第 14 章 - 安全工程

- 第1讲
- 第十四章 安全工程
- <编号>

涵盖的主题

- 安全工程与安全管理
  - 与应用相关的安全工程；基础设施的安全管理。
- 安全风险评估
  - 设计基于安全风险评估的系统。
- 安全设计
  - 如何设计系统架构以确保安全。
- 第十四章 安全工程
- <编号>

安全工程

- 支持系统开发和维护的工具、技术和方法，可以抵抗旨在破坏基于计算机的系统或其数据的恶意攻击。
- 更广泛的计算机安全领域的一个子领域。
- 假设具备可靠性和安全概念（第 10 章）和安全要求规范（第 12 章）的背景知识
- 第十四章 安全工程
- <编号>

应用程序/基础设施安全

- 应用程序安全是一个软件工程问题，其中系统旨在抵御攻击。
- 基础设施安全是一个系统管理问题，其中基础设施被配置为抵抗攻击。
- 本章的重点是应用程序安全。
- 第十四章 安全工程
- <编号>

安全性可能受到威胁的系统层

- 第十四章 安全工程
- <编号>
- ***中间件**支持分布式计算和数据库访问。*

- 当您考虑安全问题时，您必须同时考虑应用软件和构建此系统的基础设施。
- ***基础设施***

系统安全管理

- 用户和权限管理
  - 在系统中添加和删除用户并为用户设置适当的权限
- 软件部署与维护
  - 安装应用软件和中间件并配置这些系统以避免漏洞。
- 攻击监控、检测和恢复
  - 监控系统的未授权访问，设计抵御攻击的策略并制定备份和恢复策略。
- 第十四章 安全工程
- <编号>

14.1 安全风险管理

- 风险管理涉及评估系统攻击可能导致的损失，并平衡这些损失与可能减少这些损失的安全程序成本。
- 风险管理应由组织安全策略驱动。
- 风险管理涉及
  - 初步风险评估
  - 生命周期风险评估
  - 操作风险评估
- 第十四章 安全工程
- <编号>

初步风险评估

- 第十四章 安全工程
- <编号>
- **安全需求的初步风险评估流程**
- *初步风险评估侧重于推导出安全要求。*
- 在这个阶段，还没有对详细的系统需求、系统设计或实现技术做出决定。
- 此评估过程的目的是确定是否可以以合理的成本实现足够的安全级别。如果是这种情况，您就可以得出系统的特定安全要求。
- 您没有关于系统中潜在漏洞或包含在重复使用的系统组件或中间件中的控件的信息。

误用案例

- 误用案例是代表与系统恶意交互的场景（系统受到威胁的实例）。Pfleeger CP 和 Pfleeger SL(2007) 在四个标题下描述了威胁的特征，这些标题可用作识别可能的误用案例的起点。这些标题是：
    - 拦截威胁
        - 攻击者可以访问资产
    - 中断威胁
        - 攻击者使系统的一部分不可用
    - 改装威胁
        - 允许攻击者篡改系统资产
    - 制造威胁
        - 虚假信息被添加到系统中
- 第十四章 安全工程
- <编号>

资产分析

- 第十四章 安全工程
- <编号>

资产	价值	暴露
信息系统	高的。需要支持所有临床咨询。潜在的安全关键。	高的。由于诊所可能不得不取消而造成经济损失。恢复系统的成本。如果无法开出治疗处方，可能会对患者造成伤害。
患者数据库	高的。需要支持所有临床咨询。潜在的安全关键。	高的。由于诊所可能不得不取消而造成经济损失。恢复系统的成本。如果无法开出治疗处方，可能会对患者造成伤害。
个人病历	通常较低，但对于特定的高知名度患者可能较高。	低直接损失，但可能损失声誉。

威胁与控制分析

- 第十四章 安全工程
- <编号>

威胁	可能性	控制	可行性
未经授权的用户以系统管理员身份获得访问权限并使系统不可用	低的	仅允许从物理安全的特定位置进行系统管理。	实施成本低，但必须注意密钥分发，并确保在紧急情况下可以使用密钥。
未经授权的用户以系统用户身份访问并访问机密信息	高的	要求所有用户使用生物识别机制对自己进行身份验证。记录对患者信息的所有更改以跟踪系统使用情况。	技术上可行但成本高的解决方案。可能的用户阻力。实施简单透明，还支持恢复。

安全要求

- 必须在诊所会话开始时将患者信息下载到临床工作人员使用的系统客户端上的安全区域。
- 诊所会话结束后，不得在系统客户端上维护患者信息。
- 必须在与数据库服务器不同的计算机上维护对系统数据库所做的所有更改的日志。
- 第十四章 安全工程
- <编号>

14.1.1 生命周期风险评估

- 系统开发过程中和部署后的风险评估
- 可以获得更多信息 - 系统平台、中间件以及系统架构和数据组织。
- 因此，可以识别由设计选择引起的漏洞。
- 第十四章 安全工程
- <编号>

生命周期风险分析

- 第十四章 安全工程
- <编号>

使用 COTS 的设计决策

- 系统用户使用名称/密码组合进行身份验证。
- 系统架构是客户端-服务器，客户端通过标准 Web 浏览器访问数据。
- 信息以可编辑的网络表单形式呈现给用户。他们可以就地更改信息并将修改后的信息上传到服务器。
- 第十四章 安全工程
- <编号>
- 当您通过重用现有系统来开发应用程序时，您必须接受该系统开发人员做出的设计决策。
- 让我们假设其中一些决定如下：

与技术选择相关的漏洞

- 第十四章 安全工程
- <编号>
- 对于通用系统，上述设计决策是完全可以接受的，但生命周期风险分析表明它们存在相关的漏洞。下图显示了可能的漏洞示例：

安全要求

- 为解决固有漏洞而提出的要求的一些（并非全部）示例可能如下所示：
- 应提供密码检查程序并每天运行。弱密码应报告给系统管理员。
- 只有经过批准的客户端计算机才能访问系统。
- 所有客户端计算机都应有一个由系统管理员安装的、经批准的 Web 浏览器。
- 第十四章 安全工程
- <编号>

14.1.2 操作风险评估

- 继续生命周期风险评估，但提供有关系统使用环境的附加信息。
- 环境特征可能导致新的系统风险
    - 例如，假设系统在用户经常被中断的环境中使用。中断风险意味着登录的计算机无人看管。
    - 未经授权的人可能会访问系统中的信息。
    - 然后，这可能会要求在短时间不活动后运行受密码保护的屏幕保护程序。
- 第十四章 安全工程
- <编号>

14.2 安全设计

- 建筑设计
    - 架构设计决策如何影响系统的安全性?
- 良好做法
    - 在设计安全系统时，什么是公认的良好做法?
- 部署设计
    - 应该在系统中设计哪些支持以避免在部署系统以供使用时引入漏洞?
- 第十四章 安全工程
- <编号>

14.2.1 架构设计

- 在设计安全架构时，必须考虑两个基本问题。
  - 保护
    - 应如何组织系统以保护关键资产免受外部攻击?
  - 分配
    - 应该如何分配系统资产，以便将成功攻击的影响降到最低?
- 这些可能存在冲突
  - 如果资产是分布式的，那么保护它们的成本就会更高。如果资产受到保护，那么可用性和性能要求可能会受到影响。
- 第十四章 安全工程
- <编号>

保护

- 平台级保护
  - 系统运行的平台上的顶级控件。
- 应用级保护
  - 应用程序本身内置的特定保护机制，例如附加密码保护。
- 记录级保护
  - 请求访问特定信息时调用的保护
- 这些导致了下一张幻灯片中显示的分层保护架构。
- 第十四章 安全工程
- <编号>

分层保护架构

- 第十四章 安全工程
- <编号>
- 分层保护架构

分配

- 分散资产意味着对一个系统的攻击不一定会导致系统服务完全丧失
- 每个平台都有单独的保护功能，可能与其他平台不同，因此它们不会共享一个共同的漏洞
- 如果拒绝服务攻击的风险很高，分发就尤为重要
- 第十四章 安全工程
- <编号>

股权交易系统中的分布式资产

- 第十四章 安全工程
- <编号>

关键点

- 安全工程关心的是如何开发能够抵抗恶意攻击的系统
- 安全威胁可以是对系统或其数据的机密性、完整性或可用性的威胁
- 安全风险管理涉及评估攻击可能造成的损失并得出安全要求以最大限度地减少损失
- 安全设计涉及架构设计、遵循良好的设计实践并最大限度地减少系统漏洞的引入
- 第十四章 安全工程
- <编号>

第 14 章 - 安全工程

- 第二讲
- 第十四章 安全工程
- <编号>

涵盖的主题

- 安全设计指南
  - 帮助您设计安全系统的指南
- 部署设计
  - 设计使可能引入漏洞的部署问题最小化
- 系统生存能力
  - 允许系统在受到攻击时提供基本服务
- 第十四章 安全工程
- <编号>

14.2.2 安全工程设计指南

- 设计指南概括了安全系统设计中的良好实践
- 设计指南有两个目的：
  - 它们提高了软件工程团队对安全问题的认识。在做出设计决策时会考虑安全性。
  - 它们可以用作在系统验证过程中应用的审查清单的基础。
- 这里的设计指南适用于软件规范和设计

- 第十四章 安全工程
- <编号>

安全系统工程的设计指南

安全指引	
基于明确的安全策略的安全决策	
避免单点故障	
安全失败	
平衡安全性和可用性	
记录用户操作	
使用冗余和多样性来降低风险	
验证所有输入	
划分您的资产	
部署设计	
可恢复性设计	

- 第十四章 安全工程
- <编号>

设计指南 1-3

- 基于明确的安全策略做出决定
    - 为组织定义安全策略，该策略规定了适用于所有组织系统的基本安全要求。
- 避免单点故障
    - 确保只有在安全程序中出现不止一个故障时才会导致安全故障。例如，拥有密码和基于问题的身份验证。
- 安全失败
    - 当系统出现故障时，无论出于何种原因，即使正常的安全程序不可用，也要确保未经授权的用户无法访问敏感信息。
- 第十四章 安全工程
- <编号>

设计指南 4-6

- 平衡安全性和可用性
    - 尽量避免使系统难以使用的安全程序。有时您必须接受较弱的安全性才能使系统更可用。
- 记录用户操作
    - 维护用户操作日志，可以对其进行分析以发现谁做了什么。如果用户知道这样的日志，他们就不太可能以不负责任的方式行事。
- 使用冗余和多样性来降低风险
    - 保留多个数据副本并使用不同的基础设施，这样基础设施漏洞就不会成为单点故障。
- 第十四章 安全工程
- <编号>

设计指南 7-10

- 验证所有输入
    - 检查所有输入是否在范围内，以便意外输入不会导致问题。
- 划分您的资产
    - 组织系统，使资产位于不同的区域，用户只能访问他们需要的信息，而不是所有系统信息。
- 部署设计
    - 设计系统以避免部署问题
- 可恢复性设计
    - 设计系统以简化成功攻击后的可恢复性。
- 第十四章 安全工程
- <编号>

14.2.3 部署设计

- 部署涉及配置软件以在其工作环境中运行，安装系统并为操作平台配置它。
- 由于配置错误，此阶段可能会引入漏洞。
- 在系统中设计部署支持可以降低引入漏洞的可能性。
- 第十四章 安全工程
- <编号>

软件部署

- 第十四章 安全工程
- <编号>

配置漏洞

- 易受攻击的默认设置
    - 攻击者可以找出软件的默认设置。如果它们很弱（通常是为了提高可用性），那么用户在攻击系统时就可以利用它们。
- 开发而不是部署
    - 系统中的某些配置设置旨在支持开发和调试。如果这些没有关闭，它们可能是一个可以被攻击者利用的漏洞。
- 第十四章 安全工程
- <编号>

部署支持 1

- 包括对查看和分析配置的支持
    - 确保负责部署的系统管理员可以轻松查看整个配置。这使得更容易发现遗漏和错误。
- 最小化默认权限，从而限制可能造成的损害
    - 设计系统，使管理员的默认权限最小化。这意味着如果有人获得管理员访问权限，他们将无法立即访问系统的功能。
- 第十四章 安全工程
- <编号>

部署支持 2

- 本地化配置设置
    - 在设置系统时，所有与系统相同部分或组件相关的信息都应本地化，以便一次性设置所有信息。否则很容易忘记设置相关的安全功能。
- 提供修复安全漏洞的简单方法
    - 当检测到问题时，提供简单的方法（例如自动更新）来修复已部署系统中的安全漏洞。
- 第十四章 安全工程
- <编号>

14.3 系统生存能力

- 生存能力是一种紧急的系统属性，它反映了系统在受到攻击或部分系统损坏后提供基本服务的能力
- 生存性分析和设计应该是安全工程过程的一部分
- 第十四章 安全工程
- <编号>

生存能力的重要性

- 我们的经济和社会生活依赖于计算机系统
    - 关键基础设施——电力、天然气、电信、交通
    - 卫生保健
    - 政府
- 业务系统即使在短时间内丢失也会产生非常严重的经济影响
    - 航空公司预订系统
    - 电子商务系统
    - 支付系统
- 第十四章 安全工程
- <编号>

服务可用性

- 哪些系统服务对企业最关键?
- 这些服务会如何受到损害?
- 必须保持的最低服务质量是多少?
- 如何保护这些服务?
- 如果服务不可用，多快可以恢复?
- 第十四章 安全工程
- <编号>

生存策略

- 反抗
    - 通过在系统中构建抵御攻击的能力来避免问题
- 认出
    - 通过在系统中构建检测攻击和故障并评估由此造成的损害的功能来检测问题
- 恢复
    - 通过在系统中构建能力以在受到攻击时提供服务来容忍问题
- 第十四章 安全工程
- <编号>

生存能力分析的阶段

- 第十四章 安全工程
- <编号>

主要活动

- 系统理解
    - 审查目标、要求和架构
- 关键服务识别
    - 确定必须维护的服务
- 攻击模拟
    - 设计攻击场景并确定受影响的组件
- 生存能力分析
    - 确定要应用的生存策略
- 第十四章 安全工程
- <编号>

交易系统生存能力

- 跨服务器复制用户帐户和股票价格，因此提供了一些生存能力
- 要维护的关键能力是下订单的能力
- 订单必须准确并反映交易者的实际销售/采购
- 第十四章 安全工程
- <编号>

可生存的订购服务

- 必须生存的关键服务是授权用户下订单的能力
- 这需要系统的 3 个组件可用和运行可靠性：
    - 用户认证，允许授权用户登录系统
    - 价格报价，允许报价买卖价格
    - 下单，允许进行买卖订单
- 第十四章 安全工程
- <编号>

可能的攻击

- 恶意用户冒充合法用户恶意下单，为合法用户制造麻烦
- 未经授权的用户会破坏交易数据库，从而无法对销售和采购进行核对
- 第十四章 安全工程
- <编号>

股票交易系统中的生存能力分析

攻击	反抗	认出	恢复
未经授权的用户下恶意订单	需要与登录密码不同的交易密码才能下单。	通过电子邮件将订单副本发送给具有联系电话号码的授权用户（以便他们检测恶意订单）。维护用户的订单历史并检查异常交易模式。	提供自动“撤销”交易和恢复用户账户的机制。对用户因恶意交易造成的损失进行退款。确保避免间接损失。
交易数据库损坏	要求使用更强大的身份验证机制（例如数字证书）对特权用户进行授权。	在国际服务器上为办公室维护事务的只读副本。定期比较事务以检查损坏情况。维护所有交易记录的加密校验和以检测损坏。	从备份副本中恢复数据库。提供从指定时间重播交易以重新创建交易数据库的机制。

- <编号>

关键点

- 一般安全指南使设计人员对安全问题敏感并用作审查清单
- 配置可视化、设置本地化和最小化默认权限有助于减少部署错误
- 系统生存能力反映了系统在受到攻击或部分系统损坏后提供服务的能力。
- 第十四章 安全工程
- <编号>