



南開大學

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月異

汇编语言与逆向技术

课程介绍

王志

zwang@nankai.edu.cn

updated on 6th Sep. 2021

College of Cyber Science, Nankai University
2021/2022



允公允能 日新月异

汇编语言与逆向技术

- 学分：2.5
- 课程安排
 - 2021-2022学年 第一学期
 - 星期二 16:00-17:40 [1-17周]
 - 津南公教楼B区402





允公允能 日新月异

汇编语言与逆向技术

- 实验安排:

- 2021-2022学年 第一学期
- 星期二 18:30-20:10 [3-17周]
- 津南实验楼A区315、314



南开大学
Nankai University



允公允能 日新月异

汇编语言与逆向技术

- 授课教师：王志
 - 办公室：网安学院605
 - 邮箱：zwang@nankai.edu.cn



南开大学
Nankai University



允公允能 日新月异

课程教材和拓展阅读资料

- 逆向工程核心原理，【韩】李承远 著，武传海 译，人民邮电出版社；
- 加密与解密（第四版），段钢 编著，电子工业出版社；
- Intel汇编语言程序设计（第五版），Assembly Language for Intel-Based Computers（Fifth Edition），【美】Kip R. Irvine著，温玉杰、梅广宇、罗云彬等译，电子工业出版社；



南开大学
Nankai University



允公允能 日新月异

课程教材和拓展阅读资料

- **Practical Malware Analysis**, Michael Sikorski and Andrew Honig, No Starch Press;
- **Practical Reverse Engineering**, Bruce Dang, Alexandre Gazet and Elias Bachaalany, Wiley;
- **IDA Pro 权威指南（第二版）**，【美】Chris Eagle 著，石华耀、段桂菊译，人民邮电出版社
- **有趣的二进制**，【日】爱甲健二 著，周自恒 译，人民邮电出版社



南开大学
Nankai University



允公允能 日新月异

考试成绩

- 平时成绩 10%
 - 考勤、课上回答问题（雨课堂）
- 实验成绩 20%
 - 课后习题、实验报告（学堂在线）
- 期末考试 70%
 - 闭卷考试



南开大学
Nankai University



允公允能 日新月异

课程内容

- 汇编语言
 - Intel处理器 x86汇编、华为鲲鹏处理器 ARM汇编
- 逆向分析技术
 - 静态逆向分析
 - 动态逆向分析
- Windows内核
 - 可执行文件结构
 - 系统内核
- 软件保护



南开大学
Nankai University



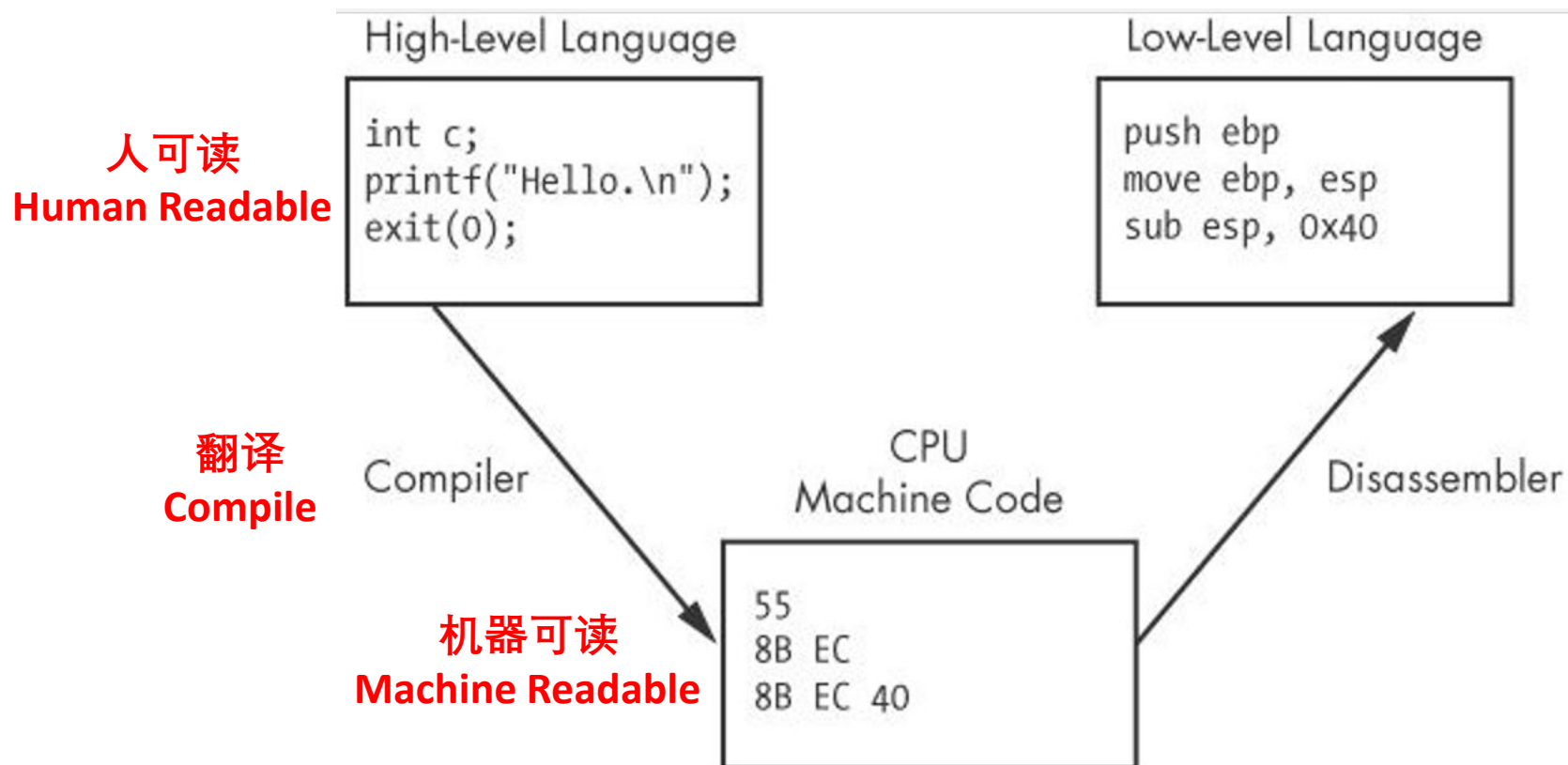
南开大学

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月异

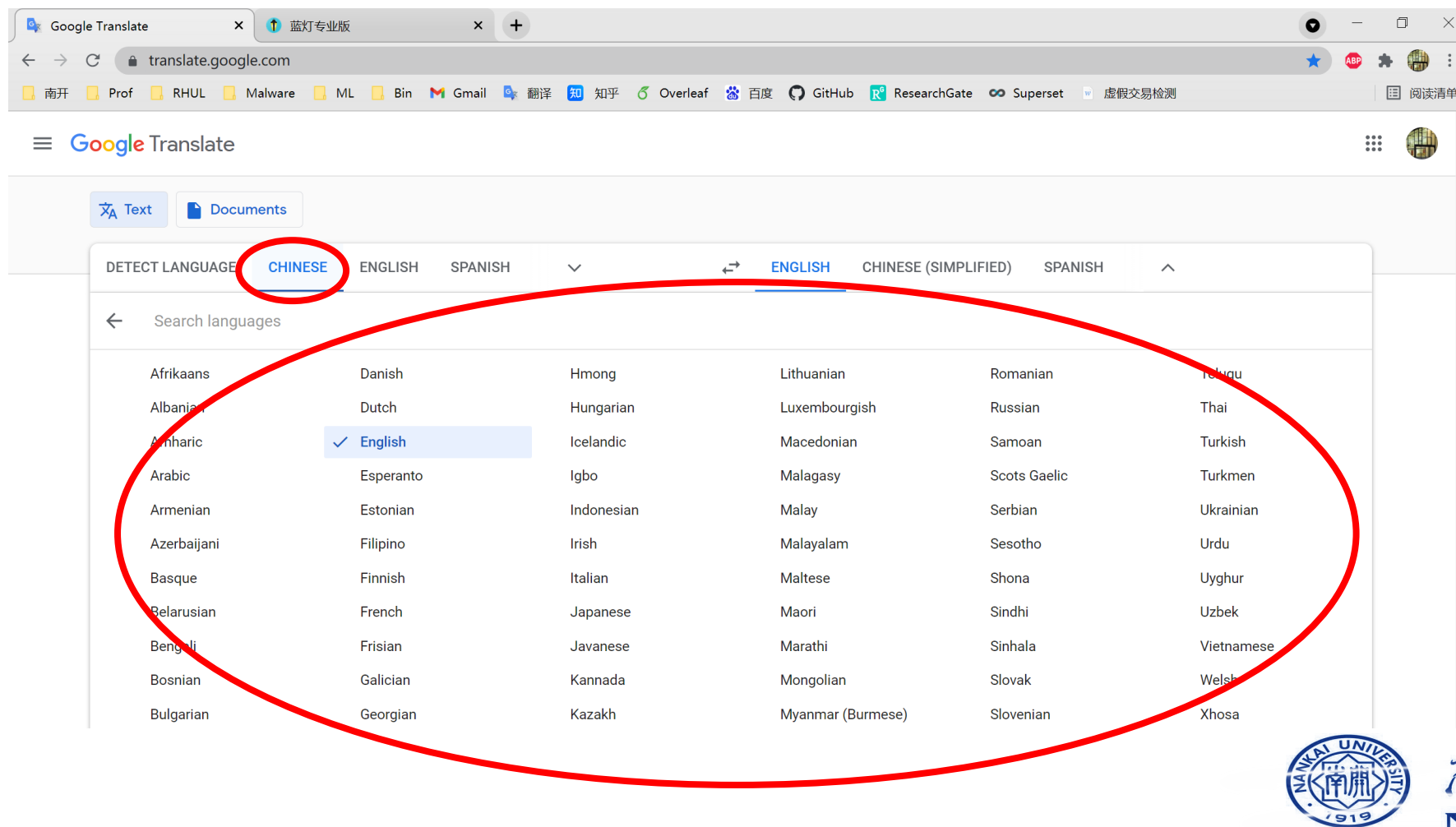
汇编语言

编译与反汇编



允公允能 日新月异

Google翻译



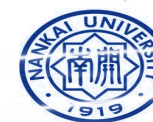
Google Translate

DETECT LANGUAGE **CHINESE** ENGLISH SPANISH

↔ ENGLISH CHINESE (SIMPLIFIED) SPANISH

Search languages

Afrikaans	Danish	Hmong	Lithuanian	Romanian	Telugu
Albanian	Dutch	Hungarian	Luxembourgish	Russian	Thai
Amharic	✓ English	Icelandic	Macedonian	Samoa	Turkish
Arabic	Esperanto	Igbo	Malagasy	Scots Gaelic	Turkmen
Armenian	Estonian	Indonesian	Malay	Serbian	Ukrainian
Azerbaijani	Filipino	Irish	Malayalam	Sesotho	Urdu
Basque	Finnish	Italian	Maltese	Shona	Uyghur
Belarusian	French	Japanese	Maori	Sindhi	Uzbek
Bengali	Frisian	Javanese	Marathi	Sinhala	Vietnamese
Bosnian	Galician	Kannada	Mongolian	Slovak	Welsh
Bulgarian	Georgian	Kazakh	Myanmar (Burmese)	Slovenian	Xhosa





允公允能 日新月异

百度翻译

百度翻译桌面端·全新上线！

轻·快的多语种翻译工具



快捷键
发起翻译

200
200+语种



极简模式



跨软件划词句



快捷键发起翻译



Nankai University



允公允能 日新月异

XcodeGhost的病毒

- Xcode 编译器是开发Mac OS 和iOS 应用程序的编译器
- Xcode编译器官方下载服务器在国外，中国下载速度非常慢
- 一些程序员为了方便，直接使用了国内下载工具下载
- 第三方的Xcode编译器有病毒，编译的时候把恶意代码输入到程序里面



南开大学
Nankai University



允公允能 日新月异

XcodeGhost的病毒

部分受病毒影响的 APP 及版本

相关 APP	版本
滴滴打车	3.9.7
同花顺	9.26.03
中国联通网上营业厅	3.2
中信银行动卡空间	3.3.12
微信 IOS	6.2.5
网易公开课	4.2.8
愤怒的小鸟 2	2.1.1
炒股公开课	3.10.02-3.10.01
股票雷达	5.6.1
南京银行	3.6-3.0.4
南方航空	2.6.5.0730-2.6.5





允公允能 日新月异

为什么学习汇编语言

- 学习汇编语言

- 需要了解**硬件**和**系统**的知识
- 可移植性差，不同的CPU使用不同的指令集
- 程序员很少直接使用汇编语言编程

- 学习英语

- 从小学或者幼儿园开始学习，直到大学的英语4、6级、托福、雅思
- 还是无法和法语、俄语、日语、韩语等等语言进行交流，可移植性差
- 平时很少用英语



南开大学
Nankai University



允公允能 日新月异

为什么要学习汇编语言

- 高速度、高效率
 - 程序优化、硬件操作（电影不用看字幕了）
- 程序的深入理解和分析
 - 计算机病毒分析、漏洞发掘
 - 软件盗版、破解、代码盗用



南开大学
Nankai University



允公允能 日新月异

为什么要学习汇编语言

- 软件**加固**（software hardening）
 - 水印、指纹、混淆、版权保护
- 软件自动**修复**（automated repair）
 - 软件补丁（patch），不用重新编译Windows系统
- 软件**插装**（instrumentation）
 - 虚拟化技术
- 软件**优化**（optimization）
- 软件**调试**（debugging）



南开大学
Nankai University



允公允能 日新月异

为什么学习汇编语言

- 汇编语言和逆向工程是**系统开发、系统安全**的基础课程
 - 系统内核开发、硬件驱动开发
 - 软件安全分析
 - 计算机病毒分析
 - 网络渗透与入侵检测
 - 漏洞分析



南开大学
Nankai University



什么是汇编语言 (Assembly Language)

- 汇编语言是所有程序设计语言中**最古老的语言**
 - 与机器语言最为接近
 - 可以直接访问硬件
 - 需要了解计算机体系结构和操作系统
- Assembly Language appeared in **1949** and soon saw wide use in Electronic Delay Storage Automatic Calculators.

BASIC, designed in 1964, was the first computer product ever made by Microsoft in its early years due to how powerful it was.

In addition to that, the 1970s saw the rise of several other languages:

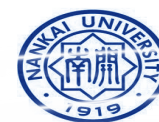
- **Smalltalk (1972)**, which introduced things that are still used today.
- **C (1972)** was the very first Unix to be used on a broad range of computers.
- **SQL (1972)** revolutionized database queries.
- **MATLAB (1978)** remains primarily used in research.



允公允能 日新月异

什么是汇编语言

- 汇编语言也称为符号语言
 - 用助记符代替机器指令的操作码
 - 机器指令 **55**，对应的汇编指令是push ebp
 - 用地址符号或标号代替指令或操作数的地址
 - 例如，将一个数据从内存读到CPU的寄存器中



汇编语言中有整数、浮点数、指针这些数据类型的吗？

正常使用主观题需2.0以上版本雨课堂

作答





允公允能 日新月异



南开大学
Nankai University



允公允能 日新月异

汇编语言

- CPU

- 寄存器
- 传送指令
- 算数指令
- 位运算指令
- 串操作指令
- 跳转指令

- 内存

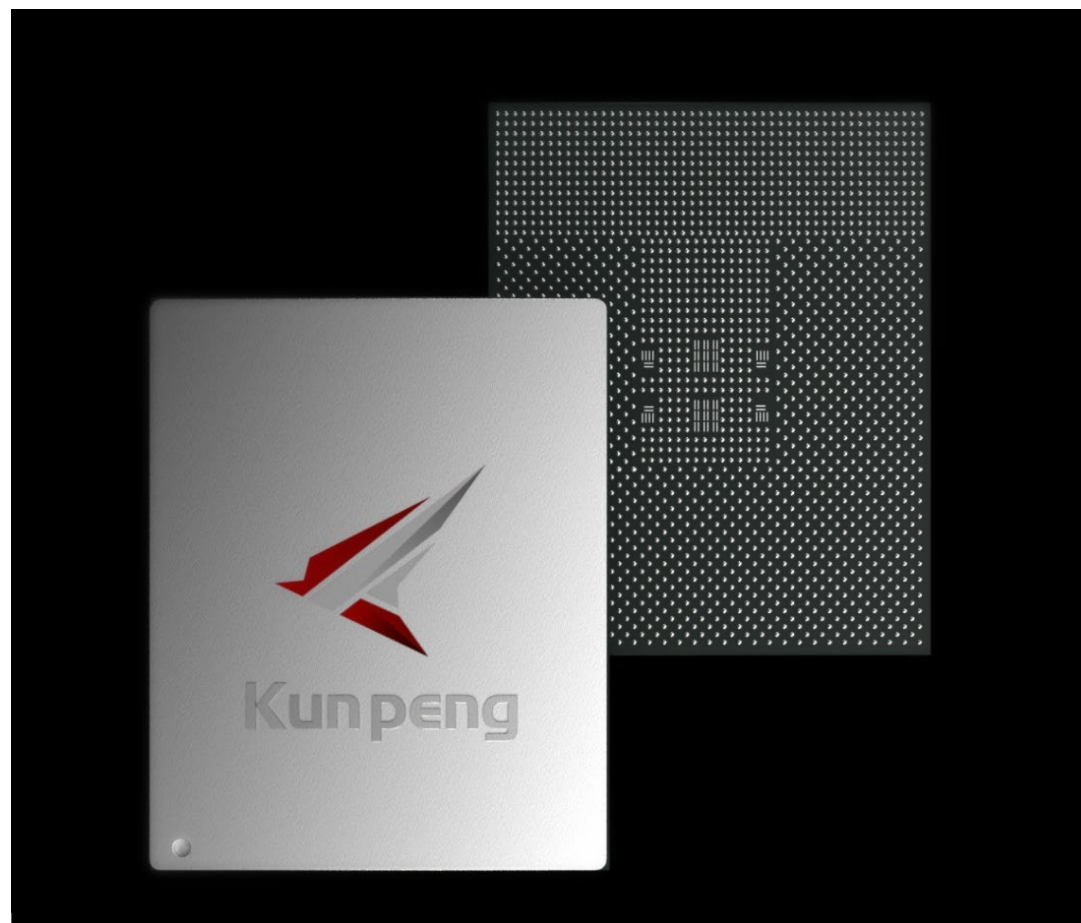
- 寻址方式



南开大学
Nankai University

基于**ARM**v8架构的**鲲鹏**处理器

- ARM寻址方式
- ARM指令集
- ARM伪指令
- ARM汇编语言程序结构
- ARM编译与调试工具





南开大学

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月异

逆向分析技术



允公允能 日新月异

逆向分析技术

- 动态逆向分析
 - OllyDbg: 用户态的动态调试
 - WinDbg: 内核态的动态调试
- 静态逆向分析
 - IDA Pro



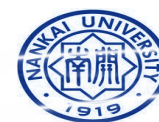
南开大学
Nankai University



允公允能 日新月异

用户态动态逆向分析

- 内存映射
- 查看线程、栈、代码
- 断点
- 加载DLL、跟踪
- 异常处理、修补
- 分析shellcode
- 插件、脚本调试

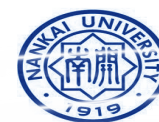




允公允能 日新月异

内核态动态逆向分析

- WinDbg
 - 驱动与内核代码
 - 双系统
 - 微软符号表
 - 内核调试
 - Rootkit





允公允能 日新月异

静态逆向分析

- 识别汇编中的C语言代码结构
- 识别if分支结构
- 识别循环
- 识别函数调用
- 识别switch结构美化
- 识别数组、结构体、链表



南开大学
Nankai University



南开大学

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月异



Windows内核



允公允能 日新月异

Windows内核

- 可执行文件结构
 - PE文件结构
- Windows内核
 - Windows内核基础
 - 异常处理

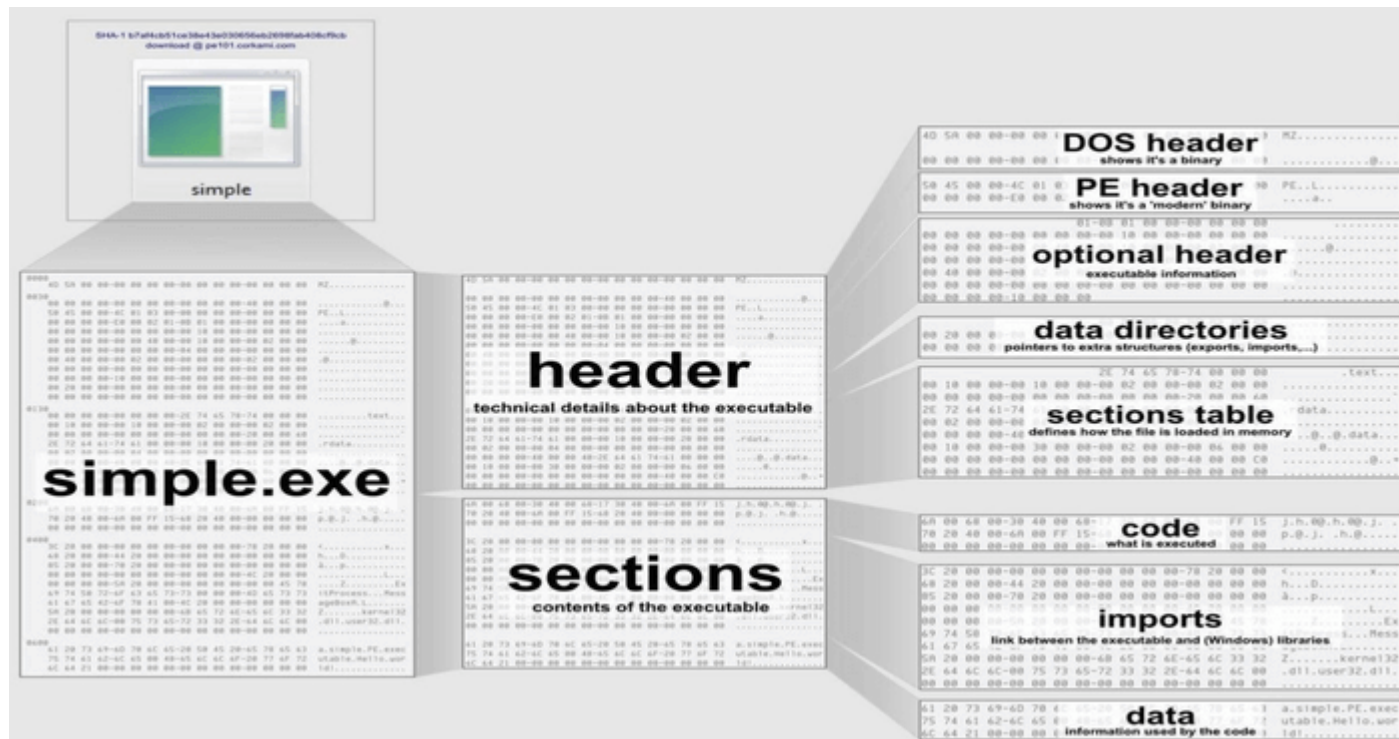


南开大学
Nankai University



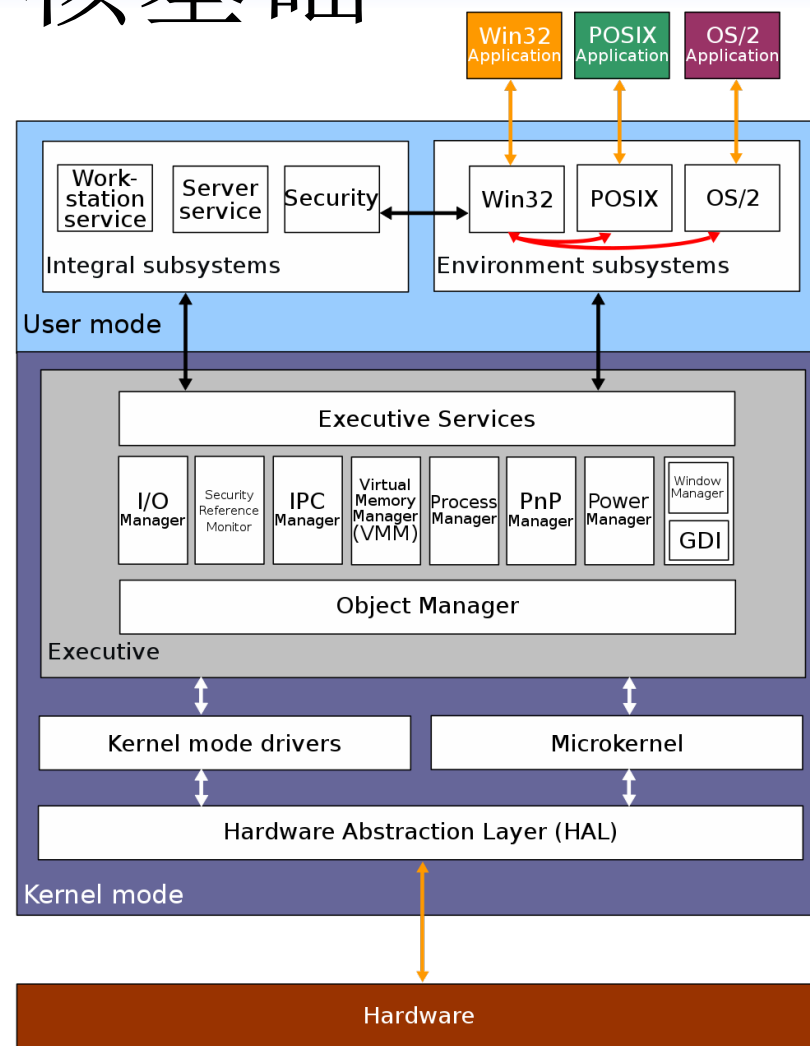
PE文件结构

- PE文件头
- 区块
- 输入表
- 输出表
- 基址重定位
- 资源
- TLS初始化、调试目录、延迟载入



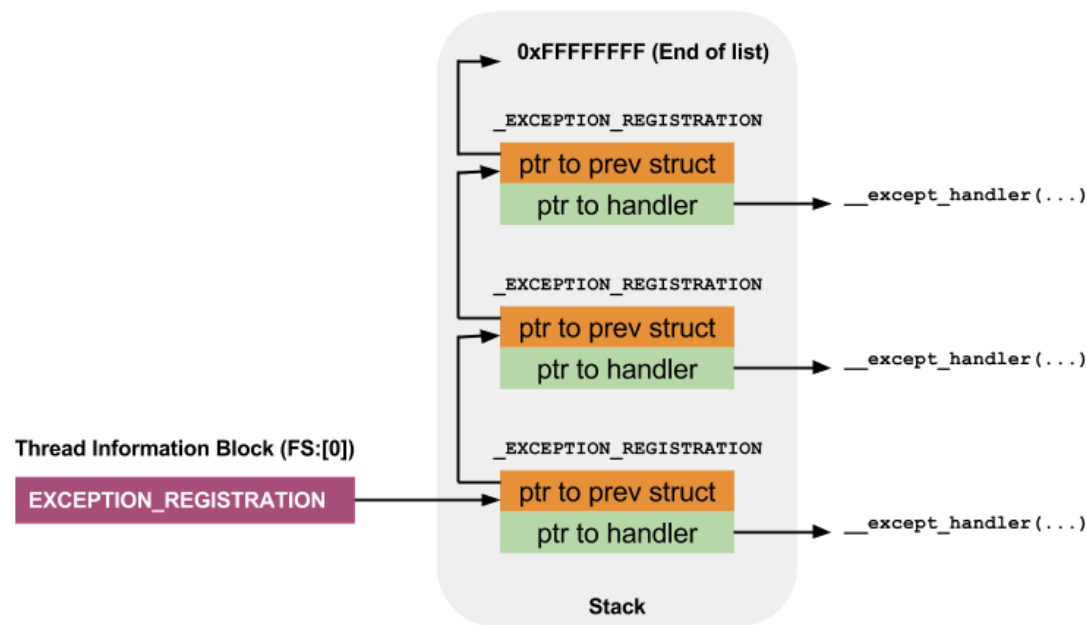
Windows内核基础

- 内存空间、权限空间布局
- Windows与内核启动过程
- Windows R3与R0通信
- 内核函数和内核驱动模块
- 内核对象
- SSDT
- TEB和PEB



Windows异常处理

- 异常处理的基本概念
- SEH的概念及基本知识
- SEH异常处理程序原理及设计
- 向量化异常处理





南開大學

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月異

软件保护



允公允能 日新月异

软件保护

- 序列号保护方式
- 警告窗口
- 时间限制
- 菜单功能限制
- KeyFile保护
- 网络验证
- 光盘检测



南开大学
Nankai University



南开大学

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月异

学习建议



允公允能 日新月异

永远保持好奇心，崇尚自由

- 永远保持好奇心，崇尚自由——既能促使探索，也能抵抗商业利益和欲望的侵袭。
- 有了好奇心，枯燥的代码世界才有了生气。



南开大学
Nankai University



允公允能 日新月异

勤奋与毅力

•“让我们搞清楚作为一名逆向工作者需要具备的基本条件，其实那并不是扎实的汇编功底和编程基础——可以完全不懂这些，秘诀就是**勤奋加上执着**！记住并做到这两点，你一样可以变得优秀。”



南开大学
Nankai University



允公允能 日新月异

扎实的**基本功**

- 精通至少一门编程语言—不仅是代码，更重要的是**编程思想**。
- 扎实的**汇编**功底和**系统**编程知识。



南开大学
Nankai University



南开大学

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月异



汇编语言与逆向技术

课程介绍

王志

zwang@nankai.edu.cn

updated on 6th Sep 2021

College of Cyber Science, Nankai University
2021/2022