

**COURSE TITLE: BINARY DIFFERENCE ANALYSIS**

Course Instructor: Halvar Flake

Course Duration: 10 days

Minimum Class Size: 10

Course Fees: S\$10,000 per students

## Course Outline:

Day 1: Introduction to C/C++ auditing with auditing exercises

*3 hours of auditing a (public) piece of code with the goal of finding as many problems as possible. Subsequent discussion of the findings.*

Day 2: (Advanced) Introduction to IDA

Day 3: C/C++ programming structures in the binary, structures, classes, inheritance, method calls etc.

*For C, data structures, code constructs (loops, switches etc.). Exercises in manual decompilation of assembly code (e.g. manually creating C code from assembly).**For C++, classes and their reconstruction via constructors and vtables, inheritance, exceptions.*

Day 4: Auditing binaries efficiently to detect problems

Day 5: Auditing binaries efficiently to detect problems

Day 6: Review of the first 5 days, exercises, questions and answers

*Using IDC scripts to scan for problematic library functions, using an IDA plugin to scan for loops. Using BinNavi to visualize the program's callgraph and identify zones that can be interesting. Documenting progress. Lots of exercises on a commercial program.*

Day 7: Reverse engineering security patches using BinDiff

*Concepts and use of BinDiff, 3-5 Microsoft patches as exercise. The class will analyze the patches and explain what was changed.*

Day 8: Navigating through binaries using BinNavi

*Working on the dangerous locations identified on day 3/4, we will use BinNavi to construct input to lead to these locations.*

Day 9: Exercises

Day 10: Examinations

## About the Instructor:

HalVar Flake is a regular speaker at CanSecWest and Blackhat. A mathematical genius, he is currently pursuing his tertiary education in Germany, while at the same time, is the CEO of SABRE Security. Originating in the fields of copy protection and digital rights management, he gravitated more and more towards network security over time as he realized that constructive copy protection is more or less fighting windmills. After writing his first few exploits he was hooked and realized that reverse engineering experience is a very handy asset when dealing with COTS software. With extensive experience in reverse engineering, network security, penetration

testing and exploit development he is one of the world most sought after reverse engineer.

On the 27<sup>th</sup> of November 2006, SABRE Security was awarded the first prize in the IT Security Innovation Award for their automated malware classification project, [VxClass](#). The prize of 100.000 Euros is awarded every two years for new research in Cryptography and IT-Security and is one of Germany's largest privately funded research prizes. The second and third prizes were awarded to research teams from Siemens AG and Deutsche Telekom Laboratories.

## About COSEINC

COSEINC is a Singapore based and privately funded company dedicated to providing highly specialized information security services to our clients. We are a young and dynamic company whose constitution are computer security experts, from diverse backgrounds and geographies, with distinguished credentials and experience. The services we offer include research, penetration testing and training.

In July 2006, a senior researcher of COSEINC, Joanna Rutkowska, created a stir in the entire IT security industry when she presented on one of COSEINC's pet project "The Blue Pill" – an undetectable rootkit-malware". The patent for "The Blue Pill" is pending.

COSEINC is also the company that organizes "SyScan" – one of the most prominent "hacker" conference in Asia. SyScan is known for the high quality of its speakers and their content.