软 件 安 全 测 评

北京邮电大学计算机学院
信息安全系
张淼

火龙果•整理
uml.org.cn

第三讲 安全威胁建模

- 威胁建模的基本概念
- 威胁模型建立的过程

火龙果•整理
uml.org.cn

威胁建模的基本观点

- 威胁建模的基本观点是:

  直到理解了所受的威胁之后才能创建安全的系统

火龙果•整理
uml.org.cn

威胁建模

- 什么是威胁建模?

威胁模型是一种基于安全的分析,有助于人们确定给产品造成的最高安全级别的安全风险,以及攻击是如何表现出来的,其目标是确定需要缓和哪些威胁,如何来缓和这些威胁.

威胁建模的重点是以一种相对正式的方式来考虑应用程序的安全性,关于威胁有很多信息,但是威胁建模却少有涉及,创建威胁模型必须认识到产品的什么地方最为危险,因而会选择合适的技术来缓和威胁,这样就使得系统更加安全.

火龙果•整理
uml.org.cn

威胁建模

- 进行威胁建模还有其他作用:
  - 威胁模型有助于更好的理解你的应用程序,因为你花时间以一种相对结构化的方式分析了应用程序的组成
  - 威胁模型可以帮助你测试应用程序查找bug
  - 可能会通过威胁模型发现其他方式不能发现的复杂bug,它们通常是由几个小故障结合而成的大灾难.
  - 威胁模型可以帮助新的小组成员理解应用程序的细节,它可能成为加速学习曲线的工具
  - 威胁模型能帮助测试人员进行测试,有助于产生设计良好的安全测试计划和产品

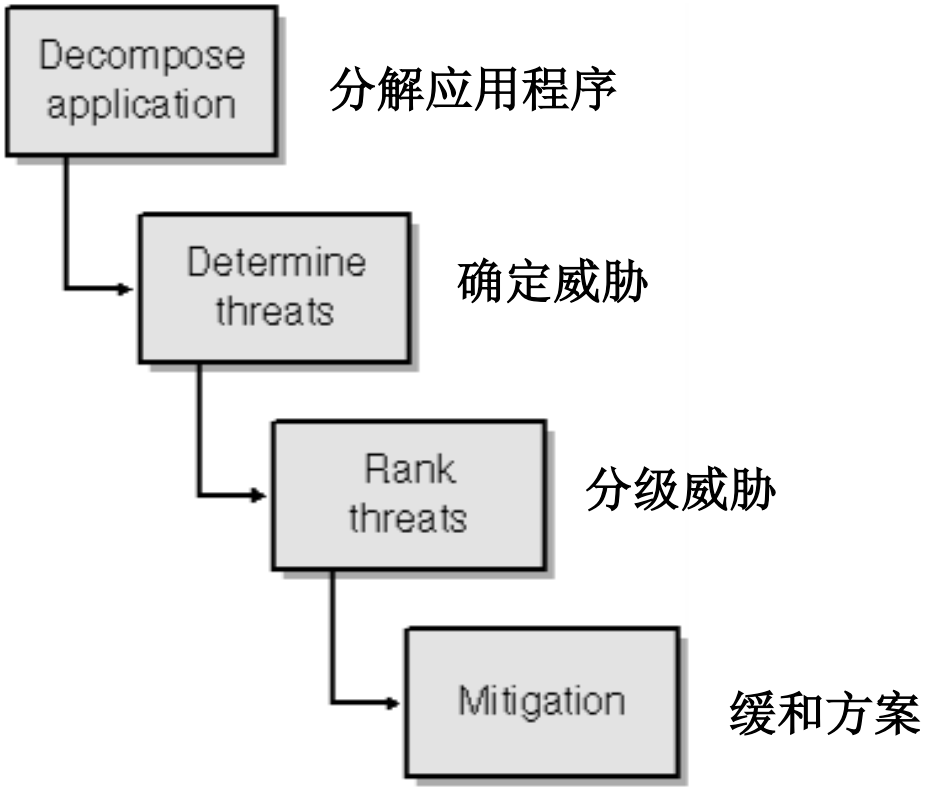
火龙果•整理
uml.org.cn

威胁模型建立过程

- 1) 成立威胁模型小组
- 2) 分解应用程序
- 3) 确定系统所面临的威胁
- 4) 以风险递减的方式给威胁排序
- 5) 选择应付威胁的方法
- 6) 选择缓和威胁的技术
- 7) 从确定下来的技术中选择适当的技术

火龙果•整理
uml.org.cn

威胁模型建立过程



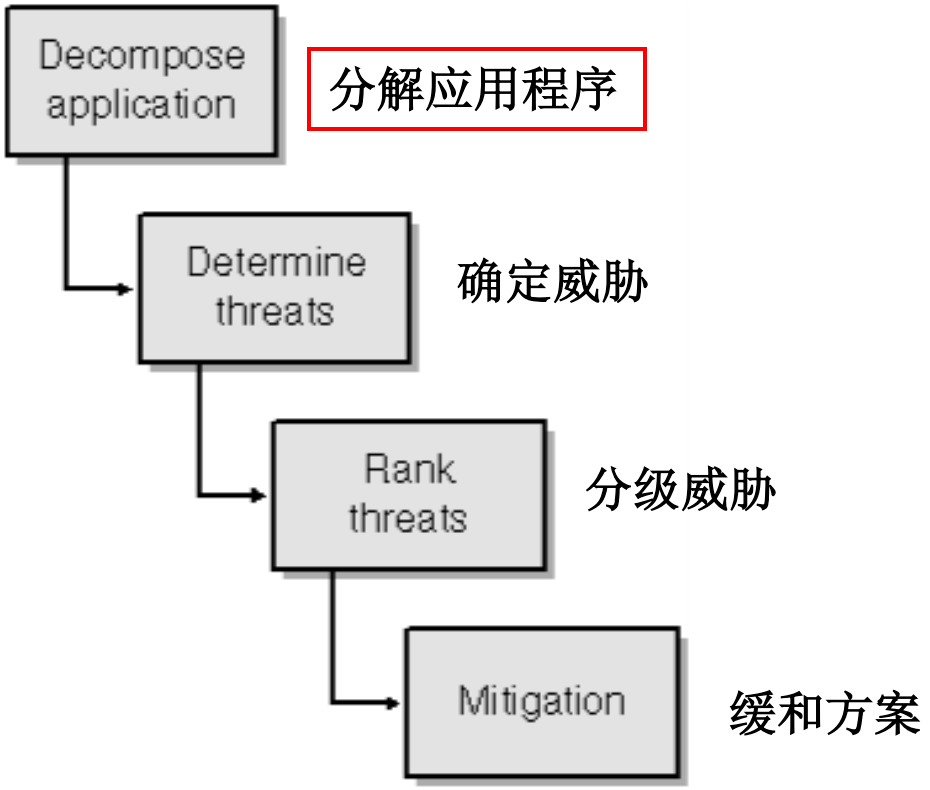
火龙果•整理
uml.org.cn

成立威胁建模小组

- 第一步是从产品小组中聚集一些人进行初步的威胁分析过程。
  - 确保每一个开发部门都至少有一个成员参加讨论，包括设计、编程、测试和文档部门。
  - 会议的目标不是解决问题,而是标识出应用程序的组成部分,之间如何交互,找到尽可能多的安全威胁

火龙果•整理
uml.org.cn

分解应用程序



火龙果•整理
uml.org.cn

分解应用程序

- 成功的威胁建模需要一种更结构化的方法，而不是简单的”想象威胁”。
- 对应用程序进行形式化分解
  - DFD (Data Flow Diagram)是威胁分解的一种形式化分解技术，能将应用程序分解为几个关键部分。
  - 统一建模语言UML，特别是活动图，非常适合记录过程，其方式和DFD相似。
  - UML活动图致力于过程之间的控制流，而DFD则是过程间的数据流。

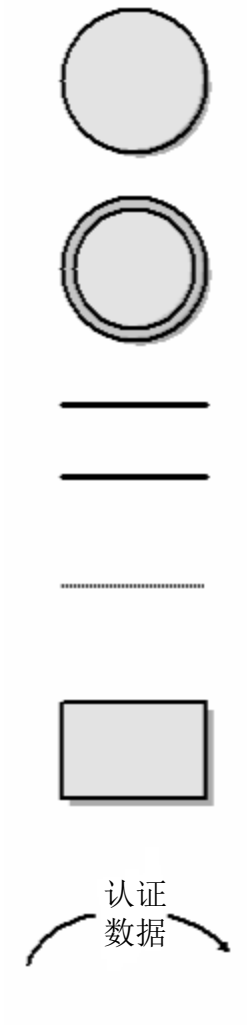
火龙果•整理
uml.org.cn

DFD:Data Flow Diagram 数据流图

- 数据流图（Data Flow Diagram，DFD）是一种能全面地描述信息系统逻辑模型的主要工具，它可以用少数几种符号综合地反映出信息在系统中的流动、处理和存储情况。
- 分类
  - 一种是以方框、连线及其变形为基本图例符号来表示数据流动过程。
  - 一种是以圆圈及连接弧线作为其基本符号来表示数据流动过程。
  - 这两种方法实际表示一个数据流程的时候，大同小异，但是针对不同的数据处理流程却各有特点。

火龙果•整理
uml.org.cn

DFD中的关键数据流图符号



一个过程
转换或操作数据

多个过程
转换或操作数据

数据存储
存储临时数据或永久数据的地点

边界
机器,物理,地址空间或信任边界

交互者
向系统输入

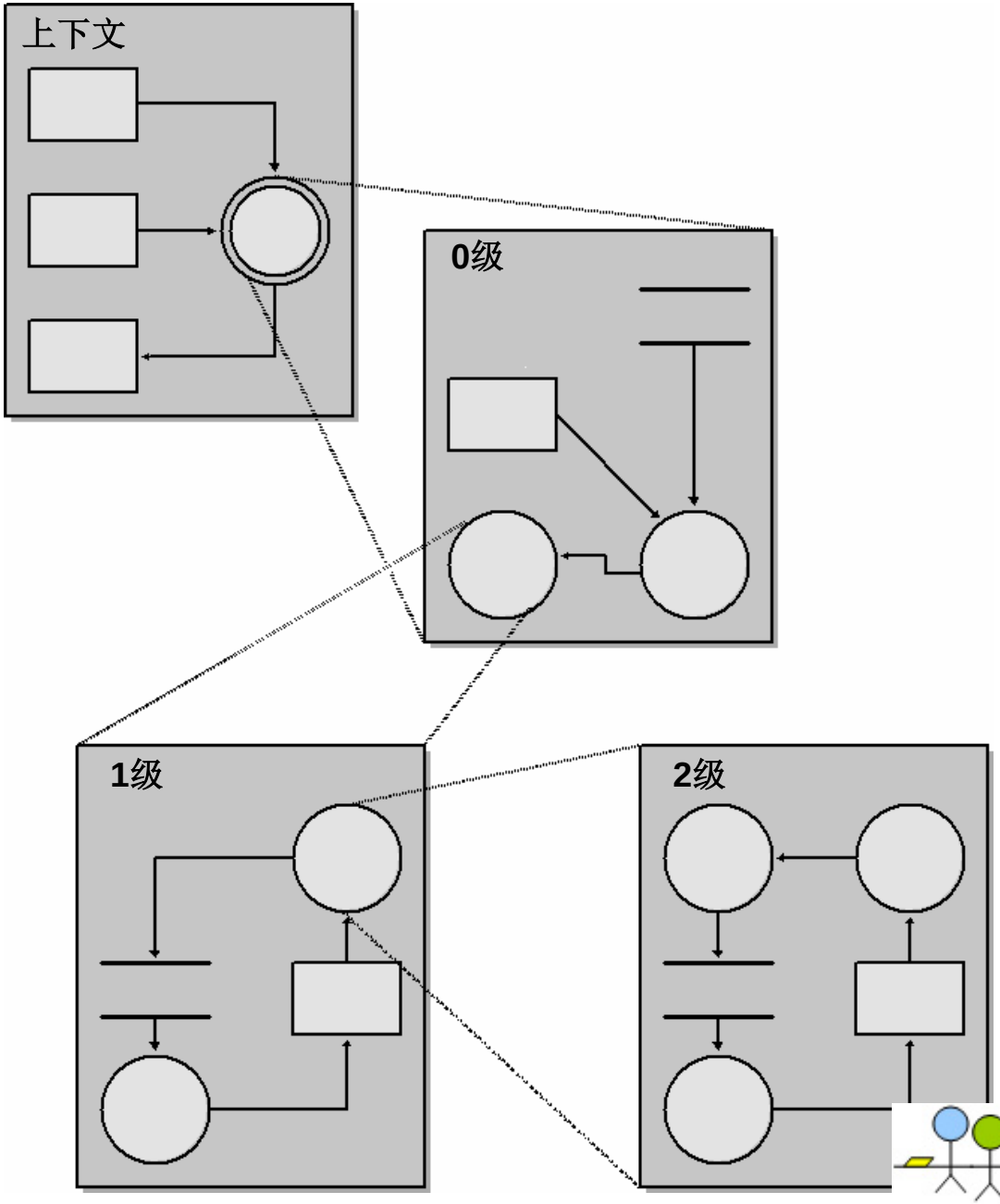
数据流
描述来自数据存储,过程或交互者的数据流

火龙果•整理
uml.org.cn

分解应用程序

- 分解的第一步是确定要分析的应用程序的边界或作用范围,并了解可信任部分与不可信任部分之间的边界,DFD使用一个高级上下文图表定义应用程序的可达范围
- 上下文图表只有一个过程,通常没有数据存储,使用0级图表,1级图表,2级图表,如图所示

火龙果•整理
uml.org.cn

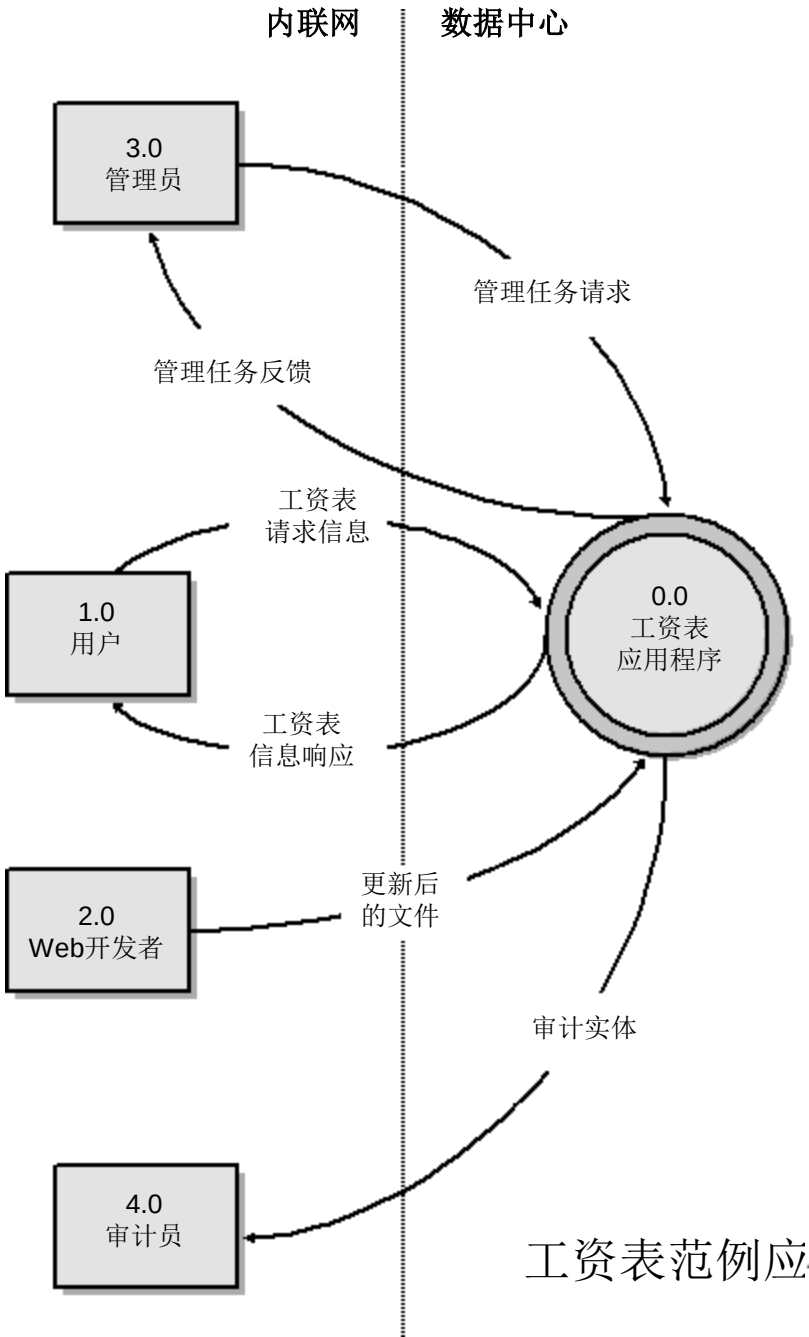


火龙果•整理
uml.org.cn

分解应用程序

- 撇开DFD理论不讲,我们先从一个范例应用程序开始,我们使用简化的基于Web的工资表应用程序

火龙果•整理
uml.org.cn



工资表范例应

火龙果•整理
uml.org.cn

分解应用程序

- 定义DFD的作用范围是,请考虑以下几点:
  - 忽略应用程序的内部工作方式
    - 工作方式无关紧要，要定义作用范围而非功能细节
  - 哪些事情和请求是系统必须响应的?
    - 例如，工资表应用程序应接收工资表信息请求
  - 程序将产生什么响应?
    - 例如，工资表应用程序应提供工资表信息响应
  - 标识出每次请求和响应相关的数据源
    - 有些是永久性的（文件、注册表、数据库等）
    - 有些是短期或暂时的（缓存数据）
  - 确定每次响应的接受者

下面将前面的DFD图表进行分解,进入1级图表

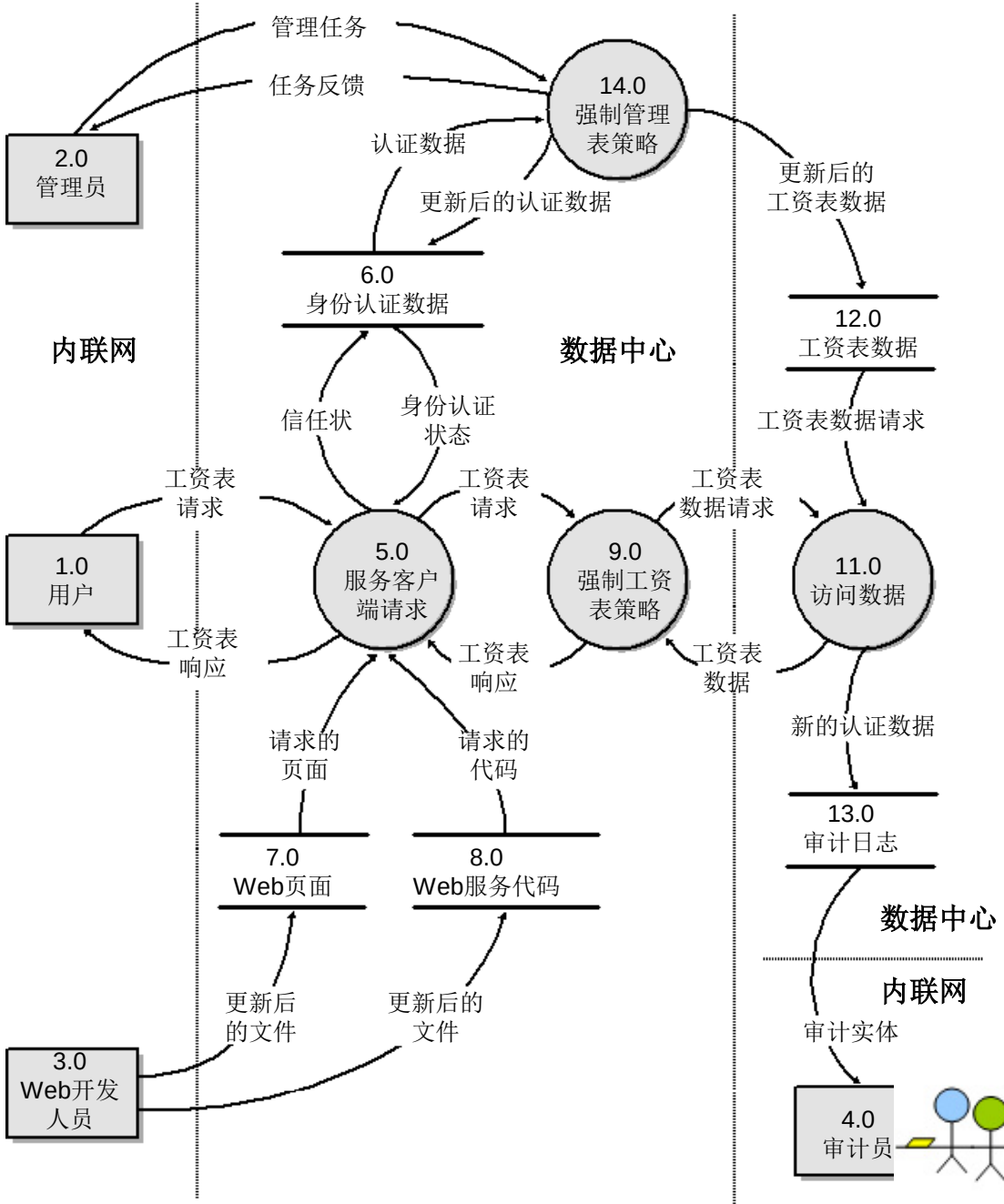
火龙果•整理
uml.org.cn

分解应用程序

- 这里有一些在DFD中创建和命名实体时遵循的简单规则:
  - 一个过程必须至少有一个数据流流入和一个数据流流出
  - 所有的数据流都从某个过程开始,到某个过程结束
  - 数据存储通过数据流与过程相连
  - 数据存储之间不能连接,他们必须通过过程相连

下面将前面的DFD图表进行分解,进入1级图表

火龙果•整理
uml.org.cn



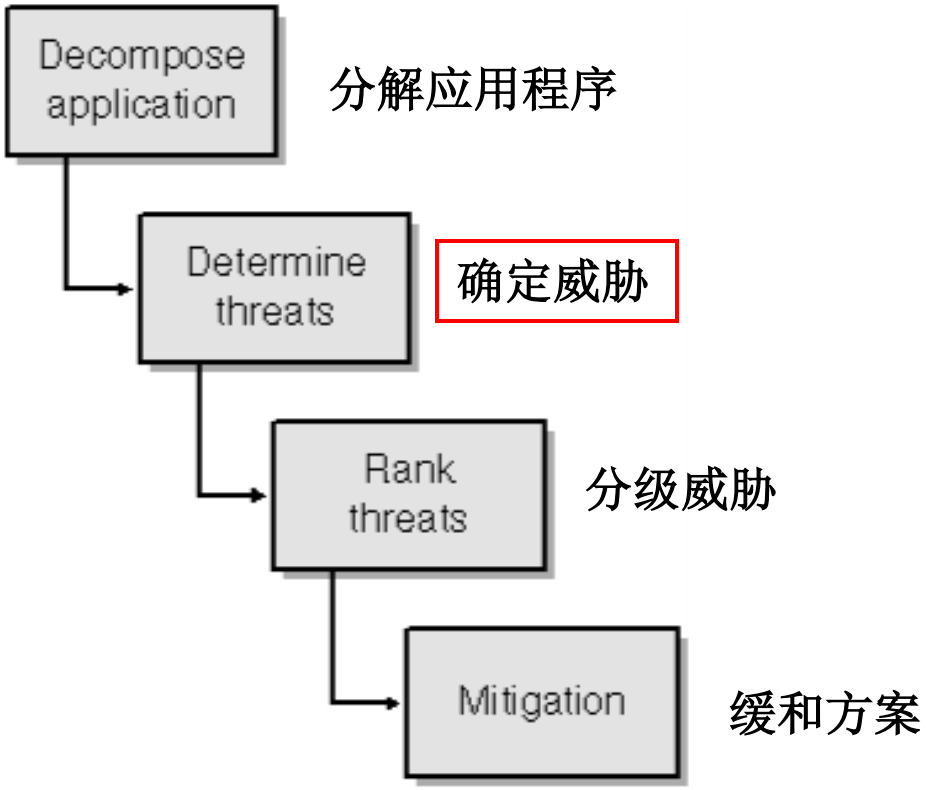
火龙果•整理
uml.org.cn

分解应用程序

最后,你会深刻理解应用程序的各个组成部分,一般来讲,如果只是进行威胁建模,那么应当只需深入到两级,三级或者四级,原则是,只要深入到足够理解你所受到的威胁就行.

火龙果•整理
uml.org.cn

确定威胁



火龙果•整理
uml.org.cn

确定系统所面临的威胁

- 1 使用STRIDE给威胁分类
  - 提出一些安全相关的问题，如
    - 未经认证的用户能否浏览秘密的网络数据？
    - 不可信任的用户能否修改数据库中患者的记录数据？
    - 是否有人能够拒绝合法用户获得应用程序的服务?
    - 是否有人能够利用某些特性或组件将自己的特权提升为管理员?

火龙果•整理
uml.org.cn

确定系统所面临的威胁

为了有助于回答这些问题,我们使用STRIDE威胁模型,它是下面这六种威胁类型的英文首字母的缩写:

- 身份欺骗 Spoofing identity
- 篡改数据 Tampering with data
- 抵赖 Repudiation
- 信息泄露 Information disclosure
- 拒绝服务 Denial of service , DoS
- 特权提升 Elevation of privilege

火龙果•整理
uml.org.cn

身份欺骗 Spoofing identity

身份欺骗允许攻击者冒充另一个用户,或者允许恶意服务器冒充合法服务器,用户身份欺骗的一个例子是非法访问,然后使用另一个用户的认证信息,例如用户名或口令.

举一个现实的例子,比如不安全的认证技术,像HTTP认证:基本的摘要访问认证(RFC2671).如果Fletcher可以在HTTP认证头里看到Blake的用户名和口令,他就可以使用此用户名和口令访问受保护的数据,如同他就是Blake.

服务器欺骗的例子包括DNS欺骗和”DNS缓存中毒”(DNS cache poisoning).

火龙果•整理
uml.org.cn

篡改数据 Tampering with data

数据篡改包括有恶意的修改数据.

这样的例子包括在未授权的情况下,修改永久性的数据,例如数据库中的数据,以及当数据通过一个开放网络(如因特网)在两台计算机直接传输时,更改数据.

现实的例子包括改变目标计算机中以弱ACL保护的文件数据,如Everyone用户的完全控制权限.

火龙果•整理
uml.org.cn

抵赖 Repudiation

与抵赖威胁相关的是用户拒绝承认从事过的一项活动,并且其他方面没有任何办法可以证明他是在抵赖.

例如,一名用户在系统中做了非法的操作,这个系统有缺少跟踪被禁止操作的能力。防抵赖(Nonrepudiation)是系统对抗否认威胁的能力,就像如果用户购买了一件商品,他必须在收据上签字,厂商就可以用这个签了字的收据来证明用户确实收到了包裹,可以想象,对于电子商务应用程序来说,认可是极其重要的.

火龙果•整理
uml.org.cn

信息泄露 Information disclosure

信息泄露威胁包括,信息被暴露给不允许对它访问的人.

例如,用户可以读到非授权访问权限的文件,入侵者可以读到在两台计算机之间传输的数据,前面讲到的欺骗的例子也是一个信息泄露的例子,因为要重放Blake的证书,Fletcher必须首先看到证书.

火龙果•整理
uml.org.cn

拒绝服务 Denial of service , DoS

拒绝服务攻击将拒绝对合法用户的服务.

例如,使Web服务器暂时不可用或无法使用,你必须提高系统的可用性和可靠性,来防止受到某些类型的DoS威胁,关于拒绝服务的非常真实的例子包括各种分布式拒绝服务攻击(DDoS),如Trinoo和Stacheldraht.

火龙果•整理
uml.org.cn

特权提升 Elevation of privilege

在这种类型的威胁下,一名没有特权的用户获得访问特权,从而有足够的能力损坏或摧毁整个系统,特权提升威胁包括这样的情况,一名攻击者已经有效的穿透了所有的防御系统,并且成为了受信任的系统自身的一部分,这确实是一个非常危险的状态.

举个例子:一个脆弱的计算机系统允许攻击者将可以执行代码放置在磁盘上,并等待下一个人登录系统,如果下一个用户是管理员,那么这些恶意代码也就会以管理员身份运行.

火龙果•整理
uml.org.cn

确定系统所面临的威胁

- 2 建立威胁树
  - 建立威胁树，系统地分析所开发的应用程序中的威胁和漏洞。
  - 众所周知，在硬件领域中有种识别可能故障模式的方法，成为“故障树”，同样的方法也适用于计算机系统领域的安全问题。
  - 威胁树的思想是， 应用程序是有威胁目标组成的，每个目标都有漏洞，任一漏洞受到攻击都可能破坏整个系统。威胁树描述了攻击者破坏各组件所经历的决策过程。

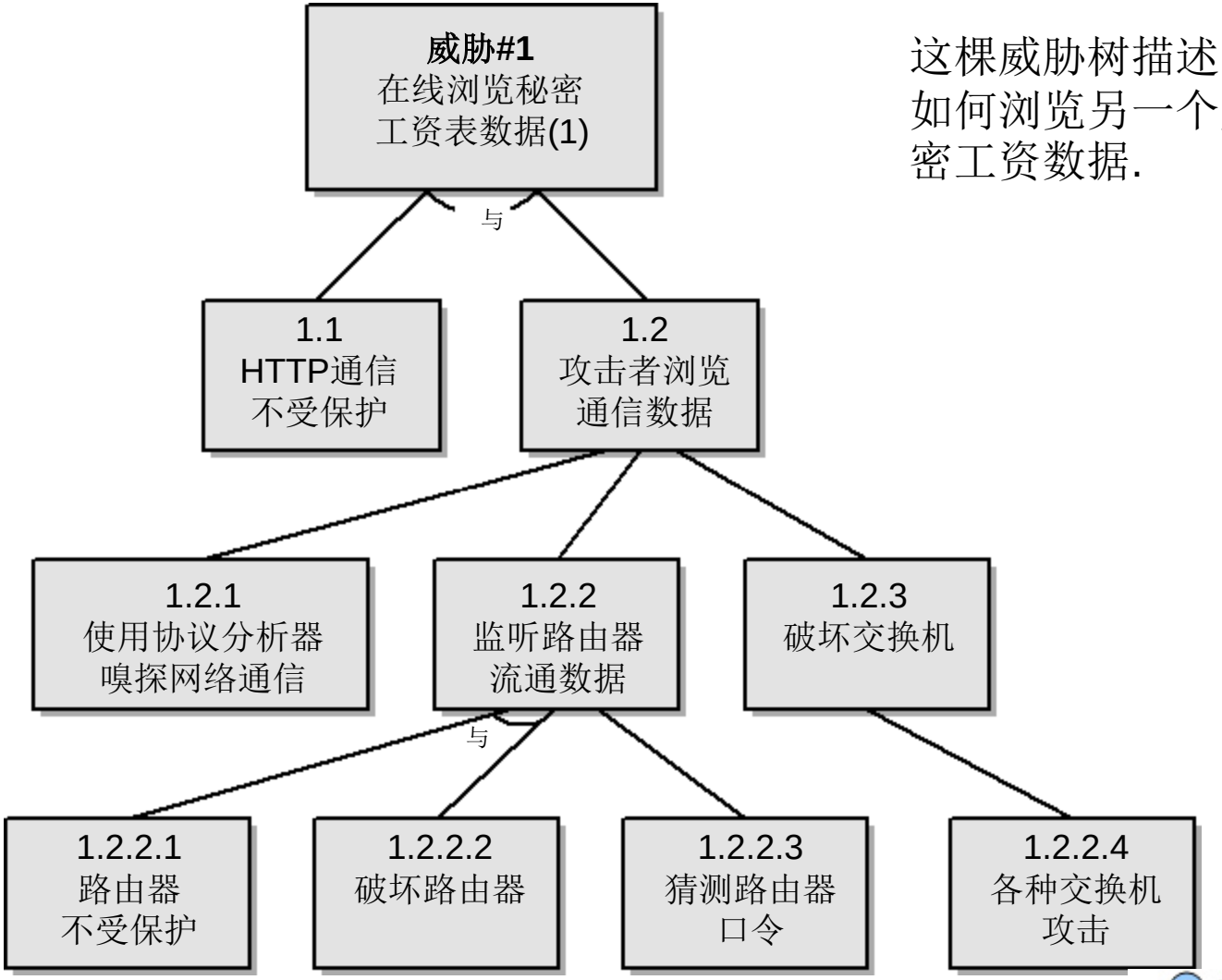
火龙果•整理
uml.org.cn

工资表范例中的流图

- 用户的工资数据是从WEB服务器计算机传向职工的计算机的。或者说是从服务客户过程传输的
- 工资信息是保密的，这意味着必须保护工资数据。
- 存在信息泄露的可能，具体威胁见下图。

火龙果•整理
uml.org.cn

简单威胁树的示例



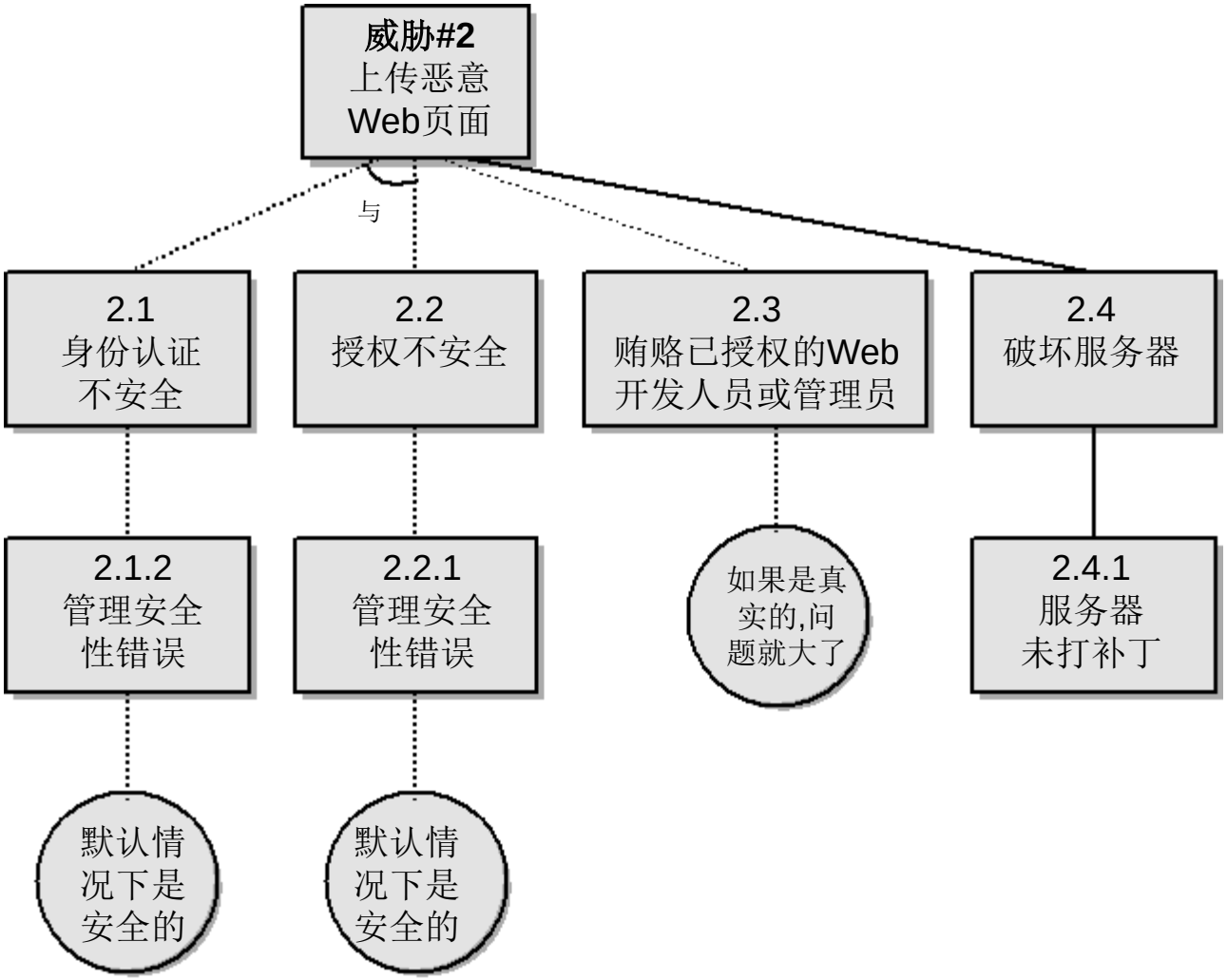
这棵威胁树描述了攻击者如何浏览另一个用户的秘密工资数据.

火龙果•整理
uml.org.cn

增加威胁树的可读性

- 可以向威胁树添加几个附件，显示最有可能的攻击向量。
- 用虚线表示最不可能的攻击点
- 用实线表示最可能的攻击点
- 在最不可能的攻击节点下放置圆圈，说明攻击为什么会减弱。

火龙果•整理
uml.org.cn



火龙果•整理
uml.org.cn

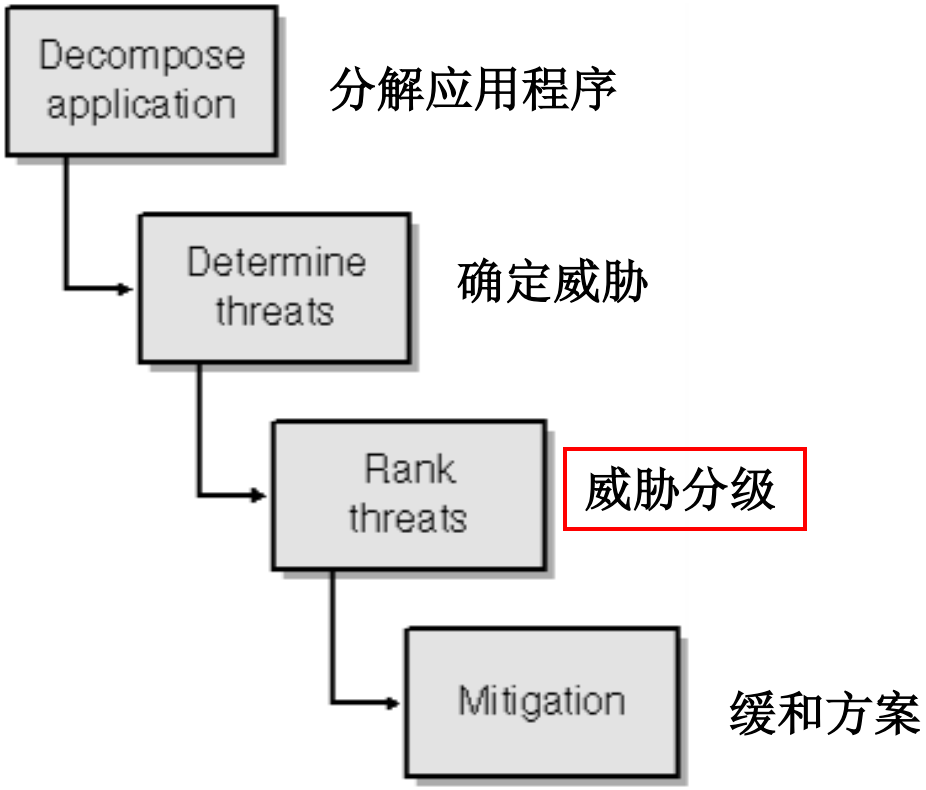
确定系统所面临的威胁

3 威胁建模需要记录的项目

项目	注释
标题	用适当的语言来描述,但是不要说得太多,威胁应该能从标题上明显地看出来,例如,”攻击者访问用户的购物车”
威胁目标	应用程序的那一部分容易受到攻击?例如,在工资表范例应用程序中,威胁目标包括工资请求数据流以及执行管理员策略的过程
威胁类型	基于STRIDE模型来记录威胁的类型,我们已经看到,一个威胁可以属于多个STRIDE类型
风险	用你喜欢的方式来计算风险,要确保一致.
攻击树	攻击者如何表示威胁呢?保持攻击树的简单性,如果太过深入,肯定会迷失方向
缓和技术(可选)	如何缓和威胁呢?如果已经使用了某种缓和技术,就记录下来,否则,进行下一个威胁,记住,建模过程并不是在试图解决问题,也应该记住要缓和威胁是困难的,有些问题要比其他问题容易缓和,
缓和状态	威胁已经被缓和了吗?回答这个问题的有效选择是:是,否,稍微缓和,以及需要继续研究
Bug数量(可选)	如果你再使用一个跟踪bug的数据库,那么就要跟踪bug的数量,请注意你的威胁模型数据库或工具,不应该替代bug数据库,最糟糕的情况就是,关于bug的文档有副本,并且其中一个文档是过期的,在威胁建模过程中,就应该捕获足够多的关于该威胁的信息,并维护你的bug跟踪数据库

火龙果•整理
uml.org.cn

威胁分级



火龙果•整理
uml.org.cn

威胁分级

- 以风险递减的顺序给威胁分级
  - 一种计算威胁风险的简单办法是隐患的危机程度乘以隐患发生的可能性。
  - 风险DREAD = 危机程度 * 发生的可能性
  - 这个数越大,威胁对系统造成的风险就越大,例如,最高的风险是100,它是由最高的危险等级10乘以最高的可能性等级所得

火龙果•整理
uml.org.cn

威胁分级

- 1. 使用DREAD计算风险

与STRIDE威胁模型类似,DREAD是下面短语的首字母缩写:

- 潜在破坏性 Damage potential
- 再现性 Reproducibility
- 可利用性 Exploitability
- 影响用户 Affected users
- 可发现性 Discoverability

火龙果•整理
uml.org.cn

潜在破坏性 Damage potential

破坏会有多严重?

衡量一下威胁可能造成的实际破坏程度,一般最糟糕的程度(10级)是指让攻击者可能绕开所有的安全限制,时间上能做任何的破坏,提升特权的威胁通常是10级,其他的例子与受保护的数据的值有关,医疗,金融,或军事数据通常等级都很高.

火龙果•整理
uml.org.cn

再现性　Reproducibility

让潜在的进攻起作用会有多简单?衡量一下将威胁变为结果的简单性,有些bug总是在起作用(10级),而其他的比如复杂的基于时间的竞争状态,却是不可预测的,可能只会偶尔起作用,同样,默认安装的特性中的安全缺陷具有很高的再现性,高再现性对多数攻击来说都是很重要的.

火龙果•整理
uml.org.cn

可利用性　Exploitability

进行一次攻击需要多少努力和专业知识?

例如,如果一个程序员新手使用一台家庭PC进行攻击就能达到目的,得分就会高达10分,但是如果需要动用大量人力物力进行一次攻击,那么得分可能仅仅为1分,同时,攻击需要的认证和授权也是需要考虑的,如果一个匿名远程用户可以攻击,那么等级为10,而仅仅本地用户且需要强证书才能进行,就具有低得多的可利用性.

火龙果•整理
uml.org.cn

影响用户　Affected users

如果威胁被利用并成为一次攻击,有多少用户受到影响?

这可以用攻击影响的用户百分数来粗略的衡量: 100%-91%为10级一直到10%-0%为1级,尽你所能去估计影响,服务器和客户机的区别是非常重要的,服务器会间接影响一大批客户机,还会潜在的影响其他网络,还需要考虑的是市场大小和用户的绝对数量,而不仅仅是百分数,1亿用户的1%难道还是小数目吗?

火龙果•整理
uml.org.cn

可发现性　Discoverability

这恐怕是最难确定的衡量标准,最好保险且省事的方式就是,假设每一个威胁都是可以被发现的,给每个威胁都定为10级.

火龙果•整理
uml.org.cn

威胁分级

- 通过平均这几个数,我们就可以确定DREAD的级别

威胁#1:恶意用户浏览网络上的秘密工资数据

8　潜在破坏性:读取用户的是由工资数据不是开玩笑的!

10　再现性:这是100%可再现的.

7　可利用性:必须在子网内,或者已经攻破了路由器.

10　影响用户:每个人,包括CEO,都会受此影响!

10　可发现性:我们就假定它会被发现!

风险DREAD : (8+10+7+10+10)/5=9

显然,9是个很严重的等级,意味着这个威胁应该尽快解决!

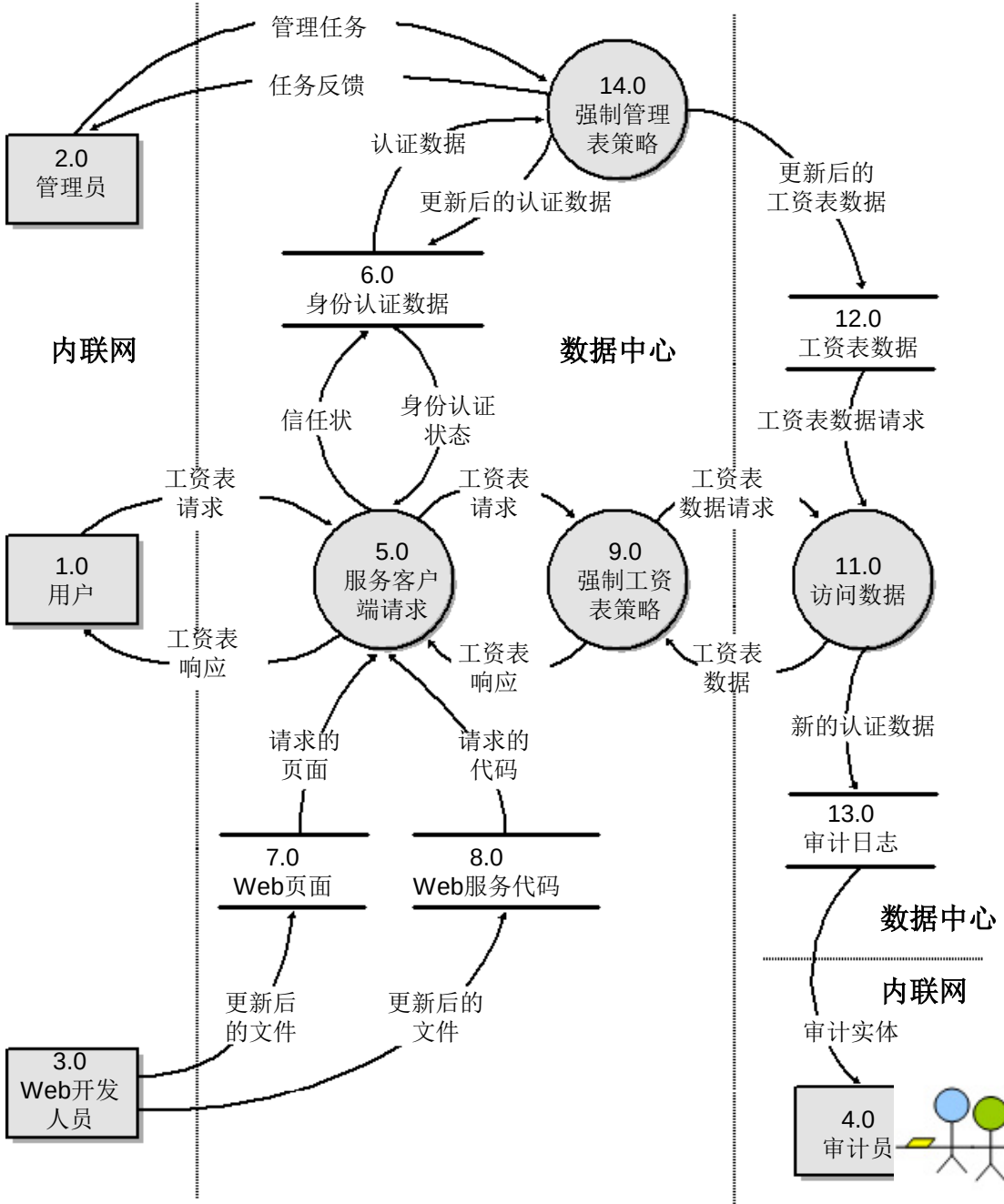
火龙果•整理
uml.org.cn

威胁分级

- 2. 结合分解,威胁树,STRIDE和DREAD
  - 从功能分解上确定威胁目标
  - 使用威胁树确定威胁如何成为隐患
  - 通过STRIDE确定每个部分面临的威胁
  - 使用DREAD对威胁进行分级

下面我们会看到工资表范例应用程序所面临的一些威胁的威胁描述,分级以及威胁树.

火龙果•整理
uml.org.cn



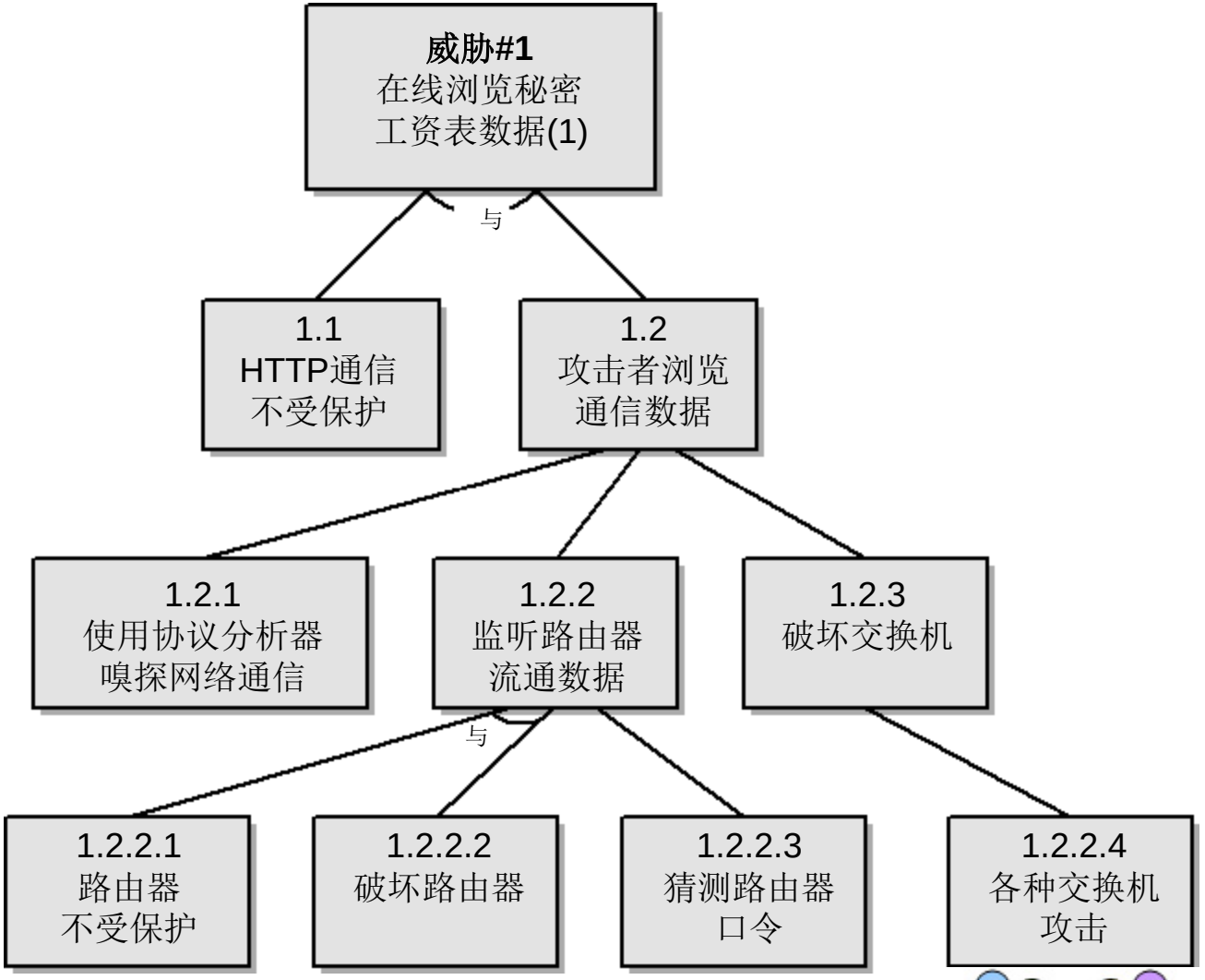
火龙果•整理
uml.org.cn

威胁#1

威胁描述	恶意用户浏览网络上的秘密工资数据
威胁目标	工资表响应(5.0 -> 1.0)
威胁类别	信息泄露
风险	潜在破坏性: 8 可再现性: 10 可利用性: 7 影响用户: 10 可发现性: 10 总计: 9
注释	多数这样的攻击来自使用协议分析器的恶意用户,因为这种攻击很容易进行,这种攻击是被动的,节约时间,精力和财力 对交换机的威胁是很重要的,因为很多人认为交换网络是安全的,不会声道嗅探攻击,而事实并非如此,如果你这样认为,请看一下 http://www.sans.org 的文章 “Why your switched network isn't secure”

火龙果•整理
uml.org.cn

威胁#1



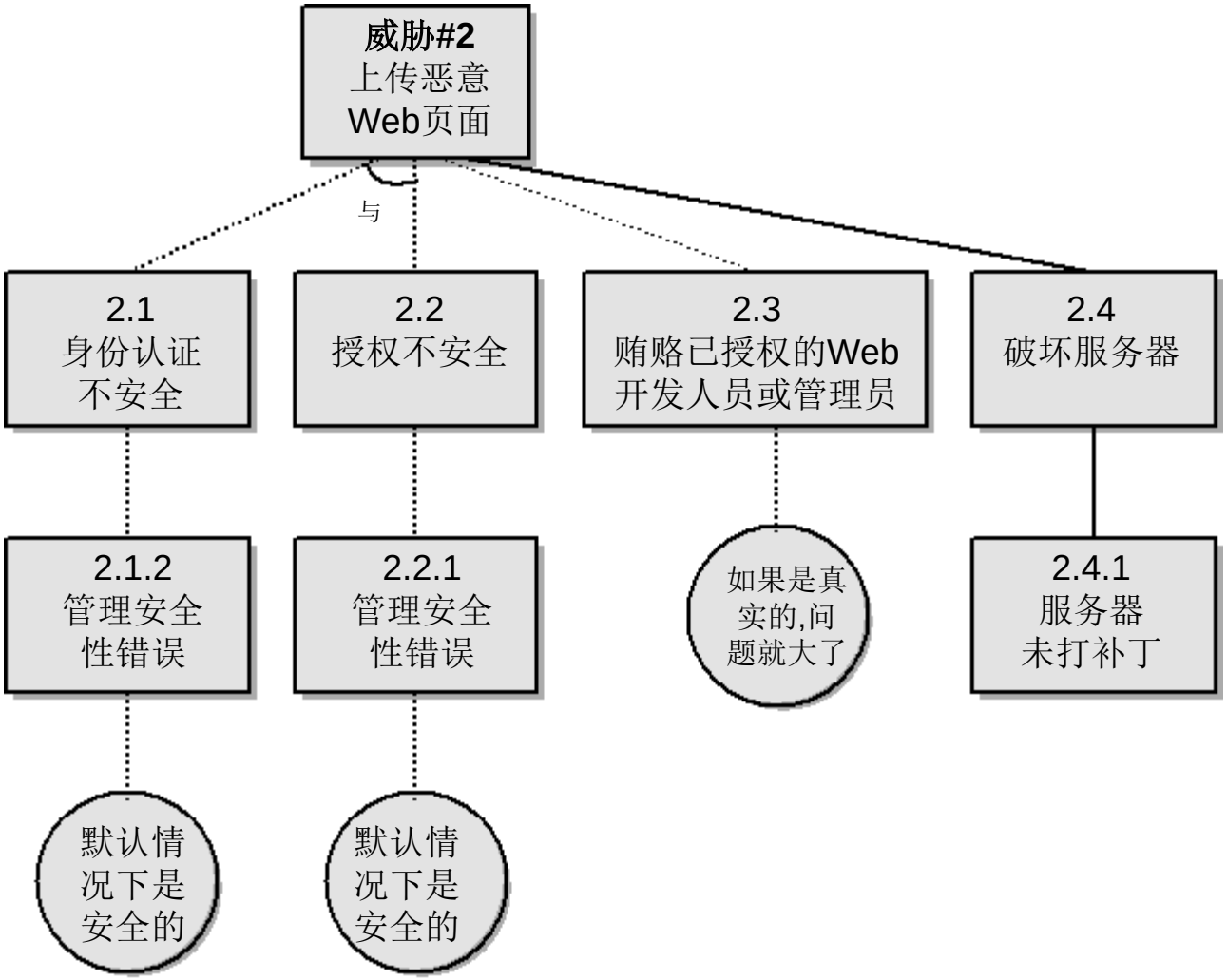
火龙果•整理
uml.org.cn

威胁#2

威胁描述	攻击者上传恶意Web页面和代码
威胁目标	Web页面(7.0)或Web服务代码(8.0)
威胁类别	篡改数据
风险	潜在破坏性: 7 可再现性: 7 可利用性: 7 影响用户: 10 可发现性: 10 总计: 8.2
注释	安装工具总是设置良好的认证授权策略,因此,通过脆弱的安全上传Web页面的唯一方法是因为管理配置错误

火龙果•整理
uml.org.cn

威胁#2



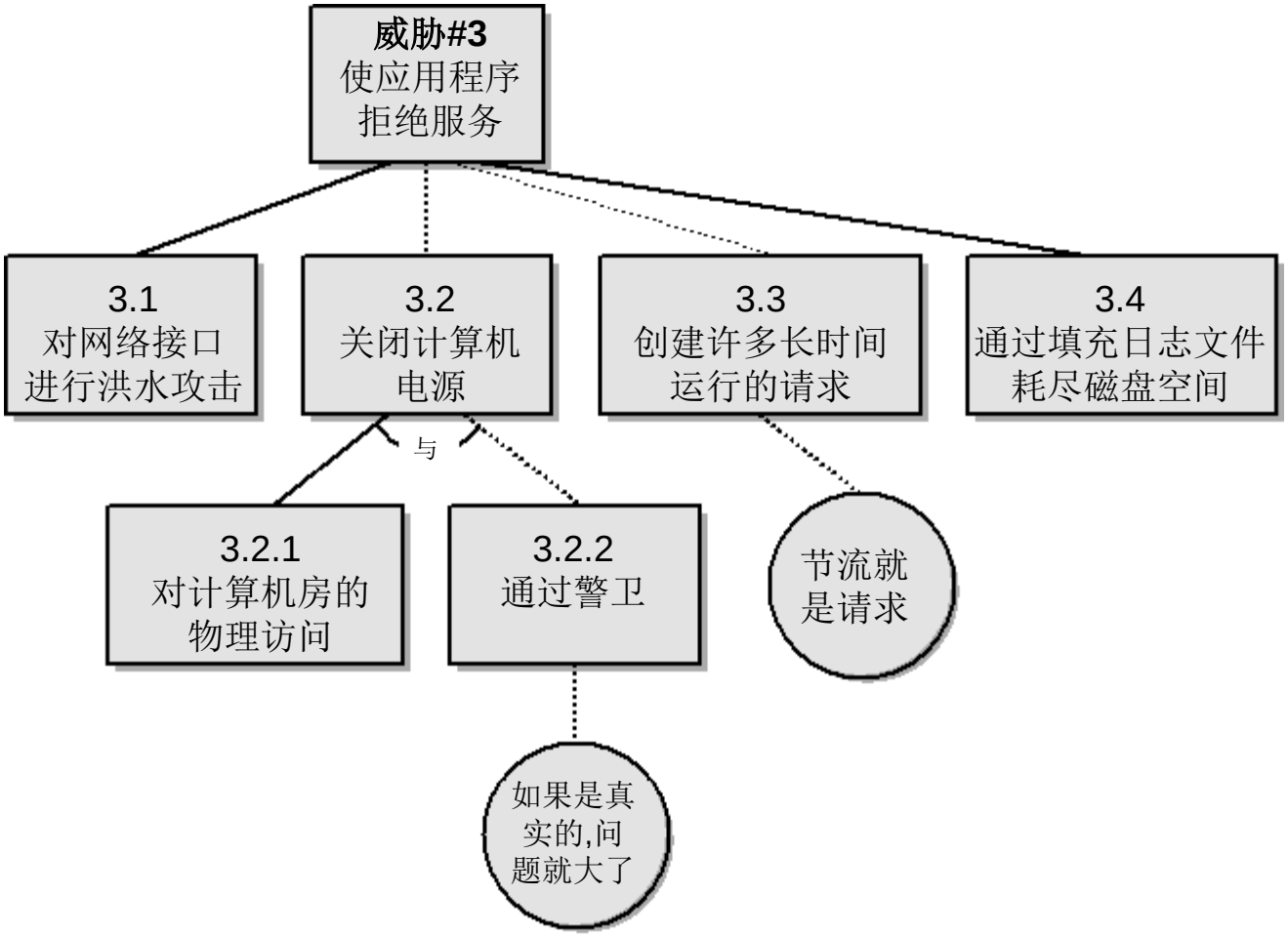
火龙果•整理
uml.org.cn

威胁#3

威胁描述	攻击者使应用程序拒绝服务
威胁目标	服务客户请求过程(5.0)
威胁类别	拒绝服务
风险	潜在破坏性: 6 可再现性: 6 可利用性: 7 影响用户: 9 可发现性: 10 总计: 7.6
注释	应用程序的其它部分可能会被拒绝服务攻击,但是,处理客户请求过程的Web服务器处于最前端,因此最容易受到攻击,如果我们保护了应用程序的这一部分,其他过程收到的攻击是可以容忍的

火龙果•整理
uml.org.cn

威胁#3



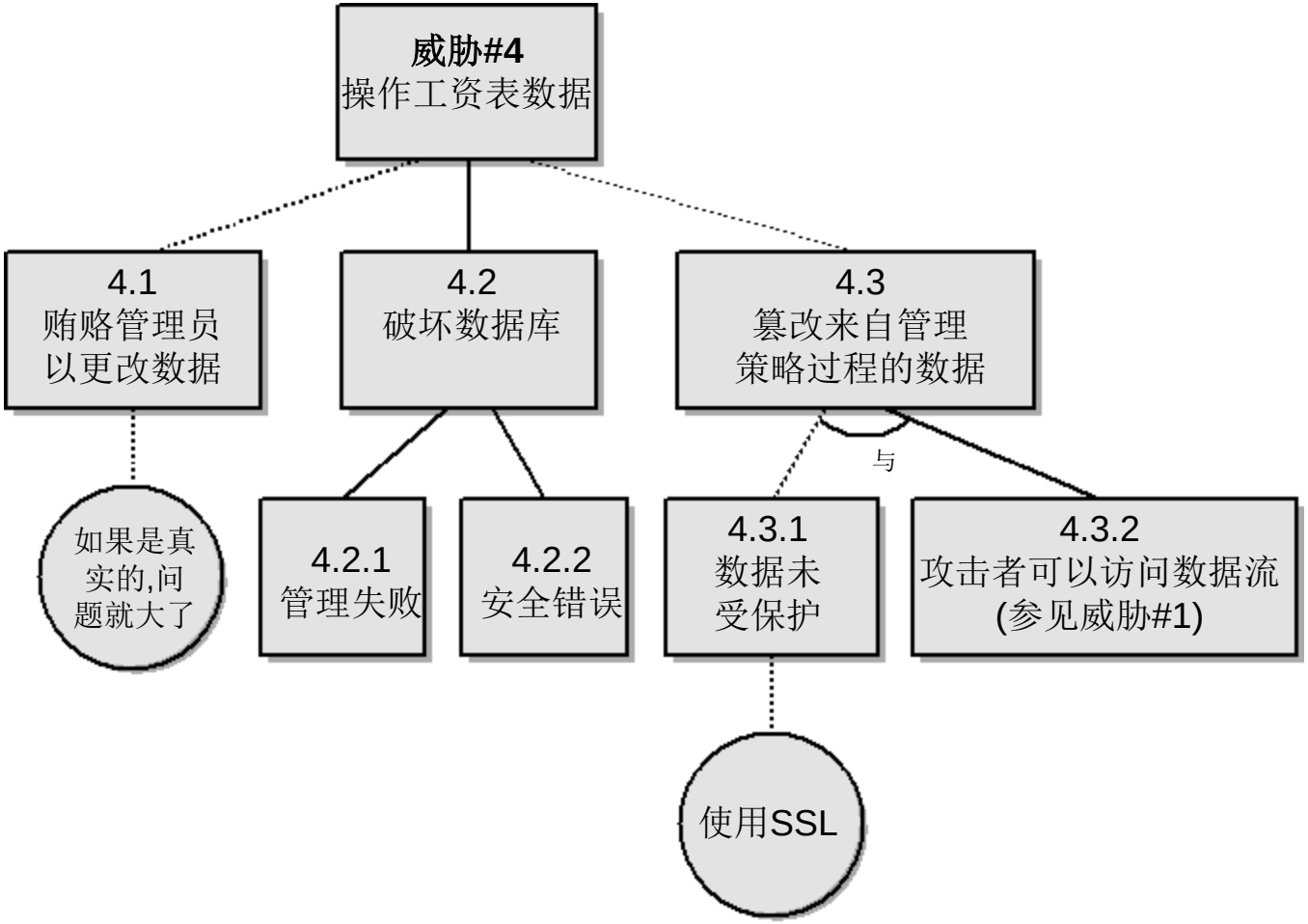
火龙果•整理
uml.org.cn

威胁#4

威胁描述	攻击者操纵工资表数据
威胁目标	工资表数据(12.0)
威胁类别	篡改数据及潜在的信息泄露
风险	潜在破坏性: 10 可再现性: 5 可利用性: 5 影响用户: 10 可发现性: 10 总计: 8
注释	指在更新工资表数据跨越网络从管理控制台(2.0)到管理策略过程(14.0),然后到攻击表数据存储(12.0)时对其进行的访问

火龙果•整理
uml.org.cn

威胁#4



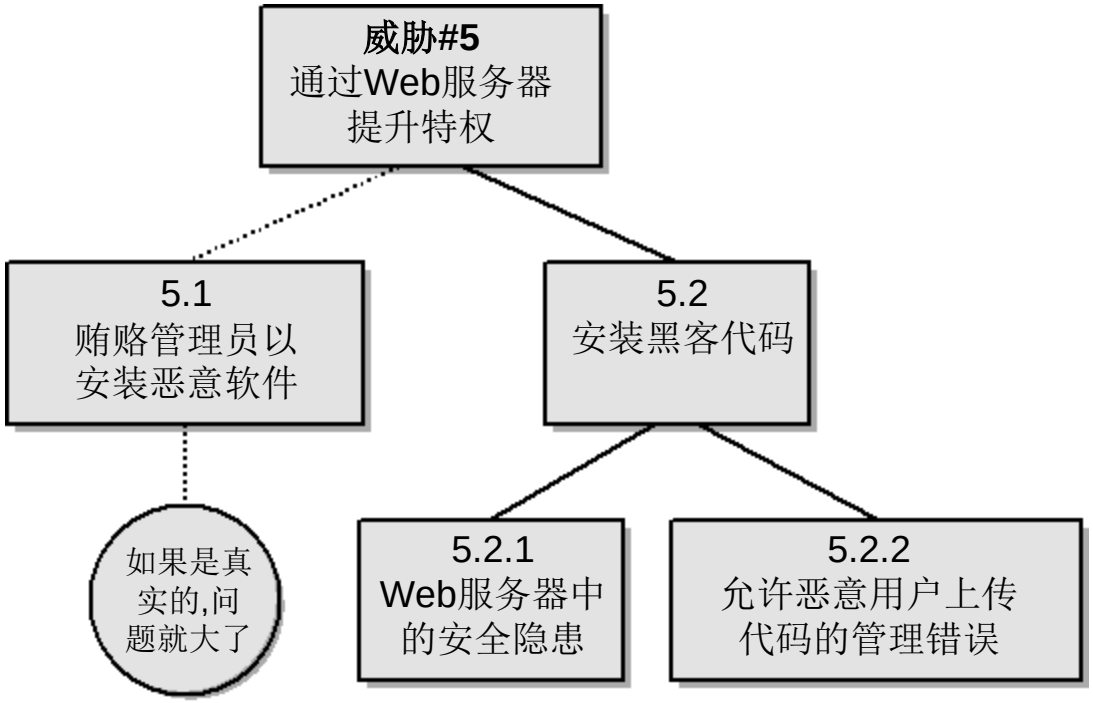
火龙果•整理
uml.org.cn

威胁#5

威胁描述	攻击者利用服务客户请求过程来提升特权
威胁目标	服务客户请求(5.0)
威胁类别	篡改数据及潜在的信息泄露
风险	潜在破坏性: 10 可再现性: 2 可利用性: 2 影响用户: 1 可发现性: 10 总计: 5
注释	这里的威胁目标运行在Web服务器环境中,而代码运行在Local System环境内,这意味着任何在这台Web服务器的该环境下运行的恶意代码也都是Local System的,可再现性和可利用性很低,因为对于攻击者,要利用这一点,唯一可行的方式就是利用Web服务器进程的安全漏洞,影响用户的因素也很低,但只有这台服务器受影响,尽管有人会争论说如果攻击者破坏了这台服务器,所有人都会受影响.

火龙果•整理
uml.org.cn

威胁#5



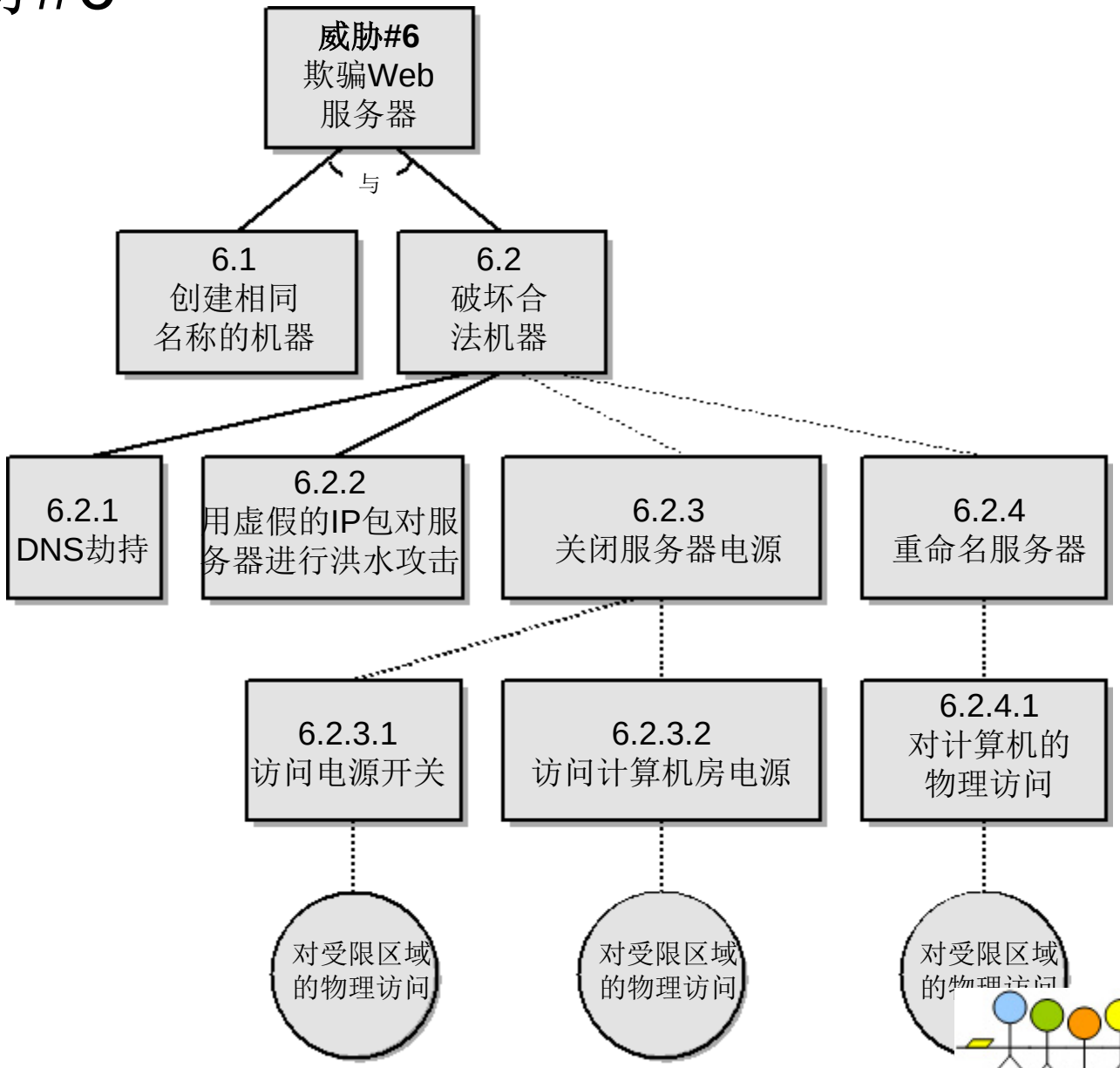
火龙果•整理
uml.org.cn

威胁#6

威胁描述	欺骗计算机执行客户请求进程
威胁目标	服务客户请求过程(5.0)
威胁类别	欺骗
风险	潜在破坏性: 10 可再现性: 2 可利用性: 2 影响用户: 8 可发现性: 10 总计: 6.4
注释	让一台合法机器脱离网络,意味着或者物理脱离(重命名计算机或关闭电源),或者使用攻击技术使之不可访问(通过DNS欺骗或洪水攻击)

火龙果•整理
uml.org.cn

威胁#6



火龙果•整理
uml.org.cn

威胁分级

- 3. 计算总体风险
  - 在威胁树中寻找抵抗最薄弱的路径,这不意味着攻击者不会沿着其他的路径攻击,只是他们更可能利用这条容易的路径.

火龙果•整理
uml.org.cn

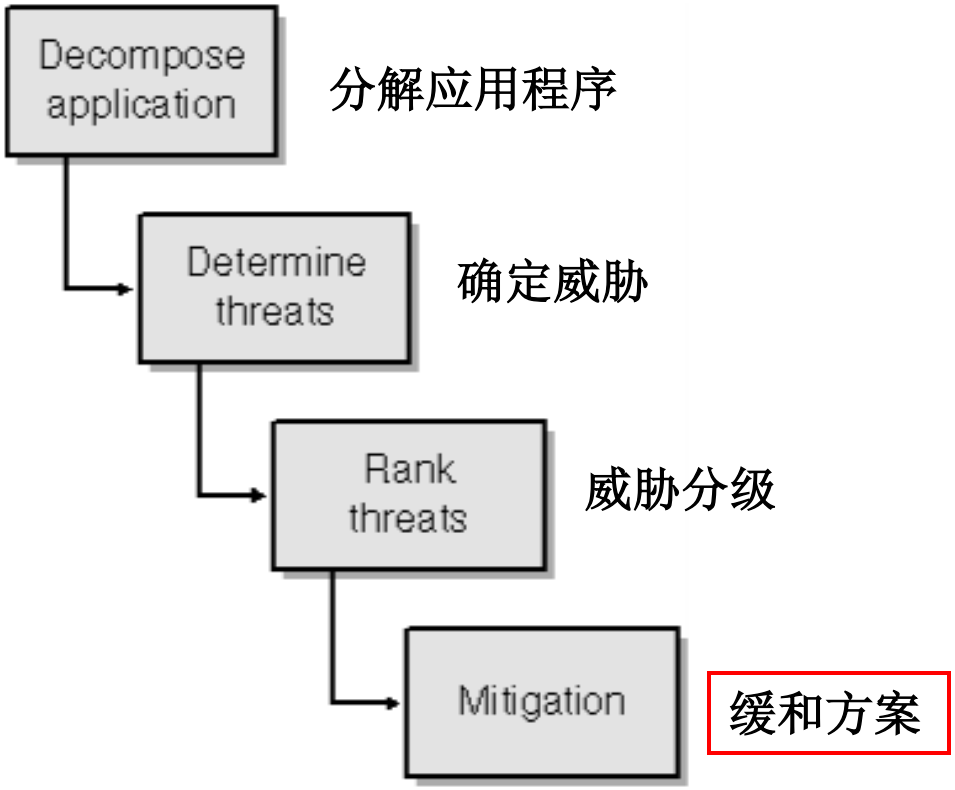
威胁分级

- 4. 复习威胁建模过程
  - 步骤1:将应用程序分解为威胁目标
  - 步骤2:使用STRIDE,给每个威胁目标标识威胁
  - 步骤3:为每一个威胁目标创建一棵或多棵威胁树
  - 步骤4:使用DREAD分级方法确定安全风险
  - 步骤5:将威胁以从高到低的顺序进行风险排序

做完威胁建模之后,下一步就是如何处理这些威胁了.

火龙果•整理
uml.org.cn

缓和方案



火龙果•整理
uml.org.cn

缓和方案

- 1.选择应付威胁的方法:
  - 什么也不做
  - 把威胁告诉用户
  - 删除功能
  - 改正问题

火龙果•整理
uml.org.cn

缓和方案

- 2.选择缓和威胁的方法:
  - 第一步判断哪些方法可以提供帮助
  - 第二步 选择最适合的方法

火龙果•整理
uml.org.cn

缓和方案

威胁类型	缓和方法	威胁类型	缓和方法
欺骗标识	认证 保护秘密 不存储秘密	信息泄露	授权 加强保密的协议 加密 保护秘密 不存储秘密
篡改数据	适当的授权 散列(Hash)表 消息认证代码 数字签名 抗篡改的协议	拒绝服务	适当的认证 适当的授权 过滤 节流(Throttling) 服务质量
否认	数字签名 时间戳 审核跟踪	特权提升	以最小权限运行

下面我们分别解释表中所列的安全方法

火龙果•整理
uml.org.cn

身份认证 Authentication

身份认证是这样的一个过程:一个实体,也被成为主体(principal),验证另一个实体是它声称的那个人或食事物,主题可以是用户,一些可执行代码,或一台计算机,认证需要证书(credential)形式的证据(evidence),证据可以使多种形式的,例如,口令,私钥,或者有可能的话,使用生物技术来做认证,比如指纹.

火龙果•整理
uml.org.cn

身份认证 Authentication

windows可以使用许多认证协议,一些被内置在系统中,一些则要求你再操作系统中使用构建块来创建你的认证系统,这些模式有:

- 基本认证
- 摘要(digest)认证
- 基于表单的认证
- Passport认证
- Windows认证
- NTLM(NT LAN Manager, NT网络管理器)认证
- Kerberos v5认证
- X.509证书认证
- IPSec (Internet Protocol Security, 网际协议安全)
- RADIUS

火龙果•整理
uml.org.cn

身份认证 Authentication

协议	认证客户?	认证服务器?
基本认证	Yes	No
摘要认证	Yes	No
表单认证	Yes	No
Passport认证	Yes	No
NTLM	Yes	No
Kerberos	Yes	Yes
X.509 证书	Yes	Yes
IPSec	Yes (computer)	Yes (computer)
RADIUS	Yes	No

火龙果•整理
uml.org.cn

1.基本认证

基本认证是一个简单的协议,它是作为HTTP 1.0协议的一部分.

虽然事实上所有的Web服务器和Web浏览器都支持这个协议,但是它是非常不安全的,因为口令没有被保护,事实上,用户名和口令是64位编码的,这很容易解码,简而言之,由于认证的不安全性,不鼓励在任何基于Web的应用程序中使用它,除非在客户机与服务器之间使用SSL/TLS或者IPSec保护连接.

火龙果•整理
uml.org.cn

2.摘要认证 Digest Authentication

摘要认证比基本认证有更多的优点,最值得注意的是,口令不是以明文的形式从浏览器传输到服务器的,同时,除了HTTP之外,其他的因特网协议如LDAP,IMAP,POP3,SMTP也可以考虑使用摘要认证.

火龙果•整理
uml.org.cn

3.基于表单的认证

基于表单的认证没有标准的实现方法,大多数站点都有他们自己的方案,然而,在微软的ASP.NET中通过FormsAuthenticationModule类,简历一个基于表单的认证,它是IHttpModule接口的一个实现.

下面,我们来说明基于表单的认证是如何工作,当一个Web页显示在用户前时,他输入用户名和口令,然后单击”提交(Submit)”或”登录(logon)”按钮,于是表单信息被发送给Web服务器,在通常情况下是通过一个SSL/TLS连接完成的.最后,Web服务器受到表单信息,然后使用这些信

火龙果•整理
uml.org.cn

例如,下面的ASP代码显示了如何从一个表单中读取用户名和口令,然后将其作为认证数据:

```
<%
    Dim strUsername, strPwd As String
    strUsername = Request.Form("Username")
    strPwd = Request.Form("Pwd")
    If IsValidCredentials(strUserName, strPwd) Then
        ' Cool! Allow the user in!
        ' Set some state data to indicate this
    Else
        ' Oops! Bad username and password
        Response.Redirect "401.html“
    End If
%>
```

火龙果•整理
uml.org.cn

4.Microsoft Passport

Passport认证是微软提供的集中式认证方法,Passport被用于许多服务,包括Microsoft Hotmail, Microsoft Instant Messenger以及大量的电子商务站点,使用它最大的好处就是,如果你已经用你的Passport登录到一个服务,之后再去另一个启用了Passport的Web服务是,你不需要再一次输入你的证书.

火龙果•整理
uml.org.cn

5.Windows 认证

Windows支持两个主要的认证协议:NTLM和Kerberos

- NTLM认证:NTLM认证是一个挑战响应协议,它被许多Windows服务使用,包括文件和打印服务,IIS, Microsoft SQL Server和Microsoft Exchange.
- Kerberos v5 认证: Kerberos v5 认证是由麻省理工学院(MIT)设计的,Windows 2000以及以后的版本实现了Kerberos,它提供一个主要优点是相互认证,换句话说,客户机和服务器的真实性都被校验,Kerberos通常被认为是比NTLM更安全的协议,并且在许多情况下它的速度更快.

火龙果•整理
uml.org.cn

6. X.509证书认证

现在X.509最实际的用法是SSL/TLS,当你用HTTPS而不是HTTP与一台Web服务器建立带有SSL/TLS的连接时,这是通过将服务器的证书中的普通名字与应用程序正在连接的主机名相比较来完成认证的,如果这两个名称不同,应用程序就会警告你,可能未与正确的服务器进行通信.

火龙果•整理
uml.org.cn

7. IPSec

IPSec与前面提到的协议有一点区别,它只认证服务器,Kerberos也能向服务器认证其他服务器,但是IPSec不能认证用户,IPSec提供的功能不只是简单的认证服务器,它还提供了数据完整性和保密性,Windows 2000及以后的版本都支持IPSec.

火龙果•整理
uml.org.cn

8. RADIUS

许多服务产品,包括Microsoft Internet认证服务(IAS)都支持RADIUS (Remote Authentication Dial-In User Service,远程验证拨入用户服务)协议,它实际上是远程用户认证的标准协议.

火龙果•整理
uml.org.cn

授权

一旦通过认证确定了主体的身份,主体通常会希望访问资源,例如打印机和文件,授权是通过执行一个访问检查,来判断这个已被认证的主题是否有权访问他请求的资源,对同样的一个资源,某些主题会比其他主题有更多的访问权.

Windows提供了很多授权机制,包括:

- ACL (Access Control List, 访问控制列表)
- 特权
- IP限制
- 服务专用权限

火龙果•整理
uml.org.cn

1.访问控制列表

在Windows NT及以后的版本中,所有的对象都可以用ACL保护,一个ACL是一系列的访问控制项(Access Control Entry, ACE),每一个ACE决定一名主机能够对一个资源做什么事情.

火龙果•整理
uml.org.cn

2.特权

特权是赋予用户的权利,用户可以执行系统范围内的操作,一些操作被认为是特许的,并且应该只授予受信任的个人,这样的例子包括调试应用程序,备份文件和远程关闭计算机.

火龙果•整理
uml.org.cn

3.IP限制

IP限制是IIS的一个功能,你可以限制Web站点的一部分,例如一个虚拟目录或一个目录,也可以限制整个Web站点,使得只有专门的IP地址,子网和DNS名可以访问它.

火龙果•整理
uml.org.cn

4.服务专用权限

许多服务提供了它们自己的访问控制形式,来保护他们自己专门的对象类型,例如,Microsoft SQL Server提供了权限,管理员用它可以决定谁有权访问哪一个表,存储过程和视图,COM+应用程序支持角色,它可以为一组组件定义一类用户,每一个角色定义了允许哪一个用户调用组件上的接口.

火龙果•整理
uml.org.cn

防篡改和增强保密性的技术

许多网络协议支持抗篡改的数据保密.抗篡改是指保护数据不被恶意的或意外的删除或修改的能力,Windows中最常见的抗篡改和加强保密的协议核技术如下:

- SSL/TLS
- IPSec
- DCOM和RPC
- EFS

火龙果•整理
uml.org.cn

1.SSL/TLS

SSL是由Netscape在90年代中期发明的,它对在服务器和客户机之间传输的数据加密,并用MAC (Message Authentication Code,消息认证代码)提供数据完整性,TLS则是IETF (Internet Engineering Task Force, Internet工程任务组)认可的SSL版本.

火龙果•整理
uml.org.cn

2.IPSec

正如前面提到的,IPSec支持认证,数据保密需要的加密,数据完整性需要的MAC,在使用了IPSec安全措施的服务器之间传输的所有数据,都被加密并做了完整性检查,利用IPSec的优点,不需要对应用程序做任何调整,因为IPSec是在TCP/IP网络的IP层实现的.

火龙果•整理
uml.org.cn

3. DCOM和RPC

分布式COM和远程调用支持认证,保密性和完整性,它对性能的影响是很小的,除非你传输大量的数据.

火龙果•整理
uml.org.cn

4. EFS

EFS (Encrypting File System, 加密文件系统)已经被包含在Windows 2000以及以后的系统中,它是一个基于文件的加密方法,这个方法是NTFS的一个功能,SSL, TLS, IPSec和DCOM/RPC关心的是网络上传输的数据,而EFS对文件加密并提供篡改检查.

火龙果•整理
uml.org.cn

保护秘密或最好不要保存秘密

保护秘密最好的办法是,不要在第一个出现的地方存储它,如果需要,允许你的用户从他们的存储中来使用它,而你不用存储它,如果你必须存储秘密数据,那么尽最大的能力保护它.

火龙果•整理
uml.org.cn

审核 Auditing / 日志 Logging

审核(auditing)也被称作日志(logging),其目的是收集成功的和失败的对对象的访问,特权的使用,以及其他重要的安全活动的信息,并将他们记录在永久的存储设备中,以便日后分析,Windows在Windows事件日志,IIS Web日志中提供了日志(审核)功能,还有许多其他的应用程序提供了专门的日志文件,包括SQL Server和Exchange日志文件.

- 要点:所有的日志文件都必须是安全的,不会受到攻击的,这一点十分重要.你应该在你的威胁模型中加入一个威胁,用于描述日志文件被读,修改甚至删除的可能性及其影响,以及应用程序不能写日志记录的可能性.

火龙果•整理
uml.org.cn

过滤,节流和服务质量

过滤(Filtering)是指对接收到的数据进行检查,并判断是接受还是拒绝这个包.这也是包通过过滤防火墙的方式,许多IP层拒绝服务威胁,都可以用过滤防火墙来缓和.

节流(Throttling)是指限制对系统请求的数量,例如,你可以只允许少量的匿名请求,同时允许更多的被认证的请求.

服务质量(Quality of Service)是一组组建,他们允许你为专门的传输类型提供优先处理,例如,你可以允许优先处理流媒体.

火龙果•整理
uml.org.cn

缓和工资表范例程序的威胁

威胁	STRIDE	缓和方法和技术
浏览网络上的工资数据	I	使用SSL/TLS加密服务器和客户间的管道,也可以使用IPSec
上传恶意Web页面或Web服务代码	T	需要对Web开发人员进行加强的认证,为文件提供加强的ACL,这样只有Web开发人员和管理人员才可以改写或删除文件
攻击者是应用程序拒绝服务	D	使用防火墙抛弃某些IP包,限制匿名用户使用的资源(如内存,磁盘空间,数据库时间),最后,将日志文件移到另一个文件卷
攻击者控制工资数据	T 和 I	根据所用的网络协议,使用SSl/TLS或带保密选项的DCOM/RPC保护更新后的数据流,这会缓和信息泄露威胁,SSL/TLS还提供了消息认证编码来检测数据篡改攻击,在选择了保密选项时DCOM/RPC还提供了完整性检查,也可以考虑使用IPSec
利用服务客户请求进程来提升特权	E	运行进程时遵循最小特权原则,如果该进程被破坏,这些代码也不能获得额外的能力
欺骗Web服务器	S	最简单的解决方案是使用SSL/TLS,如果正确配置,它允许客户软件对服务器进行认证,公司的策略规定所有的客户必须这样做,另外也可以用Kerberos认证,Kerberos提供了服务器与客户之间的相互认

火龙果•整理
uml.org.cn

本节小结

威胁建模的过程很简单:集合小组,分解应用程序,使用威胁树和STRIDE确定系统面临的威胁,使用DREAD技术分级威胁,然后根据STRIDE分类选择缓和技术.

威胁建模是设计系统是非常重要的一环,没有合适的威胁建模,你不可能知道是否已经缓和了应用程序所受的最严重的威胁,像碰运气似的在应用程序中加上一大堆安全技术,并不会使其变得更安全,而且使用的技术也不一定适合你的应用程序,经验告诉我们,大约一半的安全缺陷会在威胁模型中确定下来.

火龙果•整理
uml.org.cn