

Dismiss

Join GitHub today

GitHub is home to over 20 million developers working together to host and review code, manage projects, and build software together.

Sign up

Runtime Prevention of Return-Oriented Programming Attacks

3 commits

2 branches

0 releases

Fetching contributors

Branch: master

New pull request

Find file

Clone or download

ivanfratric Update README.txt

Latest commit e849d26 on May 3, 2015

bin	No commit message	6 years ago
common	* minor mods	6 years ago
doc	No commit message	6 years ago
ropguard	* minor mods	6 years ago
ropguarddll	* minor mods	6 years ago
vulnapp	No commit message	6 years ago
README.txt	Update README.txt	3 years ago

README.txt

RUNTIME PREVENTION OF RETURN-ORIENTED PROGRAMMING ATTACKS

ROPGuard is a system for runtime detection and prevention of return-oriented programming (ROP) attacks. It works by defining a set of checks that are performed when certain OS functions are called to determine if those functions are called from the ROP code or as a result of normal program execution. The system can be applied at runtime to any process and has a low CPU and memory overhead. The detailed project documentation can be found in the doc folder.

ROPGuard won the second prize at the Microsoft's BlueHat Prize contest at Black Hat USA 2012 (<https://www.microsoft.com/security/bluehatprize/>).

The code and other project files provided here are for educational purposes only. If you are interested in running ROPGuard to protect your computer, I recommend you download Microsoft EMET instead (<http://www.microsoft.com/emet>), as it implements protection mechanisms from ROPGuard (see: <http://www.microsoft.com/en-us/news/Press/2012/Jul12/07-25BlueHatPrizePR.aspx>), but also contains many reliability improvements and is actively maintained. I'd like to thank Elias Bachaalany of Microsoft for not only implementing ROPGuard technology into EMET but also improving it in every way.

.\\doc folder contains the documentation in .doc and .pdf format

.\\bin folders contains all executables and other files needed to run the prototype. Prototype usage is described in the documentation.

.\ropguard, .\ropguarddll and .\common folders contain all the source and project files of the prototype

.\vulnapp folder contains the source and the project files of an example vulnerable application used during the evaluation