

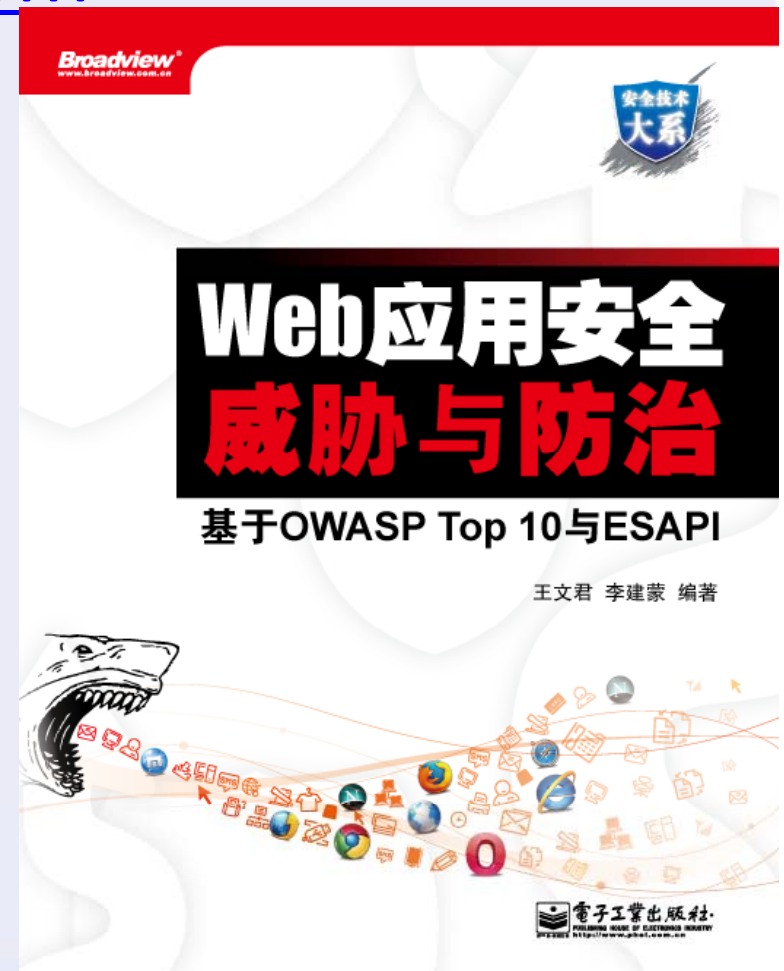
基于双因子验证加固 SaaS企业级应用



OWASP 中国
The Open Web Application Security Project



- 姓名: 王文君
- 电邮: Shanda.wang@gmail.com
- 微博: @王文君山大
- 工作: 产品安全架构师
+ OWASP上海负责人
- 爱好: 羽毛球, 网球, 古筝
- 著作: 2012年12月出版





OWASP 中国

The Open Web Application Security Project

- 基本概念 – 企业级软件, SaaS, 双因子验证
- SaaS企业级应用面临的风险及解决方案
- All In One – 基于双因子验证
- Demo



OWASP 中国
The Open Web Application Security Project

1. 基本概念介绍



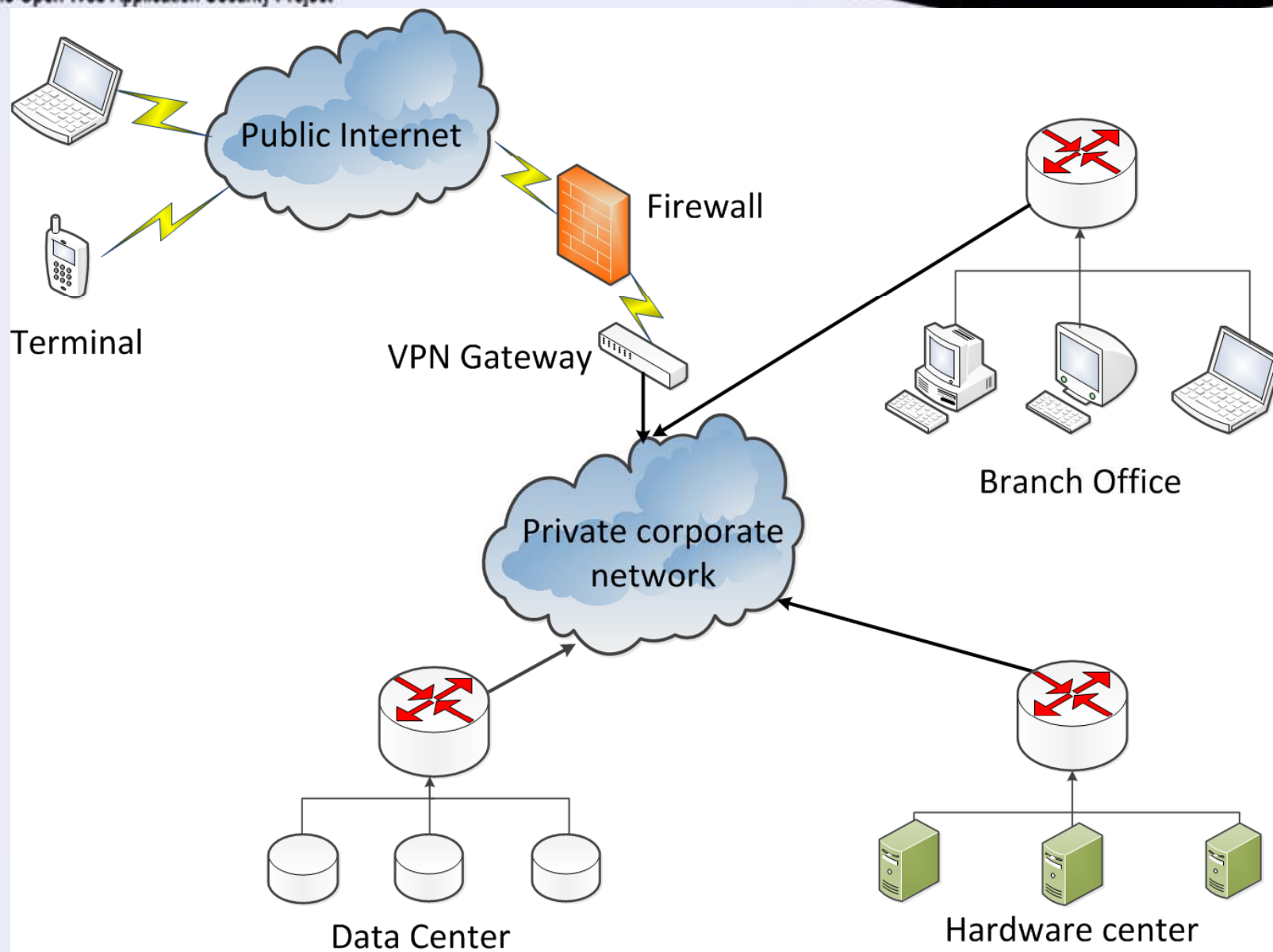
企业级软件：
支持企业各
项业务运作的软件



传统企业级软件部署方式



OWASP 中国
The Open Web Application Security Project





- SaaS – Software as a service(软件即服务)
 - 厂商部署, 用户按需订购
 - no license fee
 - 厂商维护, 用户无需关心
 - no maintenance fee
 - 更新速度快
 - Internet based, 给用户带来便利的同时, 也对安全提出了更高的要求

多因子验证



OWASP 中国
The Open Web Application Security Project

What you know

密码

密码短语

What you have

令牌

手机

What you are

指纹

视网膜



易用性



成本

我们身边的多因子验证例子



OWASP 中国
The Open Web Application Security Project



优盾



OWASP 中国
The Open Web Application Security Project

2. SaaS企业级软件 常见风险



OWASP 中国
The Open Web Application Security Project

暴力破解

CSRF

不可否认性

...

暴力破解常用的解决方案



OWASP 中国
The Open Web Application Security Project

✓ 多次登录失败锁定此账户



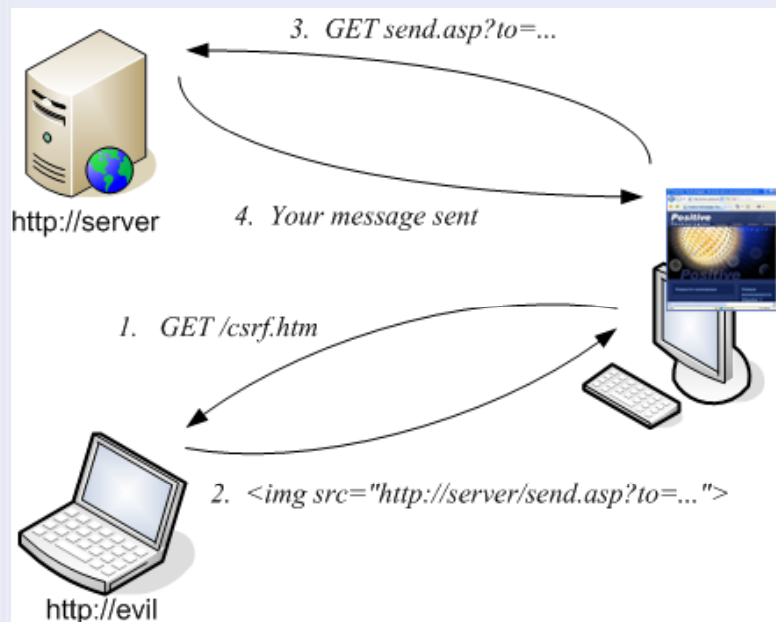
✓ CAPTCHA验证码

A CAPTCHA image showing the word 'smmm' in a stylized, cursive font.

CSRF常用的解决方案



✓ 回话强随机令牌



```
<form action="transferMoney.do"method="post">
  <input type="hidden"
    name="<%=HTTPUtilities.CSRF_TOKEN_NAME%>"
    value="<%=userToken%>" />
</form>
```

✓ 重要功能强制认证

卡号和密码

淘宝提醒您

1. 请勿将卡密发给任何人包括卖家，如有低信用帐号联系您，请勿轻信。
2. 请勿去卖家旺旺发给您的网址充值，唯一正确的充值地址在卖家的宝贝详情中：
3. 自动发货卖家绝不会用其他帐号或者分店的名义联系您！

1. 为了您的卡密安全，请输入您的支付宝账户支付密码查看卡密信息。
2. 本次操作仅用以查看卡密信息，不会导致确认收货并付款给卖家。

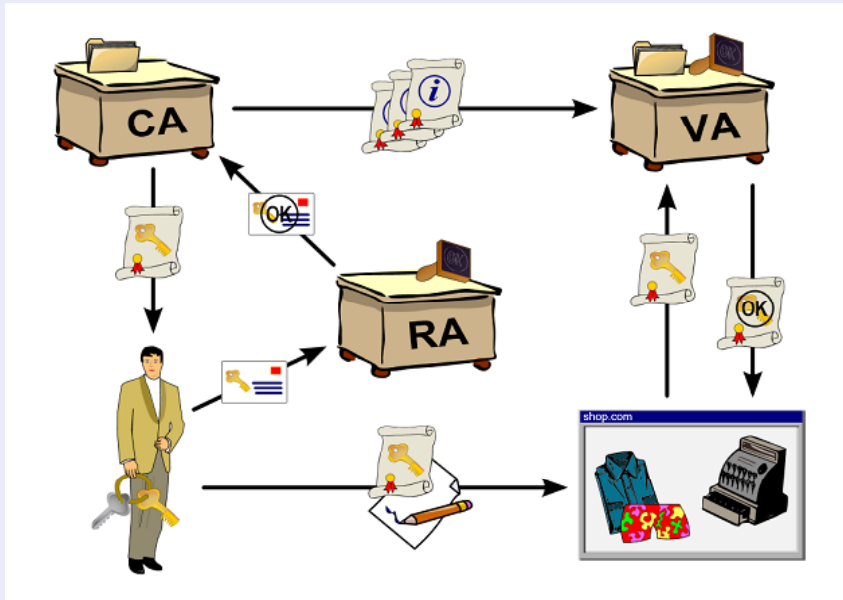
请输入支付宝账户支付密码*： 请输入

码。

不可否认性常用的解决方案



OWASP 中国
The Open Web Application Security Project



✓ 引入PKI



✓ 硬件令牌





OWASP 中国
The Open Web Application Security Project

3. All In One?

使用双因子验证保护你的应用



- What you know – 密码
- What you have – 手机

我们在智能手机上产生软令牌, 具有下列特点

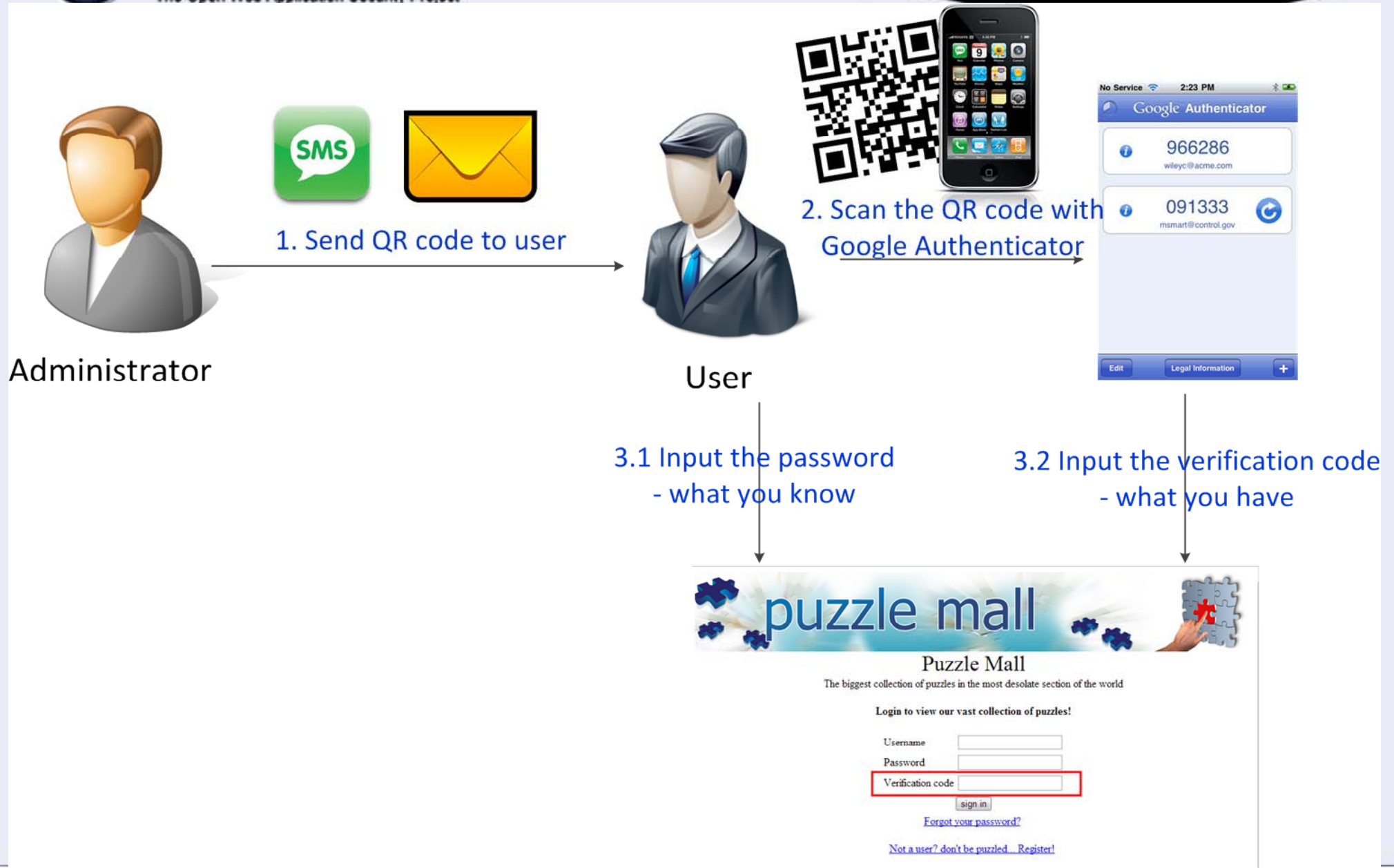
- 每个用户都唯一
- 软令牌存在的时间尽可能短, 如30秒
- 不需要额外的硬件投入



流程图



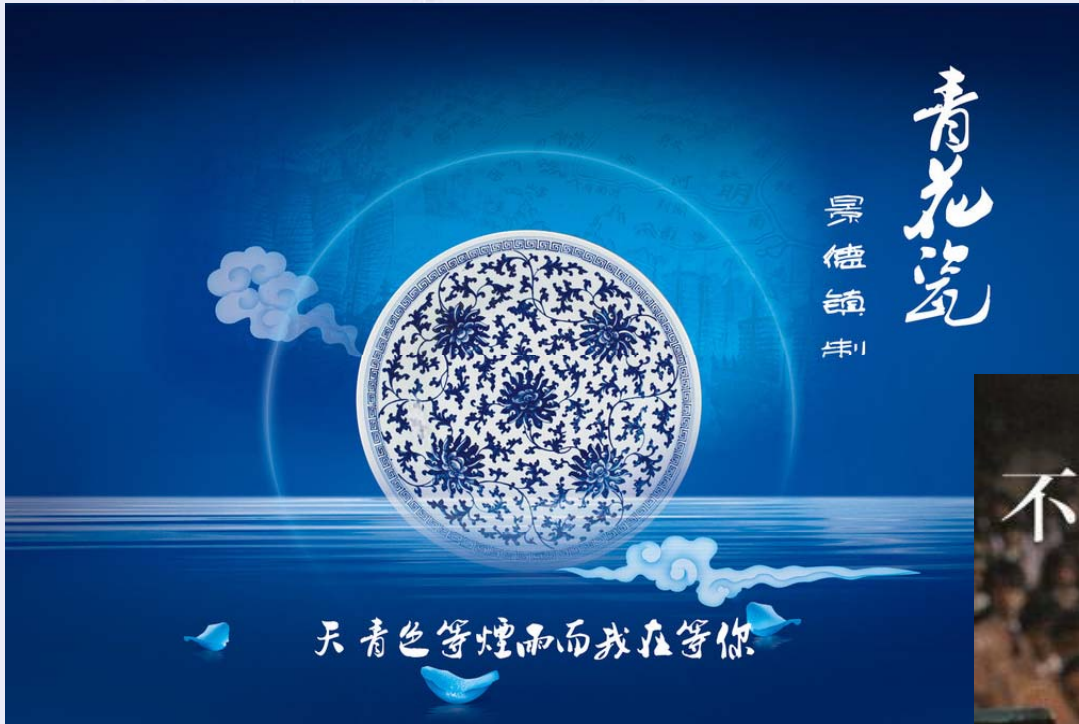
OWASP 中国
The Open Web Application Security Project



青花瓷隐藏在窑烧里的秘密



OWASP 中国
The Open Web Application Security Project



隐藏在窑烧里的秘密？



隐藏在QR码后的秘密



OWASP 中国
The Open Web Application Security Project



<https://www.google.com/chart?chs=200x200&chld=M|0&cht=qr&chl=otpauth://totp/kevin?secret=3SKVYYDJT52PE7UR>



OWASP 中国

The Open Web Application Security Project

中国联通 3G 下午5:07 90%



Google™ 身份验证器

989232

kevin

编辑

法律信息



扫描QR码后每30秒产生
一个新的验证码



- 客户端 - Google Authenticator
 - 各种手机客户端都可下载
 - TOTP(Time-based One Time Password), [RFC6238](#)
 - Secret key是80bit, 16位base 32编码(QRCode)
 - 每30秒产生一个OTP(HMAC-SHA编码, 前6位)



OWASP 中国

The Open Web Application Security Project

- 服务器端 – 我们只要实现这部分代码
 - TOTP([RFC6238](#))的实现(Java, PHP, Ruby...)
 - 用户密钥的生成以及管理
 - QR code的生成
 - 服务器端的容错



如果每次输入手机上产生的OTP, 但服务器端怎么也通不过验证, 可能的问题就是客户端和服务器的时间同步问题

– 服务器端时间同步

- NTPD(Network Time Protocol Daemon)

– 客户端时间同步

- 手机时间同步功能



算法保密？密钥保密？



OWASP 中国
The Open Web Application Security Project

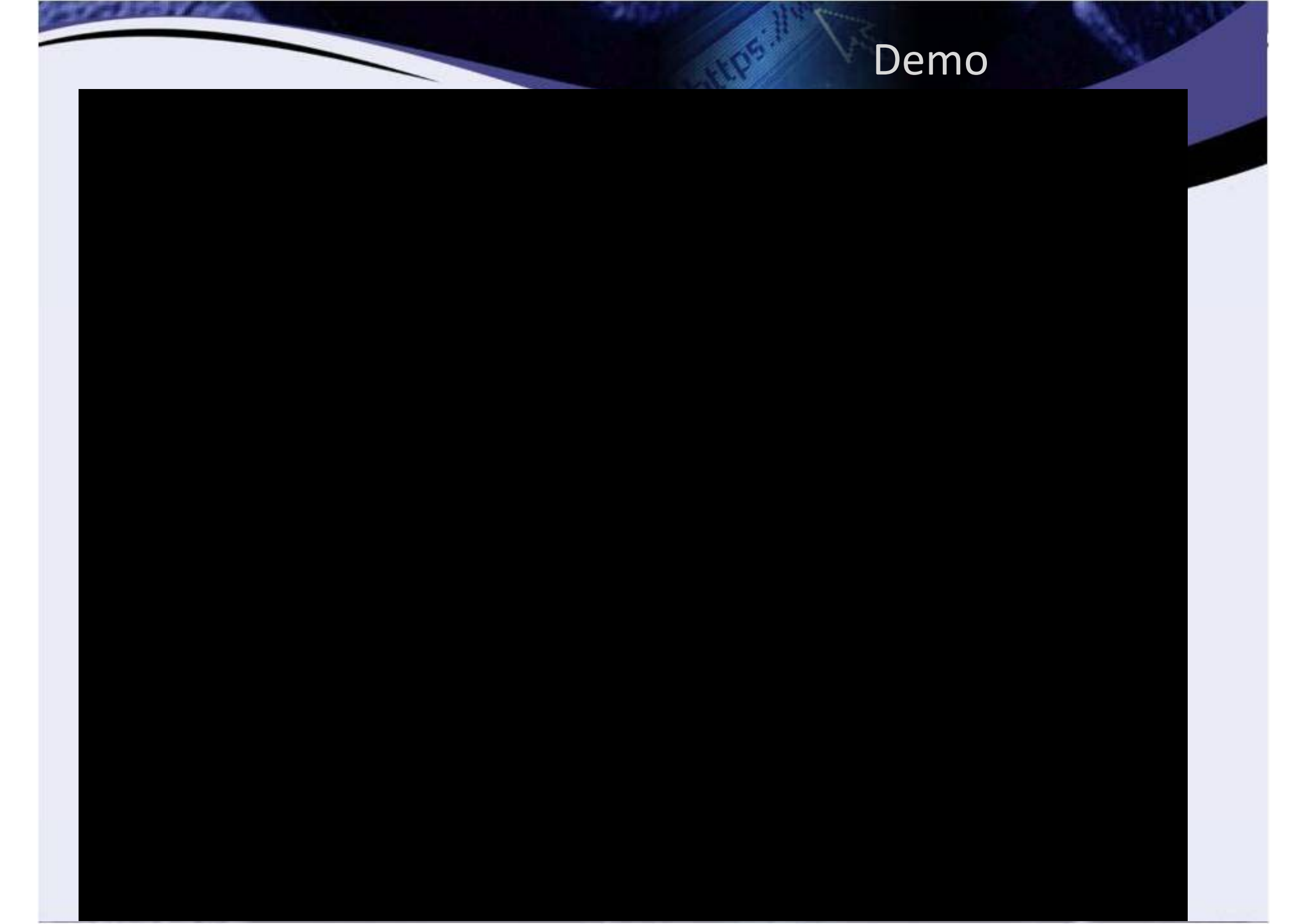
算法保密



密钥保密



- 开发成本低
 - 客户端现成，只需加入用户管理，服务器端检验
- 推广成本低
 - 现在几乎每人都用智能手机
- 使用成本低
 - 手机不必联网也可产生OTP
 - 没有短信产生的费用
- 适用面广
 - 上文介绍的暴力破解，CSRF，不可否认性等



Demo

The end



OWASP 中国
The Open Web Application Security Project

谢谢大家