要全面地认识一个安全问题，我们有很多种办法，但首先要理解安全问题的组成属性。前人通过无数实践，最后将安全的属性总结为安全三要素，简称CIA。安全三要素是安全的基本组成元素，分别是机密性（Confidentiality）、完整性（Integrity）、可用性（Availability）。

在安全领域里，我们把可能造成危害的来源称为威胁（Threat），而把可能会出现的损失称为风险（Risk）。

**什么是STRIDE模型**

威胁分析就是把所有的威胁都找出来。怎么找？一般是采用头脑风暴法。当然，也有一些比较科学的方法，比如使用一个模型，帮助我们去想，在哪些方面有可能会存在威胁，这个过程能够避免遗漏，这就是威胁建模。

微软提出的STRIDE（6个单词的首字母缩写）可以指导我们应该从哪些方面去对遭受的威胁进行建模，在分析威胁时，可以从以下6个方面去考虑。

威胁 定义 对应的安全属性

Spoofing（伪装） 冒充他人身份 认证

Tampering（篡改） 修改数据或代码 完整性

Repudiation（抵赖） 否认做过的事情 不可抵赖性

Information Disclosure（信息泄露） 机密信息泄露 机密性

Denial of Service（拒绝服务） 拒绝服务 可用性

Elevation of Privilege（提升权限） 未经授权获得许可 授权

在进行威胁分析时，要尽可能地不遗漏威胁，头脑风暴的过程可以确定攻击面（Attack Surface）。

一个威胁到底能够造成多大的危害，如何去衡量它？这就要考虑到风险了。我们判断风险高低的过程，就是风险分析的过程。

**什么是DREAD模型**

影响风险高低的因素，除了造成损失的大小外，还需要考虑到发生的可能性。地震的危害很大，但是地震、火山活动一般是在大陆板块边缘频繁出现，比如日本、印尼就处于这些地理位置，因此地震频发；而在大陆板块中心，若是地质结构以整块的岩石为主，则不太容易发生地震，因此地震的风险就要小很多。我们在考虑安全问题时，要结合具体情况，权衡事件发生的可能性，才能正确地判断出风险。

如何更科学地衡量风险呢？微软提出的DREAD（也是几个单词的首字母缩写）可以指导我们应该从哪些方面去判断一个威胁的风险程度。

Damage Potential

等级高(3)获取完全验证权限；执行管理员操作；非法上传文件

等级中(2)泄露敏感信息

等级低(1)泄露其他信息

Reproducibility

等级高(3)攻击者可以随意再次攻击

等级中(2)攻击者可以重复攻击，但有时间限制

等级低(1)攻击者很难重复攻击过程

Exploitability

等级高(3)初学者在短期内能掌握攻击方法

等级中(2)熟练的攻击者才能完成这次攻击

等级低(1)漏洞利用条件非常苛刻

Affected users

等级高(3)所有用户，默认配置，关键用户

等级中(2)部分用户，非默认配置

等级低(1)极少数用户，匿名用户

Discoverability

等级高(3)漏洞很显眼，攻击条件很容易获得

等级中(2)在私有区域，部分人能看到，需要深入挖掘漏洞

等级低(1)发现该漏洞极其困难

在DREAD模型里，每一个因素都可以分为高、中、低三个等级。在上表中，高、中、低三个等级分别以3、2、1的分数代表其权重值。我们可以具体计算出某一个威胁的风险值。

任何系统的安全属性主要包括机密性（confidentiality），完整性（integrity），可用性（availability），认证（authentication），授权（authorization）和不可抵赖性（non-repudiation）。

对应的威胁分别是：





