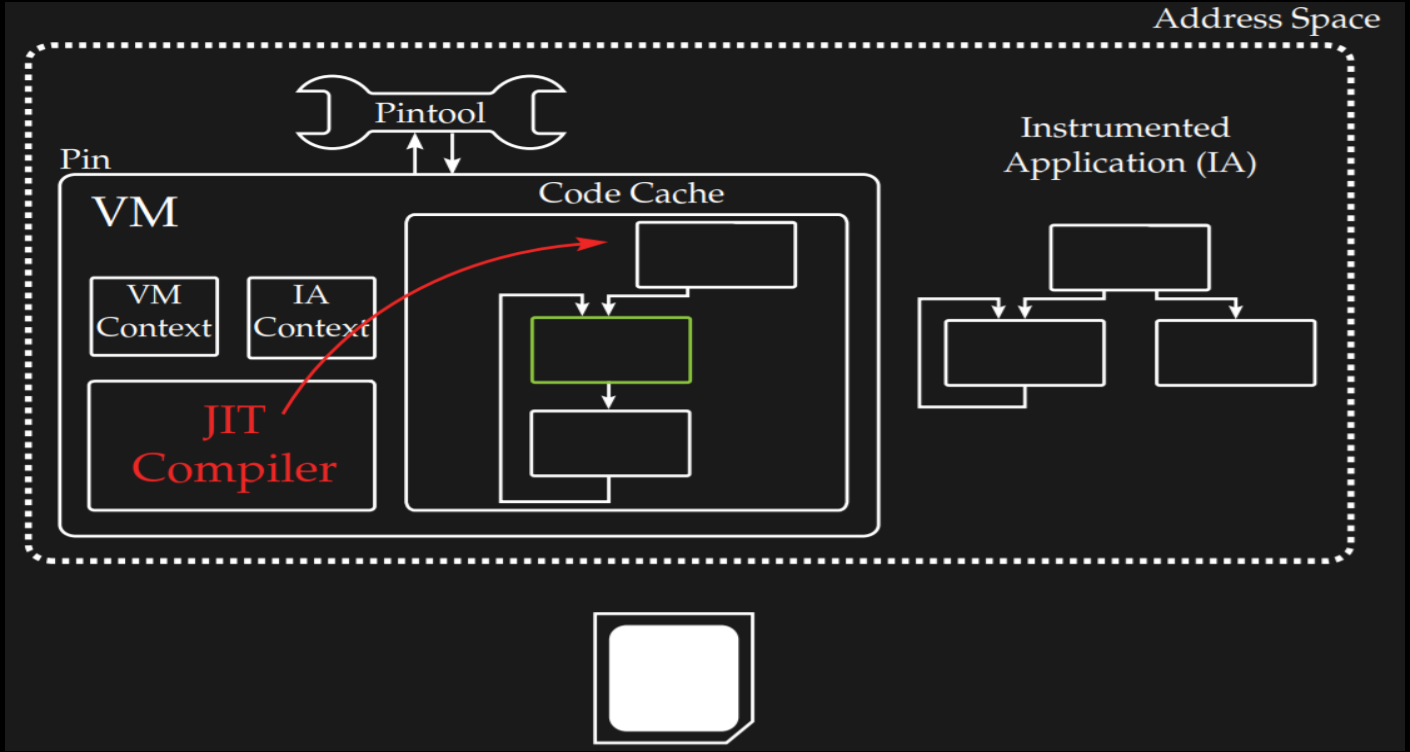
Dynamic Binary Instrumentation



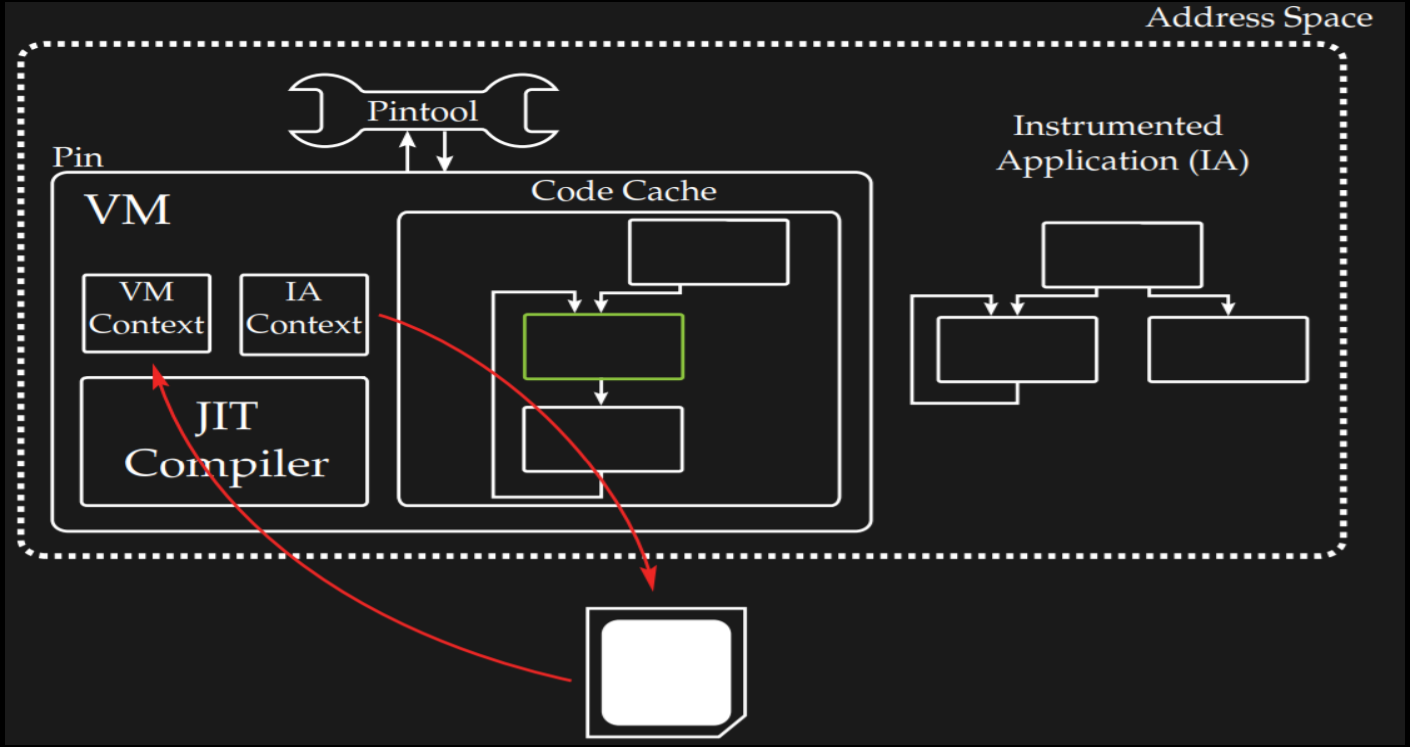
Dynamic Binary Instrumentation



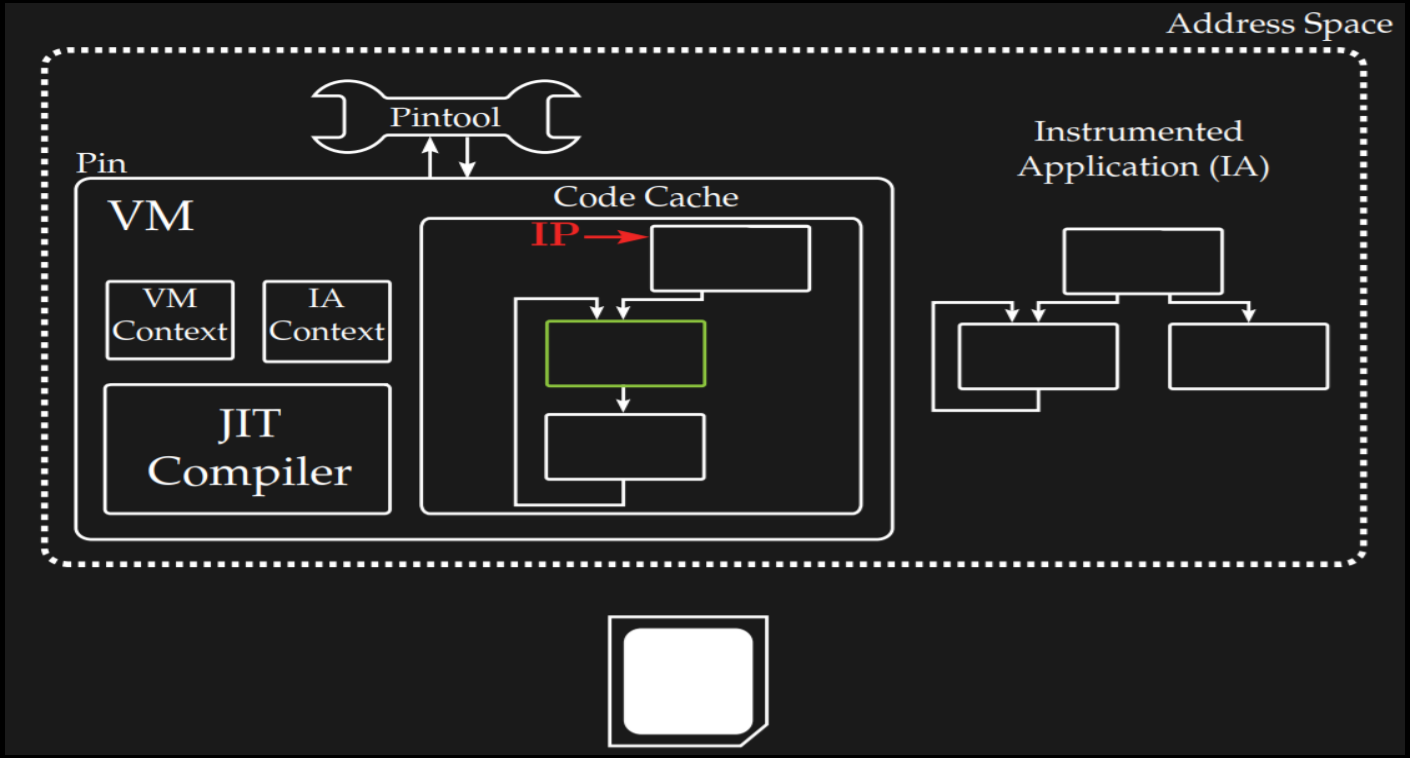
Dynamic Binary Instrumentation



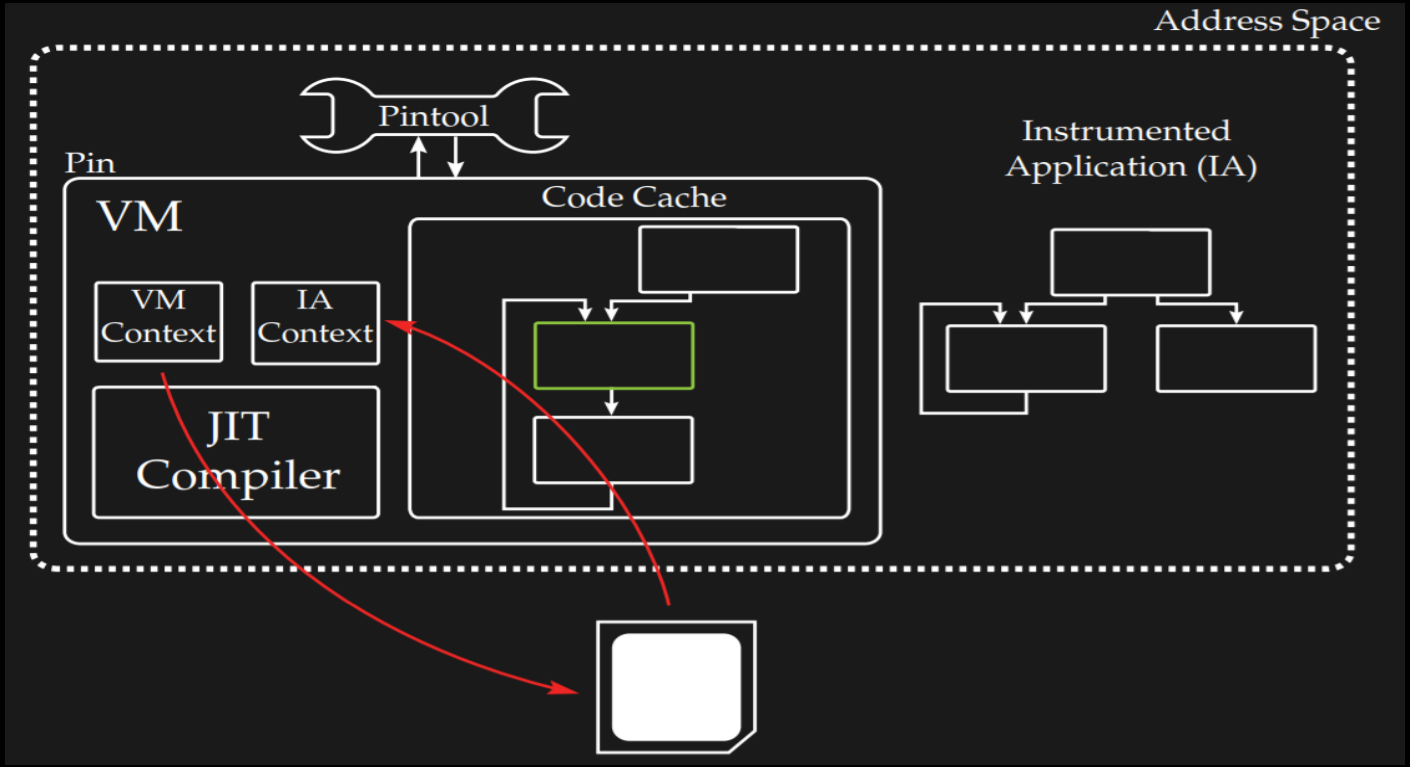
Dynamic Binary Instrumentation



Dynamic Binary Instrumentation



Dynamic Binary Instrumentation



Malware Evasion

DEMO with code

Dynamic Binary Instrumentation

➡ **Malware Evasion**

BluePill

Malware Evasion

SANDBOX

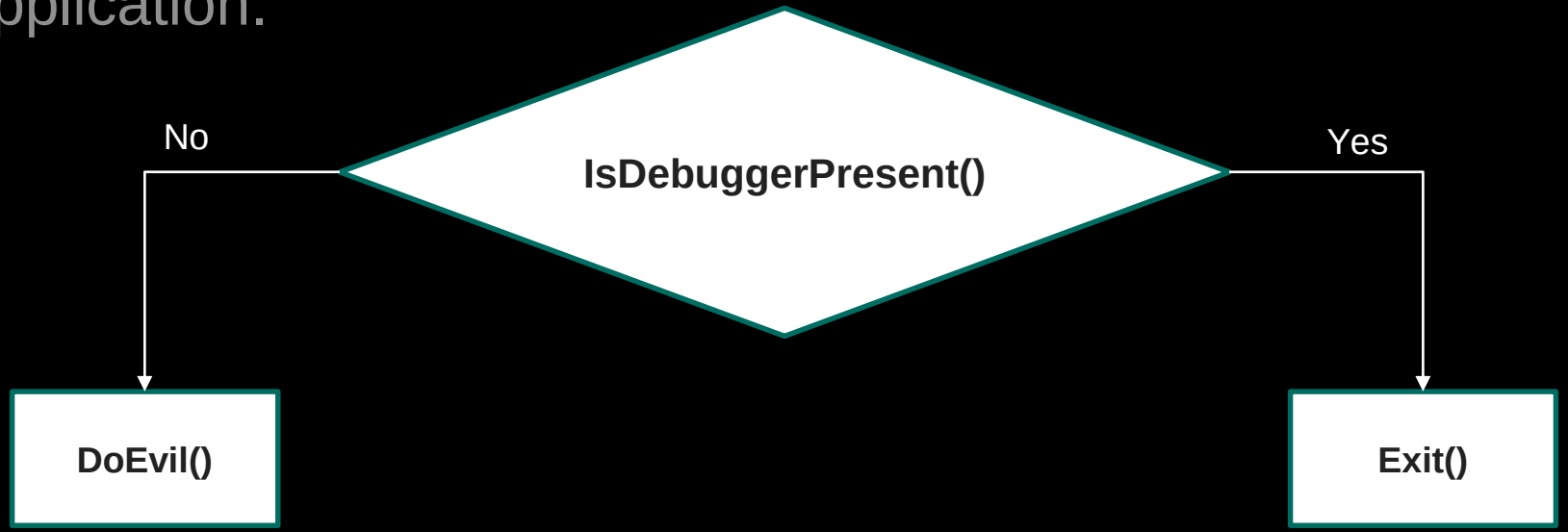
A sandbox is a controlled environment in which analysts can observe the behavior of a malware sample while it is running. These systems are made of virtual machines that can be restored in a fast way after the analysis is complete.

DEBUGGER

A debugger is a computer program used by programmers to test and debug a target program. Debuggers may use instruction-set simulators, rather than running a program directly on the processor to achieve a higher level of control over its execution. This allows debuggers to stop or halt the program according to specific conditions.

Malware Evasion

In the presence of a hostile environment, malware can change its behavior to try to be categorized as a benign application.



Malware Evasion

- Anti-debugging attacks
- Anti-injection
- Anti-Dumping
- Timing Attacks [Anti-Sandbox]
- Human Interaction / Generic [Anti-Sandbox]
- Anti-Virtualization / Full-System Emulation
- Anti-Analysis
- …

Malware Evasion

DEMO with Al-Khaser

Dynamic Binary Instrumentation

Malware Evasion

➡ **BluePill**

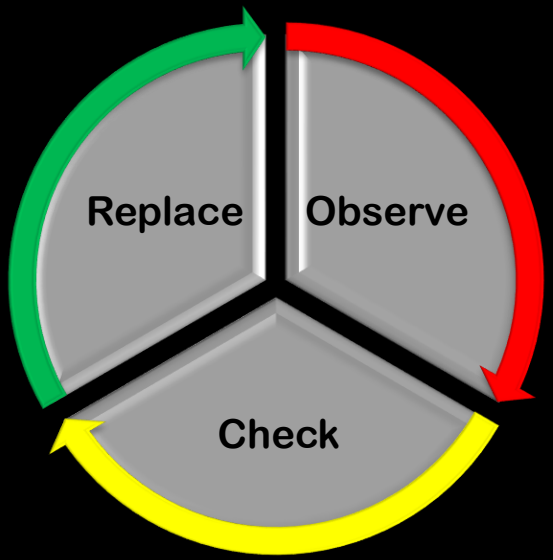
BluePill

Malware looks for known artifacts of analysis environments

Try to trick a sample by giving it fake responses as if it were in a real environment

BluePill

The process to provide fake responses to malware is based on three steps: Observe, Check and Replace



Observe: monitor all activities (e.g., calls) of running process

Check: analyze input parameters and return values of previously selected actions

Replace: fix “wrong” values with other considered valid *(as a real environment would yield)*

Malware Evasion

DEMO with Al-Khaser

Malware Evasion

DEMO with Furtim

Thank you!

QUESTIONS?

References

USEFUL PAPERS:

- Chi-Keung Luk, Robert Cohn, Robert Muth, Harish Patil, Artur Klauser, Geoff Lowney, Steven Wallace, Vijay Janapa Reddi, and Kim Hazelwood. 2005. Pin: building customized program analysis tools with dynamic instrumentation. In Proceedings of the 2005 ACM SIGPLAN conference on Programming language design and implementation (PLDI '05). ACM, New York, NY, USA, 190-200. DOI: https://doi.org/10.1145/1065010.1065034

MORE ABOUT PIN AND EVASIONS

- https://software.intel.com/en-us/articles/pin-a-dynamic-binary-instrumentation-tool
- https://recon.cx/2018/montreal/schedule/events/145.html
- https://github.com/LordNoteworthy/al-khaser
- https://www.sentinelone.com/blog/sfg-furtims-parent/