FROM RESEARCH TO INDUSTRY

cea tech

Lightning talks:

Dynamic Symbolic Execution for malware reverse-engineering

Robin David

Botconf 2015, Paris

list

3 December, 2015

digiteo

INSTITUT CARNOT CEA LIST

About Me & Lab

Me :3rd year PhD student at the CEA *(Atomic Energy Commission)*

- Subject : static/dynamic analysis combination for malware de-obfuscation
- Supervisors :
  - **Jean-Yves Marion** *(Inria Nancy, Loria)*
  - **Sébastien Bardin** *(CEA)*

Lab : LSL : Software Safety and Security Laboratory

Work on :

(Project financed by ANR)

(Disassembly / Simulation / Static Analysis / **Dynamic Symbolic Execution**) (Released as open-source soon..)

Goal/Problematic

Main goal : Recovering the original CFG from an obfuscated malware *(or a close approximation)*

Problems encountered :

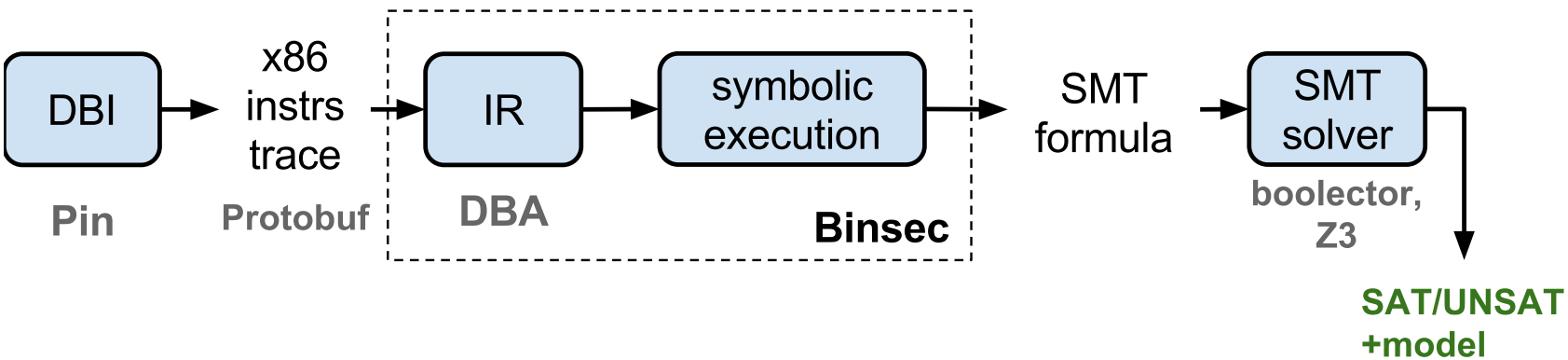
- Packer *(VM, code flattening ..)*
- opaque predicates
- Call/Ret violation
- Dynamic jump targets *(eg : jump %eax)*

Final goal $\rightarrow$ Obtaining better signatures engines (developped at the Loria)

Symbolic execution

Symbolic execution : is the mean of executing a program using symbolic values (logical symbols) rather than actual values (bitvectors) in order to obtain in-out relationship of a path.

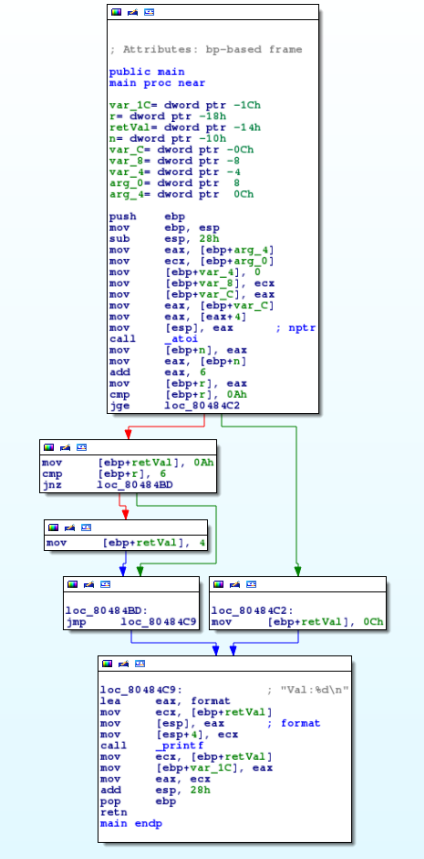
DSE (aka Concolic) : SE performed on an execution trace



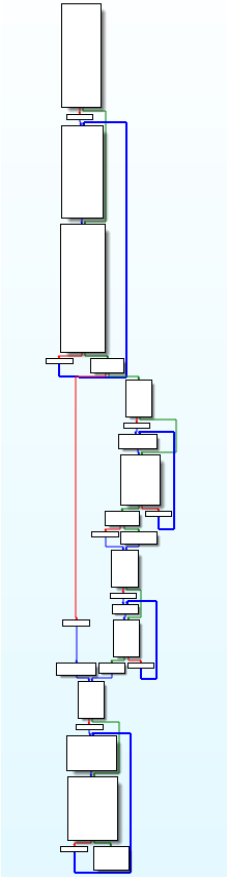
Demo !

Demo

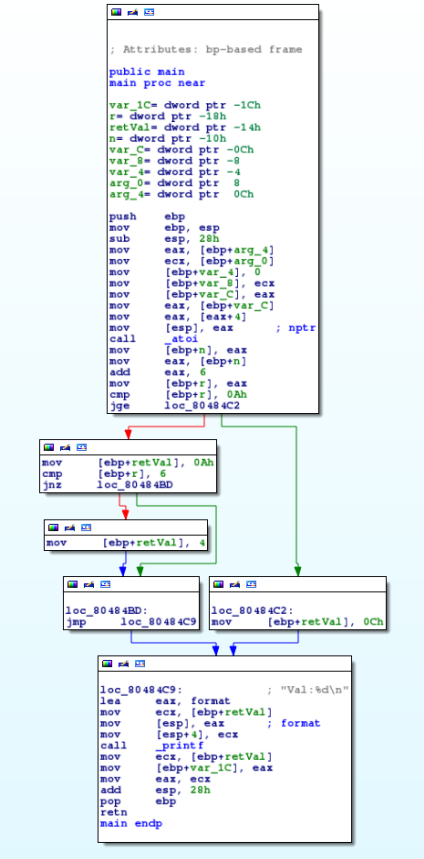
Original CFG



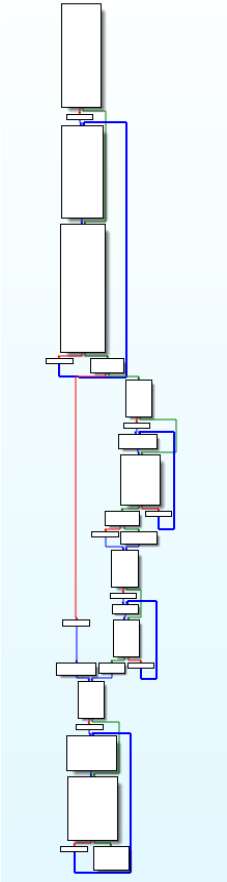
CFG Obfuscated (with OP using O-LLVM)



Original CFG



CFG Obfuscated (with OP using O-LLVM)



Results :

	#nb jmp	SAT	UNSAT
Genuine	2	2	0
Obfuscated	10	2	8

Upcoming work

- **Formula Optimizations** (for Scalability)
- **Exploring concretization/symbolization trade-offs**
- **Apply it on obfuscations**
  - Recovering VPC values for VM, code-flattening
  - possible target dynamic jumps
  - (and a lot's of others..)
- **Reversing Botnet C&C protocol ?** *(in the binary)*

→ All this in order to scale on real world packed/obfuscated malwares and large datasets

Thank you !

Direction de la Recherche Technologique
Département d'Ingénierie des Logiciels et des Systèmes
Laboratoire de Sûreté des Logiciels

Commissariat l'énergie atomique et aux énergies alternatives
Institut Carnot CEA LIST

Centre de Saclay — 91191 Gif-sur-Yvette Cedex

Etablissement public à caractère industriel et commercial — RCS Paris B 775 685 019