最近有很多朋友问令牌能不能破解。边肖结合多年经验整理出一些破解令牌对应的信息，分享给大家。

一般自我发展

传输时间间隔

设置同一号码重复发送的时间间隔，一般设置为60-120秒。这种方式可以在一定程度上防止短信界面被恶意攻击，对用户体验没有任何伤害。然而，它可以&#039；不能防止黑客更换手机号码进行攻击，防护等级低。

获取次数限制

限制手机号码在一定时间内获取短信验证码次数的上限。采用这种策略时，在产品设计过程中有几点需要注意。

定义上限值。根据真实的业务情况甚至需要考虑到未来的业务发展，设置一个合适的上限值，以避免用户因收不到短信验证码而产生投诉。

定义锁定期。可以是24小时，12小时，也可以是6小时。需要根据业务情况来定义。

IPlimit

设置单个IP地址在一定时间段内的最大传输量。这种方法可以很好的防止来自单个IP地址的攻击，但是也有两个明显的缺点：

针对频繁更换IP地址进行攻击的黑客。这种方法效果不好。

IP的限制经常造成意外伤害。比如一些使用统一无线网络的地方，很多用户连接到同一个无线网络，这个IP地址很快就很容易达到上限。因此，连接到无线网络的用户无法正常接收验证码。

图形验证码

发送短信验证码前，必须通过图形验证码的验证。这种方法可以相对防止一些攻击。所以也是目前非常常见的短信反攻击机制。但使用过程中涉及到用户体验，不能简单粗暴地套用这种策略。以下几点值得仔细考虑：

每次获取短信验证码前，是否需要用户输入图形验证码？一般来说，这样会很大程度上影响用户体验。虽然相对安全，但用户并不满意。

可以给出一个安全范围。结合手机号限制和IP限制来考虑，比如同一个手机号同一天第三次获取短信验证码。，出现一个图形验证码；比如同一个IP地址在同一天获得验证码超过100次后，就会出现图形验证码。

加密限制

通过对传输到服务器的参数进行加密，在服务器端进行解密。同时使用token作为唯一的身份验证，在后端对token进行验证。验证通过后才能正常发送短信。这种方式在保证用户体验的同时可以有效防止一些攻击，因此也是目前常见的短信反攻击机制。。同时也有明显的缺点：

中使用的加解密算法可能被破解，需要考虑使用难以破解的加解密算法。

不破解算法可以有效防止消息攻击，但不能防止浏览器模拟器攻击。

以上是几种常见的短信风险控制策略，在具体的产品设计过程中可以综合运用。

使用第三方防御

短信防火墙

为了在产品安全性和优秀的用户体验之间找到一个绝佳的平衡点，。新信科技的产品研发团队结合各种风控策略的优势，开发了短信防火墙。从以下几个方面总结一下：

为了保证优秀的用户体验，我们抛弃了目前对用户体验影响最严重的图形验证码等人机验证程序。实现无感验证。从而达到完美的用户体验。

结合用户的手机号、IP地址、设备指纹三个唯一身份，设定不同维度的风控策略。协调各维度，达到最合理的风险控制限额指标。

根据业务情况自动伸缩风控限额，检测场所被攻击时自动提高风控限额，正常时恢复正常风控标准。

考虑到新老客户的不同，特别增加了老客户的VIP通道。当受到攻击时，在风险控制指标紧张的情况下，确保老客户&#039；渠道畅通，减少误伤率。

通过以上策略，可以防止黑客通过随机切换手机号码和IP地址来盗取短信。同时增加模拟器检测、参数加密等风控策略。，有效防止黑客攻击。

可以通过风控防火墙的控制台实时观察风控的结果，达到被攻击时预警的效果。

更多资讯请关注新新科技官网：newxtc.com

。

请点击进入图片说明

请点击进入图片说明

短信防火墙

普通自开发

发送时间间隔

设置相同。，一般设置为60-120秒。这种方式可以在一定程度上防止短信界面被恶意攻击，对用户体验没有任何伤害。然而，它可以&#039；不能防止黑客更换手机号码进行攻击，防护等级低。

采集次数限制

限制手机号码在一定时间内获取短信验证码次数的上限。采用这种策略时，在产品设计过程中有几点需要注意。

定义上限值。根据实际业务情况，甚至需要考虑未来的业务发展来设定一个合适的上限。避免用户因收不到短信验证码而引发投诉。

定义锁定期。可以是24小时，12小时，也可以是6小时。需要根据业务情况来定义。

IP限制

设置单个IP地址在一定时间段内的最大传输量。这种方法可以很好的防止单个IP地址的攻击，但是也有两个明显的缺点：

对于经常更换IP地址进行攻击的黑客来说，这种方法没有什么好的效果。

IP限制经常导致意外伤害。比如在一些使用统一无线网络的地方，很多用户连接到同一个无线网络，这个IP地址很容易就会很快达到上限，从而导致连接到无线网络的用户无法正常接收验证码。

图形验证码

发送短信验证码前，必须通过图形验证码的验证。这种方式可以相对防止一些攻击，所以也是目前非常常见的短信反攻击机制。但使用过程中涉及到用户体验，不能简单粗暴地套用这种策略。。以下几点值得仔细考虑：

用户是否有必要每次都输入图形验证码才能获得短信验证码？一般来说，这样会很大程度上影响用户体验，虽然相对安全，但是用户用着不舒服。

可以给出一个安全范围。。考虑到手机号和IP的限制，比如同一个手机号在同一天第三次获取短信验证码时，出现图形验证码；比如同一个IP地址在同一天获得验证码超过100次后，就会出现图形验证码。

加密限制

通过对传输到服务器的参数进行加密，在服务器端进行解密，以token作为唯一身份验证，并在后端对token进行验证，使短信能够正常发送。这种方法可以保证用户体验，可以有效防止一些攻击，所以也是目前常见的短信反攻击机制。同时也有明显的缺点：

中使用的加解密算法可能被破解，需要考虑使用难以破解的加解密算法。

不破解算法可以有效防止消息攻击，但不能防止浏览器模拟器攻击。

以上是几种常见的短信风险控制策略，在具体的产品设计过程中可以综合运用。

使用第三方防御

短信防火墙

为了在产品安全性和优秀的用户体验之间找到一个绝佳的平衡点。新信科技的产品研发团队结合各种风控策略的优势，开发了短信防火墙。从以下几个方面总结：

为了保证优秀的用户体验，我们摒弃了目前对用户体验影响最严重的图形验证码等人机验证程序，实现了无感验证。从而达到完美的用户体验。

结合用户的手机号、IP地址、设备指纹三个唯一身份，设置不同维度的风控策略。协调各维度，达到最合理的风险控制限额指标。

根据业务情况自动伸缩风控限额。当检测场所受到攻击时，会自动增加风控限制，正常情况下回归正常风控标准。

考虑到新老客户的不同，特别增加老客户的VIP通道，保证在受到攻击时，风控指标收紧时，老客户的通道畅通无阻。，从而降低意外伤害率。

通过以上策略，可以防止黑客通过随机切换手机号码和IP地址来盗取短信。同时加入模拟器检测、参数加密等风险控制策略，有效防止黑客攻击。

可以通过风控防火墙控制台实时观察风控结果，达到被攻击时预警的效果。

更多信息请关注新新科技官网：newxtc.com

短信防火墙

。

请点击进入图片说明

请点击进入图片说明

短信防火墙

令牌是收据，但比车票温柔多了。如果票丢了，你可以再买一张。如果令牌丢失，只需重新操作并验证它。因此，丢失令牌的成本是可以忍受的。——前提是你不&#039；不要经常丢失它。如果让用户三五次认证一次，会损失用户体验。

在客户端，除非你有非常安全的方法，比如操作系统提供的私有数据的存储。，那么token肯定会有泄露问题。比如我拿了你的手机，复制了你的令牌，就可以在令牌过期之前，以你的身份在别处登录。解决这个问题的简单方法

1。存放令牌时对称存放，及时解锁。

2。结合请求URL、时间戳和令牌，添加盐和签名，服务器将检查有效性。

这两种方法的出发点都是，窃取你存储的数据比较容易，但是拆解你的程序hack，你的加解密和签名算法比较困难。不过说难不难，毕竟是防君子防小人的做法。。换句话说，如果有人打开客户端，加密和存储客户端将不会以纯文本形式存储.

方法一：可以&#039；t获取存储的密文；方法二：它不&#039；t不知道你的签名算法和盐，可以一起吃。

但是如果令牌被复制走，他可以很自然的植入到手机里，那么他的手机也可以当你用，你就瞎了。

因此，它可以为用户提供一种机制，以主动终止与过去令牌类似的机制，并可以在被盗时远程阻止损失。

如果一个人能谈论安全，他怎么能谈论安全呢&#039；他连手机都不保护.[XY002][XY001]令牌在网络级明文传输会非常危险，建议使用HTTPS，将令牌放在post体中。

都看完了嘛？相信现在你对token能否破解已经有了初步的了解！还可以收集页面获得更多破解，获得代币知识！区块链，虚拟货币，我们是认真的！