第1章作业

姓名：袁昊男 学号：2018091618008

1、什么是软件缺陷和软件漏洞？软件缺陷和软件漏洞有何区别？软件漏洞是否有可能转变为软件后门，为什么？

**答：**软件缺陷指计算机软件或程序中存在的某种破坏正常运行能力的问题、错误、或者隐藏的功能缺陷；软件漏洞指在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而使攻击者能够在未授权的情况下访问或破坏系统。

它们的区别是软件缺陷是指软件自身会出现错误；软件漏洞则需要在攻击者利用漏洞对软件程序攻击后才会产生故障、错误。软件漏洞的范围更小，软件缺陷范围更大。

软件后门意思是在软件中植入病毒等具有后门功能的代码，通过运行软件来对用户的系统造成破坏、窃取机密等。软件漏洞极有可能转变为软件后门，因为攻击者可以利用软件漏洞，利用其程序实现或安全策略上的缺陷在未授权的情况下获得软件系统的控制权，从而植入具有后门功能的病毒代码。

2、什么是沙箱与虚拟机？其在安全领域有哪些具体应用？

答：沙箱是指是一个虚拟系统程序，允许你在沙盘环境中运行浏览器或其他程序，因此运行所产生的变化可以随后删除。它创造了一个类似沙盒的独立作业环境，在其内部运行的程序并不能对硬盘产生永久性的影响。在网络安全中，沙箱指在隔离环境中，用以测试不受信任的文件或应用程序等行为的工具。虚拟机是指通过软件模拟的具有完整硬件系统功能的、运行在一个完全隔离环境中的完整计算机系统。在实体计算机中能够完成的工作在虚拟机中都能够实现。在计算机中创建虚拟机时，需要将实体机的部分硬盘和内存容量作为虚拟机的硬盘和内存容量。每个虚拟机都有独立的CMOS、硬盘和操作系统，可以像使用实体机一样对虚拟机进行操作。它们的区别是，沙箱是在计算机系统中隔离出一块区域用于目标程序的执行，其执行结果不影响此区域外的任何文件；而虚拟机则是在宿主机中划分一块内存用以安装一台真实存在的计算机及系统。

沙箱及虚拟机在安全领域可用来分析病毒程序样本、实验编制的病毒程序并跟踪其感染过程、对疑似病毒程序进行取证、作为靶机实验网络攻击过程等。

3、请选择一个安全公司的历年安全报告进行仔细阅读，请从近10年以来互联网软件安全发展趋势进行分析，给出一个简要对比分析，要求至少说明软件安全发展特点和趋势。（选做）

答：为了更好地推动软件安全的发展，参考新思科技软件质量与安全部门（Synopsys SoftwareIntegrity Group）对于软件安全发展及特点的预测。这些预测将有助于企业保持警惕，最大限度地减少软件安全风险。

(1) 设计和标准的安全性。

大部分软件仍然是在没有正式标准和流程的情况下编写的。与构建桥梁不同，软件开发并不是标准化、可重复的工作。开源持续了很长时间，现在已经司空见惯。可以想象，更多的信任将放在基于开源软件的通用构建模块中。此外，垂直领域软件开发标准将更快出现。尤其当波音公司客机连续因软件缺陷导致坠机事故时，更多的努力将放在标准、可审计性和问责制上。这些标准可能是自下而上的，也可能是由政府监管的。金融服务、区块链以及移动解决方案安全性等领域也有机会执行这样的标准。未来我们可能看到垂直市场组成联盟，以建立更多面向特定领域的安全标准，并改善信任和互换性。其中大部分可以基于开源组件构建。

(2) 继续向云迁移。

随着经济的增长，各大企业也面临着新的竞争压力。这迫使企业需要重新武装自己。数字化如火如荼，新的云环境也正在改变企业部署APP的方式。因此，企业需要在APP应用和软件安全方面保持警惕。预计将会有更多投资会放在云端安全上。此外，给员工普及应用安全和软件安全的概念以及这方面的培训需求也会越来越多。

(3) IoT攻击仍然是一个困扰。

在亚太地区，许多国家正在推进智慧城市和智能国家计划。这也为新一轮的IoT网络攻击提供了机会。不法分子可以利用数据中毒进行攻击，其中的错误信息将通过部署在目标城市或全国范围内的传感器影响决策。一些旧问题仍然存在：硬编码凭证和未修补的组件，没有良好设计的空中下载技术更新以及持续更新策略。

(4) 对开发人员使用第三方应用程序编程接口（API）的敏感性提高。

它是绝大多数IT企业的盲点，类似于十年前的开源使用。大多数公司都了解确保他们发布的API免受外部攻击的重要性，但很少有公司会通过从内到外调用第三方API来跟踪他们自己的代码在Web服务的使用。依赖第三方服务的方式还存在其它法律和业务风险。公司还必须考虑到他们可能无意中传递到防火墙外的未知和不受信任来源的机密数据。