

ICE: Circumventing Meltdown with an Advanced Binary Analysis Framework

Dean Pucsek
University of Victoria, Canada
dpucsek@uvic.ca

Jennifer Baldwin
University of Victoria, Canada
jebaldwin@cs.uvic.ca

Jonah Wall
University of Victoria, Canada
jojonah@uvic.ca

Martin Salois
Defence Research &
Development Canada
martin.salois@drdc-
rddc.gc.ca

Celina Gibbs
University of Victoria, Canada
celinag@cs.uvic.ca

Yvonne Coady
University of Victoria, Canada
ycoady@cs.uvic.ca

ABSTRACT

In this paper we propose ICE, an Integrated Comprehension Environment, designed to facilitate advanced binary analysis through an extensible framework. ICE makes extensive use of modules and a flexible intermediate representation to enable seamless integration of instruction set architectures, platforms, and analysis techniques.

Categories and Subject Descriptors

D.2.4 [Software]: Software Engineering—*Software/Program Verification*

General Terms

Security, Verification

Keywords

Intermediate Languages, Frameworks, Extensibility

1. PROPOSAL: THE ICE FRAMEWORK

A commonality of modern binary analysis frameworks, such as IDA Pro and BitBlaze [3], is that they are all dependent on the accuracy and extensibility of an intermediate language (IL). Consequently, any error in the IL is propagated throughout the framework resulting in an incorrect analysis. Furthermore, the inclusion of new instruction set architectures (ISAs), platforms, and analysis techniques is limited by the capabilities of the IL.

For example, REIL [2] introduces inaccuracies into the analysis by replacing unknown native instructions with a variant of the NOP instruction. Moreover, due to its limited instruction set REIL requires a large number of instructions to model a single native instruction.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

TOPI '11, 28-MAY-2011, Waikiki, Honolulu, USA
Copyright 2011 ACM 978-1-4503-0599-0/11/05 ...\$10.00.

To combat the extensibility issues and flaws associated with exclusive use of ILs, we propose an Integrated Comprehension Environment (ICE). In order to provide the robustness and extensibility required by an advanced binary analysis framework ICE utilizes a layered design, makes extensive use of modules, and employs a flexible intermediate representation (IR). At the base of the framework is the *Platform Substrate*, it encapsulates platform specific details in a platform independent interface. On top of the Platform Substrate is the *ICE Core* which provides facilities to manage the analysis and ISA modules. Finally, the *ICE Bridge* provides a normalized interface between the analysis and ISA modules. In order to create this interface, the ICE Bridge uses the ICE IR which is based on a series of APIs exported by the modules and ICE Core.

To date we have developed Tracks [1], a proof-of-concept tool that leverages information provided by a plug-in built on top of IDA Pro to enable advanced analysis within an Eclipse plug-in. The Tracks protocol, used between Tracks and the debugger, supports transmission of information about system calls to external modules, allows concurrent analysis on multiple executables, and provides navigation cues. It is important to note that the Tracks protocol decouples Tracks from IDA Pro so that the same functionality can easily be achieved with other debuggers.

In this paper we have identified extensibility as a key requirement for an advanced binary analysis framework and presented ICE, a binary analysis framework that allows seamless integration of ISAs, platforms, and analysis techniques.

2. REFERENCES

- [1] J. Baldwin, P. Sinha, M. Salois, and Y. Coady. Progressive user interfaces for regressive analysis: Making tracks with large, low-level systems. *AUIC 2011*, pages 1–10, Nov 2010.
- [2] T. Dullien and S. Porst. REIL: A platform-independent intermediate representation of disassembled code for static code analysis. In *CanSecWest Applied Security Conference*, 2009.
- [3] D. Song, D. Brumley, H. Yin, J. Caballero, I. Jager, M. Kang, Z. Liang, J. Newsome, P. Poosankam, and P. Saxena. Bitblaze: A new approach to computer security via binary analysis. *Information Systems Security*, pages 1–25, 2008.