开题报告

题目：计算机免疫抗原提呈模型及其在Web应用软件衰退检测中的应用

梁意文老师的问题及回答：

1.间谍软件与其它恶意软件的不同在哪里？

答：与病毒和蠕虫等恶意软件相比，间谍软件最大的不同在于它不具有被禁止的行为，如病毒的感染可执行文件或蠕虫的大量自我复制阻塞网络。单独看间谍软件的每种行为都很正常，如显示消息、监视浏览器地址栏或对修改浏览器主页，但这些行为组合起来却会泄露用户的隐私。

2.为什么你会想到使用诱导的方法？怎么诱导？

答：间谍软件的行为具有很强的隐蔽性。这不仅表现在其不具有被禁止的行为，使得通常的基于特征码的检测方法无所适从，还表现在部分间谍软件会将恶意活动隐藏在用户的活动中，使得基于行为的检测方法有时也很难发现这种隐蔽的间谍软件。因此，本文考虑通过模拟用户活动的方法，欺骗间谍软件，并引诱间谍软件实施窃取并处理这些活动的行为。这样间谍软件的行为会更明显，也更有利于间谍软件的检测。

3.哪些案例可以有效地证明你的论文的思想？

答：浏览器插件形式的间谍软件、键盘记录程序都是典型的间谍软件，也是目前研究的比较多的2种间谍软件。这两种间谍软件都具有较强的隐蔽性，可以用于作为本文的实验案例，说明论文的思想。

董红斌老师的问题及回答：

1.你大概会监测间谍软件的哪些行为？它们的关联指什么？

答：从大的类别来说，主要检测间谍软件的两类行为：收集用户的隐私信息行为以及泄露这些信息的行为。收集用户的隐私信息行为又包括跟踪用户的按键、鼠标点击、浏览过的网页地址及网页内容等；泄露隐私信息的行为包括保存文件、网络发送等。它们的关联主要指时间上的关联，即若一个进程短时间内同时产生这两种行为，则该进程为间谍软件进程的概率就很高。

2.行为指标和状态指标是分开考虑的吗？

答：是分开考虑的。行为指标主要以API调用（或系统调用）为主要载体，反映行为本身的“结构”特点。状态指标主要以系统资源使用为主要载体，反映行为发生的环境，或行为对系统资源使用造成的影响，即行为的上下文。结合上下文可以降低行为检测方法的伪肯定率。这在间谍软件检测当中是至关重要的。

3.如何说明你的模型的有效性？

答：初步考虑应与现有的间谍软件的检测方法进行对比，从正确肯定率和错误肯定率两个指标，说明本文提出的基于计算机免疫学的检测方法的有效性。

谭成予老师的问题及回答：

1.你的方法和其他人将危险理论用于恶意软件检测相比，有那些不同和改进之处？

答：现有的基于危险理论的方法主要用于检测僵尸程序。其具体方法是根据僵尸程序的行为特点，定义相应的信号，并对信号进行关联以检测僵尸程序。这种方法的一个弊端就是人为的因素较多，如人工定义信号、设置信号的阈值等。本文的方法试图用变化的方法统一描述信号，使得检测系统在运行时动态地选择有效的信号，提高系统的自适应性和智能性。此外，本文提出了诱导因子的概念，可以提高抗原的免疫原性，增强本文提出的危险理论模型的检测效果。

2.诱导因子是特异性的吗？如果是，请问检测中如何确定使用哪种诱导因子？

答：诱导因子是具有特异性的。主要根据系统中正在发生的行为去选择释放何种诱导因子。关于诱导因子更详细的作用机理有待进一步的研究。

3.你的论文准备在计算机免疫模型方面如何创新？

答：本文提出的计算机免疫学模型的创新点主要如下：首先，提出了抗原模式的自适应生成方法，增强了危险理论的自适应性；其次，提出了抗原提呈的方法，为适应性免疫系统和先天免疫系统的结合提供了必要的依据；再次，提出了诱导因子的方法，可以增强抗原的免疫原性，提高危险理论模型的检测效果，使得该模型尤其适合检测潜伏深的恶意软件（如间谍软件）的检测。