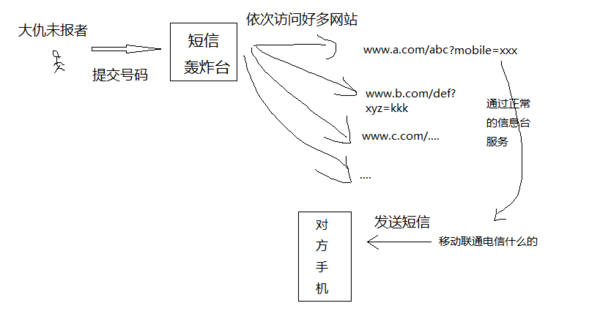
1、为什么有短信轰炸？

短信轰炸是某些不良商家出售用于报复某人使用的软件或者网页形态，该软件会搜集多家没有做好安全防范措施的客户代码，一般是用注册验证码对报复对象进行轰炸，短信发送平台跟平台客户都是受害者



2、怎么防范短信轰炸？

使用网页或者app客户端进行验证码校验注册的界面上要做如下设置

2.1点击获取验证码，当发送请求成功后，按钮默认60秒后才能重新发送（必选）

2.1.1做出刷新动作（如，按下F5），同一手机号码一分钟内无法注册（必选）

2.1.2退出网站或关闭App重新进入，同一手机号码一分钟内无法注册

交互行为：按钮倒计时继续，或点击后弹窗“您的手机一分钟内只能获取一次验证码”

2.2当多次（2-5次）同一号码请求验证码，请弹出二次验证方式，或直接采用先识别图片验证码或者图形验证码后才允许获取短信验证码的方式（推荐）

图片验证码或图形验证码来验证该操作不为机器人，二次验证方式越难被机器识别，则效果越好





2.3限制请求来源为同一ip地址的请求次数，可将次数限制为3-10次以内，根据项目实际情况进行配置（可选）

2.4 使用验证码的界面如有多个表单填写项，请设置为部分表单填写后才能使用短信验证码按钮（必选）

2.5 限制同一号码每小时3-5次请求次数，每天10次请求次数（可选）

交互：您的手机号码输入太频繁，请明天再来

2.6 在手机号码输入后，检验该手机号码是否已经在系统内存在（网易）



2.7可采用先输入手机号码，然后点击注册按钮后切换到第二个界面才能点击获取验证码，增加同一页面批量操作的难度（小米）



创蓝平台安全配置

2.8在自助通后台配置绑定API发送请求服务器地址，可绑定多个ip（必选）



如果以上措施都有做好，还是被轰炸？

可以请求创蓝技术协助查询平台接收请求的IP来源分布

如果出现非自有服务器的IP请求，则可能是账号跟密码泄露，请修改api密码和自助通密码

如果请求来源为自有服务器IP请求，则为WEB跟APP的存在漏洞，导致被轰炸程序利用，可考虑暂停短信验证服务

额外解决方案：

考虑采用上行短信验证方式



苏宁案例

http://www.codesec.net/view/54850.html