Section A – Personal Data:

Name: Edgar Barbosa

Email Address: edgarmb@gmail.com

Company: COSEINC

Brief biography

Section B – Training Class Data:

Title of Training Class:

Advanced 0Day Discovery using SMT Solvers

Brief Description of Training Class

SMT solvers are revolutionary! This class is designed for reverse engineers and security profe ssionals who want

to learn how to use this powerful tool for program analysis and automated bug finding, base d on practical

exposition of theory and exercises.

Students will learn the SMT LIB v2 language, how to translate x86/64/ARM assembly code to SMT formulas, the

API for using the solvers and how to integrate SMT solvers with fuzzers to find bugs on real s oftware.

Daily Class Outline

Day 1

Introduction to SAT and SMT solvers

SAT solvers

SMT basic concepts

The SMT-LIB v2 language

How to solve constraints with SMT- LIB v2

Using the Z3 Solver Python API

Practical exercises

Day 2

Symbolic Execution

Concolic Execution

Tools:

PySymEmu

Angr

Triton framework

Practical exercises

Day 3

Translating x86-64 and ARM instruction semantics to SMT- LIB

Introduction to Program Synthesis

Automatic input test generation

Code coverage

Practical exercises

Day 4

Intermediate Languages/Representation

REIL/VEX

Intermediate Language problems

Translation to SMT automation

Integrating the SMT solver to you Reverse Engineering toolbox

Exercises

Day 5

Whitebox fuzzing

Automated Bug finding framework

Implementation

Practical exercises on real world targets

Course Requirements

Student Requirements

Basic knowledge of x86 assembly and Python

Basic knowledge of reverse engineering

Software Requirements

Ubuntu 64-bit

Hardware Requirements

Laptop