一种基于系统管理模式的隐藏进程检测模型

赵晓参 1，任　炬 1，徐　旸 1，王国军 2
（1 中南大学 信息科学与工程学院，湖南 长沙 410083；2 广州大学 计算机科学与教育软件学院，广东 广州 510006）

摘　要：近年来，恶意程序的隐身性越来越强.针对这个问题，提出了一种基于系统管理模式（System Management Mode, SMM）的隐藏进程检测模型（SMM-based Hidden process Detection model, SHPD）.该模型能够有效地检测系统中的隐藏恶意进程，同时保证自身的透明性.模型包括客户端和监控端两部分.客户端运行在 BIOS 中，利用内外语义信息建立操作系统进程的多个视图，将建立的视图发送到监控端.监控端通过对比视图间的差异，识别出隐藏的恶意进程.在提出的 SHPD 模型理论支持下，搭建了实验原型系统，并进行了功能测试和分析，实验结果证明了该模型的有效性.

关键词：系统管理模式；恶意程序；隐藏性；视图对比

A Hidden Process Detection Model Based on System Management Mode

ZHAO Xiao-can 1, REN Ju 1, XU Yang 1, WANG Guo-jun 2
(1 College of Information Science and Engineering，Central South University, Changsha 410083,China; 2 College of Computer Science and Educational Software, Guangzhou University, Guangzhou 510006, China)

Abstract：In recent years, the stealth of malware is getting stronger and stronger. In this paper, a SMM-based Hidden process Detection model (SHPD) is proposed. SHPD can effectively detect the stealthy process in system while ensuring its own transparency. SHPD consists of two parts: the client and the monitor. The client, which implemented in BIOS, uses both internal and external semantic information to establish multiple views of processes in OS and sends those process views to the monitor. The monitor identifies the stealthy process by comparing the differences between the views. In the paper, we build a prototype system under the support of the SHPD theory, and conduct functional testing and analysis. The experimental results verify the feasibility of SHPD.

Key words：SMM; malware; stealthy; view comparison

作者简介：
赵晓参　男，（1990-），硕士研究生.研究方向为访问控制、信息安全.E-mail:992536614@qq.com.
任　炬　男，（1987-），博士，特聘教授.研究方向为无限传感器网络.
徐　旸　男，（1988-），博士研究生.研究方向为信息安全.
王国军　男，（1970-），博士，教授.研究方向为可信计算、隐私保护.