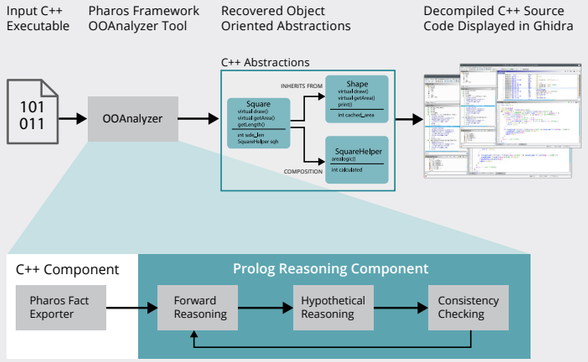
Improvements to Object-Oriented Construct Recovery Using OOAnalyzer

Problem

OOAnalyzer is the state of the art in automatically recovering object-oriented abstractions to assist reverse engineers in malware analysis, vulnerability analysis, and software assurance. First published at the ACM Conference on Computer and Communications Security, OOAnalyzer uses novel techniques to reason in the presence of uncertainty, which is unavoidable in this type of analysis. This feature is heavily dependent on OOAnalyzer's Prolog-based implementation. Unfortunately, early versions of OOAnalyzer were too slow to scale to the large and complex programs used in the DoD.

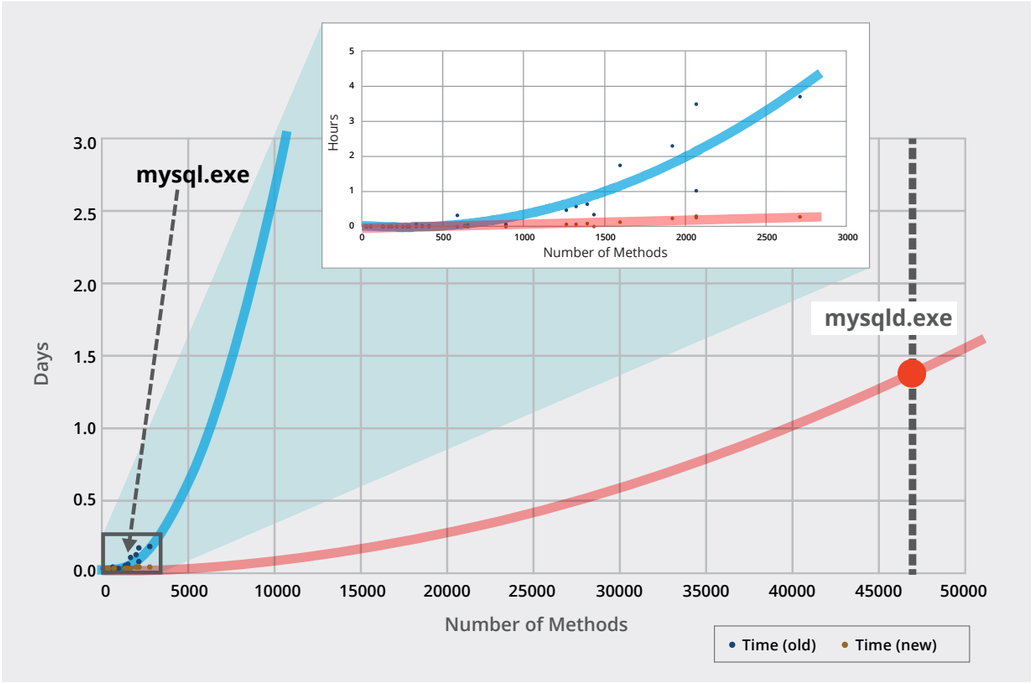
OOAnalyzer Design Overview



Solution

- We worked with the developer of SWI Prolog to create novel profiling and debugging tools for Prolog.
- Many problems were simple to fix once the problem was identified using new tools.
- Unfortunately, we identified systemic issues related to the Prolog tabling optimization.
- We avoided these issues with a new technique and are working with the SWI developers on a general solution.

OOAnalyzer was too slow to be used on the programs that the DoD needs it for the most. It is now **50x** faster and can analyze large programs.



Before and After Data

Program	# Class	# Method	Time (Old)	Time (New)	Improvement
x3c	6	28	0:00:01	0:00:01	0.6x
Malware d597bee8	19	133	0:00:04	0:00:04	0.0x
Malware 0faaa3d3	21	135	0:00:05	0:00:07	-0.3x
optionparser	11	56	0:00:05	0:00:01	3.8x
MySQL connection.dll	43	166	0:00:07	0:00:04	0.7x
Malware cfa69fff	39	182	0:00:08	0:00:09	-0.1x
light-pop3-smtp	44	290	0:00:21	0:00:14	0.5x
Malware 29be5a33	19	130	0:00:24	0:00:05	3.7x
CImg	29	220	0:00:52	0:00:11	3.6x
MySQL ha_example.dll	21	256	0:01:04	0:00:16	3.1x
Firefox	141	638	0:01:47	0:01:30	0.2x
PicoHttpD	95	656	0:03:38	0:00:37	4.9x
Malware 6098cb7c	55	339	0:03:54	0:00:15	**14.5x**
Malware 67b9be3c	400	2072	2:42:19	0:17:31	**8.3x**
MySQL cfg_editor.exe	190	1270	3:27:50	0:03:53	**52.6x**
MySQL libmysql.dll	200	1327	4:22:55	0:04:04	**63.7x**
Malware f101c05e	169	1601	4:25:34	0:07:17	**35.5x**
MySQL mysql.exe	202	1395	4:34:49	0:04:37	**58.5x**
MySQL upgrade.exe	333	2069	11:34:56	0:15:30	**43.8x**
Malware 628053dc	207	1920	11:46:38	0:14:16	**48.5x**
Malware deb6a7a1	283	2712	17:33:52	0:17:15	**60.1x**

Cory F Cohen | Dr. Edward Schwartz | info@sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM20-0860