

潘俊·第四场



用户安全验证探索

潘俊 美团点评高级前端工程师

1. 安全验证在Web服务中的位置
2. 验证的类型和优劣、强验证弱验证（对于用户识别）、扩展的动态类型的验证
3. 如何从产品整体层面来规划和制定策略

用户身份验证探索



潘 俊
美团前端开发



浏览信息和操作是Web服务的两种基本表达方式

安全验证的职责范围

01 信息安全

信息的分类与网站的性质有关系，最常见的一般分为隐私和非隐私两大类。

结合产品自身的特性来选择信息如何呈现给用户。

02 操作安全

常规操作和敏感操作对于验证的需求并不相同。

Case: [新买的手机有了别人的数据]

Case: [新注册了一个账号，发现了不属于自己的东西]

越来越少的网站只存在单一的密码登录了

密码登录

快速登录

帐号密码登录

panjun847@vip.qq.com

☐ 下次自动登录

登 录

忘记密码?

注册新帐号

意见反馈

×

登录支付宝

panjun847@gmail.com

删除

忘记密码?

登 录

立即注册

淘宝会员登录 账户激活 免费注册

帐号登录

手机动态码登录

panjun02@meituan.com

.....

☐ 7天内自动登录

忘记密码?

登 录

还没有账号? 免费注册

用合作网站账号登录

越来越少的网站只存在单一的密码登录了

密码登录的局限性

设置个简单的密码
被无脑破解

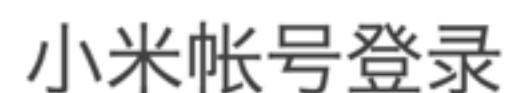
喜欢用相同的密码
被攻击就凉凉



设置复杂的
记得住么？记得住么？

用不同的密码
于是出现了密码本

短信快捷登录

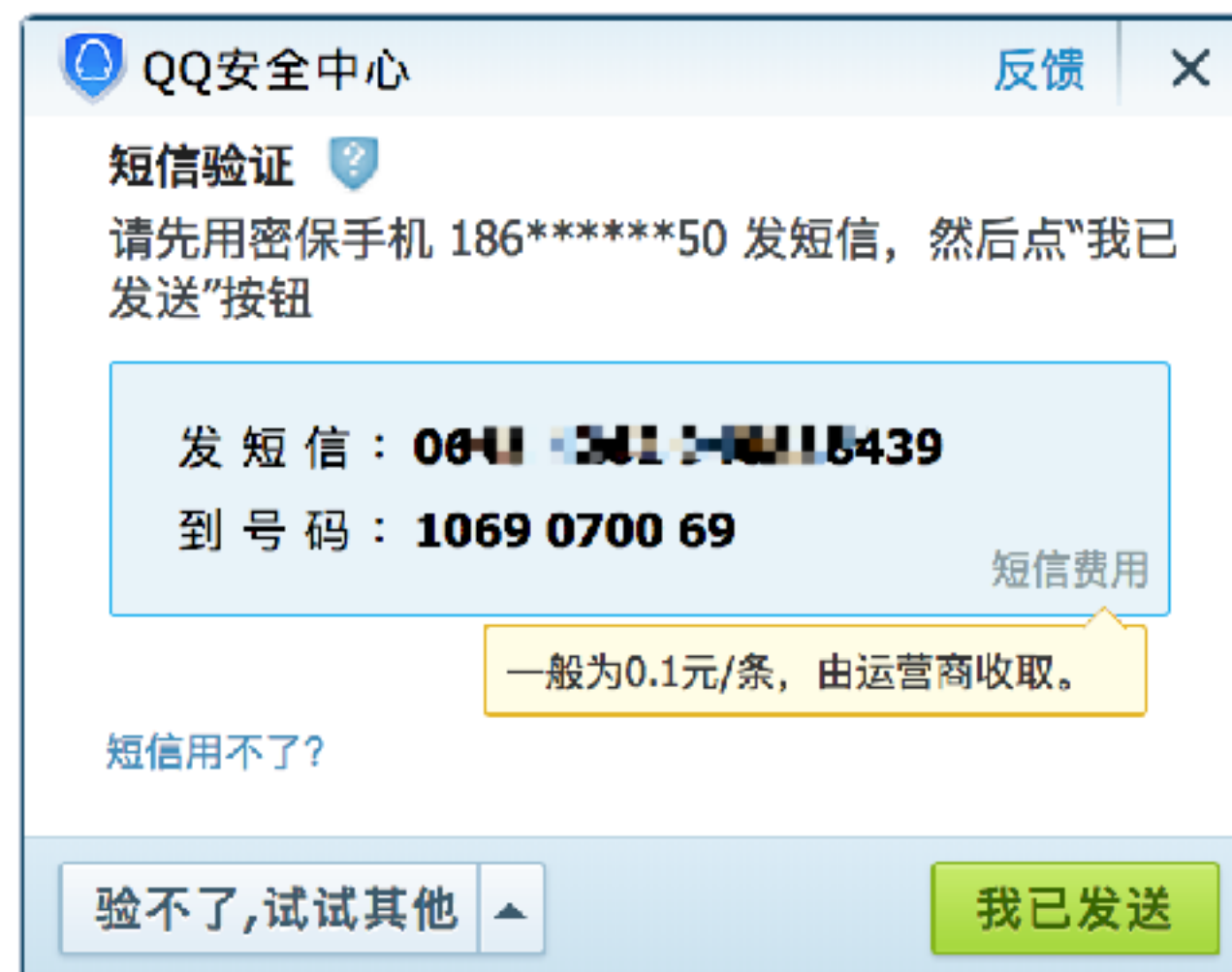



短信验证码	获取验证码
-------	-------

[立即登录/注册](#)

用户名密码登录

[其他方式登录](#)



[普通方式登录](#) 

☎ 手机号

动态码 获取手机动态码

☐ 7天内自动登录[忘记密码?](#)

登录

提示：未注册美团账号的手机号，登录时将自动注册美团账号，且代表您已同意《[美团网用户协议](#)》

用合作网站账号登录



手机短信登录对大部分网站来讲利大于弊

短信登录的兴起

验证码短信

用于发送验证码类短信，如登录验证、支付确认、登录异常等

短信使用量阶梯（条/月）	量≤10万	10万<量≤30万	30万<量≤50万	50万<量≤100万	100万<量≤300万	量>300万
单位（元/条）	¥0.045	¥0.040	¥0.039	¥0.038	¥0.037	¥0.036

短信通知

用于发送系统通知类短信，如物流通知、付款回执、状态通知等

短信使用量阶梯（条/月）	量≤10万	10万<量≤30万	30万<量≤50万	50万<量≤100万	100万<量≤300万	量>300万
单位（元/条）	¥0.045	¥0.040	¥0.039	¥0.038	¥0.037	¥0.036

要想简单，接短信发送的第三方SDK。要想便宜，就接通道商

短信开发的一些常见的问题

A

防范短信轰炸

接口限流控制（对于单个设备，单个IP，单个号码都应该设置发送次数上限）。

B

短信的有效期

有效期设置的时间要合适，时长不足容易造成短信未到达即失效，太长容易增加安全风险

C

服务商和费用

第三方不用维护通道，但是相对贵一些。自建单价会相对便宜，不过需要付出更多开发代价

手机短信登录对大部分网站来讲利大于弊

短信登录的利弊

利

简单快捷安全

- 1. 操作简单且对用户免费
- 2. 产品可选择无需注册，更快捷
- 3. 临时密码，比设置的密码更安全

弊

手机号是可以回收的

- 1. 实名制并不是终生绑定
- 2. 手机卡是实体的，可以丢失，和手机本身也并不绑定

扫码登录的本质是授权拷贝，从一个可信设备上克隆登录状态

扫码登录

2016.8

《条码支付业务规范》

当扫码变成
基本操作



使用手機微信掃碼登錄

網頁版微信需要配合手機使用

扫码成了移动互联网的一种基本表达方式

扫码的发展

技术成熟，成本低，承载信息量大，容错强
能和URL协议完美配合



用什么哪种方式来更新浏览器端的状态并不关键

扫码登录实例分析



生成
登录码

码过期



同步
码状态



扫码



确认

相关的关键字TOTP HOTP MFA

动态令牌



小米帐号登录

请输入小米安全令牌生成的动态口令

☐这是我的私人设备，以后登录无需输入口令

确定

小米令牌无法使用

安全验证

您的帐号存在安全风险，为保障帐号安全，登录前需验证身份。

验证方式

百度安全中心手机版

动态令牌 二维码扫描 一键验证

请打开您手机上的百度安全中心客户端，输入动态令牌上随机变化的六位数字：

确定

帮助中心

帐号保护已开启，请根据提示完成以下操作



请在手机中打开手机阿里云APP或者Google Authenticator应用，输入6位动态码

☐记住这台机器，7天内无需再次验证

确定

如无法提供安全码，您可选择解除MFA绑定后继续操作

动态令牌基于时间的，算是当下比较强势的一种验证方式

动态令牌的简单介绍

手机的普及加速了动态令牌的发展和应用



One-Time Password

$$\text{OTP}(K,C) = \text{Truncate}(\text{HMAC-SHA-256}(K,C))$$

HMAC-based One-Time Password

$$\text{HOTP}(K,C) = \text{Truncate}(\text{HMAC-SHA-256}(K,C))$$

Time-based One-Time Password

$$\text{TOTP}(K,C) = \text{HOTP}(K,C) = \text{Truncate}(\text{HMAC-SHA-256}(K,C))$$

信息都是有价值的，但也有价值高低之分

附加信息验证

支付宝 | 重置登录密码

你正在为账户 **pan*@gmail.com** 重置登录密码，请选择重置方式：

✓

经过检测，你在**不常用的环境**下操作，需要进行安全校验

通过银行卡验证

推荐

可使用的任意一张银行卡进行验证

立即重置

通过“验证短信+回答安全保护问题”

立即重置

通过“验证短信+验证银行卡信息”

如果你的186*****50手机还在正常使用，且记得账户绑定的银行卡号，请选择此方式

立即重置

通过人工服务

填写申请单，上传身份证件图片，我们会在48小时内受理，请耐心等待

立即重置



能做附加信息验证，首先得有数据

附加信息验证的局限性

首先得有信息才能验证

用户得能认可这么强的验证

附加信息选取的合理化

申诉的是一种主动的防御策略

人工找回服务——账号申诉

安全验证边际成本高，收益小

体系完整的必备补充

申诉能提供更多信息

1验证身份信息

2填写申请表

3等待客服审核

成功

亲，如果您的手机验证通过或正确回答了如下问题，审核进度将大幅缩短

手机号码 186*****50（如果此手机无法接收校验码，可以不验证）

校验码

问题一 您实名认证时，使用的是哪家银行的卡？

答案

问题二 请填写您实名认证时使用的身份证到期时间

答案 ☒ ☐ 长期

问题三 您在支付宝设置的信用卡还款提醒日期？

答案

一般来讲动态类型的验证比静态类型的验证安全性更高

如何减少验证次数

设备化，将浏览器也设备化（通过一个长效COOKIE标识）

增加设备关联，历史数据来决定设备与账号关系

地域，IP，甚至活跃时间段都可以当成辅助来判定当前用户是否可信

未来可期

未来可能出现的情况

操作系统底层解决
PHONEID

判定号码
运营商的辅助信息

验证正在
变得简单

微信等软件的平台化
纯微信的开发增多

TOUCHID/FACEID
生物特征识别的应用化

成本包含实现成本和交互成本

该如何选择验证方式

A 密码登录

B 短信登录

C 动态令牌

D 扫码登录

E 其他

- 1.强依赖第三方登录（微信开发）
- 2.人脸识别，指纹识别等等

成本包含实现成本和交互成本

该如何选择验证方式

★ 星数量代表推荐顺序和开发的优先级

	密码登录	手机短信	动态令牌	扫码登录	人工申诉	微信登录
纯微信开发	★★	★★★★				★★★★★
手机App为主	★★	★★★★★★		★	★★	★★
PC浏览器为主	★★★★	★★★★	★★			
多端并重	★★★★	★★★★★	★★	★★★★★		★★★★
低交互信息类	★★★★★★	★				
工具类（重资产）	★★	★★★★★★	★★★★★★	★★★	★★★★★	★★★★★
工具类（重信息）	★★	★★★★★★	★★★★★★		★★★★★	

Q&A