基于免疫原理的恶意软件检测模型

http://www.firstlight.cn 2010-06-01

针对恶意软件检测尤其是未知恶意软件检测的不足，提出一种基于免疫原理的恶意软件检测模型，该模型采用程序运行时产生的IRP请求序列作为抗原，定义系统中的正常程序为自体，恶意程序为非自体，通过选定数量的抗体，采用人工免疫原理对非自体进行识别。实验结果表明，此模型在恶意软件的检测方面具有较高的准确率，且误报和漏报率较低，是一种有效的恶意软件检测方法。

存档文本