中国科学院大学网络空间安全学院核心专业课

软件安全原理

Principle of Software Security

授课教师：邹维、陈恺、贾晓启、霍玮

助　　教：肖扬

2020-21学年秋季学期

中国科学院大学网络空间安全学院专业核心课

软件安全原理

Principle of Software Security

[第1章] 从安全视角认识软件

授课教师：邹维

授课时间：2020-09-15 (第1次课)

[第1章] 从安全视角认识软件

内容大纲

1.1 课程简介

1.2 软件在现代文明中的地位

1.3 软件发展历程

1.4 软件的概念与类型

1.5 软件存在的问题

1.6 课程安排

《软件安全原理》课程大纲

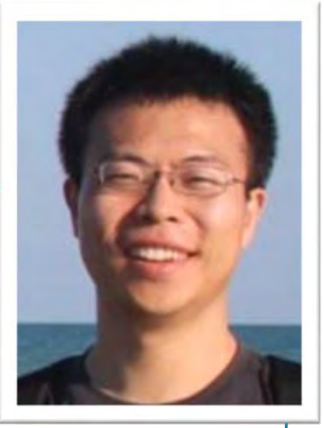
课程类型	网络空间安全学科研究生的**专业核心课**。
课程内容	讲授软件安全威胁与防御的基本原理，并结合操作系统、B/S架构支撑软件、移动终端软件等三类重要软件，讲解在软件技术发展过程中安全威胁与防御机制的**博弈演进**。另外，还介绍确保软件安全的工程化方法。
课程目的	让同学通过课程学习与动手实践 ① 从安全视角重新认识软件 ② 掌握围绕软件攻防的“**白帽**”与“**黑帽**”方法 ③ 理解软件的**安全内构**(building security in)方法 为进一步研习系统安全与网络攻防奠定基础。
参考书目	以Bruce Schneier、Gary McGraw 等国际知名学者的著作为主要参考书。

《软件安全原理》授课团队

邹维 主讲教授

- 中科院大学网络空间安全学院教授、副院长/教学委员会主任，中科院信工所研究员/博导、副所长、中科院网络评测技术重点实验室主任。
- 网络安全优秀人才奖获得者，中国计算机学会/北京大学优秀博士论文指导教师，信息安全国际顶级会议S&P 2013年程序委员会委员。
- 研究方向：网络与软件安全。

《软件安全原理》授课团队



陈恺 讲授教师

- 中科院大学网络空间安全学院教授，中科院信工所研究员/博导，信息安全国家重点实验室副主任。
- 中国保密协会隐私保护专业委员会委员，中科院青年创新促进会会员，美国宾州州立大学博士后。
- 研究方向：软件安全、智能终端安全、安全测评和隐私保护。
- 学术论文：IEEE S&P、USENIX Security、ACM CCS、ICSE、ASE、IEEE TR等发表论文50余篇。
- 主持或参与国家自然科学基金、863计划、中科院战略性先导科技专项等课题30余项。TDSC、TIFS、Computers & Security等SCI期刊评审专家，AsiaCCS、SecureComm等多个国际会议委员会成员。
- 主页：http://www.kaichen.org

《软件安全原理》授课团队

贾晓启 讲授教师

- 中科院大学网络空间安全学院教授，中科院信工所研究员/博导、第六研究室系统安全测评研究群组负责人。
- 中央国家机关青联委员，中科院青联委员，中国保密协会隐私保护委员会委员。
- 研究领域是攻防技术、操作系统安全和云计算安全。
- 在IEEE TIFS、TIFS、TSE、SCN、ICSE、ACSAC等重要国际会议和期刊上发表论文30余篇，并担任多项IEEE国际会议程序委员会委员和国际期刊审稿人。主持多个重要项目，包括国家重点研发计划课题、核高基项目子课题、国家自然科学基金课题等。

《软件安全原理》授课团队

霍玮 讲授教师

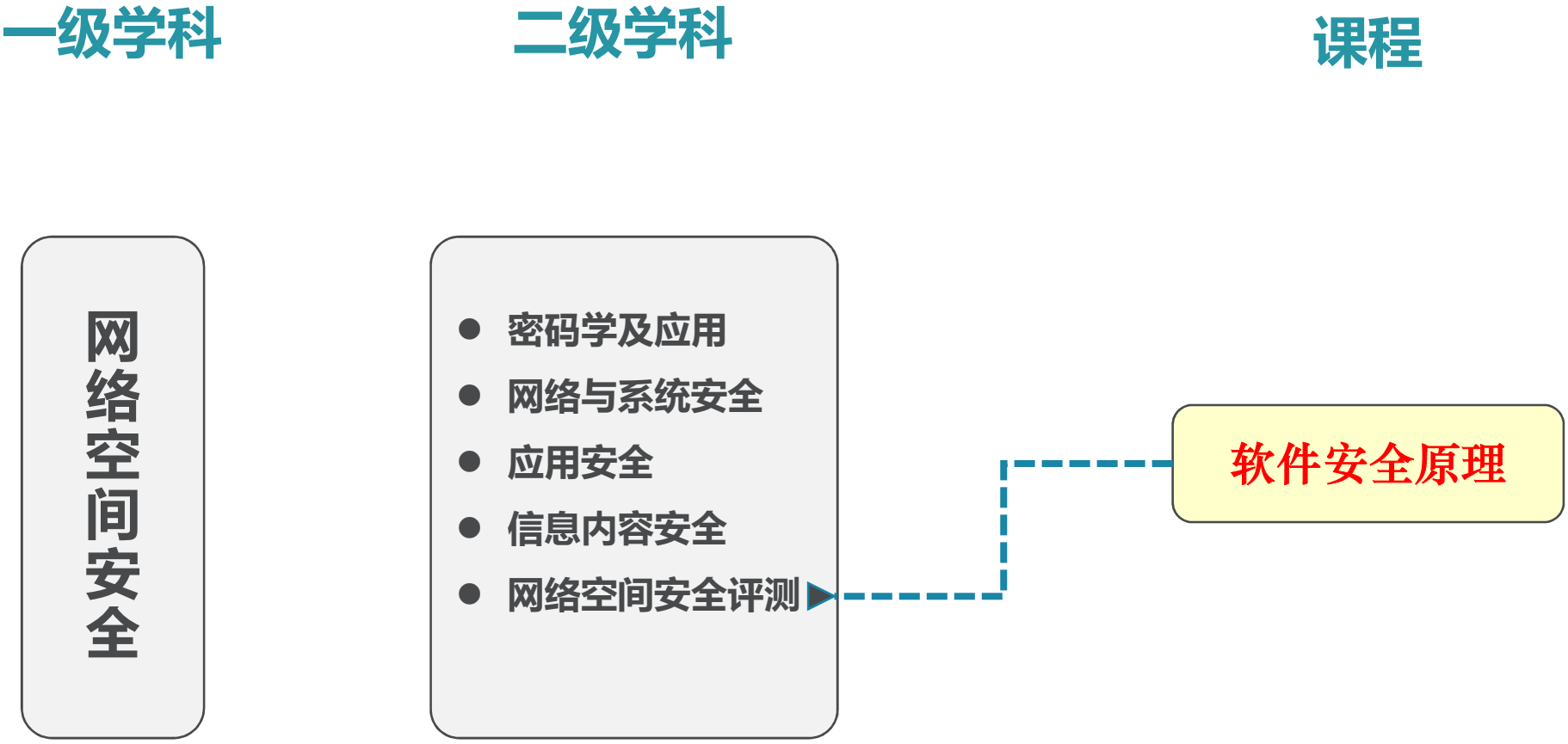
- 中国科学院信息工程研究所副研究员/博导、第六研究室软件安全分析研究群组负责人。
- 中国科学院青年创新促进会委员，信工所优秀引进人才。
- 研究领域包括软件漏洞挖掘和安全评测、基于大数据的软件安全分析、智能终端系统及应用安全分析等。
- 主持和参与项目10余项，包括主持国家级项目2项，省部级项目和横向合作项目多项。在国内外高水平会议和刊物上发表学术论文20余篇。

《软件安全原理》授课团队

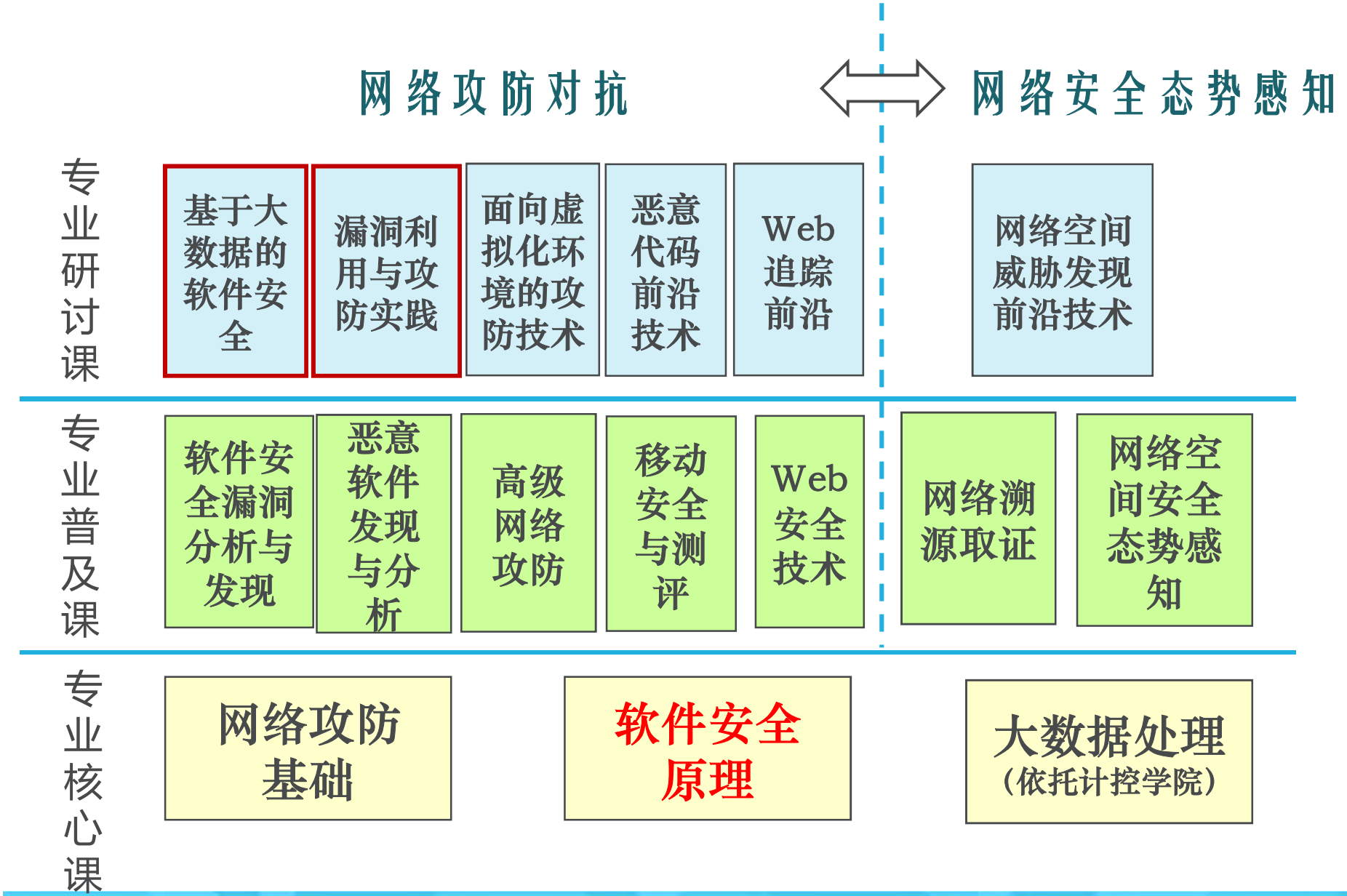
肖扬 助教

- 直博研究生，本科毕业于中山大学，2019年在南洋理工大学访学；
- 研究方向：漏洞挖掘、程序分析和漏洞知识图谱；
- 学术论文：USENIX Security, ASE, Saner, 信息安全学报；
- 成果：独立发现0day漏洞近百个（涵盖Linux kernel， FreeBSD，高通驱动等主流开源软件），获CVE收录49个；
- ASE 2020，ICSE 2020外部审稿人。

网络空间安全学科体系 (国科大网安学院)



网络空间安全评测 课程体系(2020-21学年)



《软件安全原理》课程组织

版块一 软件安全总论

- [01] 从安全视角认识软件
- [02] 软件安全
- [03] 网络与软件安全观
- [04] 逆向工程与程序理解

版块二 软件安全研究案例

- [05] 计算机基础软件概述
- [06] 操作系统安全机制演进
- [07] 计算机虚拟化技术演进
- [08] 浏览器-服务器软件架构
- [09] 浏览器安全
- [10] Web服务器软件安全
- [11] 移动终端安全概述
- [12] 移动终端操作系统
- [13] 移动App的安全

版块三 安全的软件开发

- [14] 内构安全
- [15] 安全的软件开发

[第1章] 从安全视角认识软件

内容大纲

1.1 课程简介

1.2 软件在现代文明中的地位

1.3 软件发展历程

1.4 软件的概念与类型

1.5 软件存在的问题

1.6 课程安排

像水泥一样，软件在现代文明中无处不见...

软件让一堆电缆变成了网络，软件是机器的灵魂，为事物赋予了智能

软件工程师——创建软件的人们

具有特殊天赋，具有构思和实现超级复杂和精妙算法的能力

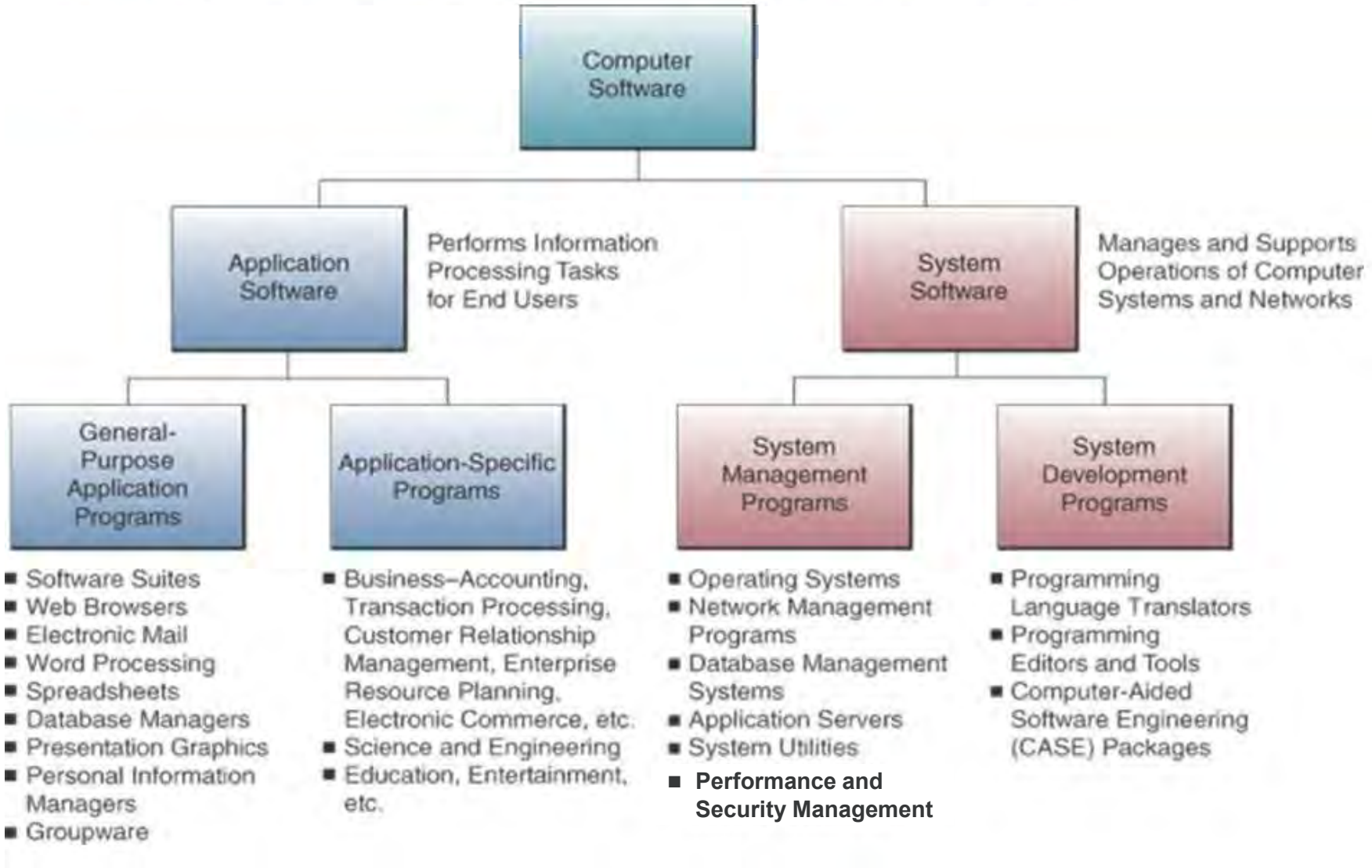
软件的分类

按版权情况划分

- 自由软件(free software)
- 开源软件(Open source)
- 免费软件(Freeware)
- 共享软件(Shareware)

软件的分类

按功能划分


Computer Software
Application Software
Performs Information Processing Tasks for End Users
System Software
Manages and Supports Operations of Computer Systems and Networks
General-Purpose Application Programs
Application-Specific Programs
System Management Programs
System Development Programs
Software Suites
Web Browsers
Electronic Mail
Word Processing
Spreadsheets
Database Managers
Presentation Graphics
Personal Information Managers
Groupware
Business–Accounting, Transaction Processing, Customer Relationship Management, Enterprise Resource Planning, Electronic Commerce, etc.
Science and Engineering
Education, Entertainment, etc.
Operating Systems
Network Management Programs
Database Management Systems
Application Servers
System Utilities
Performance and Security Management
Programming Language Translators
Programming Editors and Tools
Computer-Aided Software Engineering (CASE) Packages

软件的分类

分类：按行业应用划分

- 建筑、农业、矿产
- 能源、电力
- 电子商务、零售商业
- 金融保险
- 科研教育
- 健康、社会保障
- 艺术、电影
- 传统制造
- 政府
- 国家基础设施
- 公安
- 国防
- 运输物流
- 信息产业、互联网

[第1章] 从安全视角认识软件

内容大纲

1.1 课程简介

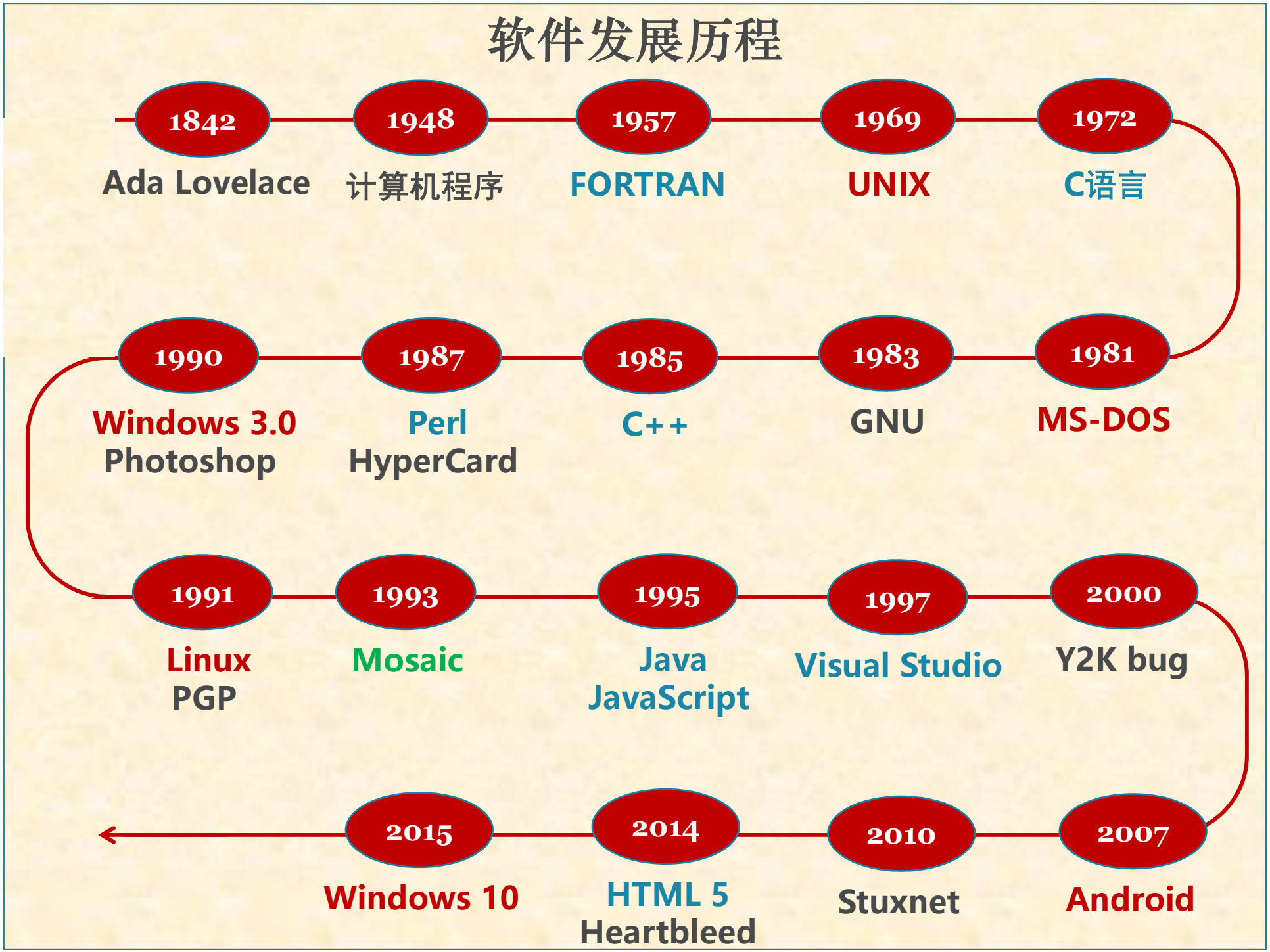
1.2 软件在现代文明中的地位

1.3 软件发展历程

1.4 软件的概念与类型

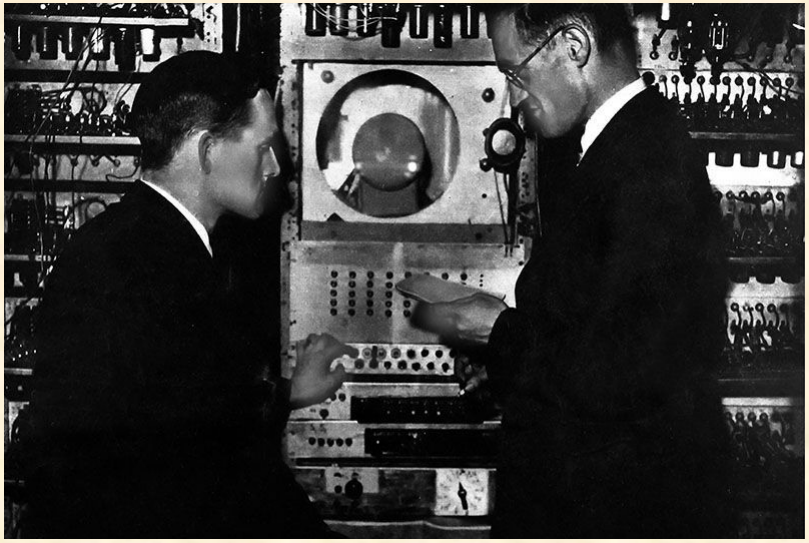
1.5 软件存在的问题

1.6 课程安排


软件发展历程
1842
Ada Lovelace
1948
计算机程序
1957
FORTRAN
1969
UNIX
1972
C语言
1981
MS-DOS
1983
GNU
1985
C++
1987
Perl
HyperCard
1990
Windows 3.0
Photoshop
1991
Linux
PGP
1993
Mosaic
1995
Java
JavaScript
1997
Visual Studio
2000
Y2K bug
2007
Android
2010
Stuxnet
2014
HTML 5
Heartbleed
2015
Windows 10

1948

第一个计算机程序



- Manchester大学 Frederic Williams, Tom Kilburn 和 Geoff Toothill 研发了实验型计算机SSEM (Small-Scale Experimental Machine)
- Kilburn 为SSEM写了一段由16条指令组成的程序
- 这是人类首个运行在电子存储式计算机上的程序

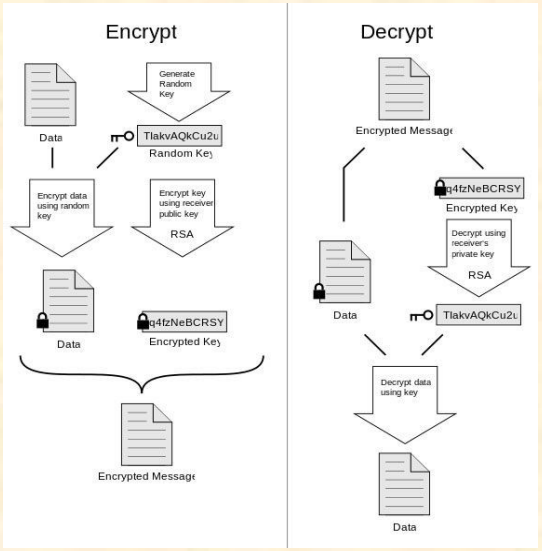
UNIX操作系统

- AT&T Bell Labs 的 Kenneth Thompson 和 Dennis Ritchie 研发
- 多任务分时操作系统
- 至今仍然是全球计算架构的基础

1991

Linux诞生

- 芬兰大学生Linus Torvalds发布了Linux kernel
- 1992年Linux成为免费软件
- 1998年Linux成为开源软件
- 至今广泛应用于从智能手机到巨型机



PGP发布

- Phil Zimmermann研制了 基于公钥的加密软件PGP (Pretty Good Privacy)
- 引起美国政府不满

浏览器Mosaic诞生

- 美国国家超级电脑应用中心(NCSA) Marc Andreessen团队研发
- 1995年Marc和J.H.Clark创办了Netscape公司
- Netscape Navigator浏览器内部代号Mozilla
- Mosaic+ Godzilla+Killa=Mozilla!

2007

Android操作系统发布

- Google发布基于Linux的自由及开源的手机操作系统Android
- 目前已成为全球装机量最大的手机OS

Windows 10发布

- Microsoft发布了Win 10
- “One Product family. One platform. One store”
- 延续其在桌面OS的优势地位，但移动智能终端仍难成气候

软件技术发展历程

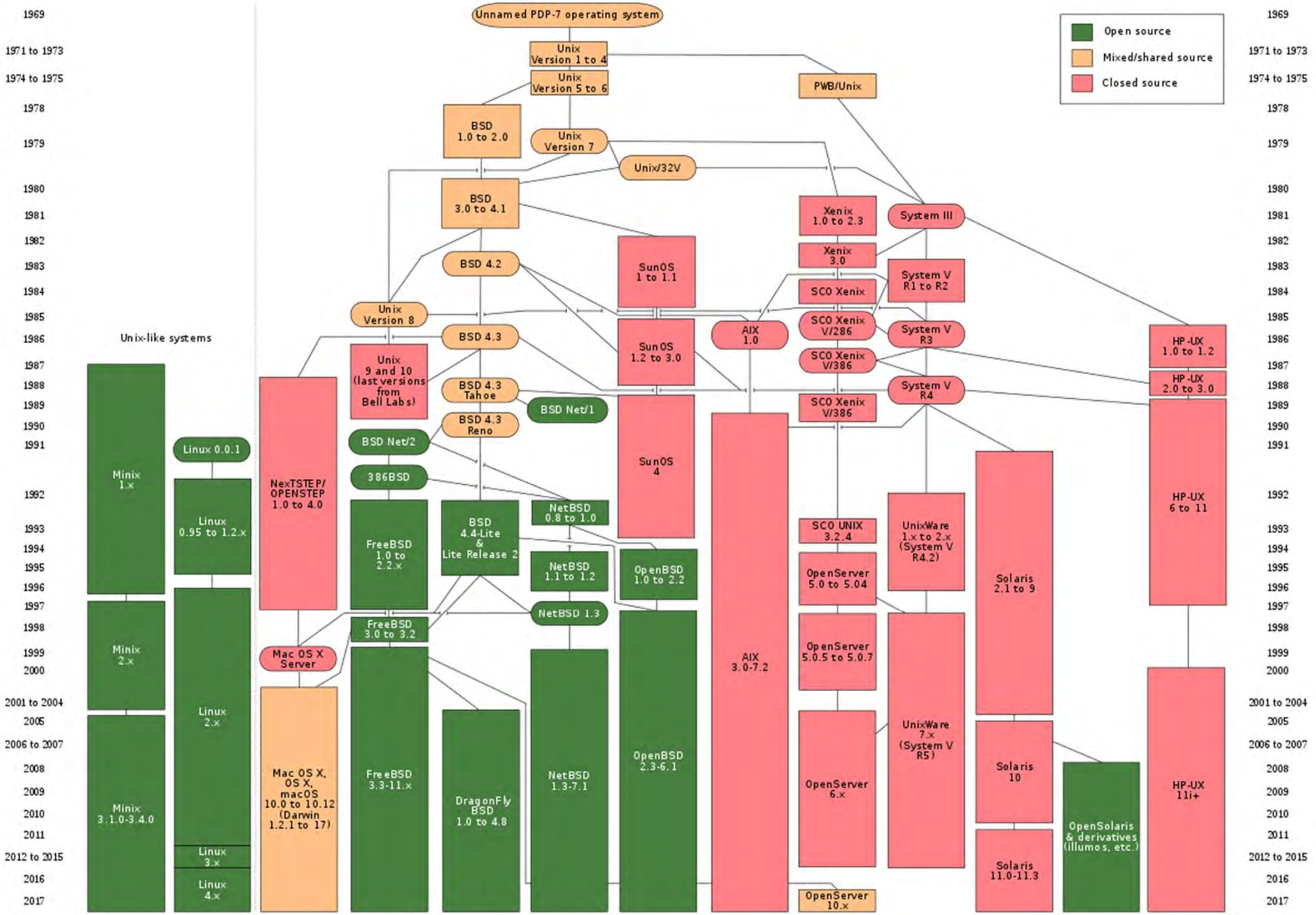
- 组件
- 更紧密的OS整合
- 封装的开始
- 无线系统的开始
- 更多PDA
- 逻辑分布式系统
- .NET的引入
- 兴起的移动代码
- Web代码和XML
- 预定服务

- IoT出现
- 真实对象的出现
- .NET和Java
- OS的封装
- 应用广泛的无线系统和嵌入式系统
- 地理分布式系统
- 外包计算
- 软件发布
- 移动代码接管

- 真实对象
- OS消失
- 计算服务
- 计算结构（普适）
- 智能设备
- 所有代码都是移动代码
- 基于位置的计算
- 自我组织系统和紧急系统

2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 ……

UNIX发展历程



参见：https://upload.wikimedia.org/wikipedia/commons/7/77/Unix_history-simple.svg

[第1章] 从安全视角认识软件

内容大纲

1.1 课程简介

1.2 软件在现代文明中的地位

1.3 软件发展历程

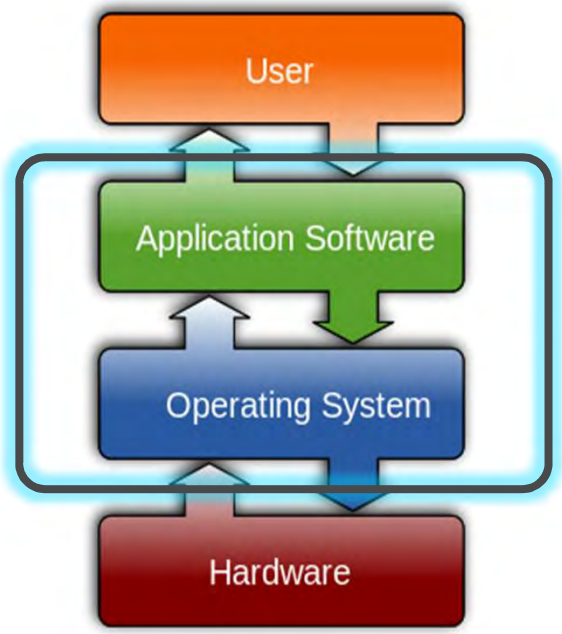
1.4 软件的概念与类型

1.5 软件存在的问题

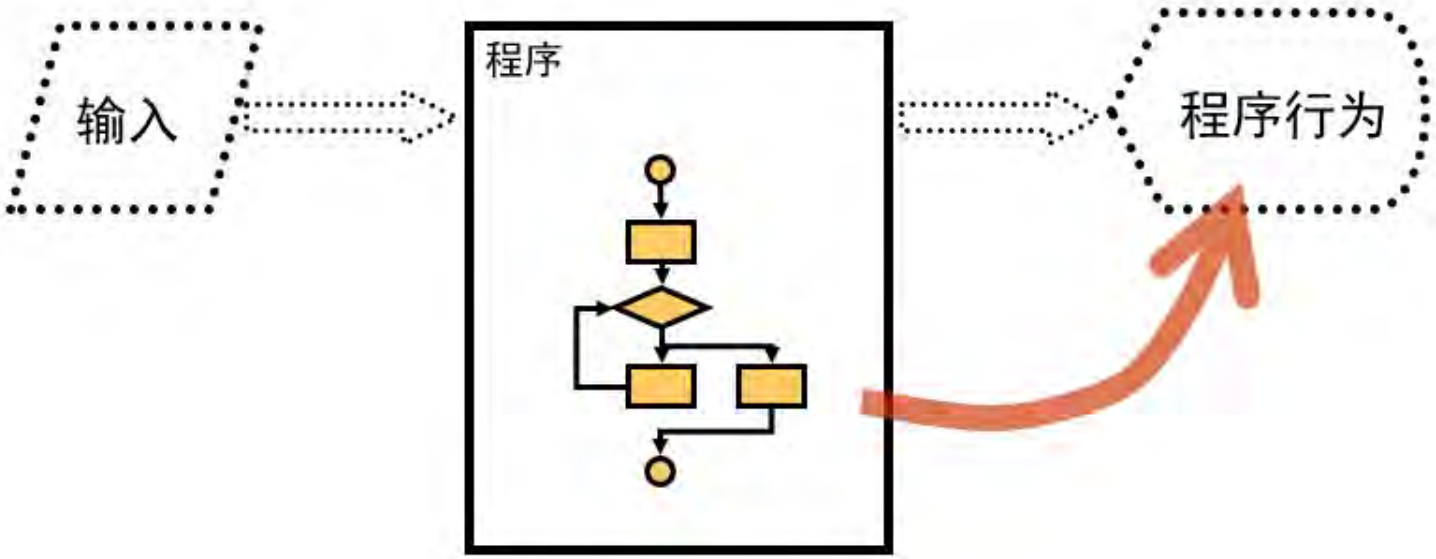
1.6 课程安排

软件与程序的定义

- **软件：**
  - 是用户与硬件之间的接口，用户通过软件与计算机交流。
  - 软件包括程序、数据和文档。
- **程序：**是一组通过计算机执行，以完成特定任务的指令。程序包括以下类型：
  - 源程序(source code)
  - 汇编代码(assembly code)
  - 目标程序(machine code)

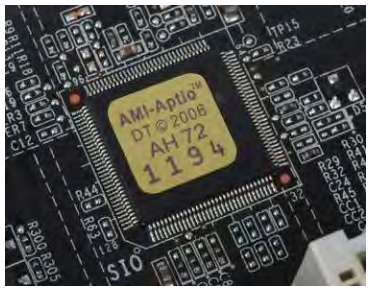


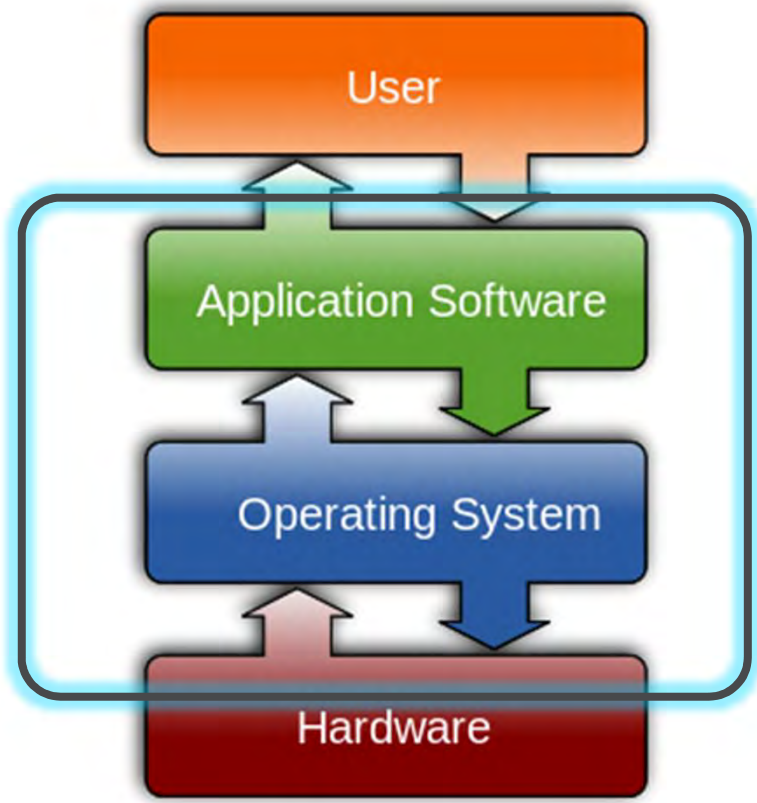
程序模型



软件工作原理

软件最本质的特性是可编程
(PROGRAMMABLE)





各种软件到底有多大?

- 代码行(LOC)— 程序大小的度量单位
- Hello.c： 9 LOC
- Google： > 2BLOC

[第1章] 从安全视角认识软件

内容大纲

1.1 课程简介

1.2 软件在现代文明中的地位

1.3 软件发展历程

1.4 软件的概念与类型

1.5 软件存在的问题

1.6 课程安排

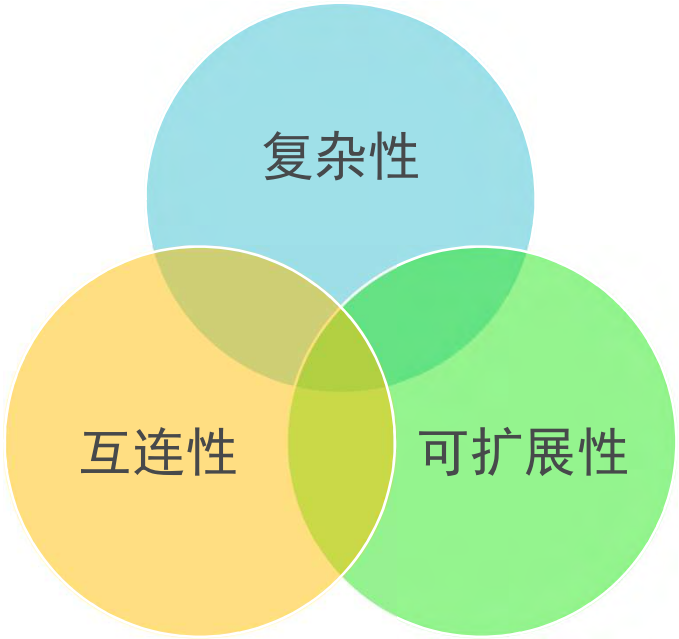
软件存在的问题

软件是“不负责任的产品”

60亿碰撞测试假人！

软件存在的问题

软件的三大问题



软件存在的问题

互连性

- 互联网增加了攻击目标的数量、简化了实施攻击的方法。
- 由于通过网络的访问不要求人工干预，因此很容易启动自动攻击。
- 企业通过门户提供服务以及业务操作增大了受攻击的风险：Web服务、SOA、中间件等。
- 过去遗留产品的集成带来两大安全隐患：1、完全依赖基于弱口令保护的主机到主机认证；2、忽略安全防护的中间件往往成为薄弱点。
- 当前的企业体系结构在互连环境下暴露出越来越多的安全隐患。

Internet无处不在，攻击者随时可以破门而入

软件存在的问题

可扩展性

- 系统扩展性是必然趋势：先提供应用软件的基本功能，再以功能插件方式提供附加功能。
- 系统更新或采用移动代码(mobile code)技术可大幅提升可扩展性，例如浏览器插件、J2EE和.NET、.....
- 可扩展系统架构，导致它难以阻止通过插件引入新漏洞。

可扩展性安全问题：易用性与安全性的矛盾

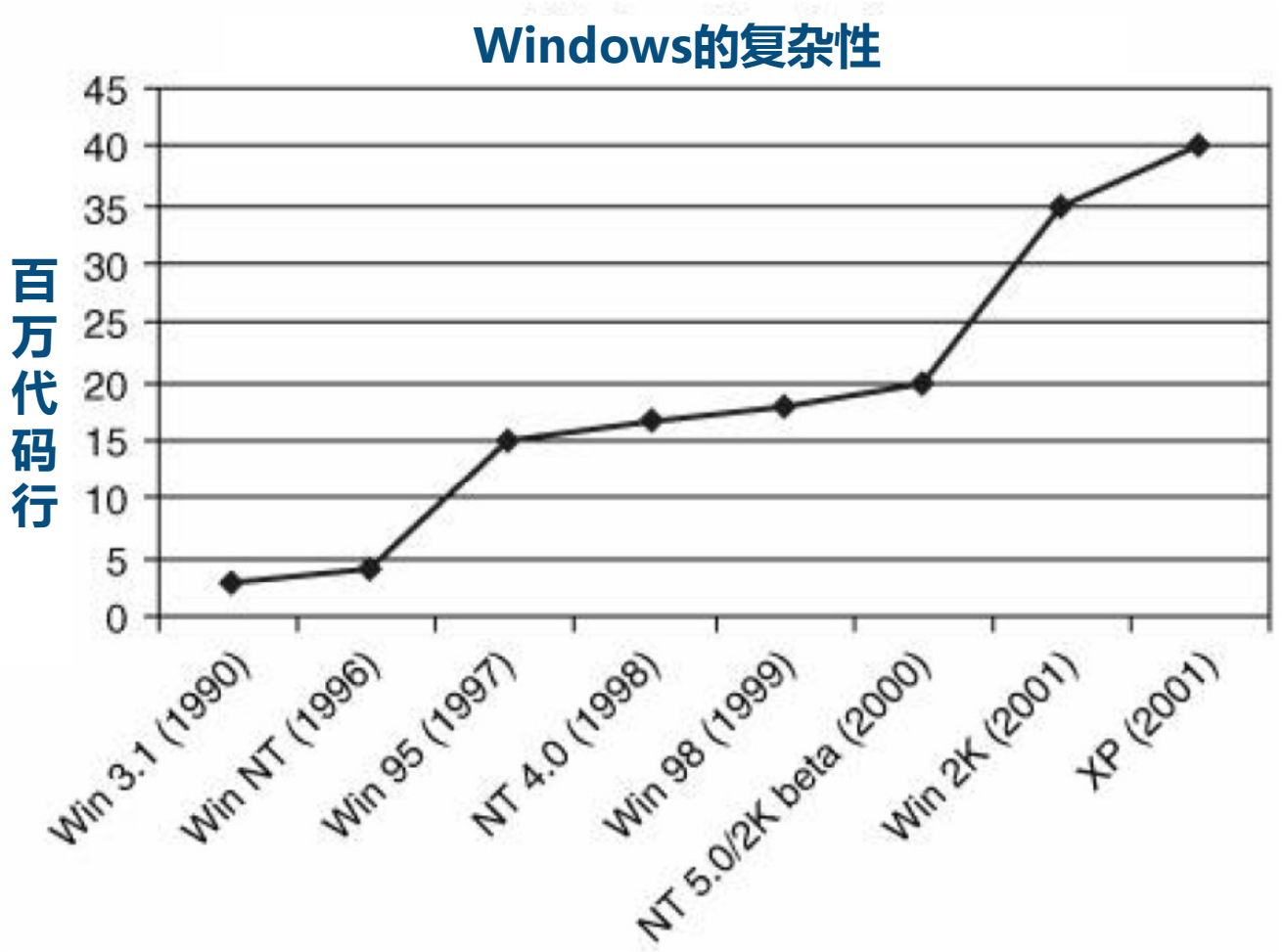
软件存在的问题

复杂性

- 现代信息系统（特别是软件系统）的规模和复杂性无节制的增长。
- 显著影响软件复杂性的因素还包括：代码集成的紧密程度、补丁与其它部署后所做的修改之间的重叠率，以及严重的体系结构问题。
- 即使源代码库显得不大，经过编译、链接生成的执行代码库也会变大，特别是基于以下功能构建程序时更加明显：数据扁平化（Java数据对象、基于容器管理的持久化）、身份管理和证明、XML解析器、MVC框架、应用服务器、数据库等。

软件存在的问题

复杂性


Windows的复杂性
百万代码行
45
40
35
30
25
20
15
10
5
0
Win 3.1 (1990)
Win NT (1996)
Win 95 (1997)
NT 4.0 (1998)
Win 98 (1999)
NT 5.0/2K beta (2000)
Win 2K (2001)
XP (2001)

软件存在的问题

复杂性

主要操作系统和内核的源代码行数

19xx	SCOMP	20,000
1979	Multics	1,000,000
2000	Red Hat 6.2	17,000,000
2000	Debian.GNU/Linux 2.2	55,000,000
2000	Linux 2.2 kernel	1,780,000
2000	XFree86 3.3.6	1,270,000
2001	Red Hat 7.1	30,000,000
2002	Mac OS X Darwin kernel	790,000

软件存在的问题

复杂性

- 软件缺点的增长速度趋向于随代码行数的平方而变化
- 不安全的编程语言（如C、C++）无法抵御缓冲区溢出之类的攻击。
- 虽然从理论上讲，我们可以分析和证明一个小程序不存在安全问题，但证明任何一个实际的桌面或企业级系统的安全性，都是不可能的。

软件规模越大、越复杂，缺陷也就越多

[第1章] 从安全视角认识软件

内容大纲

1.1 课程简介

1.2 软件在现代文明中的地位

1.3 软件发展历程

1.4 软件的概念与类型

1.5 软件存在的问题

1.6 课程安排

软件安全知识体系

软件安全三部曲

软件安全防御

从“白帽”（white hat，安全防御者）视角，研究软件的各类安全防御机制。

软件安全分析与利用

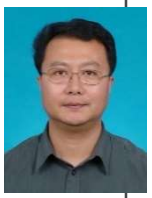
从“黑帽”（black hat，安全破坏者）视角，研究软件存在的各种安全脆弱性问题及其高效发现及利用方法。

安全的软件开发

确保软件安全的工程化方法。

《软件安全原理》课程组织

版块一 软件安全总论

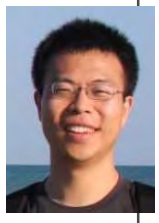


- [01] 从安全视角认识软件
- [02] 软件安全
- [03] 网络与软件安全观
- [04] 逆向工程与程序理解

版块二 软件安全研究案例

- [05] 计算机基础软件概述
- [06] 操作系统安全机制演进
- [07] 计算机虚拟化技术演进

- [08] 浏览器-服务器软件架构
- [09] 浏览器安全
- [10] Web服务器软件安全



- [11] 移动终端安全概述
- [12] 移动终端操作系统
- [13] 移动App的安全

版块三 安全的软件开发

- [14] 内构安全
- [15] 安全的软件开发

软件安全学习方法

访名师、读名著

中国系统安全知名学者代表

沈昌祥院士

方滨兴院士

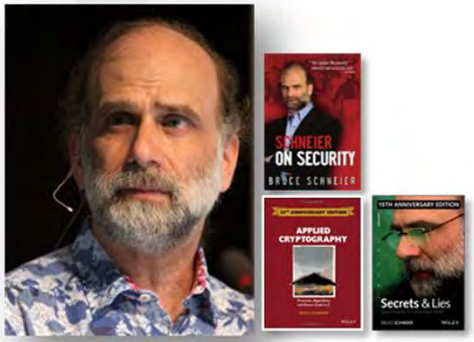
何德全院士

吴建平院士

美国系统安全SMR

取其精华
去其糟粕

Gary McGraw



Bruce Schneier

David Rice

课程安排 /课程教学说明

《中华人民共和国网络安全法》

- 第二十六条　开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。
- 第六十二条　违反本法第二十六条规定，……，由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，……对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款。

课程安排 /课程教学说明

《中华人民共和国网络安全法》

- 第二十七条　任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。
- 第六十三条　违反本法第二十七条规定，…… 尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。

合规合法地进行网络攻防实践

学习方法

动动口、动动手、动动脑

课程安排 / 课程教学说明

- 关于讲义
  - 每次课前上传课程讲义（含课程主要内容），供同学上课及复习时参考。
- 关于课堂教学
  - 作为核心专业课，以课堂讲授为主，同时鼓励同学互动交流。
  - 作为研究生课程，以启发式教学为基调。鼓励同学主动思考、调研，建立自己的知识框架，掌握必备的基础性知识。
- 关于习题与期末考试
  - 习题包括思考题、课程实践题等。
  - 期末考试：采用闭卷考试，围绕课程大纲，考察同学是否建立起合理的知识框架、是否掌握了核心理念及关键知识点，以及实践应用的基本能力。

软件安全原理

Principle of Software Security

[第1章] 从安全视角认识软件