附表四：

**北京工业大学**

毕业设计（论文）任务书

题目 基于SGX的端到端远程安全通信方法设计与实现

专业 学号 姓名

主要内容、基本要求、主要参考资料等：

主要内容

1、基于SGX的端到端远程安全通信方法设计

针对端到端远程通信的特点，分析在通信过程中存在的消息泄露、内存攻击等问题，提出基于SGX的端到端远程安全通信方法，包括：通信双方间的双向远程证明、通信密钥的协商以及结果的展示。

2、基于SGX的端到端远程安全通信方法实现

基于B/S模式实现基于SGX的端到端远程安全通信系统。

3、基于SGX的端到端远程安全通信系统测试

根据上述工作完成对基于SGX的端到端远程安全通信系统的功能性能测试。

基本要求

1、掌握与SGX技术相关的知识

2、熟悉Linux的使用

3、完成基于SGX技术的远程安全通信方法的设计、开发和测试，编写相关文档

主要参考资料

[1] Wang J, Hong Z, Zhang Y, et al. Enabling Security-enhanced Attestation With Intel SGX for Remote Terminal and IoT[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2017, PP(99):1-1.

[2] F. Schuster et al., "VC3: Trustworthy Data Analytics in the Cloud Using SGX," 2015 IEEE Symposium on Security and Privacy, San Jose, CA, 2015, pp. 38-54.doi: 10.1109/SP.2015.10

完成期限：2019.6

指导教师签章：

专业负责人签章

年 月 日

附表四：

**北京工业大学**

毕业设计（论文）任务书

题目 基于用户画像的学习行为分析

专业 学号 姓名

主要内容、基本要求、主要参考资料等：

主要内容

1、基于用户画像的学习行为分析方法设计

针对学生学习的行为特点，分析学生在学习过程中可能存在的不足，提出一种基于用户画像的学习行为分析方法，包括：基于用户画像的学习行为建模，学习行为数据处理、学习成绩预测以及相关结果的展示。

2、基于用户画像的学习行为分析方法实现

基于B/S模式实现基于用户画像的学习行为分析系统。

3、基于用户画像的学习行为分析方法系统测试

根据上述工作完成对基于用户画像的学习行为分析系统的功能性能测试。

基本要求

1、掌握与机器学习相关的知识

2、了解用户行为画像

3、完成基于用户画像的学习行为分析方法的设计、开发和测试，编写相关文档

主要参考资料

[1]李曼丽,徐舜平,孙梦嫽.MOOC学习者课程学习行为分析——以“电路原理”课程为例[J].开放教育研究,2015,21(02):63-69

[2] Sayandeep S , Dirmanto J , Sikhar P , et al. Automatic Characterization of Exploitable Faults: A Machine Learning Approach[J]. IEEE Transactions on Information Forensics and Security, 2018:1-1.

[3] J. Qiu et al.“Modeling and predicting learning behavior in MOOCs,” in Proc. 9th ACM Int. Conf. Web Search Data Mining, ACM, 2016, pp. 93–102.

完成期限：2019.6

指导教师签章：

专业负责人签章

年 月 日

**北京工业大学**

毕业设计（论文）任务书

题目 基于循环神经网络的恶意代码检测方法设计与实现

专业 学号 姓名

主要内容、基本要求、主要参考资料等：

主要内容

1、基于循环神经网络的恶意代码检测方法设计

针对现有代码检测方法难以识别未知恶意代码的问题，提出基于循环神经网络的恶意代码检测方法，包括：恶意代码行为API特征分析，恶意词向量算法，基于循环神经网络的恶意代码检测方法，以及结果展示。

2、基于循环神经网络的恶意代码检测方法实现

基于C/S模式实现基于循环神经网络的恶意代码检测系统。

3、基于循环神经网络的恶意代码检测系统测试

根据上述工作完成对基于循环神经网络的恶意代码检测系统的功能性能测试。

基本要求

1、熟悉Linux的使用，了解深度学习使用环境

2、了解恶意代码进行远程攻击时触发的API序列间的相关关系

3、完成基于循环神经网络的恶意代码检测方法的设计、开发和测试，编写相关文档

主要参考资料

[1] Kwon I, Im E G. Extracting the Representative API Call Patterns of Malware Families Using Recurrent Neural Network[C]// the International Conference. 2017:202-207..

[2]罗帆,王厚峰.结合RNN和CNN层次化网络的中文文本情感分类[J].北京大学学报(自然科学版),2018,54(03):459-465.

[3] Jinpei Y , Yong Q , Qifan R . Detecting Malware with an Ensemble Method Based on Deep Neural Network[J]. Security and Communication Networks, 2018, 2018:1-16.

完成期限：2019.6

指导教师签章：

专业负责人签章

**北京工业大学**

毕业设计（论文）任务书

题目 基于二进制动态翻译的ROP攻击检测方法研究与实现

专业 学号 姓名

主要内容、基本要求、主要参考资料等：

主要内容

1. ROP攻击及其变种攻击检测方法设计

通过对ROP攻击及其变种攻击的特点进行归纳总结，设计和实现一种基于二进制动态翻译的ROP攻击及其变种攻击的检测方法，利用二进制动态插桩框架PIN或其他工具实现ROP攻击的检测策略、JOP攻击的检测策略、return-into-libc攻击等的检测策略，及最终的攻击检测效果的实现，从而实现完整的ROP攻击及其变种攻击的检测过程。

1. ROP攻击检测方法实现

实现一个检测ROP攻击、JOP攻击及return-into-libc攻击的程序，能够检测出ROP攻击及其变种攻击，并发出相应的警告。

1. ROP攻击检测系统测试

根据上述工作完成基于B/S模式实现ROP攻击及其变种攻击检测方法的界面展示。

基本要求

1. 掌握ROP攻击原理，总结ROP攻击及其变种攻击的特点
2. 掌握二进制插桩框架PIN的使用
3. 完成ROP攻击检测方法的设计、实现和测试，编写相关文档

主要参考资料

[1] Si L., Yu J., Luo L., Ma J., Wu Q., Li S. (2016) ROP-Hunt: Detecting Return-Oriented Programming Attacks in Applications. In: Wang G., Ray I., Alcaraz Calero J., Thampi S. (eds) Security, Privacy, and Anonymity in Computation, Communication, and Storage. SpaCCS 2016. Lecture Notes in Computer Science, vol 10066. Springer, Cham

[2] Shacham H.The geometry of innocent flesh on the bone: return-into-libc without function calls (on the x86) [C] // proc of the 14th ACM Conf on Computer and Communications Security. New York: ACM,2007:552-561

完成期限：2019.6

指导教师签章：

专业负责人签章