安全性设计方案

系统资源的分析

电子公文传输系统就是利用计算机网络和安全技术，实现政府部门与部门之间、单位与单位之间政府红头文件的起草、制作、分发、接收等功能，以现代的电子公文传输模式取代传统的纸质公文传输模式。若需紧急状况公文立即传输，可能导致重要文件的传输不能按时到达。本项目主要是为了节约人力物力与时间，在相对安全的情况下传输公文。

其中包含的资源主要是信息资源，不同级别的部门和人员查看资源的权限也是不同的，具体如下:

- 部门信息（部门编号、部门名称）
- 组织信息（组织编号、组织名称）
- 人员信息（人员编号、登录名、登陆密码、真实姓名、所属角色编号、所属部门编号、职位、电话号码、邮箱、性别）
- 文件类型信息（类型编号、类型名称）
- 文件信息（文件编号、文件名称、文件简介、文件链接、发送日期、发送者、接收者、状态、文件类型编号）
- 其他信息（字体、字号、电子公章等）

以上资源在系统和传送过程中均需进行保密传输，并且在不同的组织和部门下，人员可以查看的信息也是有区别的。为保护安全，我们对用户进行安全性设计如下：

- 身份认证
- 数据加密
- 数字签名
- 访问控制
- 证书配置
- 安全审计

本系统为规范使用，还针对部分功能进行划分：

用户

用户可对公文文件进行发送、接收，对自己的文件浏览、查询、打印等。

- 公文传输：在安全登录情况下，从电脑中将需处理的公文上传至电子公文系统。
- 公文管理：使用者根据自己所发布或所接收的文件，按照密级、紧急程度等进行分类归档。
- 公文加密：将公文使用密码算法加密进行加密发送。
- 公文接收：对相应接收到的公文进行判断并解密，安全保存至用户公文系统。
- 公文验证：登录者可根据自己的需求对公文进行验证。
- 公文查询：根据签发部门，密级，紧急程度等查询公文。

管理员

管理员可以发布所有文件，普通用户只能阅读自己对应权限下的文件。

- 用户管理：管理员可增加、删除和修改系统角色信息。管理员可根据系统设置的安全规则、安全策略对不同级别的用户分配不同的权限。
- 公文设置管理：管理员可进入后台选择文件列表，查看用户发布及签收文件的情况。管理员可查询所有发布和接收的公文，可对所有使用者用户发布的文件进行修改。
- 系统管理：管理员可以对数据进行备份，以便后续审计工作。管理员可以进行事务配置。

STRIDE应对方法

威胁建模

威胁建模是一个非常有用的工具，它的核心是像攻击者一样思考。威胁建模强迫我们站在攻击者角度去评估产品的安全性，分析产品中每个组件是否可能被篡改、仿冒，是否可能造成信息泄露、拒绝攻击。

威胁建模流程

1. 绘制数据流图
2. 识别威胁
3. 提出缓解措施
4. 安全验证

数据流图

元素	仿冒	篡改	抵赖	泄露	拒绝服务	权限提升
外部实体	1	0	0	0	0	0
处理过程	1	1	1	1	1	1
数据存储	0	1	0	1	1	0
数据流	0	1	0	1	0	0

提出缓解措施

威胁类型	缓解措施
仿冒	认证
篡改	完整性保护
抵赖	数字签名
信息泄露	保密性
权限提升	访问控制

安全验证

在威胁建模完成后，需要对整个过程进行回顾，不仅要确认缓解措施是否能够真正缓解潜在威胁，同时验证数据流图是否符合设计，代码是否符合预期等。

基于DREAD模型的风险分析

分析背景

威胁建模工具是 Microsoft 安全开发生命周期 (SDL) 的核心要素。潜在安全问题处于无需花费过多成本即可相对容易解决的阶段，软件架构师可以使用威胁建模工具提前识别这些问题。因此，它能大幅减少开发总成本。此外，我们设计该工具时考虑到了非安全专家的体验，为他们提供有关创建和分析威胁模型的清晰指导，让所有开发人员都可以更轻松地使用威胁建模。

通过使用Microsoft threat-modeling工具进行威胁建模后，我们需要对威胁进行评级，进行优先排序。

DREAD威胁评级模型

DREAD分别是威胁评级的5个指标的英文首字母：

- 潜在损失(Damage Potential)
  - 0 = 没有损失
  - 5 = 个人用户数据被盗用或影响
  - 10 = 整体的系统或数据破坏
- 重现性(Reproducibility)
  - 0 = 非常困难或者不可能，即时对于应用管理员
  - 5 = 需要一步或两步，可能需要变成授权用户
  - 10 = 仅仅一个浏览器和地址栏就完成攻击,不需要身份认证
- 可利用性(Exploitability)
  - 0 = 高级程序和网络知识，以定制的或高级攻击工具
  - 5 = 互联网上存在恶意软件，此漏洞可被轻易地利用和可用的攻击工具
  - 10 = 仅仅一个web浏览器就可以
- 受影响的用户(Affected users)
  - 0 = 没有
  - 5 = 一些用户，但不多
  - 10 = 所有用户

- 可发现性(Discoverability)
  - 0 = 非常困难，甚至不可能； 需要源码或者管理员权限
  - 5 = 可以通过猜测或者监测网络活动来发现
  - 9 = 错误的细节已经在公共平台上披露，可以用搜索引擎轻易发现
  - 10 = 信息在web浏览器的地址栏或者表单里可见

等级	高(3)	中(2)	低(1)
潜在的损失 (Damage Potential)	获取完全验证权限，执行管理员操作非法上传文件	泄露敏感信息	泄露其他信息
重现性 (Reproducibility)	攻击者可以随意再次攻击	攻击者可以重复攻击，但有时间限制	攻击者很难重复攻击过程
可利用性 (Exploitability)	初学者短期能掌握攻击方法	熟练的攻击者才能完成这次攻击	漏洞利用条件非常苛刻
受影响用户 (Affected users)	所有用户，默认配置，关键用户	部分用户，非默认配置	极少数用户，匿名用户
可发现性 (Discoverability)	漏洞很显眼，攻击条件很容易获得	在私有区域，部分人能看到，需要深入挖掘漏洞	发现漏洞极其困难

计算风险等级

由以上五个指标加权平均算出危险评级：

- 严重：9-10
- 高危：6-8
- 中危：3-5
- 低危：1-2
- 忽略：0

DREAD模型的计算方式：

等级[忽略(0),严重(10)]=(潜在损失[0,10]+重现性[0,10]+可利用性[0,10]+受影响用户[0,10]+可发现性[0,10])/2

其中，

1. 潜在损失、重现性、可利用性任意一个值为0，总分即为0；
2. 等级为0总分除以2后取整。

风险校正和缓解措施

根据DREAD模型计算的5个维度的权重都是1，而通常情况下更多人更看重漏洞危害对等级的影响，或者有的只看重危害和利用难度，或者有的只看重危害+利用难度+影响用户，那么权重是不是需要调整呢，或者删掉一些维度呢？

这个需要大量的数据和实践来支撑，目前DREAD模型的标准权重是1，这个是模型的理论基础，后续结合实际情况再看是否和如何调整。

此外，大部分时间计算下来的漏洞都是中危以上，基本上很难计算出来低危的漏洞，而实际上确实有低危的情况。这可以通过以下方法来解决：

1. 方法一：引入部分漏洞类型，当选择这些类型的时候，会默认给出一些参考值。
2. 方法二：调整漏洞等级的大分和小分的值，例如现有低危计算是12，可以调整为0.5~3.5都是低危。

除了常见的5个维度，有些情况下，如果通盘考虑，除了传统意义上的安全风险，可能还有覆盖不全的？这需要考虑安全维度本身、公关风险和法律风险等因素。

安全验证

在威胁建模完成后，需要对整个过程进行回顾，不仅要确认缓解措施是否能够真正缓解潜在威胁，同时验证数据流图是否符合设计，代码是否符合预期等。

人员分工

- 20211108 俞振阳：DREAD应对方法
- 20211120 刘钟徽：STRIDE应对方法
- 20211125 苗靖章：基于DREAD模型的风险分析
- 20211106 隋吉达：安全性设计方案
- 20211112 周子凯：基于STRIDE模型的威胁分析、系统资源分析