

《系统安全工艺》

图书基本信息

书名：《系统安全工艺》

13位ISBN编号：9787302194729

10位ISBN编号：7302194726

出版时间：2009-4

出版社：SeanSmith、John Marchesini、黄清元、李化 清华大学出版社 (2009-04出版)

作者：Sean Smith,John Marchesini

页数：380

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《系统安全工艺》

前言

“我认为这本《系统安全工艺》是当今市面上最棒的软件安全书籍之一。其内容广而深、覆盖的内容有密码学、网络构建、操作系统、Web、人机交互、以及如何通过改进硬件来提高软件系统安全性。简而言之，《系统安全工艺》适合所有系统安全从业者，并且也可以选作大学计算机科学课程的教材。”——Edward Bonver, CISSP (信息系统安全认证专业人员)、Symantec公司产品安全的资深QA工程师“这将会是一次有趣的、令人兴奋的阅读：该书囊括了各种有关计算机安全应用和误用的实例，是一本独特而新颖的书籍。我期望《系统安全工艺》能够激发广大学生朋友投身到安全技术领域中来；同时，该书还能够满足安全专家们的需要。”——L.Felipe Perrone, Bucknell大学计算机科学系教授过去，仅有专家对计算机安全感兴趣，但是，现在它已经成为社会中每个人都需要关注的内容。生活中经常需要计算，一旦计算机遭到破坏将会引发非常严重的后果。但试图掌控计算中的全部细节问题几乎是不可能的，参与计算的多个方面都存在复杂性问题，如独立构件和计算硬件、操作系统、应用程序、网络协议，以及使用这些系统的人为因素等。安全是每个人都应关注的问题，一个非常直接的问题是如何让每个参与者都明白安全方面的知识和安全的重要性。从软件工程师、经理、律师，以及任何其他人的职业生涯可以看出，研究者和从业者不仅需要关注安全涉及的广度，还需要关注其深度，如安全的发展趋势和准则等。现在，安全研究文献过多关注于系统管理、密码学体制、桔皮书或者NSA标准，计算机科学研究人员和计算机安全从业人员能够轻易地发现详细描述某些特定工具的书籍，这些工具可以用来对系统安全性进行评估，但是，这些书籍并没有向读者阐述更为本质的问题：人们为什么要开发这些工具？如何和何时使用恰当的工具来解决特定的问题。此外，现有文献也无法辅助人们开发出安全的系统，很多工具能够有效地辅助系统审计员进行审计，但对于安全系统开发人员则没有帮助。

《系统安全工艺》

内容概要

《系统安全工艺》首先快速回顾了计算机安全方面的历史，随后窥视了安全的前景，展示了安全的新挑战和如何应对这些挑战，并提供了一套体系以帮助理解当前的系统安全及其薄弱点。接下来，《系统安全工艺》系统地介绍了构建系统安全的基本构建块，还将这些构建块运用到现在的应用中，并思考了当前涌现的一些重要技术，如基于硬件的安全技术等。不论是系统安全从业者、开发人员、责任者还是管理员，都能够通过《系统安全工艺》更深层地理解安全形势以应对新的安全问题挑战。

《系统安全工艺》

作者简介

Sean Smith，博士，是Dartmouth大学的教授，负责教授计算机科学和研究真实世界可信系统的开发，他所致力项目（研究Good Samaritans对wikipedia的影响）被NetworkWodd杂志评选为25大最酷，最前沿的IT研究项目之一，他投身于信息安全方向的研究已15年，拥有多项专利成果，著有Trusted Computing、Platforms：Designand Applications一书。

John Marchesini，博士，拥有休斯顿大学的硕士学位和达特茅斯学院的计算机科学博士学位，他曾经是Symantec公司的资深安全工程师，还是产品安全组的一员，现在是EminentWare LLC的首席安全架构师。

书籍目录

目录

第一部分 历史背景

第1章 安全概述

3

1.1 安全的传统定义

3

1.2 访问控制矩阵

5

1.3 其他观点

7

1.3.1 正确性

7

1.3.2 风险管理

10

1.4 安全状态和访问控制矩阵

11

1.4.1 可计算性理论

11

1.4.2 安全性问题

11

1.5 其他安全难题

12

1.5.1 敌手是谁

12

1.5.2 系统的安全边界在哪里

13

1.5.3 如何量化成长性

14

1.5.4 检测还是阻止

14

1.5.5 安全的代价有多大

14

1.6 本章小结

14

1.7 思考和实践

15

第2章 旧约

17

2.1 基本框架

17

2.2 安全模型

18

2.2.1 信息流和偏序

18

2.2.2 Bell-LaPadula模型

21

2.2.3 其他安全模型

22	
2.3 桔皮书	
24	
2.3.1 访问控制矩阵	
25	
2.3.2 访问控制矩阵方法的扩充	
25	
2.3.3 系统的结构	
27	
2.3.4 软件工程	
28	
2.3.5 系统保障	
28	
2.3.6 案例研究	
29	
2.4 信息安全、作业安全和工作安全	
30	
2.5 本章小结	
31	
2.6 思考和实践	
31	
第3章 旧准则，新环境	
33	
3.1 桔皮书是否解决了错误问题	
33	
3.2 是否因缺乏政府支持而虎头蛇尾	
35	
3.3 旧准则是否太不实用	
36	
3.4 Saltzer和Schroeder	
38	
3.5 旧准则在现代计算环境中的适用性	
40	
3.6 本章小结	
40	
3.7 思考和实践	
41	
第 部分 安全与现代计算场景	
第4章 操作系统安全	
45	
4.1 操作系统的背景	
45	
4.1.1 计算机体系结构	
45	
4.1.2 操作系统的功用	
46	
4.1.3 基本元素	
47	
4.2 操作系统安全的基本概念和原理	

50	
4.2.1	进程隔离和内存保护
50	
4.2.2	用户
51	
4.2.3	文件系统访问控制
51	
4.2.4	引用监视器
53	
4.2.5	可信计算基础(TCB)
53	
4.3	真实操作系统：几乎实现了所有功能
53	
4.3.1	操作系统的访问
53	
4.3.2	远程过程调用支持
54	
4.3.3	密码学支持
55	
4.3.4	内核扩展
55	
4.4	针对操作系统的攻击
56	
4.4.1	通用攻击策略
56	
4.4.2	通用攻击技术
57	
4.4.3	按键记录器和Rootkit
58	
4.5	选择何种操作系统
60	
4.5.1	Windows和Linux
60	
4.5.2	其他操作系统
61	
4.6	本章小结
62	
4.7	思考和实践
63	
	第5章 网络安全
65	
5.1	基本框架
65	
5.1.1	大概原理
66	
5.1.2	查找联网机器
67	
5.1.3	联网机器的使用
69	

5.1.4 其他网络栈	70
5.1.5 网络和操作系统	72
5.1.6 企业网络体系结构	72
5.2 协议	74
5.2.1 SSL/TLS	74
5.2.2 IPsec	75
5.2.3 DNSSEC	76
5.2.4 (S)BGP	76
5.3 网络攻防	77
5.3.1 攻击	78
5.3.2 防御	81
5.4 新技术、新问题	83
5.4.1 无线局域网	83
5.4.2 蓝牙	87
5.5 本章小结	89
5.6 思考和实践	90
第6章 安全实现	91
6.1 缓冲区溢出	92
6.1.1 程序内存环境简述	92
6.1.2 栈溢出	94
6.1.3 溢出剖析	94
6.1.4 其他溢出攻击方法	95
6.1.5 防御	95
6.2 参数验证和其他问题	97
6.2.1 模糊测试	

97	
6.2.2 格式化字符串	
97	
6.2.3 整数溢出	
98	
6.2.4 转义序列	
100	
6.2.5 内部验证	
101	
6.3 TOCTOU	
101	
6.4 恶意软件	
102	
6.4.1 类型	
103	
6.4.2 著名示例	
103	
6.5 编程语言安全	
104	
6.5.1 内存管理	
104	
6.5.2 类型安全	
105	
6.5.3 信息流	
106	
6.5.4 过去和未来的解决方法	
107	
6.5.5 工具	
107	
6.6 开发周期内的安全	
108	
6.6.1 开发周期	
108	
6.6.2 两全齐美是不可能的	
108	
6.6.3 内嵌安全性	
109	
6.7 本章小结	
110	
6.8 思考与实践	
110	
第 部分 安全系统的构成模块	
第7章 密码学	
113	
7.1 框架和术语	
113	
7.1.1 转换	
114	
7.1.2 复杂性	

115
7.1.3 一些攻击策略
115
7.2 随机化
115
7.3 对称密码学
117
7.3.1 信息论
118
7.3.2 流加密和分组加密
119
7.3.3 链接
120
7.3.4 分组迭代
121
7.4 对称密码学的应用
124
7.4.1 加密
124
7.4.2 消息认证码
124
7.4.3 单向函数
125
7.4.4 伪随机数产生器
126
7.5 公钥密码学
126
7.5.1 基础
126
7.5.2 加密
126
7.5.3 签名
127
7.5.4 术语警告
127
7.5.5 RSA
128
7.5.6 其他算法
128
7.6 hash函数
130
7.6.1 介绍
130
7.6.2 函数构造
130
7.6.3 基本应用
130
7.7 公钥的实现问题
132

7.7.1 编码	132
7.7.2 性能	133
7.7.3 填充	134
7.8 过去和未来	135
7.9 本章小结	135
7.10 思考与实践	135
第8章 密码破解	137
8.1 非暴力破解对称密钥	137
8.1.1 非开源的随机数产生算法	138
8.1.2 开源的随机数产生器	138
8.2 暴力破解对称密钥	139
8.3 非因式分解方法破解公钥	140
8.3.1 智力扑克欺骗问题	141
8.3.2 基本RSA	141
8.3.3 填充函数	143
8.3.4 hash函数	144
8.4 密码机制实现破解	147
8.4.1 RSA时序攻击	147
8.4.2 缓冲时序攻击	148
8.4.3 硬件旁路攻击	149
8.4.4 Keyjacking	150
8.4.5 理论依据	151
8.5 模数分解的可能性	152
8.5.1 量子力学和量子计算机	152
8.5.2 BQP问题	

153	
8.6 本章小结	153
8.7 思考与实践	154
第9章 身份认证	155
9.1 基本框架	155
9.2 人的身份认证	156
9.2.1 口令	156
9.2.2 生物学身份认证	157
9.2.3 令牌	158
9.3 人为因素	159
9.3.1 口令	159
9.3.2 证书恢复	159
9.3.3 其他基于知识的方法	160
9.3.4 生物特征	160
9.3.5 口令共享	160
9.4 从机器的角度看身份认证	161
9.5 高级方法	163
9.5.1 一次性口令	163
9.5.2 密码学方法	165
9.5.3 双向认证	167
9.5.4 会话劫持	169
9.5.5 需考虑的必要因素	169
9.5.6 零知识	169
9.6 案例研究	171
9.6.1 Kerberos	171

9.6.2 SSH	174
9.7 其他问题	175
9.7.1 名字	175
9.7.2 授权	176
9.7.3 信任协商	177
9.7.4 信任管理	178
9.7.5 证明	178
9.8 本章小结	178
9.9 思考与实践	179
第10章 公钥基础设施	181
10.1 基本定义	182
10.2 基本结构	183
10.3 复杂性	184
10.3.1 注册	184
10.3.2 密钥托管和密钥恢复	185
10.4 多证书中心	187
10.5 证书回收	190
10.5.1 主流方法	190
10.5.2 其他方法	191
10.5.3 复杂性和语义	192
10.6 X.509方案	192
10.6.1 基本观点	192
10.6.2 X.509的变种	192
10.6.3 X.509的替代方案	194
10.7 反对观点	

194
10.7.1 Ellison
195
10.7.2 Whitten
195
10.7.3 Garfinkel
196
10.7.4 Gutmann
196
10.8 当前存在的问题
196
10.8.1 密钥存储
196
10.8.2 信任流的表示
197
10.8.3 端用户信任决策
197
10.8.4 历史的观点
197
10.9 本章小结
197
10.10 思考与实践
198
第11章 标准、实施和测试
199
11.1 标准
200
11.1.1 常见标准
201
11.1.2 美国标准与技术研究院
201
11.1.3 美国国家标准研究院
202
11.1.4 公钥密码学标准
203
11.1.5 RFC
203
11.1.6 标准的缺陷
203
11.2 策略实施
204
11.2.1 HIPAA
204
11.2.2 SOX法案
205
11.2.3 GLBA法案
205
11.2.4 最佳实践框架
206

11.2.5 审计	207
11.3 测试	208
11.3.1 实验测试	209
11.3.2 测试方案	209
11.3.3 开发者的作用	210
11.3.4 负面测试	210
11.3.5 现场测试	211
11.3.6 观察	212
11.3.7 模糊化	212
11.3.8 漏洞发现	213
11.4 本章小结	213
11.5 思考和实践	214
第 部分 应用	
第12章 Web及其安全	217
12.1 基本结构	218
12.1.1 基本动作	218
12.1.2 页面请求	218
12.1.3 页面内容	221
12.1.4 状态	224
12.1.5 网络问题	226
12.2 安全技术	227
12.2.1 基本访问控制	227
12.2.2 服务器端SSL	228
12.2.3 客户端SSL	232
12.3 隐私问题	236

12.3.1 客户端问题	236
12.3.2 服务器端问题	237
12.3.3 第三方服务器	237
12.3.4 跨会话信息泄露	238
12.3.5 秘密浏览技术	238
12.3.6 P3P	239
12.4 Web服务	239
12.5 本章小结	240
12.6 思考与实践	241
第13章 办公工具及其安全	243
13.1 Word	243
13.1.1 概要	244
13.1.2 真实趣闻	247
13.1.3 Word的bug	250
13.1.4 Word表单保护	250
13.1.5 宏	251
13.2 Lotus 1-2-3	252
13.3 PDF	253
13.3.1 崩溃	253
13.3.2 编写	253
13.3.3 可随意修改性	254
13.4 剪切-粘贴	255
13.5 PKI和办公工具	258
13.6 概念模型	259
13.6.1 文本该何去何从？	

259
13.6.2 Google
260
13.7 本章小结
261
13.8 思考与实践
261
第14章 货币、时间、属性
263
14.1 货币
263
14.1.1 类型
263
14.1.2 属性
264
14.1.3 其他问题
265
14.1.4 密码学工具箱
265
14.1.5 DigiCash
268
14.1.6 其他电子货币系统
270
14.2 时间
270
14.2.1 数字时间戳
271
14.2.2 整合hash函数
272
14.3 属性
274
14.3.1 信息隐藏和盗版
274
14.3.2 囚犯问题
275
14.3.3 水印示例
275
14.3.4 水印应用
276
14.3.5 攻击
277
14.4 本章小结
278
14.5 思考与实践
278
第 部分 新型工具
第15章 形式化方法和安全
281
15.1 规范

282	
15.2 逻辑	
284	
15.2.1 布尔逻辑	
284	
15.2.2 命题逻辑	
284	
15.2.3 一阶逻辑	
285	
15.2.4 时态逻辑	
286	
15.2.5 BAN逻辑	
286	
15.2.6 一些安全例子	
288	
15.3 实现	
290	
15.4 案例研究	
290	
15.5 了解你的银行账号	
291	
15.6 自动形式化方法的不足	
293	
15.7 本章小结	
294	
15.8 思考与实践	
294	
第16章 基于硬件的安全	
297	
16.1 数据残留	
298	
16.1.1 磁介质	
298	
16.1.2 FLASH	
298	
16.1.3 RAM	
299	
16.1.4 系统	
300	
16.1.5 旁通道	
300	
16.2 攻击和防御	
300	
16.2.1 物理攻击	
300	
16.2.2 防御策略	
302	
16.3 工具	
305	

16.3.1 安全协处理器	305
16.3.2 密码加速器	306
16.3.3 外部CPU功能性	308
16.3.4 可携带令牌	311
16.4 其他体系结构	311
16.4.1 常用机器	312
16.4.2 虚拟化	313
16.4.3 多核	315
16.4.4 受保护CPU	315
16.4.5 标记	315
16.5 发展趋势	316
16.5.1 虚拟化和安全	316
16.5.2 证明和鉴别	318
16.5.3 摩尔定律的未来	319
16.5.4 未来的个人令牌	320
16.5.5 射频识别	320
16.6 本章小结	320
16.7 思考与实践	321
第17章 搜索有害位	323
17.1 AI工具	324
17.2 应用分类	327
17.3 案例研究	329
17.3.1 环境	329
17.3.2 问题	330
17.3.3 技术	

330	
17.3.4 特征集	
331	
17.3.5 实验	
332	
17.4 实现	
333	
17.5 本章小结	
334	
17.6 思考与实践	
334	
第18章 人为因素	
335	
18.1 最后一程	
336	
18.2 设计准则	
338	
18.2.1 这不是你的错	
338	
18.2.2 概念模型	
339	
18.2.3 映射	
341	
18.2.4 约束、可用性、反馈	
341	
18.2.5 Yee的准则	
343	
18.3 其他因素	
343	
18.4 信任	
345	
18.4.1 信任为什么重要	
345	
18.4.2 促进信任	
346	
18.5 本章小结	
346	
18.6 思考与实践	
347	
附录A 相关理论	
349	
A.1 关系、序、格	
349	
A.2 函数	
350	
A.3 可计算性理论	
351	
A.3.1 不可数	
351	

A.3.2不可计算

353

A.4 框架

354

A.5 量子物理和量子计算

355

A.5.1 物理的发展

355

A.5.2 量子力学

356

A.5.3 Root-Not门

357

参考文献

359

章节摘录

插图：从定义上来看，广域网是范围较广的网络。如果按照每英尺的开销来看，广域网虽然速度较慢，但也比较便宜。现实的广域网所使用的介质要超出人们的想象：电话线、卫星等。广域网络也引发了一些范围较大时需要关注的问题，如拓扑和分割。现实世界的网络拓扑非常有趣。例如，美国的电信网络最近出现了异常，就是由网络拓扑的概念模型和物理真实模型不匹配引发的；有人设法破坏了关键网络线路和其备用线路，通过复杂的业务关系，最终也会引发网络拓扑概念模型与物理真实模型的不匹配。另外一个例子，人们在绘制广域网络拓扑时发现，企业之间的链接有聚合的趋势，但是为什么出现聚合则原因不明。5.1.2查找联网机器一旦有大量的机器参与网络互联，下一步就是设法找到那些机器。首先，需要命名这些机器，即主机名（hostname）。主机名是人类可理解的机器名，如WWW.CS.dartmouth.edu。这些名称遵循特定的层次结构：.edu域、在该域的.dartmouth组织以及.cs子组。简单说来，主机名是唯一的，每台机器对应一个主机名，反之亦然。但实际中可能并非如此，例如，一个服务器名可能对应很多台主机，这主要是出于负载均衡的考虑，一台机器也可能有两个不同的名称。

《系统安全工艺》

编辑推荐

《系统安全工艺》是深受读者喜爱的。权威专家旁征博引，深入剖析安全体系的竭诚之作最新的系统安全及其薄弱的详细说明；为全面认识安全体系，拥有解决问题的敏锐思维铺路搭桥内容涉猎广泛，叙述客观、生动，见解独到

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：www.tushu000.com