

《威胁建模》

图书基本信息

书名：《威胁建模》

13位ISBN编号：9787111498070

出版时间：2015-4

作者：adam shostack

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

《威胁建模》

内容概要

如果你是一名软件开发人员、系统管理人员或者安全专业人员，本书将告诉你在安全开发软件生命周期中或者软件和系统总体设计的过程中如何使用威胁建模方法。在本书中，安全技术专家Adam Shostack系统且深入阐释了自己对威胁建模的理解与实践。与其他书籍不同，本书详细介绍如何从开始设计软件、计算机服务和计算机系统时就构建与提升其安全性。

在安全事件威胁到你或者你的客户之前及时发现并修复。

帮助软件开发人员、IT专业人员和安全爱好者学习使用实用且操作性极强的工具、技术和方法。

探寻以软件为关键要素的威胁建模方法的微妙之处，探索其应用于软件和信息系统在构建及设计、维护等阶段威胁建模方法。

在复杂系统管理中应用威胁建模方法提升其安全性。

采用结构化理论框架管理潜在的安全威胁。

发现并识别不断变化的安全威胁。

本书提及的方法对于任何软件类型、操作系统、编程方法和技术均有效。其操作性极强，且其已在微软和其他顶级IT公司中得到印证。

书籍目录

译者序：威胁建模——网络安全的“银弹”

前言

鸣谢

第一部分 入门指南

第1章 潜心开始威胁建模 3

1.1 学习威胁建模 4

1.1.1 你正在构建什么 4

1.1.2 哪些地方可能会出错 6

1.1.3 解决每个威胁 9

1.1.4 检查你的工作 17

1.2 独立威胁建模 19

1.3 潜心开始威胁建模的检查列表 19

1.4 小结 20

第2章 威胁建模策略 21

2.1 “你的威胁模型是什么样？” 21

2.2 集体研讨 22

2.2.1 集体研讨的变种方法 23

2.2.2 文献检索 24

2.2.3 集体研讨方法的观点 25

2.3 系统的威胁建模方法 25

2.3.1 关注资产 27

2.3.2 关注攻击者 29

2.3.3 关注软件 30

2.4 软件模型 31

2.4.1 图表类型 32

2.4.2 数据流图 32

2.4.3 信任边界 36

2.4.4 图表中包含的内容 37

2.4.5 复杂图 38

2.4.6 图的标签 38

2.4.7 图中的颜色 39

2.4.8 入口点 39

2.4.9 表验证 39

2.5 小结 41

第二部分 发现威胁

第3章 STRIDE方法 45

3.1 理解STRIDE方法及其为何有用 45

3.2 假冒威胁 47

3.2.1 在同一台机器上假冒一个进程或文件 48

3.2.2 假冒一台机器 48

3.2.3 人员假冒 48

3.3 篡改威胁 49

3.3.1 篡改文件 49

3.3.2 篡改内存 49

3.3.3 篡改网络 50

3.4 否认威胁 50

3.4.1 攻击日志 50

- 3.4.2 否认一种行为 51
- 3.5 信息泄露威胁 51
 - 3.5.1 进程信息泄露 52
 - 3.5.2 数据存储信息泄露 52
 - 3.5.3 数据流中的信息泄露 52
- 3.6 拒绝服务威胁 53
- 3.7 权限提升威胁 53
 - 3.7.1 通过崩溃进程提升权限 53
 - 3.7.2 通过授权失效提升权限 54
- 3.8 扩展示例：针对Acme-DB的STRIDE威胁 54
- 3.9 STRIDE变种 56
 - 3.9.1 STRIDE-per-Element 56
 - 3.9.2 STRIDE-per-Interaction 58
 - 3.9.3 DESIST方法 61
- 3.10 准出条件 61
- 3.11 小结 62
- 第4章 攻击树 63
 - 4.1 使用攻击树 63
 - 4.1.1 利用攻击树寻找威胁 64
 - 4.1.2 创建新的攻击树 64
 - 4.2 展现一个攻击树 66
 - 4.2.1 人类可识别的表现形式 66
 - 4.2.2 结构化的表示法 70
 - 4.3 攻击树示例 70
 - 4.4 真实的攻击树 71
 - 4.4.1 诈骗攻击树 71
 - 4.4.2 选举操作评估威胁树 73
 - 4.4.3 思维导图 73
 - 4.5 有关攻击树的观点 75
 - 4.6 小结 75
- 第5章 攻击库 76
 - 5.1 攻击库属性 76
 - 5.1.1 攻击库及检查列表 77
 - 5.1.2 攻击库与文档检查 78
 - 5.2 CAPEC 78
 - 5.2.1 准出条件 80
 - 5.2.2 有关CAPEC的观点 81
 - 5.3 OWASP前十名 81
 - 5.4 小结 82
- 第6章 隐私工具 83
 - 6.1 Solove的隐私分类 84
 - 6.2 互联网协议的隐私考虑 85
 - 6.3 隐私影响评估 86
 - 6.4 Nymity Slider和隐私棘轮 86
 - 6.5 语境完整性 88
 - 6.5.1 语境完整性启发式决策 88
 - 6.5.2 扩大的语境完整性启发法 89
 - 6.5.3 有关语境完整性的观点 89
 - 6.6 LINDDUN助记符 90

6.7 小结 91

第三部分 管理和解决威胁

第7章 处理和管理威胁 95

7.1 开始威胁建模项目 95

7.1.1 何时开始威胁建模 95

7.1.2 从哪里开始和（计划）在哪结束 97

7.1.3 从哪里入手 97

7.2 深入分析减缓方法 99

7.2.1 减缓顺序 99

7.2.2 下棋 100

7.2.3 目标优选 100

7.2.4 逃避熊的袭击 100

7.3 利用表格和列表跟踪 101

7.3.1 追踪威胁 101

7.3.2 建立假设 103

7.3.3 外部安全注解 103

7.4 威胁建模的特定场景元素 105

7.4.1 客户/供应商信任边界 105

7.4.2 新技术 105

7.4.3 对API威胁建模 107

7.5 小结 108

第8章 防御策略及技术 109

8.1 减缓威胁的策略及技术 109

8.1.1 认证：减缓欺骗威胁 110

8.1.2 完整性：减缓篡改威胁 111

8.1.3 不可否认性：减缓否认威胁 113

8.1.4 机密性：减缓信息暴露威胁 115

8.1.5 可用性：减缓拒绝服务威胁 117

8.1.6 授权：减缓权限提升威胁 118

8.1.7 策略和技术陷阱 119

8.2 利用模式解决威胁 120

8.2.1 标准部署 120

8.2.2 解决CAPEC威胁 120

8.3 减缓隐私威胁 120

8.3.1 最小化 120

8.3.2 加密 121

8.3.3 遵从性和政策 123

8.4 小结 123

第9章 解决威胁时的权衡 125

9.1 风险管理的经典策略 125

9.1.1 回避风险 126

9.1.2 解决风险 126

9.1.3 接受风险 126

9.1.4 转移风险 126

9.1.5 忽略风险 127

9.2 为风险管理选择减缓措施 127

9.2.1 改变设计 127

9.2.2 应用标准减缓技术 130

9.2.3 设计定制的减缓措施 132

- 9.2.4 模糊编码不是减缓威胁措施 132
- 9.3 针对特定威胁的优先级方法 133
 - 9.3.1 简单方法 133
 - 9.3.2 利用错误栏威胁排序 134
 - 9.3.3 成本估算方法 135
- 9.4 通过接受风险来减缓威胁 138
- 9.5 减缓策略中的军备竞赛 139
- 9.6 小结 139
- 第10章 验证威胁是否已解决 141
 - 10.1 测试威胁减缓 142
 - 10.1.1 测试过程完整性 142
 - 10.1.2 如何测试减缓 142
 - 10.1.3 渗透测试 143
 - 10.2 检查你获取的代码 143
 - 10.2.1 构建软件模型 144
 - 10.2.2 利用软件模型 145
 - 10.3 问答式威胁建模 145
 - 10.3.1 模型/现实一致性 146
 - 10.3.2 任务和过程的完成 146
 - 10.3.3 漏洞检查 146
 - 10.4 解决威胁的过程各方面 147
 - 10.4.1 威胁建模授权测试；测试授权威胁建模 147
 - 10.4.2 验证/转换 147
 - 10.4.3 操作过程中记录假设 148
 - 10.5 表格与列表 148
 - 10.6 小结 150
- 第11章 威胁建模工具 151
 - 11.1 通用工具 151
 - 11.1.1 白板 151
 - 11.1.2 办公套件 152
 - 11.1.3 漏洞跟踪系统 152
 - 11.2 开放源代码工具 153
 - 11.2.1 TRIKE 153
 - 11.2.2 SeaMonster 153
 - 11.2.3 权限提升纸牌游戏 153
 - 11.3 商业工具 154
 - 11.3.1 Threat Modeler 155
 - 11.3.2 Corporate Threat Modeller 155
 - 11.3.3 SecurITree 155
 - 11.3.4 Little-JIL 155
 - 11.3.5 微软的SDL威胁建模工具 155
 - 11.4 尚不存在的工具 158
 - 11.5 小结 159
- 第四部分 科技和棘手领域的威胁建模
- 第12章 需求手册 163
 - 12.1 为何需要“手册” 163
 - 12.2 需求、威胁、减缓威胁之间相互作用 164
 - 12.3 商业需求 165

- 12.3.1 优于竞争 165
- 12.3.2 产业需求 165
- 12.3.3 场景驱动的需求 166
- 12.4 防御/检测/响应需求框架 166
 - 12.4.1 防御 166
 - 12.4.2 检测 168
 - 12.4.3 响应 169
- 12.5 人员/过程/技术作为需求的框架 170
 - 12.5.1 人员 170
 - 12.5.2 过程 170
 - 12.5.3 技术 170
- 12.6 开发需求与采购需求 171
- 12.7 合规性驱动的需求 171
 - 12.7.1 云服务安全联盟 171
 - 12.7.2 NISTPublication200 172
 - 12.7.3 支付卡行业数据安全标准 173
- 12.8 隐私需求 173
 - 12.8.1 公平信息处理条例 173
 - 12.8.2 从设计着手保护隐私 174
 - 12.8.3 身份识别七法则 174
 - 12.8.4 微软开发隐私标准 175
- 12.9 STRIDE需求 175
 - 12.9.1 认证 176
 - 12.9.2 完整性 177
 - 12.9.3 不可否认性 178
 - 12.9.4 机密性 178
 - 12.9.5 可用性 178
 - 12.9.6 授权 178
- 12.10 非需求 179
 - 12.10.1 操作非需求 180
 - 12.10.2 警告和提示 180
 - 12.10.3 微软的“十个不变法则” 180
- 12.11 小结 181
- 第13章 网络与云威胁 182
 - 13.1 网络威胁 182
 - 13.1.1 网站威胁 182
 - 13.1.2 网络浏览器和插件威胁 183
 - 13.2 云租户威胁 184
 - 13.2.1 内部威胁 184
 - 13.2.2 合租威胁 185
 - 13.2.3 合规性威胁 185
 - 13.2.4 法律威胁 185
 - 13.2.5 电子取证响应威胁 186
 - 13.2.6 各种各样的威胁 186
 - 13.3 云供应者威胁 186
 - 13.3.1 直接来自租户的威胁 186
 - 13.3.2 租户行为导致的威胁 187
 - 13.4 移动威胁 187
 - 13.5 小结 188

- 第14章 账户与身份识别 189
 - 14.1 账户生命周期 190
 - 14.1.1 创建账户 190
 - 14.1.2 账户维护 192
 - 14.1.3 账户终止 192
 - 14.1.4 账户生命周期检查列表 193
 - 14.2 认证 193
 - 14.2.1 登录 194
 - 14.2.2 登录失败 195
 - 14.2.3 对于“你所拥有的”威胁 197
 - 14.2.4 对“你是谁”的威胁 197
 - 14.2.5 对“你所知道的”威胁 199
 - 14.2.6 认证检查列表 202
 - 14.3 账户恢复 202
 - 14.3.1 时间和账户恢复 203
 - 14.3.2 账户恢复邮件 204
 - 14.3.3 基于知识的认证 204
 - 14.3.4 社会认证 207
 - 14.3.5 账户恢复的攻击者驱动分析 208
 - 14.3.6 多渠道认证 209
 - 14.3.7 账户恢复检查列表 209
 - 14.4 姓名、ID和SSN 210
 - 14.4.1 姓名 210
 - 14.4.2 身份证明文件 212
 - 14.4.3 社保号及其他国家身份识别号 213
 - 14.4.4 身份盗用 215
 - 14.4.5 姓名、ID及SSN检查列表 215
 - 14.5 小结 216
- 第15章 人类因素与可用性 217
 - 15.1 人的模型 218
 - 15.1.1 应用人的行为模型 218
 - 15.1.2 人的模型认知科学 220
 - 15.1.3 人的启发式模型 223
 - 15.2 软件情景模型 225
 - 15.2.1 对软件进行建模 225
 - 15.2.2 软件模型的图表 227
 - 15.2.3 对电子社会工程攻击的建模 229
 - 15.3 威胁引出技术 229
 - 15.3.1 集体研讨 230
 - 15.3.2 威胁建模的仪式方法 230
 - 15.3.3 仪式分析启发式 230
 - 15.3.4 将可用性融于四步框架 233
 - 15.4 解决人类因素的工具和技术 233
 - 15.4.1 抑制人类因素作用的谬见 233
 - 15.4.2 良好的设计决策模型 234
 - 15.4.3 良好学习环境的设计模型 236
 - 15.5 用户界面工具和技术 237
 - 15.5.1 配置 237
 - 15.5.2 显式警示 238

- 15.5.3 吸引注意力的模型 239
- 15.6 测试人类因素 240
 - 15.6.1 良好和恶劣的情景 240
 - 15.6.2 生态有效性 241
- 15.7 有关可用性与仪式的观点 242
- 15.8 小结 243
- 第16章 密码系统威胁 244
 - 16.1 密码原语 245
 - 16.1.1 基本原语 245
 - 16.1.2 隐私原语 248
 - 16.1.3 现代加密原语 248
 - 16.2 典型威胁角色 250
 - 16.3 针对密码系统的攻击 251
 - 16.4 用密码创建 253
 - 16.4.1 做决定 253
 - 16.4.2 准备升级 254
 - 16.4.3 密钥管理 254
 - 16.4.4 解密之前验证 255
 - 16.5 关于密码需要记住的事情 255
 - 16.5.1 使用专业人士设计的密码系统 255
 - 16.5.2 用专业人士创建或测试的密码代码 255
 - 16.5.3 密码不是安全魔尘 256
 - 16.5.4 假设都会公开 256
 - 16.5.5 你仍需要管理密钥 256
 - 16.6 加密系统：Kerckhoffs及其原则 256
 - 16.7 小结 257
- 第五部分 更上一层楼
- 第17章 将威胁建模带到你的组织机构中 261
 - 17.1 如何引入威胁建模 262
 - 17.1.1 说服个体贡献者 263
 - 17.1.2 说服管理层 263
 - 17.2 谁做什么 264
 - 17.2.1 威胁建模与项目管理 264
 - 17.2.2 先决条件 265
 - 17.2.3 可交付物 265
 - 17.2.4 个体角色及责任 266
 - 17.2.5 小组交互 267
 - 17.2.6 威胁建模团队的多样化 270
 - 17.3 在开发生命周期中的威胁建模 270
 - 17.3.1 开发过程问题 270
 - 17.3.2 组织问题 275
 - 17.3.3 为你的组织机构定制一个过程 278
 - 17.4 克服对威胁建模的反对声音 279
 - 17.4.1 对资源的反对声音 279
 - 17.4.2 价值反对声音 280
 - 17.4.3 对计划的反对声音 281
 - 17.5 小结 281
- 第18章 试验方法 283
 - 18.1 查看缝隙 283

18.2	操作威胁模型	285
18.2.1	FlipIT	285
18.2.2	杀戮链	285
18.3	“宽街”分类法	288
18.4	博弈机器学习	293
18.5	对一家企业进行威胁建模	293
18.6	针对威胁建模方法的威胁	294
18.6.1	危险可交付物	294
18.6.2	危险方法	295
18.7	如何实验	297
18.7.1	明确问题	297
18.7.2	寻找要衡量的方面，进行衡量	297
18.7.3	研究你的结果	298
18.8	小结	298
第19章	成功的设计	299
19.1	理解流程	299
19.1.1	流程与威胁建模	300
19.1.2	妨碍人们	302
19.1.3	注意认知负荷	302
19.1.4	避免创造者失明	302
19.1.5	资产与攻击者	303
19.2	了解参与者	303
19.3	边界对象	304
19.4	“最好”是“好”的敌人	305
19.5	展望未来	306
19.5.1	“威胁模型改变了”	306
19.5.2	有关艺术性	307
19.6	小结	308
附录A	有用的工具	309
附录B	威胁树	315
附录C	攻击者列表	349
附录D	权限提升纸牌游戏	365
附录E	案例研究	372
	术语表	388

精彩短评

1、一般

《威胁建模》

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