**Origin-Bound Certificates: A Fresh Approach to Strong Client**  
**Authentication for the Web**

1. 简介
2. OBC Origin-Bound Certificates介绍
3. OBCs由用户浏览器产生的证书，相当于和用户的浏览器进行了绑定。它是一种Client自签名的证书（X 509），在TLS连接阶段作为Client的身份凭证。能够辅助用户认证并且抵抗攻击（主要针对MITM）；
4. OBCs不含有用户的信息，只包括证书标示以及Origin网站标示（不需要和用户进行交互）；
5. OBCs使用TSL扩展的形式，而非TLS Client-Auth 流程
6. OBCs需要和其它的认证技术进行结合；
7. OBC和Cookie结合认证
8. 本文介绍了将OBCs和Cookie进行绑定，并将Cookie作为认证令牌进行登录并抵抗中间恩攻击的情况；
9. OBCs-Cookie认证依赖初始化阶段（用户使用认证凭证（用户名，密码）获取认证令牌（Cookie））
10. OBCs使用Cookie-OBCs认证，分为两个阶段：
    1. 和服务器建立TLS连接的阶段，Server请求用户使用OBC证书对Client身份进行申明（只是记录用户是持有某个OBC1的Client）
    2. 使用绑定OBC（OBC2）的Cookie对用户的网站用户进行识别
    3. 检查OBC1和OBC2是否相同，如果OBC1 = OBC2 那么用户是合法的。如果不同，那么Client只是窃取了用户Cookie的非法用户
11. 问题
12. 如何保证OBCs首次认证的安全性？(首次认证指Server端产生Cookie并将Cookie发给客户端的那次)
13. TLS-OBCs客户端认证的流程是否有相应的变化，还是说OBCs Client-Auth遵循TLS Client-Auth的认证流程？
14. OBCs除了和Cookie结合还有哪些好的结合方式？（文章中还提到了与OpenID的结合）