聊聊短信验证码安全——安全小课堂第二十四期

京东安全应急响应中心 2016-08-26

安全小课堂第二十四期

讲到短信验证码就不得不先说一说密码，作为保护安全技术手段的典型代表，如果密码泄露，用户安全防御的最后底线就没了，短信验证码的兴起对用户密码找回、网购银行交易是一种安全性很高的身份识别方式。本期我们来聊一聊短信验证码安全。

本期邀请到
360安全专家XEM
安全白帽子BMa
大家欢迎~

/ 01 /

豌豆妹

短信验证码的作用是什么？

葫芦娃 

讲到短信验证码就不得不先说一说密码，作为保护安全技术手段典型代表如果密码泄露用户安全防御的最后底线就没有秘密可言，短信验证码兴起对用户密码找回，网购银行交易是一种安全性很高的身份识别方式！

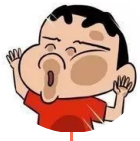
小丸子 

信验证码主要还是用于验证用户身份，常用在注册、登录、找回密码、修改用户信息、支付以及其他与用户身份相关的流程中。

豌豆妹

短信验证码存在的安全问题可太多啦~咱们举三个最典型的例子呗，并分别说明该问题的产生原因描述以及解决建议。

小新



1、手机木马：主要集中在 Android手机利用钓鱼或漏洞方式手机被下载安装APK木马从而控制手机获取短信验证码，安装手机木马查杀软件不要浏览安装不明APK 安装包；

2、蜂窝网络GSM 嗅探：伪基站和 GSM 嗅探，目前3G 的普及问题，当然攻击者也可以有办法屏蔽或干扰3G信号，这时候手机就会自动转为2G，这样GSM短信仍然可以监听到了；

3、云同步软件及验证码服务商： 手机自带云同步功能。例如黑客使用社工库泄漏密码登陆云同步平台，通过这个方式可以获取短信验证码，其次验证码云服务商平台漏洞，导致被黑客入侵短信验证可以被截取。

柴可夫斯基

楼上小伙伴总结的太棒了，我这里还有一些自己的补充。

1、先说说短信验证码的泄漏吧，一般web应用中存在的短信验证码泄漏基本上是直接返回出来，例如url，body，http头都可能存在，我常用的检测方式是bp抓包后，输入手机收到的验证码，看看返回数据中是否存在，还有可能是云端的泄漏，如短信提供商、管理邮箱、管理接口等。泄漏的方式有多种：直接明文、md5。原因多种：debug的问题、短信验证码验证的逻辑问题（前端验证）。建议：回显中删除即可。这是应用的处理方式，对于云端的泄漏，基本上是由于云端管理帐号的问题了。
2、此外，短信验证码功能在设计上存在缺陷的话也会产生很多安全问题：如短信风暴、验证逻辑绕过、短信验证码泄露、验证码暴力破解等。
3、然后，就是常见的验证逻辑绕过，验证逻辑没有通用的绕过，取决于后端服务的验证逻辑，常见的逻辑是：前端验证、不验证、固定短信验证码、只验证短信验证码有效而不验证与用户身份是否匹配。

/ 03 /

豌豆妹

能分享个经典案例么~

哆啦A梦

有个固定短信验证码的经典案例。不知道这个888888 是fuzz出来的，还是猜的。如

果是fuzz出来的，那就与短信验证码的爆破有关了。

微信账号任意手机号绑定漏洞

创建时间: 2015/2/15 更新时间: 2015/2/15 大小: 92KB

手机号码任意输入未绑定过的号码，验证码888888，手机号即更换成功，详情参见图片：

/ 04 /

豌豆妹

那如何防范短信验证码带来的安全隐患呢？

葫芦娃 

主要在于两个方面：验证码的健壮性、后端的验证逻辑。

健壮性：长度、随机性
验证逻辑：有效验证次数、验证频率、二次验证。
验证逻辑这块，还是要根据不同的业务场景，梳理业务流程，然后再对各种类型的问题加以防范。验证逻辑各种奇葩的情况都有，自己用的时候，不要太奇葩就行。上线前还要做好逻辑漏洞这一方面的安全测试。

豌豆妹

验证的太多影响了用户的体验，往往受到产品方强烈反对。忍住眼泪不哭~~

葫芦娃 

一般现在短信验证码会用在密码找回、注册 、支付，现在都是标配了。

豌豆妹

请教下大牛们，短信的应用接口被恶意调用，目前有什么好的防御办法？

葫芦娃 

以前用了一个笨办法（说是笨办法是因为影响用户体验），发短信时加上图片验证码，1分钟才允许发一次，1分钟以内短信验证码有效，超时失效。

豌豆妹

见过短信轰炸平台，他们专门搜集了各个电商、p2p金融等验证码请求的URL，请求时替换手机号，即可对应手机号的手机发起短信轰炸。

葫芦娃

有二次验证还是能起很大作用。用户体验也不会很差，例如现在比较流行的滑动验证。

豌豆妹

谢谢小伙伴的精彩回答。屏幕前的你，想和大牛们隔空交流哪个话题呢？可以把你的想法回复给我，豌豆妹会在后台收集，选出最有代表性的那一个话题哟~**被选中的小伙伴将会获得神秘礼物一份**。(。·∀·)ﾉﾞ下期见！

安全小课堂往期回顾：

1、论安全响应中心的初衷；
2、安全应急响应中心之威胁情报探索；
3、论安全漏洞响应机制扩展；
4、企业级未授权访问漏洞防御实践；
5、浅谈企业SQL注入漏洞的危害与防御；
6、信息泄露之配置不当；
7、XSS之攻击与防御；
8、电商和O2O行业诈骗那些事儿（上）；
9、电商和O2O行业诈骗那些事儿（下）；
10、CSRF的攻击与防御；
11、账户体系安全管理探讨；
12、远程代码执行漏洞的探讨；
13、服务器安全管控的探讨；
14、畅谈端口安全配置；
15、谈一谈github泄露；
16、撞库攻击是场持久战；
17、url重定向攻击的探讨；
18、聊聊弱口令的危害（一）；
19、聊聊弱口令的危害（二）；

20、聊聊XML注入攻击；
21、聊聊暴力破解；
22、谈谈上传漏洞；
23、浅谈内网渗透。