technicolor

Technicolor R&D France Snc
975 av des Champs Blancs – CS 17616
35576 Cesson-Sévigné Cedex - France

tél. + 33 (0)2 99 27 30 00
fax + 33 (0)2 99 27 30 01

Internship proposal for 2014
Proposal ref : PSL_SCP_002

PSL_SCP_002: Control Flow Graph based attacks

Summary of the internship

Modern reverse-engineering techniques allow attackers to understand underlying algorithms structure of the software. A common method consists in studying its control flow graph (CFG) that statically shows all possible paths of executed instructions. To counter this kind of attack, encryption protection is not always possible and often not sufficient, so there is a need to evaluate alternative solutions. A known technique to make reverse engineering more complex consists in flattening its Control Flow Graph*. The goal of the internship is to analyse some implementations of this technique.

* Wang, C., Davidson, J., Hill, J., & Knight, J. (2001, July). Protection of software-based survivability mechanisms. In *Dependable Systems and Networks, 2001.*

Detailed description

Context

Modern reverse-engineering techniques allow attackers to understand underlying algorithms structure of the software. A common method consists in studying its control flow graph (CFG) that statically shows all possible paths of executed instructions. To counter this kind of attack, encryption protection is not always possible and often not sufficient, so we need to evaluate alternative solutions. A known technique to make reverse engineering more complex consists in flattening its Control Flow Graph*.
The efficiency of the CFG flattening is very dependent on its implementation. Technicolor would like to study different implementations and needs some new reversing tools to evaluate them.

* Wang, C., Davidson, J., Hill, J., & Knight, J. (2001, July). Protection of software-based survivability mechanisms. In *Dependable Systems and Networks, 2001.*

Objective

The goal of this internship is to design and develop some tools to reverse binaries protected with CFG flattening. This should allow us to evaluate and improve some CFG flattening implementation.

Task description

The student will study the state of the art in CFG flattening and in reversing techniques.
Following this study, he will design innovating methods and tools for attacking protected binaries. These tools should reconstruct a readable CFG and evaluate its level of protection using information collected during the execution of the application.

Keywords

Disassembly, reverse, security, software protection, software obfuscation, hacking, decompilation

Working environment

Security & Content Protection Labs in Cesson Sévigné, Rennes, France

technicolor

Technicolor R&D France Snc
975 av des Champs Blancs – CS 17616
35576 Cesson-Sévigné Cedex - France

tél. + 33 (0)2 99 27 30 00
fax + 33 (0)2 99 27 30 01

Internship proposal for 2014
Proposal ref : PSL_SCP_002

Profile of the applicant / Prerequisites

Multiplatform environment (Android or IOS ARM binaries, X86)
Skilled in reverse engineering/ debugging at instruction level.
Experience in at least one assembly language would be an advantage.

Internship period & duration

Six months beginning between February and April 2014