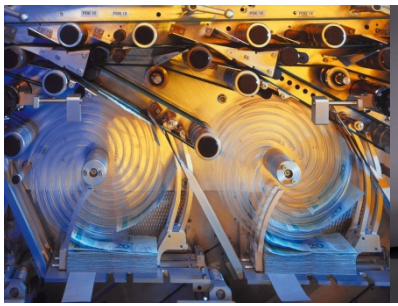
Development and Industrial Application of Multi-Domain Security Testing Technologies

Innovation Sheet

Malwasm and its Application to Testing




ITEA 2
INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

Malwasm
Description

Malwasm is an open source tool designed by itrust consulting in order to help reverse engineers understand what a binary does.

The tool works in the following steps:

1. It starts a virtual machine using VirtualBox;
2. It executes the binary of the malware on the virtual machine;
3. A pintool application logs all the activity (and partial activity) of the binary;
4. All the activity is stored in a postgres database;
5. A web browser opens (Firefox or Google Chrome) where the data can be viewed.

Malwasm
Features

- Offline program debugging;
- Possibility to go backwards and forwards in the time of the execution;
- States of registers and flags;
- Values of the stack/heap/data;
- "Following dump" options;
- Supports x86 architecture;
- Supports multithreads.

Malwasm
State of the art

Presently, we can identify two ways to perform reverse engineering:
- Static analysis
- Dynamic analysis

The static analysis consists of getting the assembly code of an application to understand how the application works. Today, the majority of malware use obfuscation to hide their activities. For example, the Windows registries name modified by a malware can be hidden using compression or encryption.

The dynamic analysis consists of executing a program step by step, instruction by instruction. In this case, the analysis can take a long time. If the analyst goes too far, he has no way to go back and the only solution is to restart the analysis from the beginning.

Malwasm

Advances beyond the state of the art

Malwasm is an innovative tool. No other tool exists with the same approach to reverse engineering.

A regular debugger can follow the execution of a binary, however, it does not give us the possibility to go back using a timeline like malwasm does.

The malwasm tool provides both a static and dynamic malware analysis.

Malwasm
Exploitation and application to case studies

Malwasm can be used during every reverse engineering session. The interest of reverse engineering can be:

- Malware analysis
- Interoperability
- Debugging
- ...

The tool is used during the writing of malware analysis articles for our website malware.lu.

We used it during the case study about smartcards. Malwasm was used to debug our developments and understand how smartcards work.