

T-110.6220: Malware Analysis and Antivirus Technologies

Antti Tikkanen, F-Secure Corporation

F-SECURE®



BE SURE.

Introduction

The course teaches students what malicious code is and how it can be detected and analyzed.

Topics of the course include

- Reverse engineering and debugging malware
- Unpacking and decrypting malware
- Windows with an antivirus perspective
- Antivirus engine basics
- Spyware and mobile malware

This course includes a homework project that requires programming skills

Course staff



Lecturer

- Antti Tikkanen, F-Secure Corporation

Assistant

- Laura Takkinen

Visiting lecturers from F-Secure

- Mikko Hyppönen
- Gergely Erdelyi (reverse engineering)
- Jarkko Turkulainen (unpacking)
- Jarno Niemelä (mobile)
- Stefan Lundström (spyware)

Course information



Lectures Wednesdays at 16-18 in lecture hall TU1 (TUAS building)

- A few exceptions, see the web page
- All lectures (as well as all other material) are in English

To pass this course, you must complete:

1. three homework rounds
2. the course project

Grade based on points from homeworks and project

Prerequisites

1. T-110.4100 Computer networks
2. T-106.1220 Data Structures and Algorithms
3. Basic understanding of Windows OS or other OS internals
(e.g. "T-106.5150 Operating Systems Project")
4. Computer architecture
(e.g. "S-87.3190 Computer Architecture")
5. C or Assembly programming skills

Course material



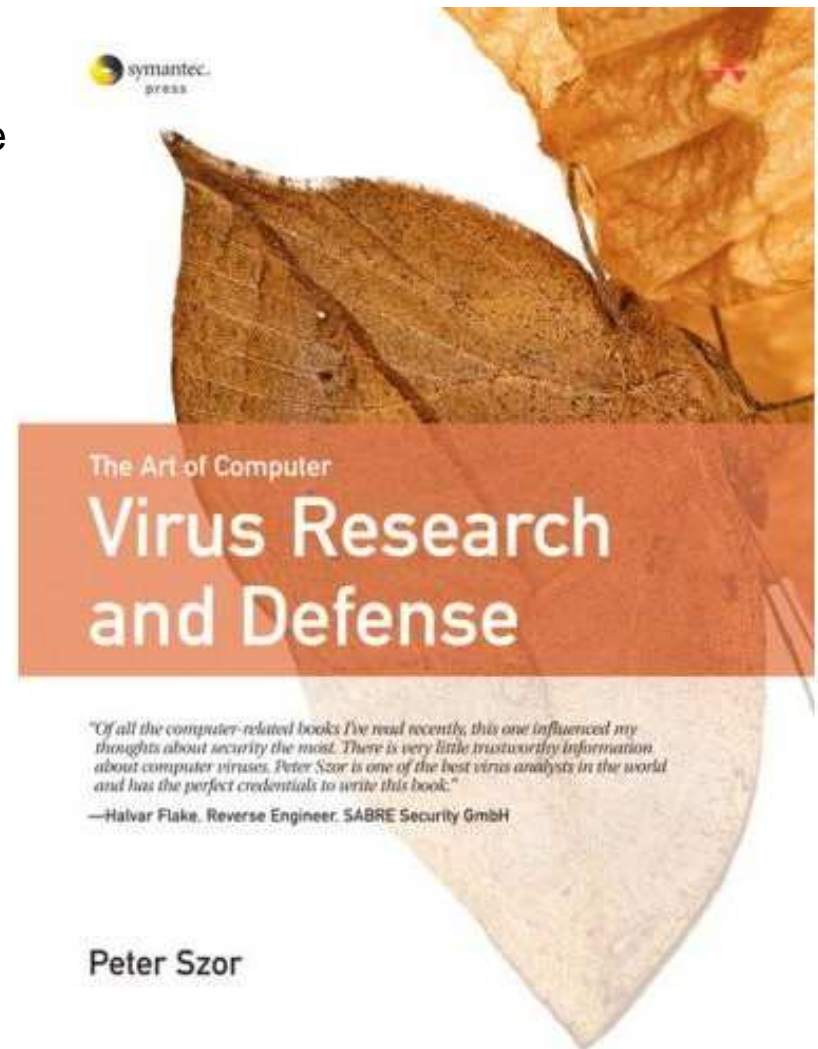
The Art of Computer Virus Research and Defense

Peter Szor (Author)

ISBN 978-0321304544,

Addison-Wesley Professional, 2005

We won't go through all of the book, but lecturers will refer to it quite often for additional information.



Course material (tools for homeworks)

IDA Pro 4.9 Disassembler and Debugger

- <http://www.hex-rays.com/idapro/idadownfreeware.htm>

OllyDbg 1.10 Debugger

- <http://www.ollydbg.de>

Debugging Tools for Windows

- <http://www.microsoft.com/whdc/devtools/debugging/default.msp>

You can freely install these to your own machines as well!

Contact information

Course web page:

- <http://www.tml.tkk.fi/Opinnot/T-110.6220/>

Mailing list

- T-110.6220@tml.hut.fi (both lecturer and assistant)

Signing up



By e-mail, see instructions here:

- http://www.tml.tkk.fi/Opinnot/T-110.6220/2008/sign_up.html

We can only accept 40 students

- If needed, we'll prioritize based on completed pre-requirement courses and your study programme

Deadline for sign up is Sunday 20th January at midnight!

More about course content

We have three important themes:

- 1. Reverse engineering (RE).** The process of discovering the technological principles of a device, object or system through analysis of its structure, function and operation (Wikipedia).
- 2. Windows.** To understand the sample you are reversing, you need to understand the environment (the OS) at a low level.
- 3. Antivirus technologies.** We focus on the classical part of client side technology, the file scanning engine.

Homeworks



The course includes three individual homework assignments

1. Reverse engineering with IDA Pro
2. Debugging with OllyDbg/WinDbg
3. Malware taxonomy and malware in 2008

We will have a lab session to introduce the tools (TBA)

- Not mandatory, but very warmly recommended to pass the homework

Detailed descriptions published later

You will not be handling real malware!

Course project

Topic: Designing and implementing an antivirus engine

- Details given on the lecture of Wednesday 9th April

Submission will include

1. Source code of the engine
(we like C/C++, but you can go for Java or Python as well)
2. A short whitepaper explaining the solution
3. A demo session

This is also an individual assignment

Fighting Online Crime



F-Secure's CRO Mikko Hyppönen gives our first real lecture

Fighting Online Crime

- Who is the enemy? Where is he from?
- How money is being made with malware
- How modern antivirus labs work
- Where do we find the new samples
- How do we analyse them
- How to locate the criminals

Tuesday 22nd January in T1, 16-18

Questions?

