TC260-PG-20182A

网络安全实践指南

—应对截获短信验证码实施网络身份假冒攻击的技术指引

全国信息安全标准化技术委员会秘书处

2018 年 2 月 11 日

本文档可从以下网址获得：

https://www.tc260.org.cn/front/postDetail.html?id=20180211153548

全国信息安全标准化技术委员会

NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

声　明

本指南内容基于已有行业实践进行总结，使用指南推荐措施所产生的风险由使用者自行承担。全国信息安全标准化技术委员会不对采取本指南所列措施产生的风险承担任何相关责任。

技术支持单位

本实践指南得到中国电子技术标准化研究院、中国电子信息产业发展研究院、中国电信集团有限公司、中国移动通信集团有限公司、中国联合网络通信集团有限公司、腾讯、蚂蚁金服、百度、京东、360、华为等单位的技术支持。

一、问题描述

当前，使用短信验证码验证用户身份的技术被广泛应用于各类移动应用、网站服务。由于GSM网络存在单向鉴权和短信内容无加密传输等局限性，且短信截获攻击呈现工具化和自动化趋势，使利用此类威胁实施攻击的门槛大幅降低，基于短信验证码实现身份验证的安全风险显著增加。

典型案例。近期，各地出现了多起利用手机信号劫持设备等工具，非法截获受害者短信验证码、手机号码，实施网络身份假冒攻击，并结合社工（如钓鱼网站）或黑产交易等方式获得受害者身份证号码、银行卡号、支付平台账号等其他敏感信息，进而盗刷受害者银行卡、骗取借款等。

特征分析。该类攻击主要利用了短信验证码在用户身份验证方面存在的安全缺陷，具有如下特点：

——攻击手法工具化。截获短信的攻击手段早在 2010 年已出现，由于攻击技术实施难度大，当时仅掌握在少数高级攻击者手中，难以大规模利用。目前，该攻击手法各主要环节已经工具化和自动化，攻击门槛降低，一般攻击者可通过购买工具实施攻击，威胁骤增。

——攻击影响范围广。由于短信验证码技术被广泛用于各类移动应用、网站服务的身份验证，短信截获攻击手段一旦被大规模利用，安全风险高，可能导致基于短信验证码实现身份认证的技术失效，造成公民财产损失，危害互联网生

态安全。

——缺陷修复难度大。目前，GSM 网络使用单向鉴权技术，且短信内容以明文形式传输，该缺陷由 GSM 设计造成，且 GSM 网络覆盖范围广，因此修复难度大、成本高。

——攻击过程全链条化。攻击者在利用手机信号劫持设备等工具非法截获短信验证码、手机号码的基础上，并通过社工或黑产交易等方式获取身份证号码、银行账号、支付平台账号等敏感信息，已组合形成攻击产业链。

——攻击过程隐匿化。攻击过程中，受害者的手机信号被劫持，攻击者假冒受害者身份接入通信网络，受害者一般难以觉察。

二、风险分析

此类攻击主要对依赖短信验证码进行用户身份验证的移动应用、网站服务提供商造成安全威胁。攻击者在截获短信验证码后，能够假冒受害者身份，成功通过移动应用、网站服务提供商的身份验证安全机制，实施信用卡盗刷等网络犯罪，给用户带来经济损失。

三、措施建议

建议各移动应用、网站服务提供商对业务系统中短信验证码的使用方式进行摸底，例如在用户注册、密码找回、资金支付等环节的短信验证码使用情况，并评估相关安全风险，优化用户身份验证措施。以下身份验证措施，建议选用一种

或采用多种方式组合，加强安全性：

1. 短信上行验证。提供由用户主动发送短信用以验证身份的功能，如要求用户在规定时间内（如 60 秒），使用已绑定的手机号码向移动应用、网站服务提供商指定的短信服务号码发送指定内容短信，移动应用、网站服务根据短信内容对用户身份进行验证。

2. 语音通话传输验证码。提供通过语音通话传输验证码的功能，需要验证用户身份时，由用户向移动应用、网站服务发送验证码请求，移动应用、网站服务提供商拨打用户绑定的手机号码，以语音通话方式告知用户验证码。

3. 常用设备绑定。提供将用户账号与常用设备绑定的功能，原则上支付、转账等敏感操作只能通过该绑定设备执行。设备绑定、更换等操作应采用短信上行验证、语音通话传输验证码等方式，并采用诸如要求用户回答预设问题、提供注册时填写的相关用户信息或核对该用户账号近期操作记录等方法进一步确认用户身份。

4. 生物特征识别。提供通过生物特征识别技术验证用户身份的功能，采用指纹识别、人脸识别等生物特征识别技术验证用户身份。

5. 动态选择身份验证方式。提供动态选择用户身份验证的方式，当需要验证用户身份时，移动应用、网站服务提供商随机选择短信验证、语音通话验证、生物特征验证等方式

中的一种或多种，进行用户身份验证。

此外，个人用户应做好手机号、身份证号、银行卡号、支付平台账号等敏感信息的保护。在收到来历不明的短信验证码等异常情况时，提高警惕，及时联系相关移动应用、网站服务提供商。