《WLAN安全问题与解决方案研究》

参会人员：

刘利军、一个女生、曹阳、李祥军、王超

信息安全管理部委托

网络安全部：网络安全

信息安全部：客户信息安全

## Cookie安全问题？

一般安全考虑：

·不存储客户私密信息，但仍需加密（1用户名、时间等信息2在客户端的安全）

·选择这种方式的原因：cookie走HTTPs的渠道、cookie方案符合上级需求

·cookie提供认证、但用户不感知

·取消静态密码认证方式？

问题：

·cookie中存储的内容？（是固定的还是根据现实情况而定？）

·cookie能否用于认证？一般情况下，自动登录是如何实现的（是通过cookie么）？

## 伪AP检测

·检测并定位非法AP能否实现（规范中强制要求支持检测非法AP功能）？对现网有无影响？

## 用户冒用

·新问题：在WLAN中，ip+mac仍然存在冒用问题？（攻击者与正常用户使用同一个身份同时在线、免费上网）

AC无法区分、AP区分？

终端、AP、AC等的底层交互过程？

## ARP攻击

VLAN与LAN的同异？

《WLAN设备规范》中强制要求支持VLAN功能。

## 利用DNS端口绕过计费？？

·李祥军提出了一种新问题：攻击者申请一个域名欺骗用户

·在未连接前，对第一次的DNS请求，AC处理？

## 对AP的DOS攻击

## 伪DHCP服务器

·AC可以直接定位DHCP服务器，因此该问题不存在。