题 目：Linux 内核的漏洞态势感知与预测

学院：计算机与信息技术学院 专业：信息安全 学生姓名：陈力恒 学号：14281055

文献综述：

目前，国内外如 NVD 这样的漏洞库日益完善，关于软件漏洞态势的研究越来越多，旨在指导相关单位对相关漏洞进行修补并且在新一轮软件开发过程中尽量避免此类漏洞的出现，提高软件的质量。

基本的研究方法是针对漏洞数据库等数据源中的信息对漏洞信息统计、分析、汇总、制图并最终给相关人员提出具有指导意义的结果。

如今很少有研究者对漏洞信息的各个特征进行相关联性进行研究，并建立模型，因此本毕业设计旨在填补该空白。此外，目前尚未出现关于漏洞存在到被发现时间间隔这个因子的研究，本论文期望预测 Linux 内核关键漏洞的存在到被发现时间间隔以计算出 Linux 内核稳定化时长并确定哪些 Linux 内核是一定程度上稳定的，用于向基于 Linux 内核定制系统的人员提供稳定的 Linux 内核的版本参考，给定制系统提供一层内核级别的稳定性保障。

本毕业设计最终期望提供最新几年的漏洞趋势，建立包括漏洞存在到被发现时间间隔在内的漏洞特征的多因素模型，预测 Linux 内核的稳定化时长，并为未来更为深入的漏洞态势的研究提供基础。

研究方案：

研究方案步骤大致如下：

1. 通过 NVD 获取 Linux 内核的 CVE 信息，通过 GitHub 等获取 CVE 的发现修复时间、补丁代码，在 Linux Kernel 官网中下载 Linux 内核源代码；
2. 编写漏洞检测工具判断 CVE 所存在的那些 Linux 内核版本，利用 CVE 漏洞最早存在的版本计算漏洞最早存在的时间，然后计算得出漏洞最早存在到被发现的时间间隔；
3. 所需要的漏洞特征因子获取完毕，将漏洞特征因子用于神经网络的训练；
4. 根据漏洞危害程度、漏洞数量、关注程度等确定 Linux 内核的关键漏洞，并预测关键漏洞的最早存在到被发现的时间间隔；
5. 计算 Linux 内核稳定化时长。

主要参考文献：

- Kuhn D R, Raunak M S, Kacker R. An Analysis of Vulnerability Trends, 2008-2016[C]// IEEE International Conference on Software Quality, Reliability and Security Companion. IEEE, 2017:587-588.
- Slabý J, Strejček J, Trtík M. ClabureDB: Classified Bug-Reports Database Tool for Developers of Program Analysis Tools[J]. 2013.
- Lee S C, Davis L B. Learning from experience: operating system vulnerability trends[J]. It Professional, 2003, 5(1):17-24.
- Grieco G, Grinblat G L, Uzal L, et al. Toward Large-Scale Vulnerability Discovery using Machine Learning[C]// ACM Conference on Data and Application Security and Privacy. ACM, 2016:85-96.
- Abal, Iago, Brabrand, Claus, Wasowski, Andrzej. 42 variability bugs in the linux kernel: a qualitative analysis[J]. 2014.
- Woo M, Sang K C, Gottlieb S, et al. Scheduling black-box mutational fuzzing[C]// ACM Sigsac Conference on Computer & Communications Security. ACM, 2013:511-522.
- Homaei H, Shahriari H R. Seven Years of Software Vulnerabilities: The Ebb and Flow[J]. IEEE Security & Privacy, 2017, 15(1):58-65.
- Chang Y Y, Zavarsky P, Ruhl R, et al. Trend Analysis of the CVE for Software Vulnerability Management[C]// IEEE Third International Conference on Privacy, Security, Risk and Trust. IEEE, 2012:1290-1293.

- Kuhn R, Johnson C. Vulnerability Trends: Measuring Progress[J]. It Professional, 2009, 12(4):51-53.
- 何晶. 基于 WooYun 的视听新媒体网站漏洞统计分析[J]. 电视技术, 2014, 38(16):65-69.
- 佚名. 赛门铁克互联网安全威胁报告[J]. 软件和集成电路, 2003(6):64-64.
- Ullah N, Morisio M, Vetrò A. Selecting the Best Reliability Model to Predict Residual Defects in Open Source Software[J]. Computer, 2015, 48(6):50-58.
- Okamura H, Dohi T. Towards comprehensive software reliability evaluation in open source software[C]// IEEE, International Symposium on Software Reliability Engineering. IEEE Computer Society, 2015:121-129.
- Rahimi S, Zargham M. Vulnerability Scrying Method for Software Vulnerability Discovery Prediction Without a Vulnerability Database[J]. IEEE Transactions on Reliability, 2013, 62(2):395-407.

毕业设计（论文）进度安排：

序号	毕业设计（论文）各阶段内容	时间安排	备注
1	阅读漏洞态势感知与预测相关论文	第 1 周	
2	对 Linux 内核的漏洞、补丁的信息代码汇总	第 2 周	
3	对漏洞信息进行统计、分析	第 3-4 周	
4	对漏洞信息中的特征重点观察	第 5 周	
5	发掘漏洞特征之间的关联性	第 6 周	
6	建立漏洞特征模型	第 7-10 周	
7	后续的答辩展示等	第 10 周以后	

指导教师意见：

文献调研全面，计划可行，同意开题。

指导教师（审核签名）： _____ **审核日期：** 2018 年 3 月 5 日