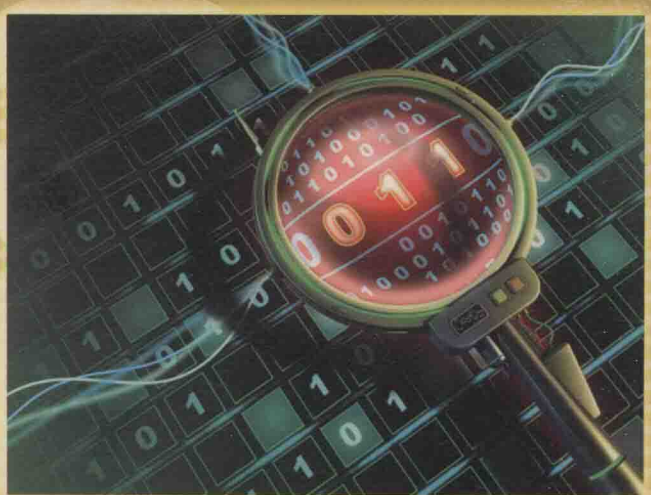
“十三五”国家重点出版物出版规划项目

“十三五”江苏省高等学校重点教材　　高等教育网络空间安全规划教材

软件安全技术

陈波　于泠　编著



提供电子课件、拓展阅读材料

http://www.cmpedu.com

机械工业出版社
CHINA MACHINE PRESS

“十三五”国家重点出版物出版规划项目

“十三五”江苏省高等学校重点教材（编号：2017-2-037）

高等教育网络空间安全规划教材

软件安全技术

陈　波　于　泠　编著

机械工业出版社

本书介绍在软件开发过程中从根本上提高软件安全性的基本技术。全书分4个部分共14章。第1部分为软件安全概述，第2～4部分分别针对三大类软件安全威胁：软件自身的安全（软件漏洞）、恶意代码及软件侵权展开介绍。第2部分为软件安全开发，包括软件漏洞概述、Windows系统典型漏洞分析和Web漏洞分析3章，还包括软件安全开发模型，以及软件安全开发生命周期每一个环节中的安全技术共6章。第3部分为恶意代码防护，包括两章内容，分别介绍恶意代码分析基本技术，以及恶意代码法律防治措施和技术防治技术。第4部分为软件侵权保护，包括两章内容，分别介绍开源软件及其安全性，以及软件知识产权法律保护和技术保护措施。

本书可作为信息安全、计算机和软件工程等专业的教材，也适用于软件开发人员、软件架构师和软件测试等从业人员、还可供注册软件生命周期安全师、注册软件安全专业人员、注册信息安全专业人员，以及计算机软件开发人员或编程爱好者参考和使用。

本书配有授课电子课件，需要的教师可登录www.cmpedu.com免费注册，审核通过后下载，或联系编辑索取（QQ：2850823885，电话：010-88379739）。

图书在版编目(CIP)数据

软件安全技术/陈波，于泠编著. —北京：机械工业出版社，2018.6
“十三五”国家重点出版物出版规划项目　高等教育网络空间安全规划教材
ISBN 978-7-111-60100-5

Ⅰ.①软…　Ⅱ.①陈…　②于…　Ⅲ.①软件开发-安全技术-高等学校-教材　Ⅳ.①TP311.522

中国版本图书馆CIP数据核字(2018)第142849号

机械工业出版社(北京市百万庄大街22号　邮政编码100037)
责任编辑：郝建伟
责任校对：张艳霞
责任印制：张　博
三河市宏达印刷有限公司印刷
2018年8月第1版·第1次印刷
184mm×260mm·25印张·612千字
0001-2500册
标准书号：ISBN 978-7-111-60100-5
定价：79.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务	网络服务
服务咨询热线：(010)88379833	机 工 官 网：www.cmpbook.com
读者购书热线：(010)88379649	机 工 官 博：weibo.com/cmp1952
	教育服务网：www.cmpedu.com
封面无防伪标均为盗版	金　书　网：www.golden-book.com

高等教育网络空间安全规划教材
编委会成员名单

前　言

近年来，国内外由于软件系统缺陷而引发的重大信息安全事件日益增多，给相关机构和企业带来了不良社会影响和重大经济损失。重视软件安全已是《国家网络空间安全战略》中明确的战略任务。要实现软件安全，就必须提升软件开发从业人员关于软件安全开发的知识和技能，从软件诞生的源头着手，减少软件安全缺陷与漏洞，从而提高软件运行的安全性。

目前，关于软件安全的书籍不多，适合于普通高校本科专业的教材也很少。本书作为江苏省“十三五”高等学校重点教材（新编）、江苏省高等教育教学改革重点课题(2015JSJG034)、江苏省教育科学十二五规划重点资助课题：泛在知识环境下的大学生信息安全素养教育——培养体系及课程化实践、南京师范大学精品资源共享课“软件安全”建设项目及南京师范大学“信息安全素养与软件工程实践创新教学团队”建设项目的成果，历经4年多编写完成，讲义几易其稿。

本书遵循《高等学校信息安全专业指导性专业规范》，全面梳理了国内外软件安全开发最佳实践，跟踪研究安全开发理论发展，汇集国内诸多专家学者智慧，并汲取软件漏洞分析经验，全面介绍了在软件开发过程中从根本上提高软件安全性的基本技术，用以培养软件开发人员的安全开发意识，增强对软件安全威胁的认识，提高安全开发水平，提升IT产品和软件系统的抗攻击能力。

本书在编写中力求体现以下三大特色。

1. 知识结构系统，内容全面

本书内容结构如图1所示，分为四大部分，共14章。

第1部分为软件安全概述，分别介绍软件安全的重要性、软件面临的三大类安全威胁、软件安全的概念及软件安全的研究内容。

第2部分为软件安全开发，首先用3章的篇幅分别介绍了软件漏洞概述、Windows系统典型漏洞分析和Web漏洞分析，接着，用6章的篇幅介绍了软件安全开发模型、软件安全需求分析、软件安全设计、软件安全编码、软件安全测试及软件安全部署等软件安全开发生命周期每一个环节中的安全技术。

软件安全开发是一种系统化的应用安全解决方法，它将一系列安全活动、安全管理实践和安全开发工具有机地结合在一起，在整个软件开发生命周期中，贯彻安全开发的思想，从源头着手，减少软件安全缺陷与漏洞，从而提高软件运行的安全性。与软件运行阶段解决安全问题相比，在软件开发阶段考虑安全问题更有效、更经济。该部分同时较为全面地分析了软件安全开发最新理论研究成果和产业界的最佳实践经验。

第3部分为恶意代码防护，用两章的篇幅分别介绍了计算机启动过程、程序的生成和执行、PE文件和程序逆向分析等恶意代码分析常用的基本技术，以及恶意代码法律防治措施和技术防治技术。

第 4 部分为软件侵权保护，用两章的篇幅分别介绍了开源软件及其安全性，以及软件知识产权法律保护和技术保护措施，包括云环境下软件版权保护的新技术。

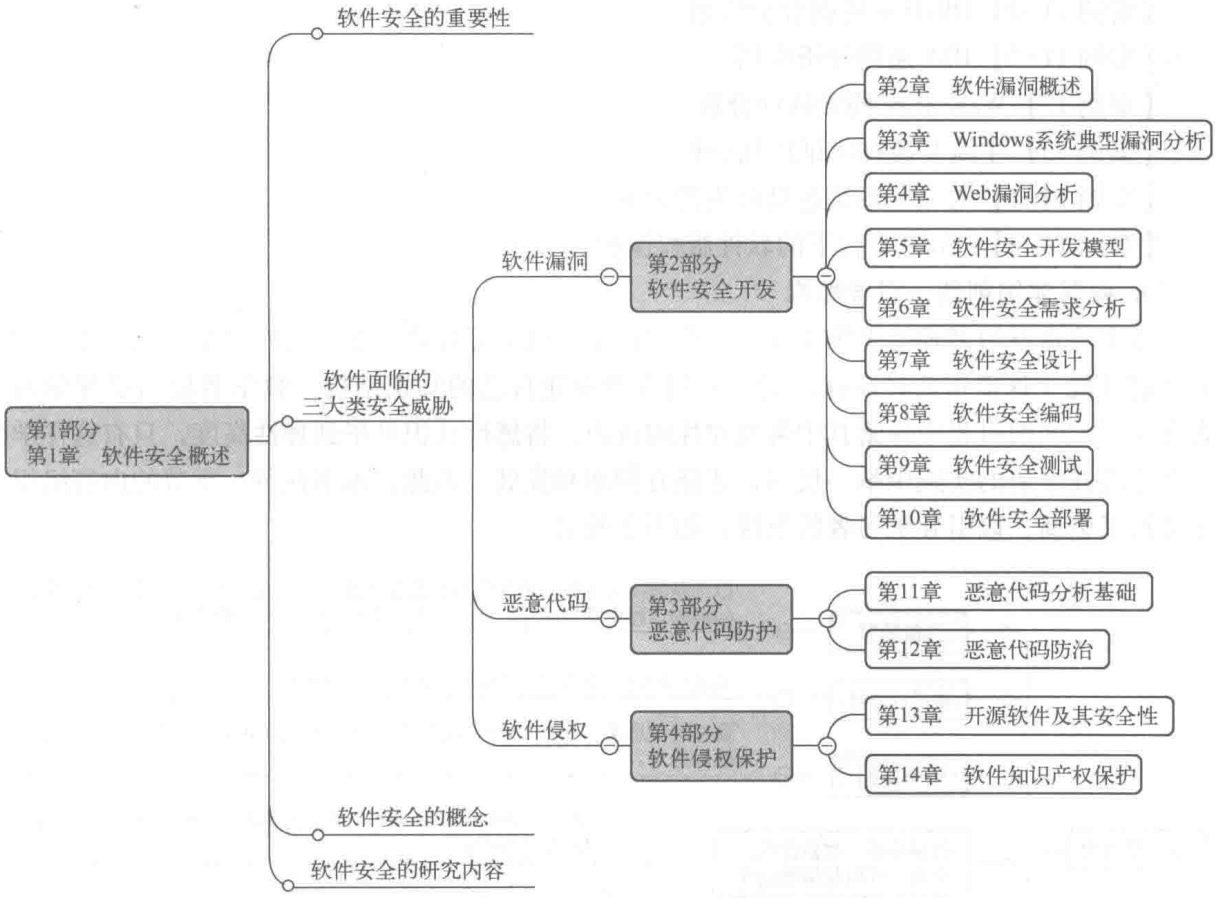


图 1　本书内容结构

2. 理论实践结合，案例丰富

本书注重理论与实践结合，通过对 19 个案例的分析、工具介绍等方式，帮助读者更好地掌握软件安全开发、恶意代码防治及软件版权保护等关键技术。

【案例 1】零日攻击、网络战与软件安全

【案例 2-1】白帽黑客的罪与罚

【案例 2-2】阿里巴巴月饼门

【案例 3】Windows 安全漏洞保护技术应用

【案例 4-1】SQL 注入漏洞源代码层分析

【案例 4-2】XSS 漏洞源代码层分析

【案例 5】Web 应用漏洞消减模型设计

【案例 6】一个在线学习系统的安全需求分析

【案例 7】对一个简单的 Web 应用系统进行威胁建模

【案例 8】基于 OpenSSL 的 C/S 安全通信程序

【案例 9】Web 应用安全测试与安全评估

【案例 10】SSL/TLS 协议的安全实现与安全部署

【案例 11-1】构造一个 PE 格式的可执行文件

【案例 11-2】OllyDbg 逆向分析应用

【案例 11-3】IDA 逆向分析应用

【案例 12】WannaCry 勒索软件分析

【案例 13】主流开源许可证应用分析

【案例 14-1】对 iOS 系统越狱行为的分析

【案例 14-2】.NET 平台下的软件版权保护

3. 编写体例创新，引导思维

本书注重学习者理性思维引导。按照建构主义的学习理论，学习者作为学习的主体，应在客观环境（这里指教材内容）的交互过程中构建自己的知识结构。教学者应当引导学习者在学习和实践过程中探索其中带规律性的认识，将感性认识升华到理性高度，只有这样学习者才能在今后的实践中举一反三，才能有创新和发展。为此，本书在每一章节的内容组织上进行了创新，以引导学习者的思维，如图 2 所示。

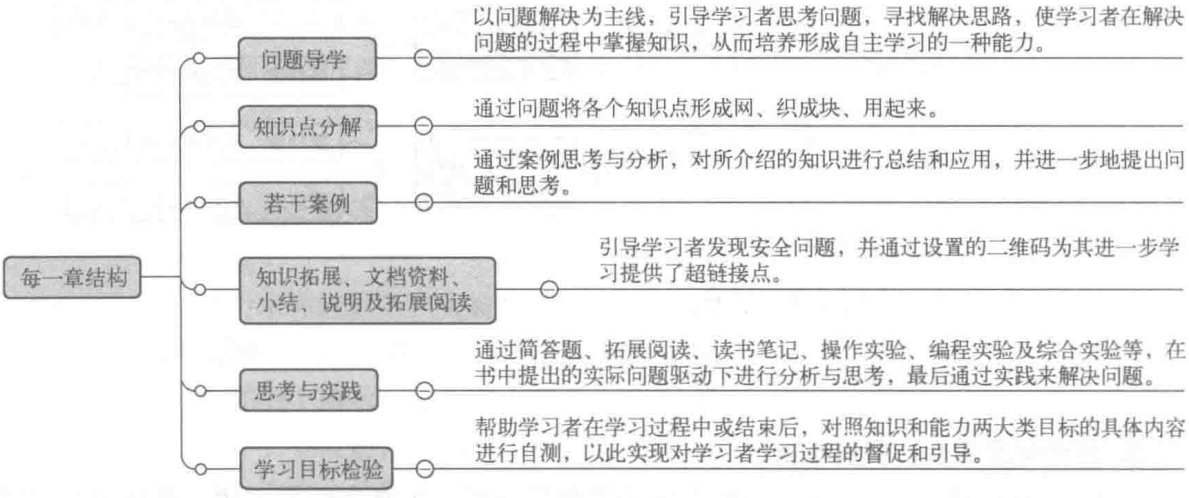


图 2　本书内容组织

本书知识编排体系也为教师有效地组织课堂教学提供了便利，教师可以根据教材资源，对学习者进行问题引导、疑难精讲、质疑点拨、检测评估。

本书由陈波和于泠执笔完成。于浩佳、陈思远、刘蓉、张敬然、麻益通、孙铭扬也参与完成了资料整理、部分图表绘制等工作。本书在写作过程中查阅和参考了大量的文献和资料，限于篇幅，未能在书后的参考文献中全部列出，在此一并致谢。本书的完成也要感谢机械工业出版社的郝建伟编辑一直以来对作者的指导和支持。

本书可作为信息安全、计算机和软件工程等专业的教材，也适用于软件开发人员、软件架构师、软件测试等从业人员，还可供注册软件生命周期安全师（Certified Secure Software Lifecycle Professional，CSSLP）、注册软件安全专业人员（Certified Secure Software Professional，CWASP CSSP）、注册信息安全专业人员（Certified Information Security Profes-

sional，CISP），以及计算机软件开发人员或编程爱好者参考和使用。

由于编者水平有限，书中难免有疏漏之处，恳请广大读者批评指正。作者为了让读者能够直接访问相关资源进行学习和了解，在书中加入了大量链接，虽然已对链接地址经过认真确认，但是可能由于网站的变化而不能访问，请予谅解。读者在阅读本书的过程中若有疑问，也欢迎与作者联系，电子邮箱是：SecLab@ 163. com。

编　者

目　录

第1章　软件安全概述

导学问题

- 为什么说要有效应对当前的全球网络空间安全威胁，必须对软件安全给予强烈关注？☞1.1节
- 软件安全面临哪些安全威胁？☞1.2节
- 如何理解软件安全的概念？☞1.3.1节和1.3.2节
- 软件安全与信息安全、网络空间安全的关系是什么？☞1.3.3节
- 软件安全与软件故障、软件可信等软件要求有何区别与联系？☞1.3.3节
- 软件安全问题的主要解决思路是什么？涉及的主要方法和技术有哪些？☞1.4节

1.1　软件安全的重要性

当前，软件已融入人们日常生活的方方面面，已经成为国家和社会关键基础设施的重要组成部分，因此，软件的安全关乎信息系统的安全，关乎关键基础设施的安全，关乎个人安全乃至社会和国家的安全。本节将通过介绍震网病毒进行零日攻击的案例带领大家来认识软件安全的重要性。

【案例1】零日攻击、网络战与软件安全

曝光美国棱镜计划的爱德华·斯诺登（Edward Snowdon）证实，为了破坏伊朗的核项目，美国国家安全局和以色列合作研制了震网（Stuxnet）病毒，以入侵伊朗核设施网络，改变其数千台离心机的运行速度。

震网病毒攻击目标精准，主要利用了德国西门子公司的SIMATIC WinCC系统的漏洞。WinCC系统是一款数据采集与监视控制（SCADA）系统，被伊朗广泛应用于国防基础工业设施中。病毒到达装有WinCC系统用于控制离心机的主机后，首先记录离心机正常运转时的数据，如某个阀门的状态或操作温度，然后将这个数据不断地发送到监控设备上，以使工作人员认为离心机工作正常。与此同时，病毒控制WinCC系统向合法的控制代码提供预先准备好的虚假输入信号，以控制原有程序。这时，离心机就会得到错误的控制信息，使其运转速度失控，最后达到令离心机瘫痪乃至报废的目的。而核设施工作人员在一定时间内会被监控设备上显示的虚假数据所蒙骗，误认为离心机仍在正常工作，等到他们察觉到异常时为时已晚，很多离心机已经遭到不可挽回的损坏。

2014年，美国自由撰稿人金·泽特（Kim Zetter）出版了*Countdown to Zero Day: Stuxnet*

and the Launch of the World's First Digital Weapon(《零日攻击：震网病毒全揭秘》)一书，如图1-1所示。该书是目前关于震网病毒入侵伊朗核设施事件最为全面和权威的读物，也为人们揭开了零日漏洞攻击的神秘面纱。

2016年，美国导演亚历克斯·吉布尼（Alex Gibney）执导的纪录片*Zero Days*(《零日》)讲述了震网病毒攻击伊朗核设施的故事，揭露了网络武器的巨大危险性。

图1-1 《零日攻击》一书封面

【案例1思考与分析】

【案例1】中提及的书籍和影片向人们清晰展示了恶意软件作为网络战武器对国家关键基础设施乃至整个国家的巨大破坏力。攻击者为了能够有效达到窃取数据、破坏系统的目的，可以通过挖掘或是购买零日漏洞，开发针对零日漏洞的攻击工具实施攻击。

零日漏洞是指未被公开披露的软件漏洞，没有给软件的作者或厂商以时间去为漏洞打补丁或是给出解决方案建议，从而使攻击者能够利用这种漏洞破坏计算机程序、数据及设备。注意，零日漏洞并不是指软件发布后被立刻发现的漏洞。

利用零日漏洞开发攻击工具进行的攻击称为零日攻击。零日攻击所针对的漏洞由于软件厂商还没有发现或是还未提供相应的补丁，所以零日攻击的成功率高，造成的破坏大。

从日常黑客攻击到军事领域的对抗，从震网病毒到棱镜门事件，信息空间的几乎所有攻防对抗都是以软件安全问题为焦点展开的。

本节接下来将从软件的定义和应用普遍性进一步展开分析软件安全的重要性。

1. 软件的定义

国家标准GB/T 11457—2006《信息技术 软件工程术语》给出的软件定义是：计算机程序、规则和可能相关的文档。

美国电气和电子工程师协会（Institute of Electrical and Electronics Engineers，IEEE）1990发布的《软件工程术语标准词汇表》（Standard Glossary of Software Engineering Terminology）给出的软件定义是："Computer programs, procedures, and possibly associated documentation and data pertaining to the operation of a computer system"。

以上两个标准文档都认为，软件是程序、数据和文档的集合体。程序是完成特定功能和满足性能要求的指令序列；数据是程序运行的基础和操作的对象；文档是与程序开发、维护和使用有关的图文资料。

然而，在这两个重要的与软件相关的标准文档中均未涉及"软件安全"。

2. 软件无处不在

现在是一个信息化的时代，每时每刻都有无数的软件系统在运行着。这是一个"互联网+"的时代，物联网、云计算、大数据、移动终端、可穿戴设备和无人驾驶汽车等各种新兴IT技术正改变着人们的生活和工作，改变着这个世界，推动着人类文明的发展。

这也是一个软件的时代，各种新兴IT技术借助社交网络、即时通信、电子邮件、移动商务、网络游戏和智能家居等各种网络应用软件发挥着作用。无论是人们手中的笔记本电脑、智能手机，还是守护人们健康的医疗器械，亦或是出行乘坐的汽车、飞机，还有保家卫国的战斗机、航母，都离不开软件。一个不可否认的事实是，软件已融入人们日常生活的方方面面，已经成为国家和社会关键基础设施的重要组成部分。

3. 软件规模日益庞大

随着软件应用范围日益广泛，软件规模也大幅增加。

常见软件代码规模统计
来源：http://www.informationisbeautiful.net/visualizations/million-lines-of-code
请访问网站链接或是扫描二维码查看。

常见软件代码规模统计图表显示，20 世纪 70 年代的早期民航客机波音 747 使用了大约 40 万行代码写成软件，而 2011 年的新型波音 787 所用软件的源代码是波音 747 的 16 倍——650 万行，规模十分庞大。而迄今 Google 包含的因特网服务应用软件规模更是达到了惊人的 2 亿行。

再来看看大家熟悉的微软操作系统 Windows。问世于 1985 年的微软操作系统仅仅是 DOS 环境，后续的系统版本由于微软不断更新升级，逐渐成为当前应用范围最为广泛的操作系统。同时，Windows 系统代码行数、开发难度、参与人员的数量、开发的时间长度也在不断增长。据统计，Windows XP 大约有 4000 万行代码，Windows 7 大约有 5000 万行代码，Windows 8 和 Windows 10 估计超过亿行了。Windows 7 开发时有 23 个小组，每个小组约 40 人，总共将近 1000 人。这仅仅是 Windows 团队的人数，其余为其做出贡献的人更是数不胜数。

随着软件功能的增强，软件的规模不断增长。软件在互联网时代的社会中发挥的作用越来越大，但同时软件担负的责任也越来越重要。无论是对于软件开发者还是软件的使用者，软件功能的创新都是值得期待的，但是软件一旦出现设计上的错误、缺陷或是漏洞，创新应用也就成为了泡影，甚至会带来灾难。

4. 软件漏洞普遍存在，零日漏洞成为主要安全威胁

辩证唯物论的认识论和辩证唯物论的知行统一观认为，人们对于客观世界的认识是有局限性的，人们对于客观世界的认识过程是螺旋上升的。软件是人们为了实现解决生产生活实际问题而开发的某种完成特定功能的计算机程序，因而必然存在缺陷或漏洞。

软件漏洞是普遍存在的，系统软件、应用软件和第三方软件，它们在开发、部署和应用中的问题层出不穷。

现在应用最广泛的 Windows 系列操作系统从诞生之日起就不断地被发现存有安全漏洞。Windows 系统不是“有没有漏洞”的问题，而是“何时被发现”的问题。微软定期发布的《安全情报报告 SIR》会及时披露微软和其他第三方软件的漏洞情况和对安全的影响。微软产品的漏洞数量与第三方软件漏洞总数的比例基本是 1∶10，与第三方软件的漏洞数量相比，微软产品的漏洞数量还是一个较小的比例。

2014 年 4 月，著名的开源代码软件包 OpenSSL“心脏滴血”（Heart Bleeding）漏洞大规模爆发。OpenSSL 是一个支持 SSL 和 TLS 安全协议的安全套接层密码函数库，Apache 使用它加密 HTTPS，OpenSSH 使用它加密 SSH，很多涉及资金交易的平台都用它来做加密工具，因此，全世界数量庞大的网站和厂商受到影响。

国内外还有很多白帽子漏洞发布平台（如补天漏洞平台 https://butian.360.cn）及地下软件漏洞交易黑市，每天都在发布各种漏洞。披露的漏洞增长速度之快，漏洞数量之多，涉及厂商之众，涉及软件产品之广，令人咋舌。

以前的大规模军队作战、昂贵的武器系统、武装抢劫、特工信息窃取、暴力抗议活动和武装叛乱正在被网络战和网络犯罪所替代。本章【案例1】就向大家展示了攻击者利用软件漏洞实施的网络攻击在网络战中的巨大威力。这一现象产生的根本原因是软件产品本身存在安全漏洞。这些漏洞不止发生在操作系统、数据库或者 Web 浏览器中，也发生在各种应用程序中，特别是与关键业务相关的应用程序系统中。据统计，有超过 70%的漏洞来自于应用程序软件，而当前最为热点的移动互联网 App 存在安全漏洞的比例高达 90%以上。各种安全漏洞可以为因特网远程访问、进行系统穿透和实现系统破坏大开方便之门。

在工业生产领域，随着计算机技术、通信技术、控制技术的发展和信息化与工业化的深度融合，传统的工业控制系统（Industrial Control System，ICS）逐渐向网络化转变，黑客、病毒和木马等威胁正在向 ICS 扩散，ICS 面临的信息安全形势日益严峻。

在日常生活中，包括智能手表、智能电视、冰箱、洗衣机乃至电饭煲，每天越来越多的新设备联入互联网，万物互联的时代已经开启，这些新型网络中的软件安全问题引人关注。以车联网为例，2014 年，美国一名 14 岁男孩演示了仅凭 15 美元购买的简单电子设备，轻而易举地侵入联网汽车；德国安全专家曝光了宝马诸多车型的中控系统可被破解，在数分钟内即可解除车锁，该漏洞存在于 220 万辆宝马、Mini 和劳斯莱斯汽车中。

现在智能联网汽车的安全风险日渐突出。其主要原因是汽车控制系统由车载电脑实现，典型的豪华车包含大约 1 亿行代码的软件，同时汽车系统在开发时存在多处安全缺陷。从被曝光的漏洞中可以发现，宝马车在验证解锁信号时，只是向宝马服务器发送一个简单的 HTTP Get 请求，在传输过程中并没有使用 SSL/TLS 加密，致使黑客可以截获传输信息。另外汽车的消息验证机制也存在缺陷，汽车通过查看消息中的车辆标识码（Vehicle Identification Number，VIN）来检查收到消息的目的地址，如果不匹配它就不会执行发送命令；另一方面，当不能接收到有效的 VIN 码时，它会发送一条错误消息并附上自己的 VIN 来标识。

现在大多数的网络攻击利用了软件（尤其是应用软件）的漏洞。根据统计分析，绝大多数成功的攻击都是针对和利用已知的、未打补丁的软件漏洞和不安全的软件配置，而这些软件安全问题都是在软件设计和开发过程中产生的。

5. 软件安全应当引起重视，应当成为当务之急，甚至成为国家的一项竞争优势

人们已经清醒地认识到全球网络空间安全威胁正在持续增加，必须认真应对安全威胁。然而一些错误的认识使得人们至今仍然疲于应付，焦头烂额。

错误认识一：应对安全威胁的主要手段是密码技术，是添置边界防护等各种安全设备。

调查数据显示，企业的信息安全预算中主要的投资方向仍集中于传统的防病毒、防火墙、VPN 及身份认证等方法，这些以网络边界安全防护为主的传统安全解决方案可以减少漏洞被利用的机会，然而却不能有效减少系统本身漏洞的存在，仍属于检测型或补偿型控制的被动防护方法。尽管如微软等核心软件公司能够定期发布安全补丁，较为及时地对操作系统、数据库等核心软件的漏洞进行修复，但对于一些零日攻击系统几乎没有防范能力。加之大多数的应用软件开发人员没有能力及时地对应用软件漏洞进行修复，使得系统的运行处于一种危机四伏的状态。传统的安全控制效果不尽如人意，信息安全问题越来越多，攻击形势越来越隐蔽（如 APT 攻击），智能程度越来越高（技术水平越来越高），组织方式多样化

（由最初的单个人员入侵发展到利益驱动的有组织、有计划的产业行为），危害程度日益严重。

是什么真正引发了当今世界大多数的信息安全问题？有人会回答，是黑客的存在。那么黑客和网络犯罪分子的主要目标是什么？有人会回答，是重要的信息资产，是各类敏感数据。这样的回答看起来不错，但是再往深处想一想，黑客是如何实现盗取重要信息资产的？黑客成功实施攻击的途径是什么？那就是发现、挖掘和利用信息系统的漏洞。

因此，应该着眼于源头安全，而不是仅仅采取如试图保护网络基础设施等阻挡入侵的方法来解决安全问题。源头安全需要软件安全，这是网络基础设施安全的核心。边界安全和深度防御在安全领域中占有一席之地，但软件自身的安全是安全防护的第一关，应该是第一位的。即使在软件源头中存在较少的漏洞，这些漏洞也足以被利用，成为侵犯国家利益的武器，或者成为有组织犯罪的网络武器储备。

错误认识二：不值得在关注软件安全，降低糟糕的软件开发、集成和部署带来的风险上花费成本。

软件项目由于受限于成本和严格的开发进程，往往牺牲安全，主要表现在以下两个方面。

- 软件工程人员缺乏安全意识和教育的专门培训。开发者需要在巨大的压力下和预算内按时提供更多的软件功能，因此一部分开发者很少能够抽出时间来认真审查他们的代码以发现潜在的安全漏洞。而他们即使能够抽出时间，又因为没有经过安全方面的培训，事倍功半。事实上，开发者需要获得激励、更好的工具和适当的培训，使他们有安全开发的动力，有具备编写安全代码所需的能力。
- 软件产品开发中通常在开发后期进行测试以消除编码中的错误或缺陷。这种做法对于减少软件产品中的漏洞数量有一定的作用，但是系统设计逻辑上的一些缺陷在测试阶段是无法发现的，往往这些漏洞会增加后期系统维护的成本，并且给用户带来巨大的潜在风险。

开发出安全漏洞尽可能少的软件应当是软件开发者或者说是软件厂商追求的目标。不仅要把软件做得更好，而且要更安全，同时，根据现实世界的经验，必须保证该解决方案具有较好的成本效益、操作相关性和可行性，以及投资的可行性。

事实上，软件安全开发的最佳实践是采用从软件开发之初就不允许漏洞发生的方式，在软件开发的各个环节尽可能消除漏洞，这不仅使得软件及其用户更安全，关键基础设施更具弹性，还将节省软件企业的开发成本。

100%安全的软件和系统是不存在的，软件产品存在漏洞是当前信息安全领域面临的最大困境。由于漏洞的产生、利用及相互作用的机理复杂，因此，如何有效减少系统漏洞数量，提高信息系统整体安全性，成为当前急需解决的挑战性问题。

软件已经渗透到社会、经济与国防建设的方方面面，是信息时代所依赖的重要技术与手段，其安全直接关系到国计民生与国家安全，因此，软件安全关乎国家竞争力。

6. 软件安全之路

从第一个大规模针对软件的攻击开始，到20世纪80年代后期，软件安全已经走过了漫长的道路。当时的软件并没有过多地考虑安全问题（如UNIX代码、TCP/IP协议栈）。随着微软Windows及网页（Web）的出现，攻击开始变得复杂和频繁，因此软件的安全性才逐渐