硕士学位论文
Dissertation for Master's Degree
(工程硕士)
(Master of Engineering)

恶意代码行为提取及分类系统
MALICIOUS CODE BEHAVIOR EXTRACTION AND CLASSIFICATION SYSTEM

王维

国内图书分类号：TP311　　学校代码：10213
国际图书分类号：681　　密级：公开

工程硕士学位论文
Dissertation for the Master's Degree in Engineering
(工程硕士)
(Master of Engineering)

恶意代码行为提取及分类系统
MALICIOUS CODE BEHAVIOR EXTRACTION AND CLASSIFICATION SYSTEM

Candidate：Your Name
Supervisor：HIT Supervisor's Name and Title
Associate Supervisor: LiU Supervisor's Name and Title
Industrial Supervisor: Internship Supervisor's Name and Title
Academic Degree Applied for：Master of Engineering
Speciality：Software Engineering
Affiliation：School of Software
Date of Defence：September, 2014
Degree-Conferring-Institution：Harbin Institute of Technology

Abstract

近年来，随着互联网技术的兴起，恶意代码也随之泛滥成灾，使企业或个人的计算机安全受到严重威胁，窃密、盗号、网络欺诈事件频频发生，经济利益受到严重损失。面对每日捕获到如此庞大的恶意代码样本，如何进行有效的判定、分类和评估，成为反病毒厂商长期探索的方向，也是目前技术研究的热点。[This is only a paragraph of Example,]

关键词：关键词 1，关键词 2，关键词 3，关键词 4，关键词 5

In recent years, with the rise of Internet technology, malicious code number also be flooded, so that enterprises or individuals under serious threat of computer security, theft, hacking, phishing frequent occurrence of serious loss of economic interests. Captured the so such a huge of malicious code samples in one day, how to effectively determine, classification and evaluation it, as anti-virus vendors to explore the long-term direction of technology. [This is only a paragraph of Example]

Keywords: Keyword1; Keyword2; Keyword3; Keyword4; Keyword5

Contents

摘要 **i**

Abstract **i**

Contents **iii**

1 Introduction **1**
1.1 Motivation 1
1.2 Aim 1
1.3 Research questions 1
1.4 Delimitations 2

Chapter 1

Introduction

The introduction shall be divided into these sections:

1.1 Motivation

This is where the studied problem is described from a general point of view and put in a context which makes it clear that it is interesting and well worth studying. The aim is to make the reader interested in the work and create an urge to continue reading.

1.2 Aim

What is the underlying purpose of the thesis project?

1.3 Research questions

This is where the research questions are described. Formulate these as explicit questions, terminated with a question mark. A report will usually contain several different research questions that are somehow thematically connected. There are usually 2-4 questions in total.

Examples of common types of research questions (simplified and generalized):

1. How does technique X affect the possibility of achieving the effect Y?
2. How can a system (or a solution) for X be realized so that the effect Y is achieved?
3. What are the alternatives to achieving X, and which alternative gives the best effect considering Y and Z? (This research question is normally broken down in to 2 separate questions.)

Observe that a very specific research question almost always leads to a better thesis report than a general research question (it is simply much more difficult to make something good from a general research question.)

The best way to achieve a really good and specific research question is to conduct a thorough literature review and get familiarized with related research and practice. This leads to ideas and terminology which allows one to express oneself with precision and also have something valuable to say in the discussion chapter. And once a detailed

research question has been specified, it is much easier to establish a suitable method and thus carry out the actual thesis work much faster than when starting with a fairly general research question. In the end, it usually pays off to spend some extra time in the beginning working on the literature review. The thesis supervisor can be of assistance in deciding when the research question is sufficiently specific and well-grounded in related research.

1.4 Delimitations

This is where the main delimitations are described. For example, this could be that one has focused the study on a specific application domain or target user group. In the normal case, the delimitations need not be justified.