

网 络 安 全

孙毅

谈谈安全

- 没有绝对的安全
 - 只能证明一个对象是不安全的
 - 分类：不安全和暂时安全
- 安全是相对的
 - 棱镜门事件
 - IPv6 IPsec



课程内容

- 网络安全概述
- 密码技术
- 网络攻击
- 移动互联网安全
- 未来互联网安全

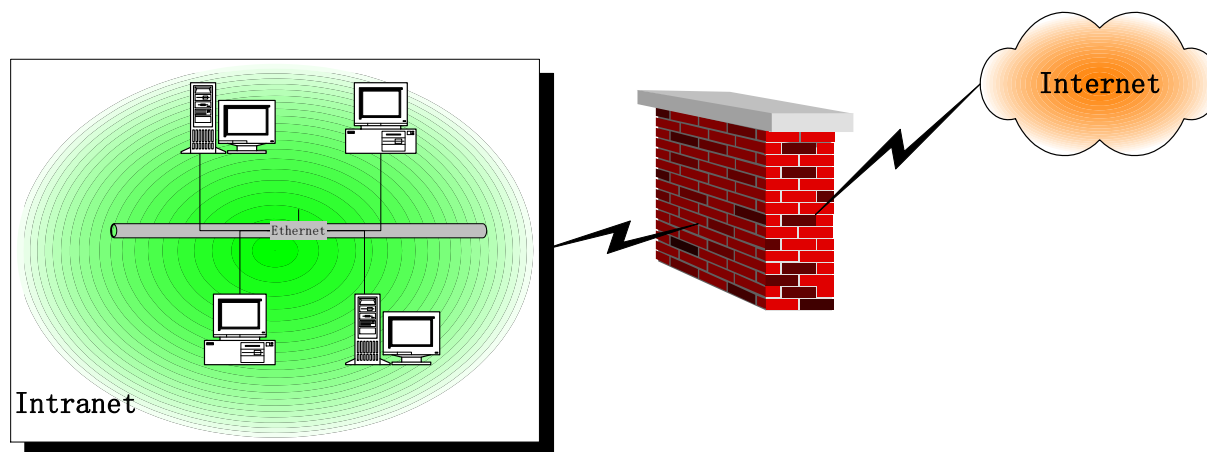
网络安全概述

概念

- **网络安全**的一个通用定义指网络信息系统的**硬件、软件及其系统中的数据**受到保护，不因偶然的或者恶意的**破坏、更改、泄露**，系统能连续、可靠、正常地运行，服务不中断。
- **网络安全**简单的说是在网络环境下能够识别和消除不安全因素的能力。

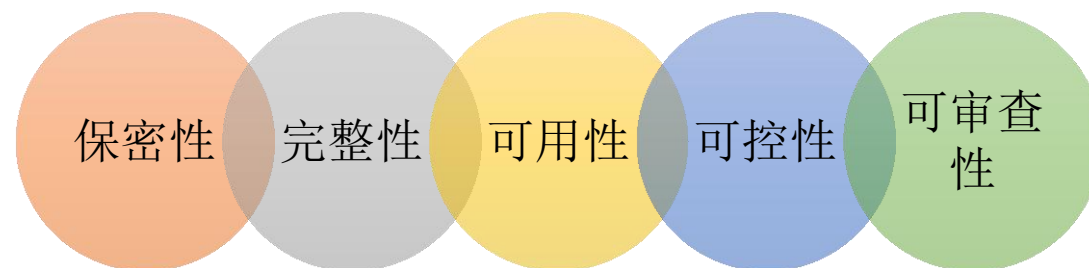
概念

- 大多数安全性问题的出现都是由于有恶意的人试图获得某种好处或损害某些人而故意引起的。
- 必须清楚地认识到，能够制止仍然实施破坏行为的敌人的方法对那些惯于作案的老手来说，收效甚微。
 - 道高一尺，魔高一丈



网络安全的5大要素

- 保密性
 - 保护数据避免非授权泄露，保障数据来源的可靠性
- 完整性
 - 阻止对数据进行非授权篡改
- 可用性
 - 数据可访问，无延迟
- 可控性
 - 控制数据传播范围和方式
- 可审查性
 - 对出现的网络安全问题提供调查的依据和手段



安全机制位于协议栈的哪一层

- 没有一个单独的位置，因为安全性与**每一层**都有关
 - 物理层**：传输线封装在包含高压氦气的密封管，漏气报警
 - 数据链路层**：点到点线路加解密，不能经过中间路由器
 - 网络层**：防火墙、IP报文头的安全域
 - 传输层**：端到端连接的加解密
 - 应用层**：大多数安全机制都集中在此层

网络安全现状

网络安全事件回顾

- 支付宝机房电缆被挖断 部分区域服务中断
 - 2015年5月27日，支付宝大面积瘫痪，电脑端和移动端均无法进行转账付款，缘由是杭州市萧山区某地光缆被挖断，进而导致支付宝一个主要机房受影响，导致部分地区的支付宝服务中断数小时。



网络安全事件回顾

- 熊猫烧香病毒

- 十几年前，中国骇客whboy（李俊）发布熊猫烧香病毒，因中毒电脑桌面上出现“熊猫烧香”图案名噪一时，这也成为了当时一度让人谈网色变的病毒。
- 可通过感染系统的*.exe、*.com、*.pif、*.src、*.html、*.asp文件，导致打开网页文件时IE自动跳转到指定病毒网址中下载病毒，同时出现蓝屏、频繁重启以及系统硬盘中数据文件被破坏等现象



网络安全事件回顾

- 勒索病毒

- 2017年5月12日，全英国上下16家医院遭到大范围网络攻击，医院的内网被攻陷，导致这16家机构基本中断了与外界联系。这场网络攻击的罪魁祸首就是一种叫WannaCrypt的勒索病毒。
- 2020年9月，德国杜塞尔多夫大学医院遭受勒索软件攻击，医院系统瘫痪导致抢救延误，德国警方也将案件性质调升为谋杀案。



网络安全事件回顾

- 携程网内部员工误删除代码 网站整体宕机12小时
 - 2015年5月28日，携程官网和App客户端大面积瘫痪，多项功能无法使用，直至晚上22时45分，携程官方才确认除个别业务外，携程网站及APP恢复正常，数据没有丢失。而造成事故原因“内部人员错误操作导致”。业内分析，若按携程一季度营收3.37亿美元估算，“宕机”一小时的平均损失为106.48万美元，从瘫痪到修复，携程“宕机”近12小时，算下来总损失超过1200万美元，折合人民币7400多万。



网络安全事件回顾

- XcodeGhost黑了至少一亿台iPhone, ios开发有鬼
 - 2015年9月16日, CNCERT国家互联网应急中心发布XcodeGhost病毒安全风险提示, AppStore上超过4000多款应用中中招, 包括微信、网易云音乐、网易公开课、同花顺、南京银行、南方航空、中信银行、行动空间等等比较熟知的应用。安装以上应用的iPhone/iPad用户或有可能泄露基本信息, 受影响用户超过1亿!

XcodeGhost

"XcodeGhost" Source 关于所谓"XcodeGhost"的澄清

首先, 我为XcodeGhost事件给大家带来的困惑致歉。XcodeGhost源于我自己的实验, 没有任何威胁性行为, 详情见源代码:<https://github.com/XcodeGhostSource/XcodeGhost>

所谓的XcodeGhost实际是苦逼iOS开发者的一次意外发现: 修改Xcode编译配置文本可以加载指定的代码文件, 于是我写下上述附件中的代码去尝试, 并上传到自己的网盘中。

在代码中获取的全部数据实际为基本的app信息: 应用名、应用版本号、系统版本号、语言、国家名、开发者符号、app安装时间、设备名称、设备类型。除此之外, 没有获取任何其他数据。需要郑重说明的是: 出于私心, 我在代码加入了广告功能, 希望将来可以推广自己的应用(有心人可以比对附件源代码做校验)。但实际上, 从开始到最终关闭服务器, 我并未使用过广告功能。而在10天前, 我已主动关闭服务器, 并删除所有数据, 更不会对任何人有任何影响。

愿谣言止于真相, 所谓的"XcodeGhost", 以前是一次错误的实验, 以后只是彻底死亡的代码而已。

需要强调的是, XcodeGhost不会影响任何App的使用, 更不会获取隐私数据, 仅仅是一段已经死亡的代码。

再次真诚的致歉, 愿大家周末愉快

网络安全事件回顾

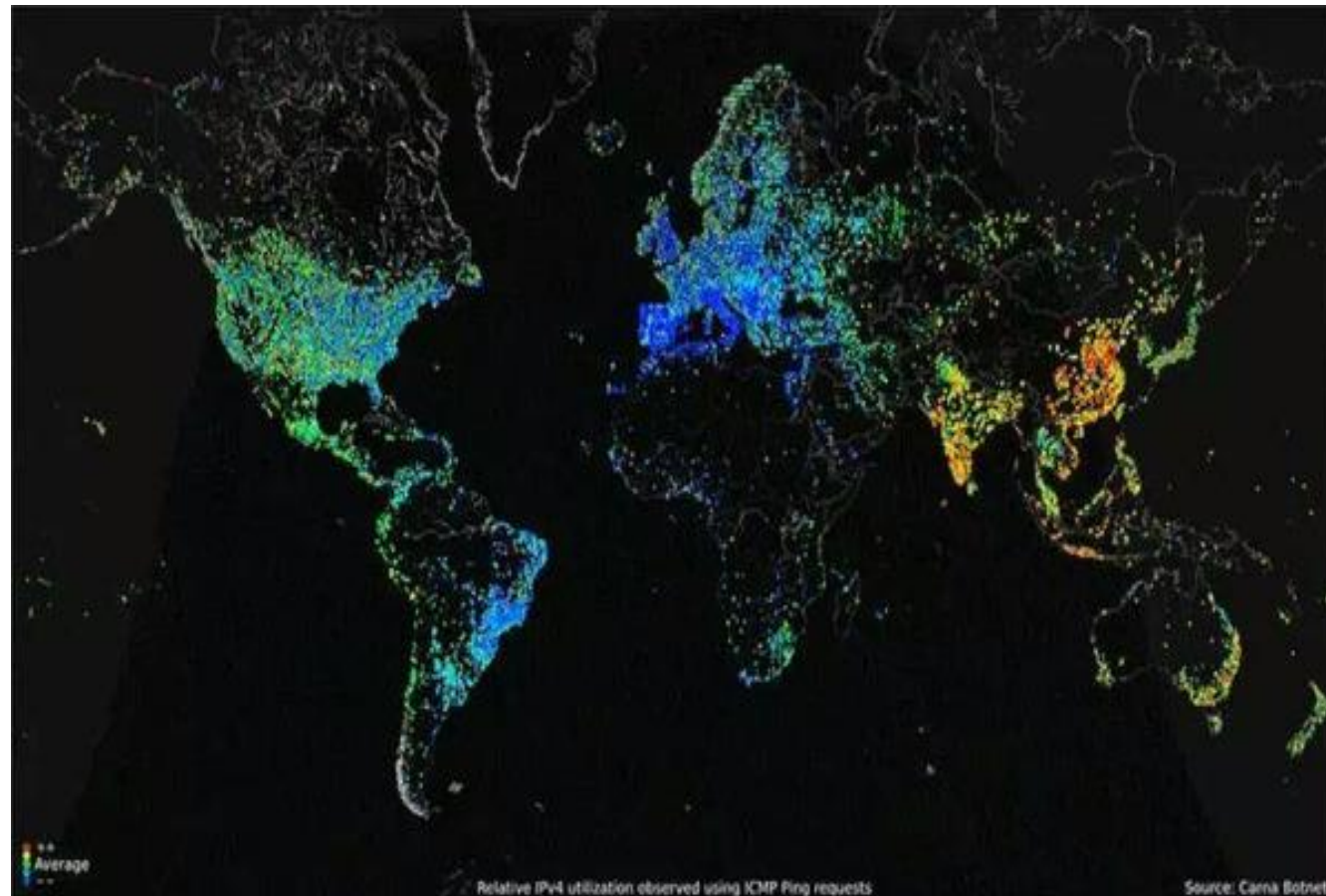
- 2015年7月境外偷情网站Ashley Madison被黑客攻击

- ✓ 3200万客户信息被泄露
- ✓ 15000个用户使用.gov和.mil后缀邮箱



网络安全事件回顾

- 2016年10月21日美国互联网大面积断网，DYN公司的DNS服务器遭受DDoS攻击，导致Twitter、Facebook、Netflix、CNN等网站无法连接。



网络安全事件回顾

- 希拉里邮件门，其竞选经理John Podesta，在最错误的时间，点了一封最错误的邮件，他点开了一封黑客发给他的钓鱼邮件，无意间泄露了自己的密码，由此，他自己的邮箱很快就被黑客翻了个遍，之后，黑客很快就把战果全部交给了维基解密



安全性问题是一个国际难题

- 据统计，由于网络安全问题（恶意攻击、病毒等），每年全球因安全问题造成的损失约1800亿美元。
- “一带一路”势必带来网络的开放，互联网金融等进一步繁荣，安全隐患更加突出

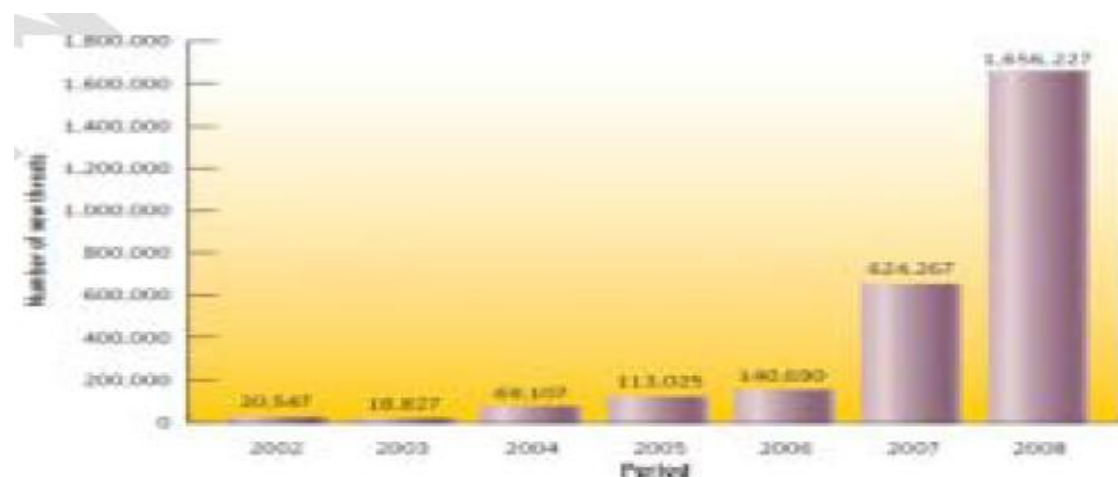
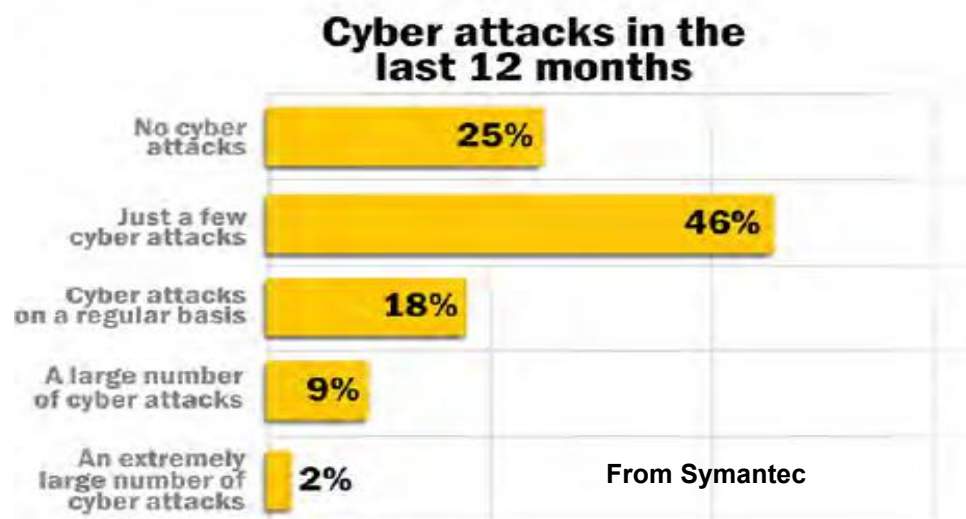
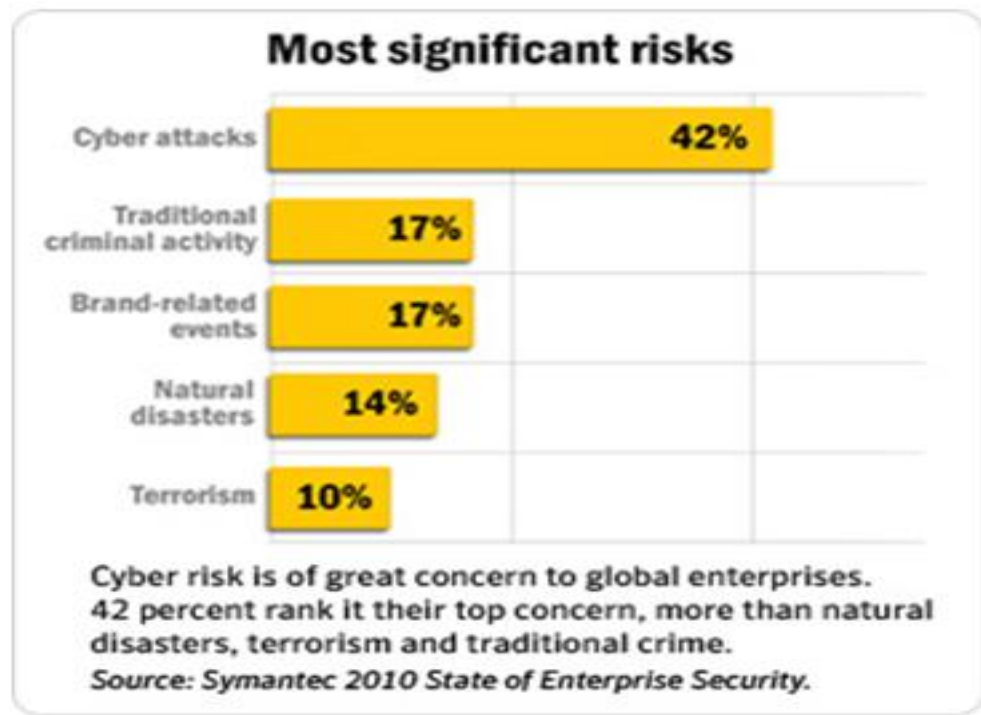


图 1 我国互联网安全威胁增长率



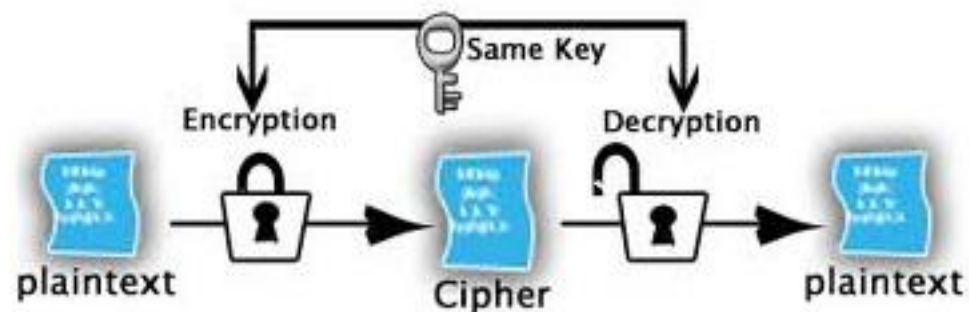
加密技术

定义

- 利用技术手段把数据变为乱码（加密）传送，到达目的地后再用相同或不同的手段还原（解密）
- 加密类型
 - 哈希：无密钥，单向
 - 单密钥加密：1个密钥(key)
 - 公开密钥加密：2个密钥(key)，公钥和私钥

单密钥加密又称对称加密

- 密文长度约等于明文长度
- 经典算法：DES, 3-DES, AES, IDEA, SMS4, RC5, TRIVIUM
- 优点：加解密速度快
- 单密钥加密三个问题：
 - 1. 密钥管理量大
 - 2. 密钥传输信道安全性更高
 - 3. 数字签名的问题



单密钥加密三个问题

- 1. 密钥管理量大
 - 两两使用一对密钥， n 个用户通信需要多少对密钥？
 - 需要 $C(n, 2)$ 个密钥
 - 用户量增大时，密钥管理空间剧增



单密钥加密三个问题

- 2. 密钥传输信道要求更高安全性
 - 密钥传输和密文在同一信道传输
 - 同时被窃取，很容易被破解出明文，并不安全
- 3. 数字签名的问题
 - CRC校验和固定长度
 - 无法有效进行完整性检验

DES算法

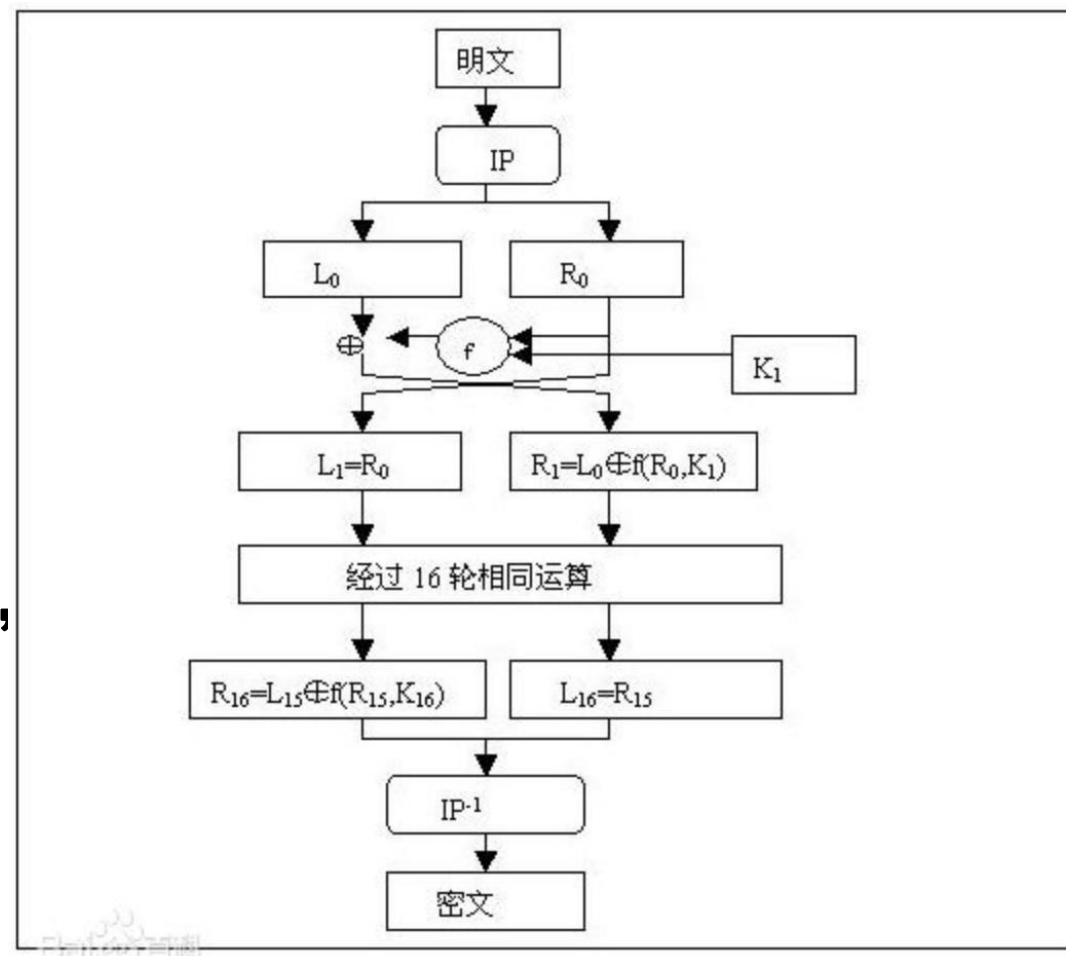
- Data Encryption Standard, 即数据加密标准, 1976年成为美国数据加密标准
- 输入参数
 - Key 密钥 56位
 - Data 数据 64位
 - Mode 模式, 加密和解密两种模式
- 破解方法: 穷举搜索法
 - 普通PC: 每秒搜索1,000,000个密钥, 需要2285年;
 - 特殊的并行处理硬件: 几个小时

DES工作原理

- 第一步：明文按64位分组，每组明文经初始排列
- 第二步：通过子密钥 $k_1 \sim k_{16}$ 进行16次乘积变换
- 第三步：通过最终排列（第3步）得到64位密文

$k_1 \sim k_{16}$ 由初始密钥经过16次移位交换产生，用以对经过初始排列的64位明文做16次乘积变换。

解密运算与加密运算一样，只是所取子密钥的顺序相反，从 k_{16} 到 k_1 。



公开密钥加密

- 该思想最早由瑞夫·墨克（Ralph C. Merkle）在1974年提出。之后在1976年，惠特菲尔德·迪菲（Whitfield Diffie）与马丁·赫尔曼（Martin Hellman）两位学者以单向函数与单向暗门函数为基础，为发讯与收讯的两方创建密钥。
- 两个密钥：私钥，公钥
- 非对称加密算法
- 经典算法：RSA、ElGamal、Elliptic Curve Cryptography, ECC
- 公钥密码学的提出是为了解决两个问题：
 - 密钥的分配
 - 数字签名

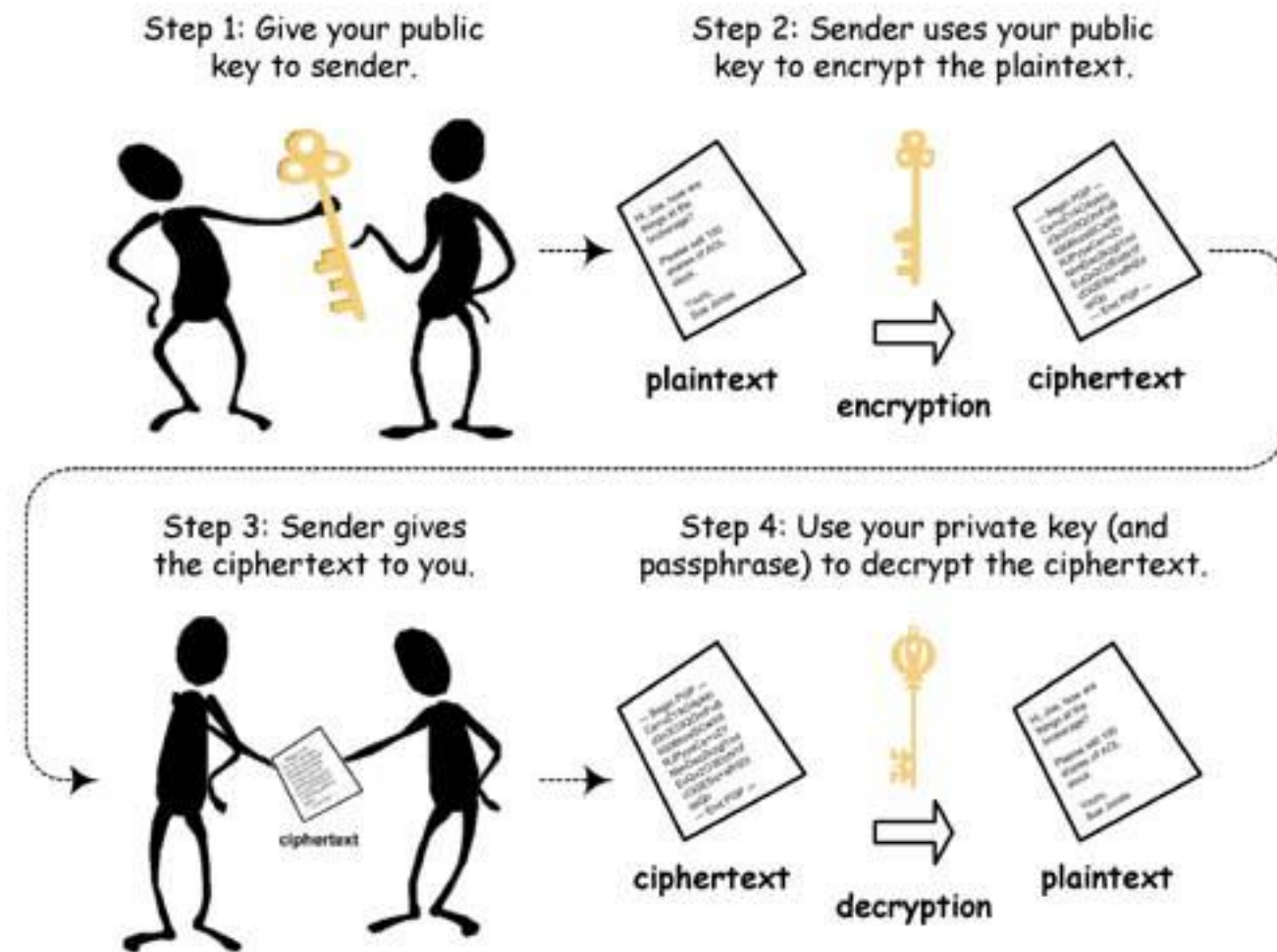
公开密钥加密

Step1:共享你的公钥

Step2:发信者对明文使用你的公钥加密

Step3:发信者将加密后的密文发给你

Step4:使用你的私钥解密，读取明文



数字签名认证

Step1:共享你的公钥

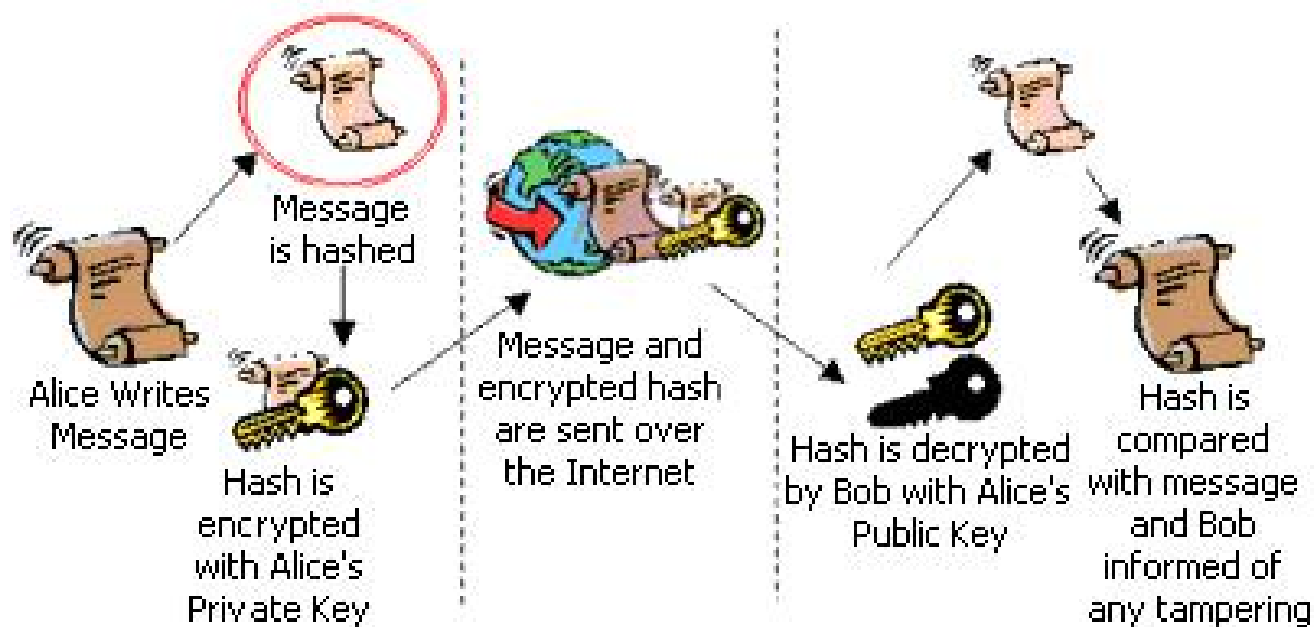
Step2:对你的数据进行哈希

Step3:把哈希值进行用私钥加密

Step4:发送数据和加密的哈希值

Step5:受信者对哈希值用公钥解密

Step6:把接收的数据进行哈希，与解密后的哈希值对比，判断数据是否被篡改



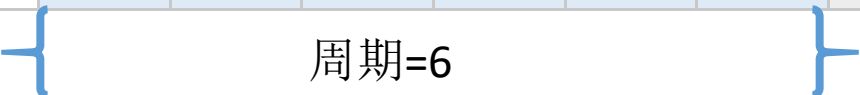
公开密钥加密的主要特点

- 加密和解密能力分开，私钥不能由公钥推导出来
- 多个用户加密的消息只能由一个用户解读(用于公共网络中实现保密通信)
- 只能由一个用户加密消息而使多个用户可以解读(数字签名)
- 无需事先分配密钥
- 密钥持有量大大减少
- 加解密速度慢

RSA算法

- MIT三位研究人员（ Rivest、Shamir和Adleman ）在1978年提出
- Fermat小定理：
 - 如果 n 是一个质数的话，那么对于任意一个数 a ，随着 i 的增加， a 的 i 次方除以 n 的余数将会呈现出长度为 $n - 1$ 的周期性。
 - $a=3, n=7$ 的情况如下

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3^i	3	9	27	81	243	729	2187	6561	19683	59049	177147	531441	1594323	4782969	14348907
$3^i \bmod 7$	3	2	6	4	5	1	3	2	6	4	5	1	3	2	6



RSA工作原理

RSA算法:

- (1) 选择两个大素数， p 和 q ，均应大于 10^{100} ；
- (2) 计算 $n = p \times q$ 和 $z = (p-1) \times (q-1)$ ；
- (3) 选择一个与 z 互为质数的数，令其为 d ；
- (4) 找到一个 e 使其满足 $e \times d = 1 \bmod z$ 。

有了这些预先计算好的参数，我们即可准备开始加密了。把明文（看作一个比特串）划分成块，使得每个明文报文 m 落在 $0 \leq m \leq n$ 之间。这可以通过将明文分成每块有 k 位的组来实现，并且 k 是使得 $2^k < n$ 成立的最大整数。

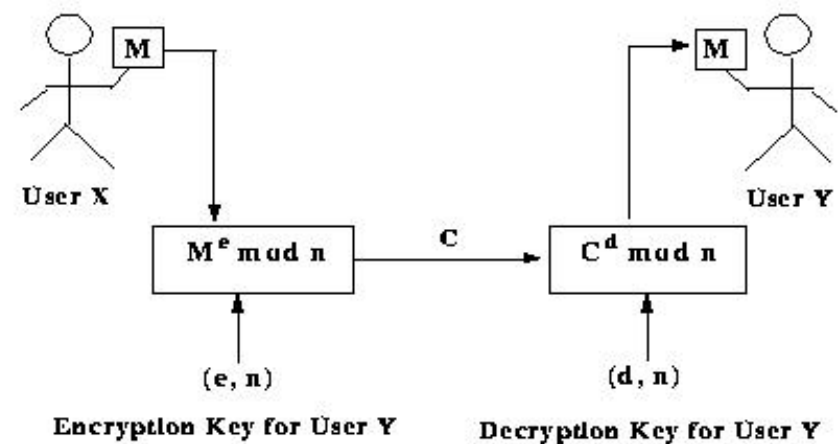
加密一个报文 m ，需计算 $c = m^e \pmod{n}$ ，解密密文 c 要计算 $m = c^d \pmod{n}$ 。

可以证明，在指定范围内的所有 m ，加密函数和解密函数互为反函数。

实施加密需要 e 和 n ，实施解密需要 d 和 n 。因此，公开密钥由 (e, n) 构成，秘密密钥由 (d, n) 或只是 d 构成。 n 限制明文块的大小。

RSA算法

- 取 $p = 7$, $q = 11$
- $n = p * q = 77$, $z = (p-1) * (q-1) = 60$
- 取 $e = 43$, $d = 7$ 使得 $e * d \bmod z = 301 \bmod 60 = 1$
- 得到公钥 $(e=43, n=77)$, 密钥 $(d=7, n=77)$
- 设我们的明文为 $M = 42$
- 加密 $C = M^e \bmod n = 42^{43} \bmod 77 = 14$
- 解密 $M = C^d \bmod n = 14^7 \bmod 77 = 42$



RSA算法破解方法

- 为什么RSA算法是有效的非对称加密算法？
- 因为即使我们有了公钥 (e, n) ，我们很难找到其对应的私钥 (d, n)
 - 要得到私钥，我们需要知道 $z = (p-1) * (q-1)$ ，即必须将 n 分解为 $p * q$
 - 而当 p, q 为大质数时，除了试除法，没有更有效的方法能将 n 分解
- 大数分解难题产生的不对称性也就是 RSA 算法的理论基础

数字签名

- 现实生活：手写签名随处可见账单、邀请信、签发文件
- 设计一个代替手迹签名的方案，从根本上说，我们需要这样一个系统，一方通过该系统能以如下方式向另一方发送已签名的文件：
 - (1) 接收方能够验证出发送方所宣称的身份；
 - (2) 发送方以后不能否认报文是他发的；
 - (3) 接收方不能伪造对报文的签名。

数字签名

- 在面向连接的系统中，身份验证可以在建立会话时完成
 - 输入口令：(1) 易被窃听； (2) 口令表保存有开销、有风险
- 采用公开密钥加密技术可以安全地实施身份验证，而无需保存任何口令。
- 防抵赖：出现争议时接收者可以出示发送者用私钥签名过的消息。

单向校验和的使用

- 在许多应用中，身份验证是必须的，而保密则不是。
- 单向校验和（CK）：不需要对整个报文加密的身份验证模式
 - 假定有一明文报文P，计算出CK（P）必须比较容易，但从CK（P）几乎不可能找出P
 - 有很多这种单向性质的数学函数

基于单向校验和的身份验证

要在明文报文 m 中签名，发送者 A 首先计算 $CK(m)$ ，然后用私人密钥将其加密，产生出 $D_A(CK(m))$ ，最后将 $[m, D_A(CK(m))]$ 对偶传送到 B 。报文本身可以用明文发送（或者用公开密钥或传统加密技术加密），后跟加了密的校验和。

当报文及校验和到达 B 后， B 对签名部分（即 $D_A(CK(m))$ ）应用 E_A ，得到 $CK(m)$ 。至此， B 有 3 样东西： m 、 $CK(m)$ ，以及 $D_A(CK(m))$ 。现在 B 对 m 应用 CK ，以看此结果是否与收到的 $CK(m)$ 一致。若是，则知此报文未遭篡改；若否，则说明报文已被篡改。

争议解决

- 如果以后发生争议，B可出示这三样东西，以证明A确实发送过报文 m
 - 即使B能伪造出P和CK(m)，但B若未得到A的私钥就无法伪造出 $D_A(CK(m))$ 。这种方法的优点是无论报文有多长，只有很短的检验和。
- CK单向特征的重要性
 - 如果能从CK(m)得到明文报文 m ，那么B就可以生成与 m 具有相同检验和的新报文 m' ，并把 m' 、CK(m')以及 $DA(CK(m'))$ 出示给法官。
- 无法解决的争议情况
 - 发送者公开私钥
 - 发送者更新私钥

报文鉴别和报文摘要

- 报文鉴别是一个过程，它使得通信的接收方能够验证所收到的报文的真伪。报文鉴别码是用一个密钥生成的一个小的数据块追加在报文的后面。这种技术假定通信的双方共享一个密钥K。
- 报文摘要是报文鉴别码的一个变种，将可变长度的报文M作为单向散列函数的输入，然后得出一个固定长度的标志H（M），这个H（M）就称为报文摘要MD。
 - 常用算法：MD5，SHA

网络攻击

主动攻击

- 主动攻击会导致某些数据流的篡改和虚假数据流的产生。这类攻击可分为篡改、伪造消息数据和终端，拒绝服务。
- (1) 篡改消息
 - 篡改消息是指一个合法消息的某些部分被改变、删除，消息被延迟或改变顺序，通常用以产生一个未经授权的效果。如修改传输消息中的数据，将“允许甲执行操作”改为“允许乙执行操作”。
- (2) 伪造
 - 伪造指的是某个实体（人或系统）发出含有其他实体身份信息的数据信息，假扮成其他实体，从而以欺骗方式获取一些合法用户的权利和特权。
- (3) 拒绝服务
 - 拒绝服务即常说的DoS（Deny of Service），会导致对通讯设备正常使用或管理被无条件地终端。通常是对整个网络实施破坏，以达到降低性能、终端服务的目的。这种攻击也可能有一个特定的目标，如到某一特定目的地（如安全审计服务）的所有数据包都被组织。

被动攻击

- 被动攻击中攻击者不对数据信息做任何修改，截取/窃听是指在未经用户同意的情况下攻击者获得了信息。通常包括窃听、流量分析、破解弱加密的数据流等攻击方式。
- (1) 流量分析
 - 流量分析攻击方式适用于一些特殊场合，例如敏感信息都是保密的，攻击者虽然从截获的消息中无法得到消息的真实内容，但攻击者还能通过观察这些数据报的模式，分析确定出通信双方的位置、通信的次数及消息的长度，获知相关的敏感信息，这种攻击方式称为流量分析。
- (2) 窃听
 - 目前应用最广泛的局域网上的数据传送是基于广播方式进行的，这就使一台主机有可能受到本子网上传送的所有信息。而计算机的网卡工作在杂收模式时，它就可以将网路上传送的所有信息传送到上层，以供进一步分析。如果没有采取加密措施，通过协议分析，可以完全掌握通信的全部内容。

口令入侵

- 所谓口令入侵是指使用某些合法用户的帐号和口令登录到目的主机，然后再实施攻击活动。这种方法的前提是必须先得到该主机上的某个合法用户的帐号，然后再进行合法用户口令的破译。

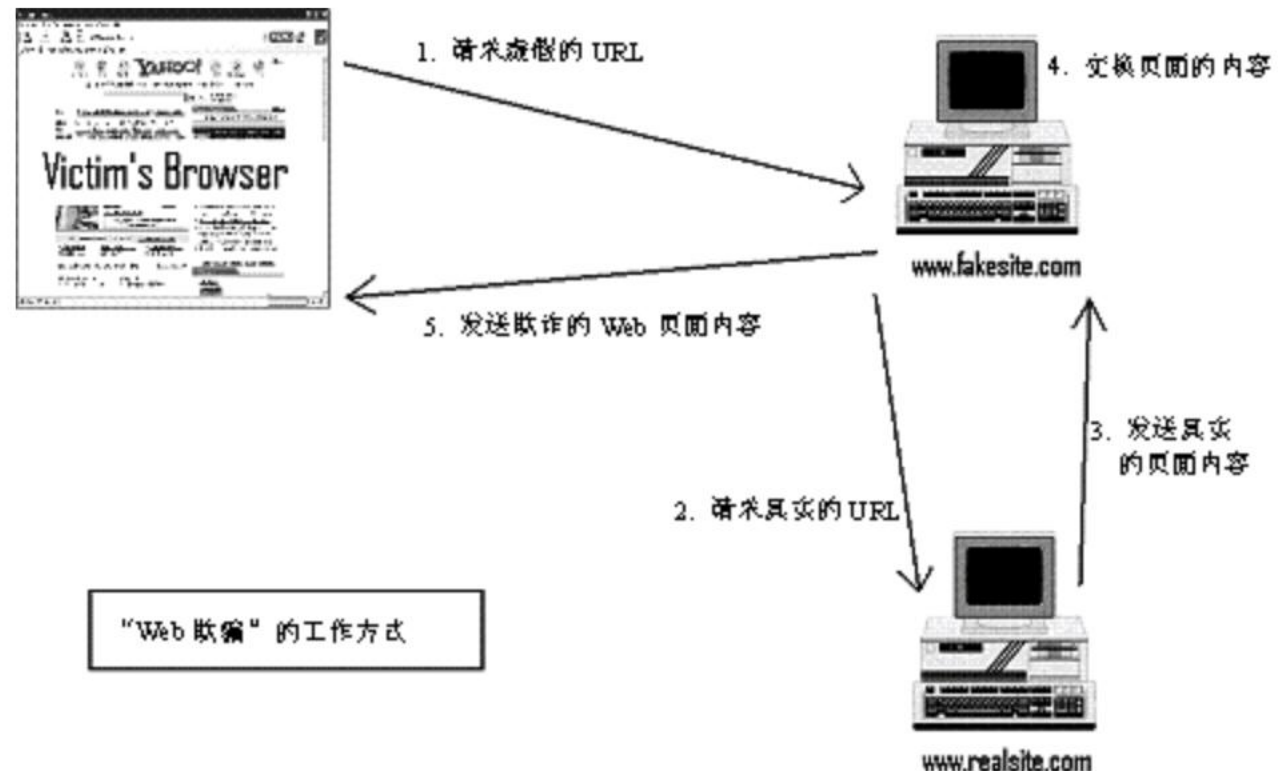


特洛伊木马

- 放置特洛伊木马程式能直接侵入用户的计算机并进行破坏，常被伪装成工具程式或游戏等诱使用户打开带有特洛伊木马程序的邮件附件或从网上直接下载，一旦用户打开了这些邮件的附件或执行了这些程序之后，就会在自己的计算机启动时悄悄执行的程序。
- 当你连接到因特网上时，这个程序就会通知攻击者，来报告你的IP地址及预先设定的端口。攻击者在收到这些信息后，再利用这个潜伏在其中的程序，就能任意地修改你的计算机的参数设定、复制文件、窥视你整个硬盘中的内容等，从而达到控制你的计算机的目的。

Web欺骗

- Web欺骗是一种电子信息欺骗，攻击者在创造了整个Web世界的一个令人信服但是完全错误的拷贝。错误的Web看起来十分逼真，它拥有相同的网页和链接。然而，攻击者控制着错误的Web站点，这样受攻击者浏览器和Web之间的所有网络信息完全被攻击者所截获。

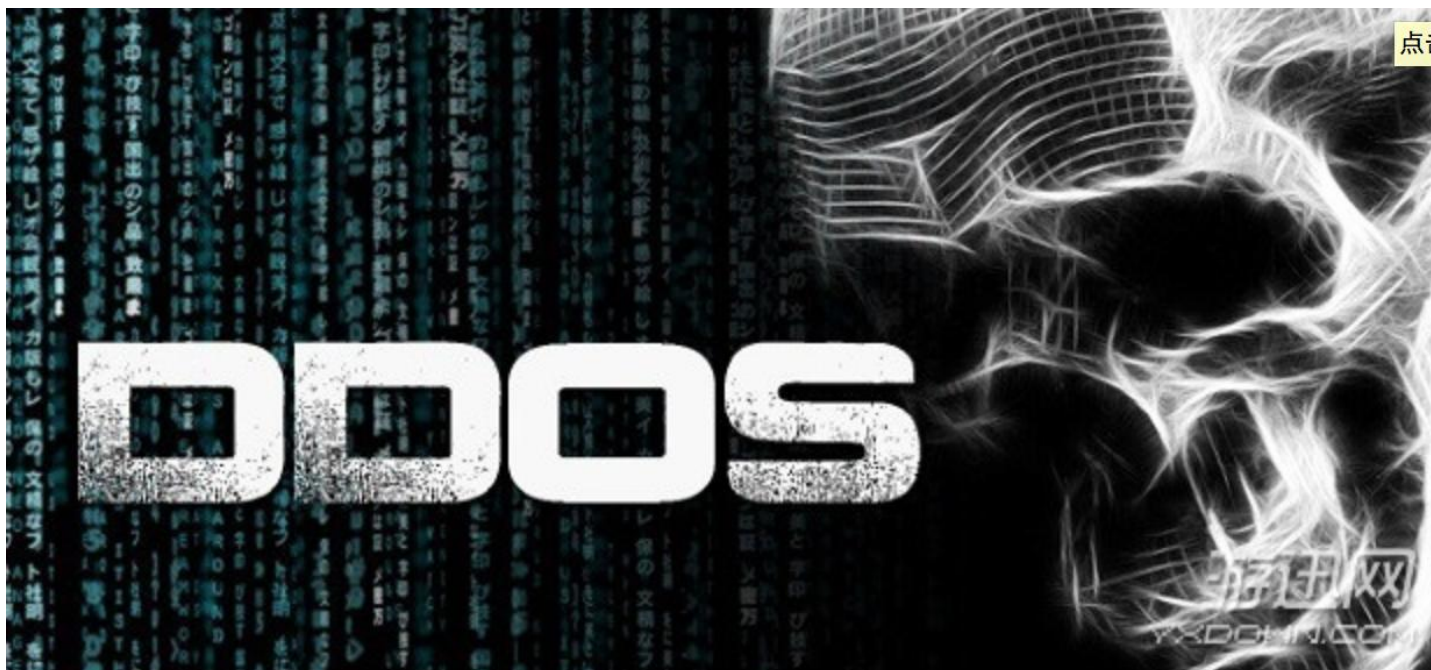


网络监听

- 网络监听是主机的一种工作模式，在这种模式下，主机能接收到本网段在同一条物理通道上传输的所有信息，而不管这些信息的发送方和接收方是谁。
- 因为系统在进行密码校验时，用户输入的密码需要从用户端传送到服务器端，而攻击者就能在两端之间进行数据监听。此时若两台主机进行通信的信息没有加密，只要使用某些网络监听工具就可轻而易举地截取包括口令和帐号在内的信息资料。
- 虽然网络监听获得的用户帐号和口令具有一定的局限性，但监听者往往能够获得其所在网段的所有用户帐号及口令。

DOS攻击

- DoS攻击是指故意的攻击网络协议实现的缺陷或直接通过向目标网络发送大量数据包耗尽被攻击对象的资源，目的是让目标计算机或网络无法提供正常的服务或资源访问，使目标系统服务停止响应甚至崩溃。
- DDoS: Distributed Denial of Service，即分布式拒绝服务攻击。借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DDoS攻击，从而成倍地提高拒绝服务攻击的威力。



区块链与比特币

区块链技术受关注度居高不下



热度随时间变化的趋势 ?

Google Trends 关键字: Blockchain 2012. 10-2017. 10



区块链

搜索指数

百度指数 关键字: 区块链 2011. 1-2017. 10

© index.baidu.com

2011年

2012年

2013年

2014年

2015年

2016年

2017年

平均值

8,400
7,200
6,000
4,800
3,600
2,400
1,200

区块链是一种传递信任的技术体系



区块链是实现**价值点对点传递**及**信任全网络**
多层级传递的技术体系

信任
依赖于算法

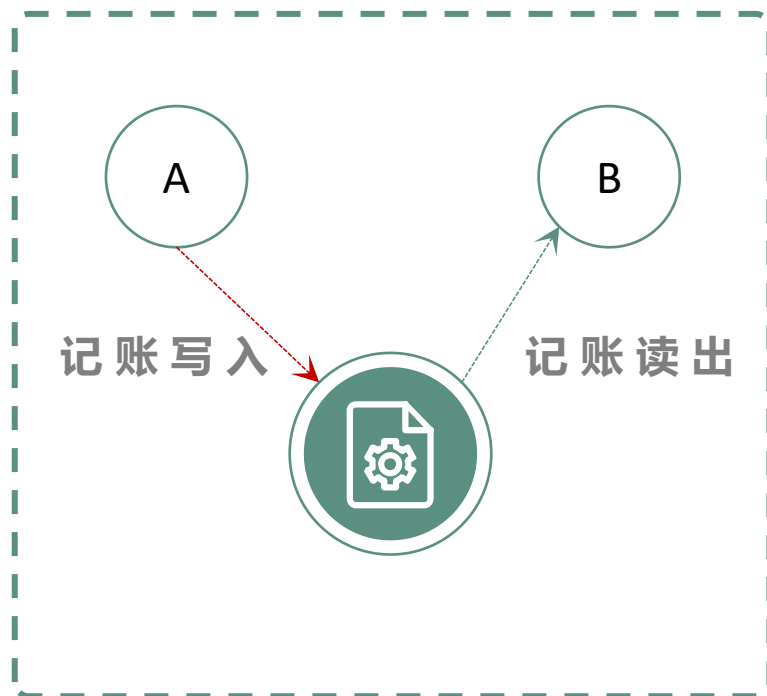
传递
避免重复支付

由多中心网络取代中心机构进行记账

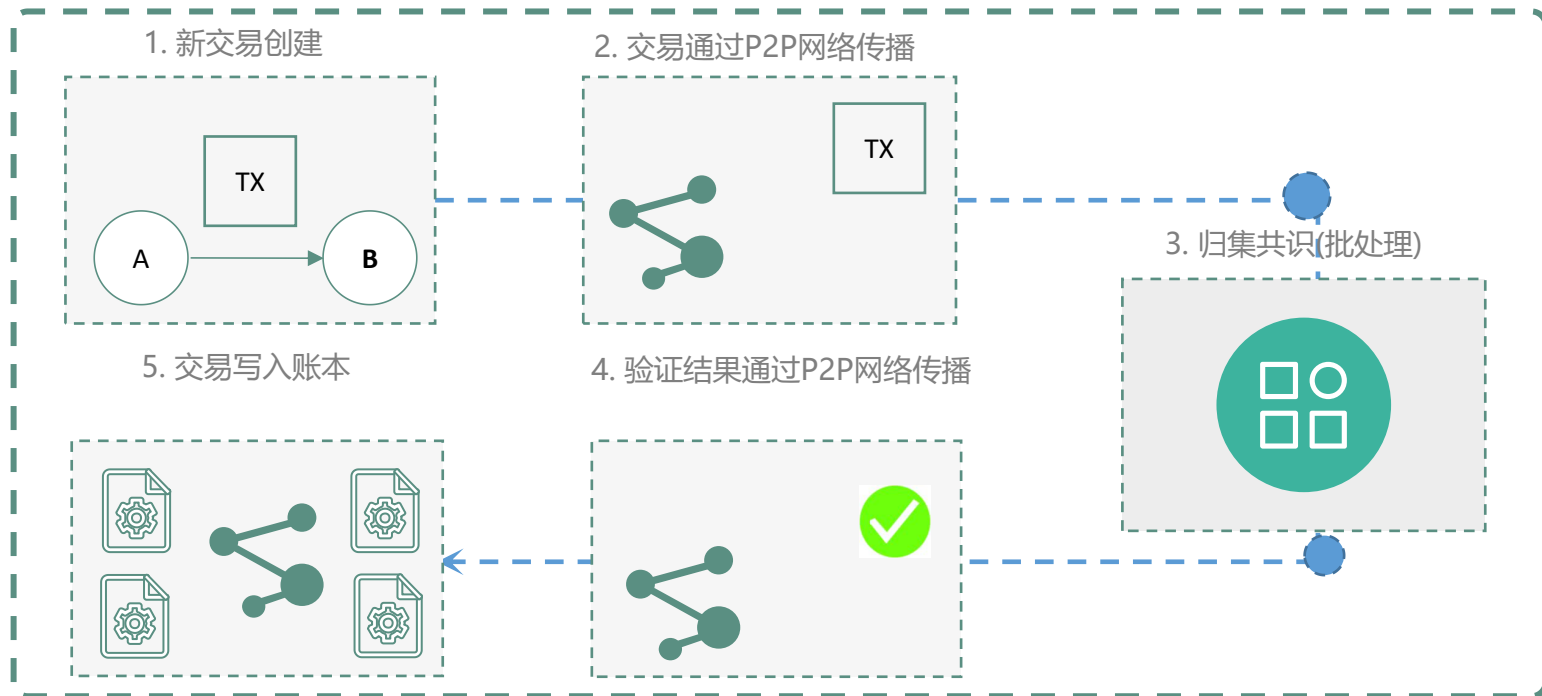
Blockchain

价值互联网的基石

传统中心化记账Vs区块链分布式记账



传统的中心化记账



区块链的分布式记账

分布式记账，不依赖单个中心

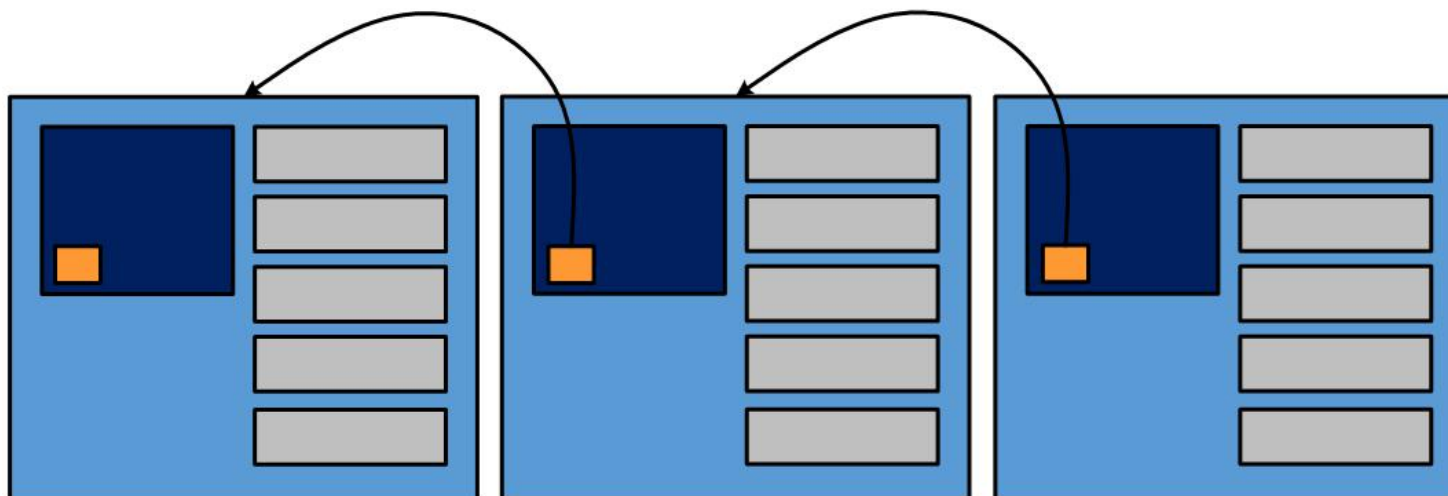
区块链 (Blockchain) - 区块连接方式

Blockchain

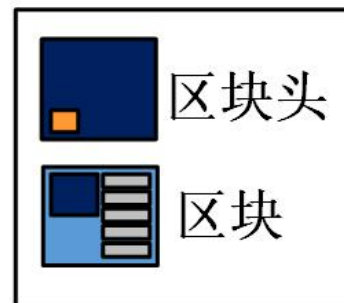
日志



后一区块头中包含
前一区块头Hash值



时间 →



区块链的技术本质与核心价值

技术本质

区块链（Block chain）是一种创新的分布式交易验证和数据共享技术，也被称为分布式账本技术。

核心价值

区块链通过构建P2P自组织网络、时间有序不可篡改的密码学共享账本、分布式共识机制，从而实现去中心化信任。

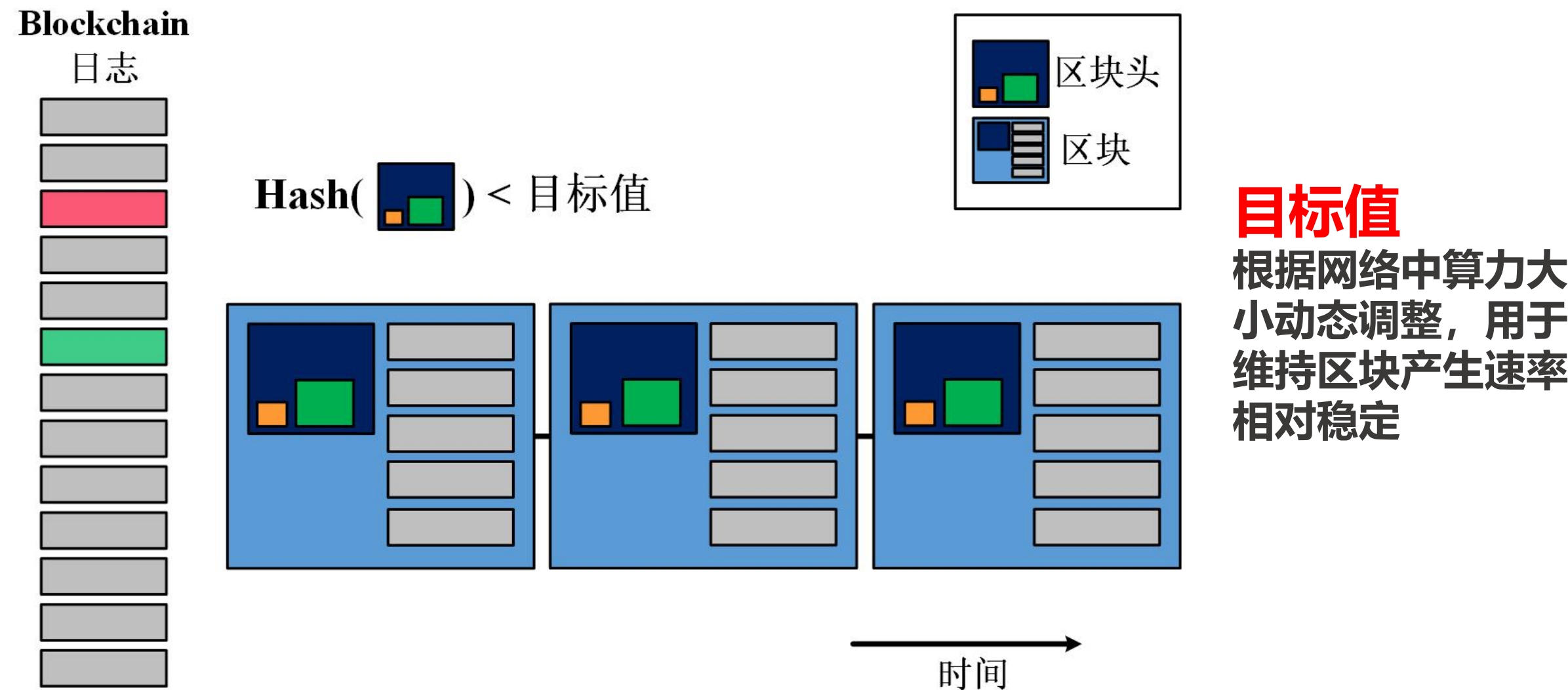
- 宏观本质：**分布式平等部署系统；**全网节点**协作完成交易验证和存储；**无单一**控制中心；
- 微观本质：**数据存储**在块（Block）**中，块在逻辑上串联起来构成**链条（Chain）**；应用数字签名与完整性校验保证块数据的**真实性、时序性、完整性**；
- 在技术层面具有**不可伪造、不可抵赖、不可篡改、不可撤销**等属性，在应用层面具有分布式的**公开透明、交易可跟踪**等特征；
- 区块链**并非某项特定技术**，实际是一种**技术组合**，是一种**实践创新/组合创新/集成创新**。

区块链核心特性



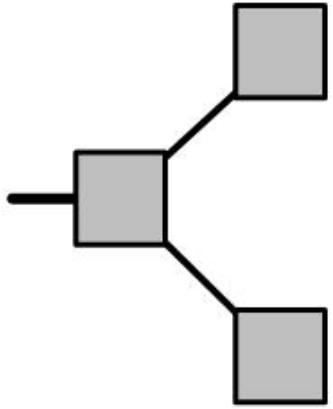
区块链 (Blockchain) - 挖矿、共识

一种以密码学算法为基础的点对点分布式账本技术



区块链 (Blockchain) - 分叉

一种以密码学算法为基础的点对点分布式账本技术

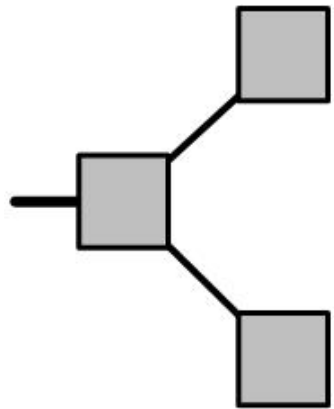


由于区块需经过**分布式共识**
区块链分叉较为**常见**

分叉

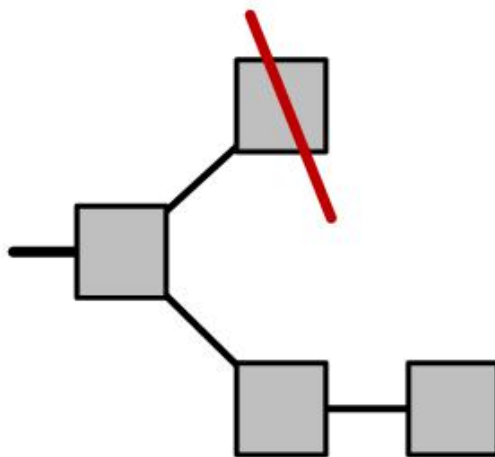
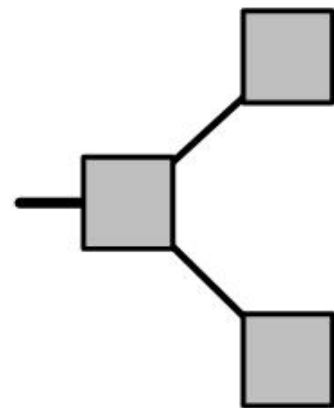
区块链 (Blockchain) - 分叉

一种以密码学算法为基础的点对点分布式账本技术



由于区块需经过**分布式共识**
区块链分叉较为**常见**

分叉

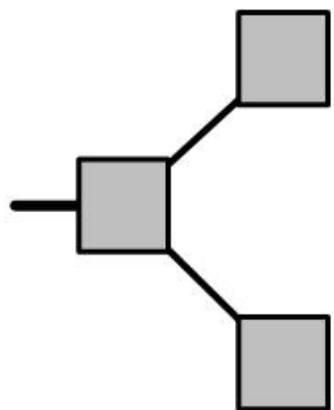


最长(重)链 Win!

- 包含交易最多
- 避免自私挖矿

区块链 (Blockchain) - 分叉

一种以密码学算法为基础的点对点分布式账本技术



由于区块需经过**分布式共识**
区块链分叉较为**常见**

分叉



交易确认：双花

交易打包进区块后，需等待其后区块长度大于某值（比特币为6）时才确认生效

区块链应用

- 金融领域
- 供应链管理
- 版权交易
- 物联网
- 医疗&慈善

金融领域应用

● 特点

- 多方参与
- 不需要统一的信任主体
- 存在价值/信任的流动和流转

● 应用举例

- 贷款：供应链金融
- 收款：支付清算结算



供应链金融—需求痛点

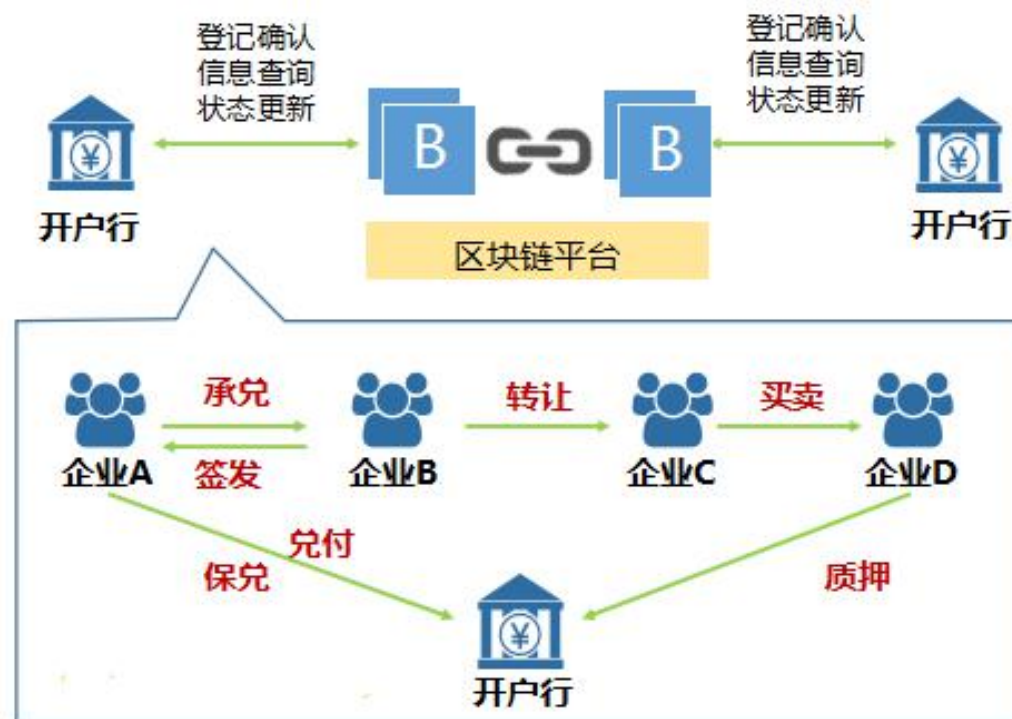
● 痛点

- **融资难**：中小企业难以获得**核心企业背书**。



● 解决方案

- 维护**统一的区块链副本**，打破信息孤岛。
- 共同维护包含**应收账款**信息的凭证，上下游企业对**应收账款**的流动状况进行**全过程签名**。
- 利用区块链的**可追溯特性**，金融机构跟踪凭证的**全生命周期**，完成针对中小企业的融资。



支付、清算与结算

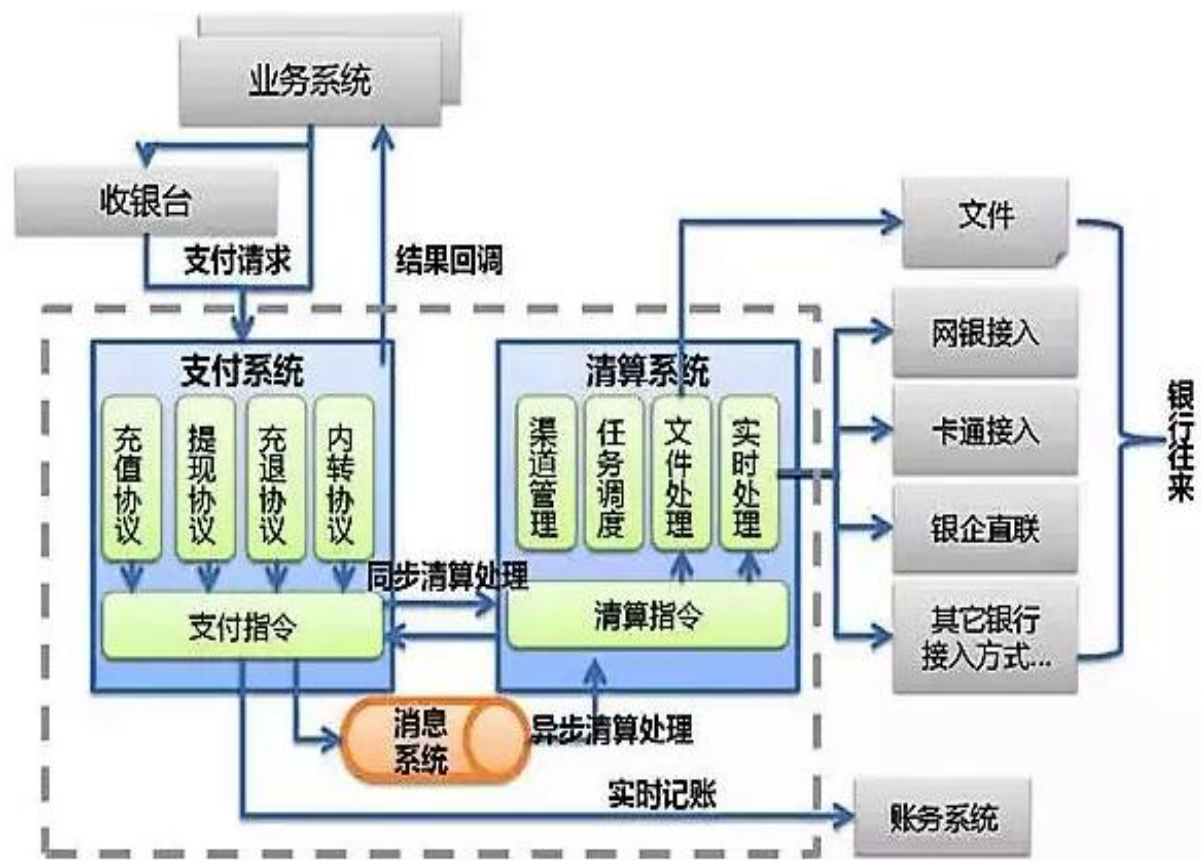
● 痛点

- 资金滞后：例如证券系统T+1到账。
- 成本高昂：不同金融机构使用**割裂的独立账本**，对账过程复杂，耗时耗力，特别是跨行、跨境转账会引发高昂业务成本。



● 解决方案

- 不同金融机构维护**一致的区块链账本**。
- 支付清算指令在各方共同见证下自动执行，**迅速达成共识**。



图片来源：联动优势

移动互联网安全及隐私保护

移动互联网迅速发展

- 近年来，移动互联网在中国得到迅速发展，智能手机的普及率随之攀升。
 - 截至 2014 年 6 月，我国手机网民规模为 5.27 亿，使用手机上网的人群占比进一步提升，由 2013 年的 81.0% 提升至 83.4%。

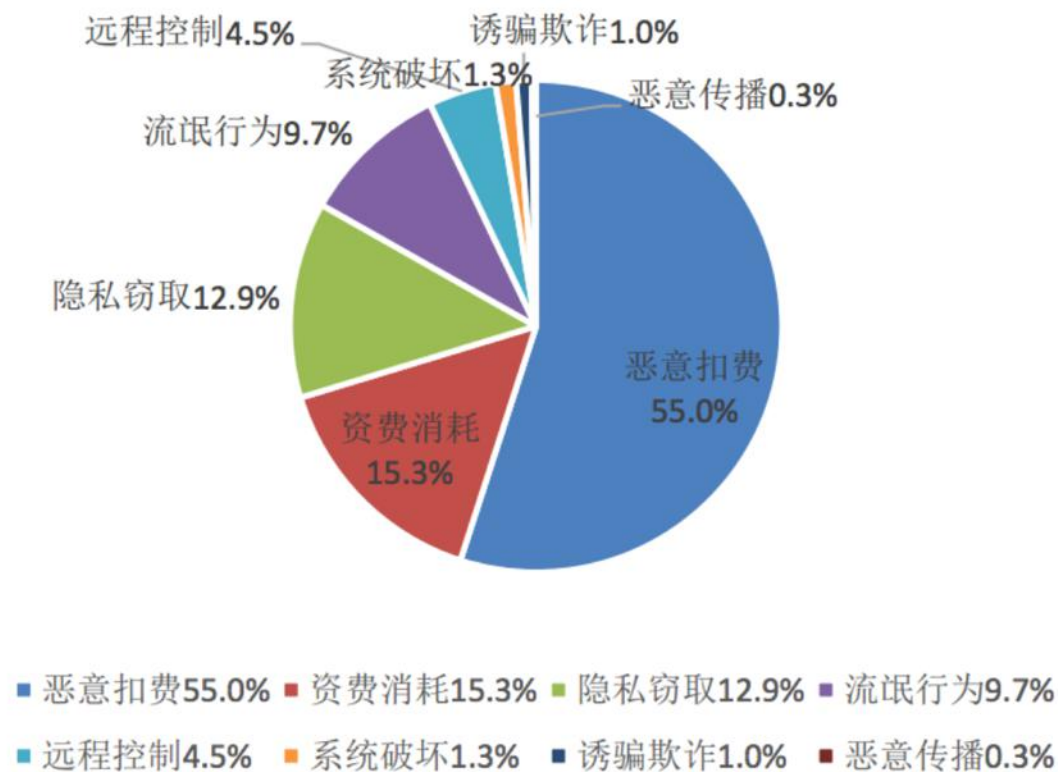


移动终端的安全威胁

- 恶意程序

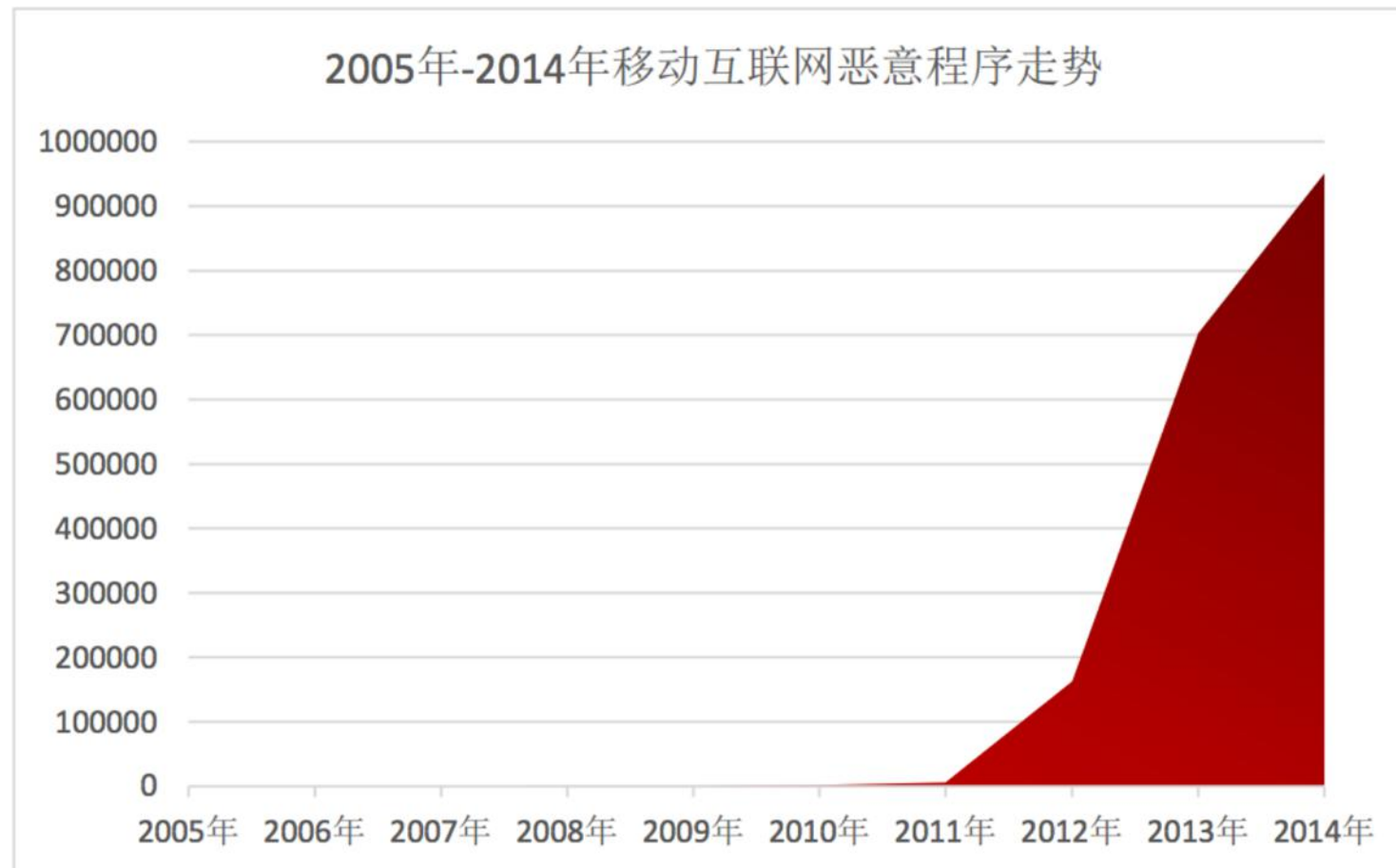
- 据抽样监测, 2014 年我国感染移动恶意程序的用户数量达 2292 万, 其中感染安卓平台恶意程序的用户数量最多, 达 1575 万余个, 也发现约 30 万用户感染基于苹果 iOS 平台的恶意程序, 如“Panda”、“Wirelurker”等。

2014年移动互联网恶意程序数量按行为属性统计



来源：2014我国互联网网络安全态势报告

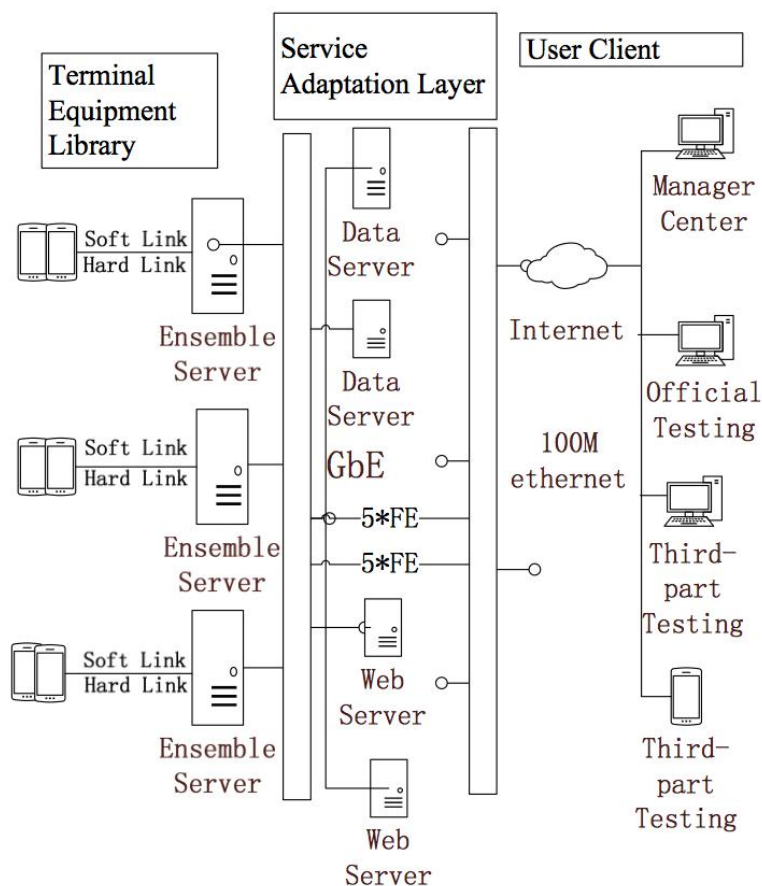
移动互联网恶意程序走势



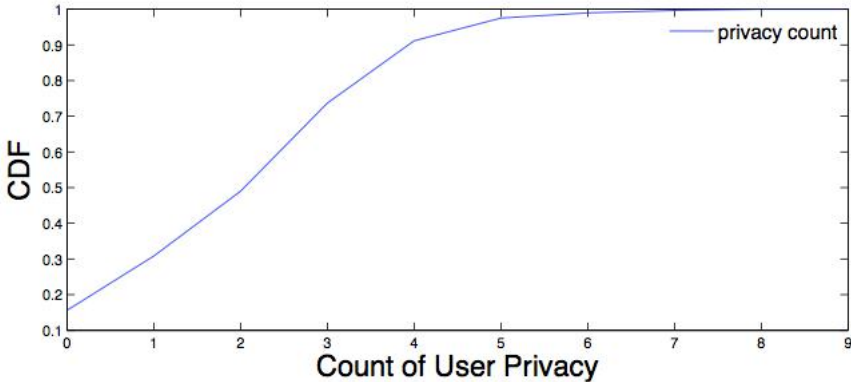
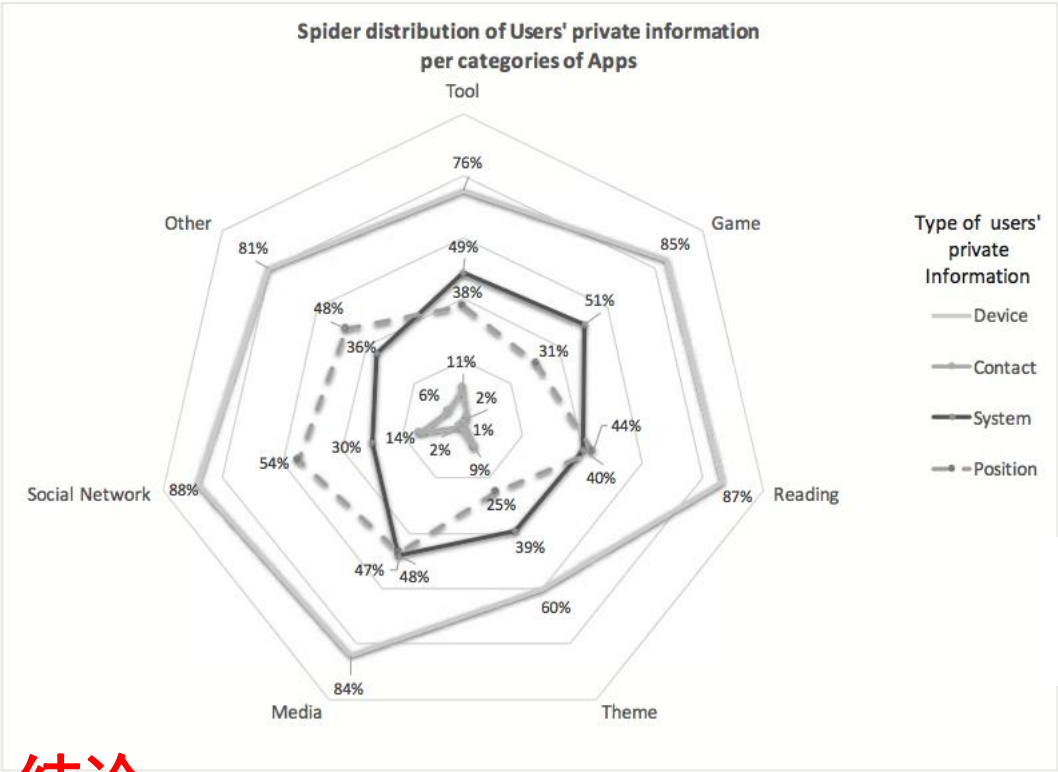
来源：2014我国互联网网络安全态势报告

安卓市场健康度分析

- 数据集：监测9个月，来自中国超过50个应用商城上超过18万个应用
- 系统：硬件+软件
- 测试方法：
 - 自动+手动
 - 静态+动态



用户隐私的获取比例

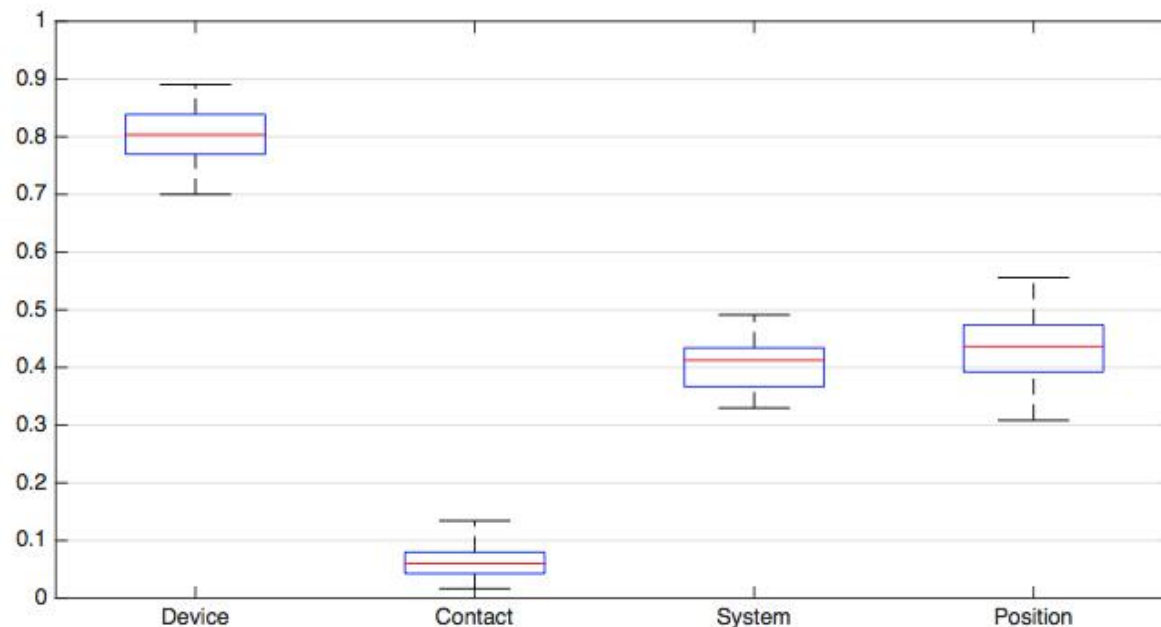


IMEI	IMSI	Location	Installed app list	Tel No.
79.2%	50.6%	35.9%	35.4%	15.8%

结论：

1. 超过90%的应用都获取各种用户隐私；
2. 设备类信息（设备标识等）是最常被获取的用户隐私；
3. 媒体、社交类容易获取位置信息；工具、游戏类最愿意获取系统信息

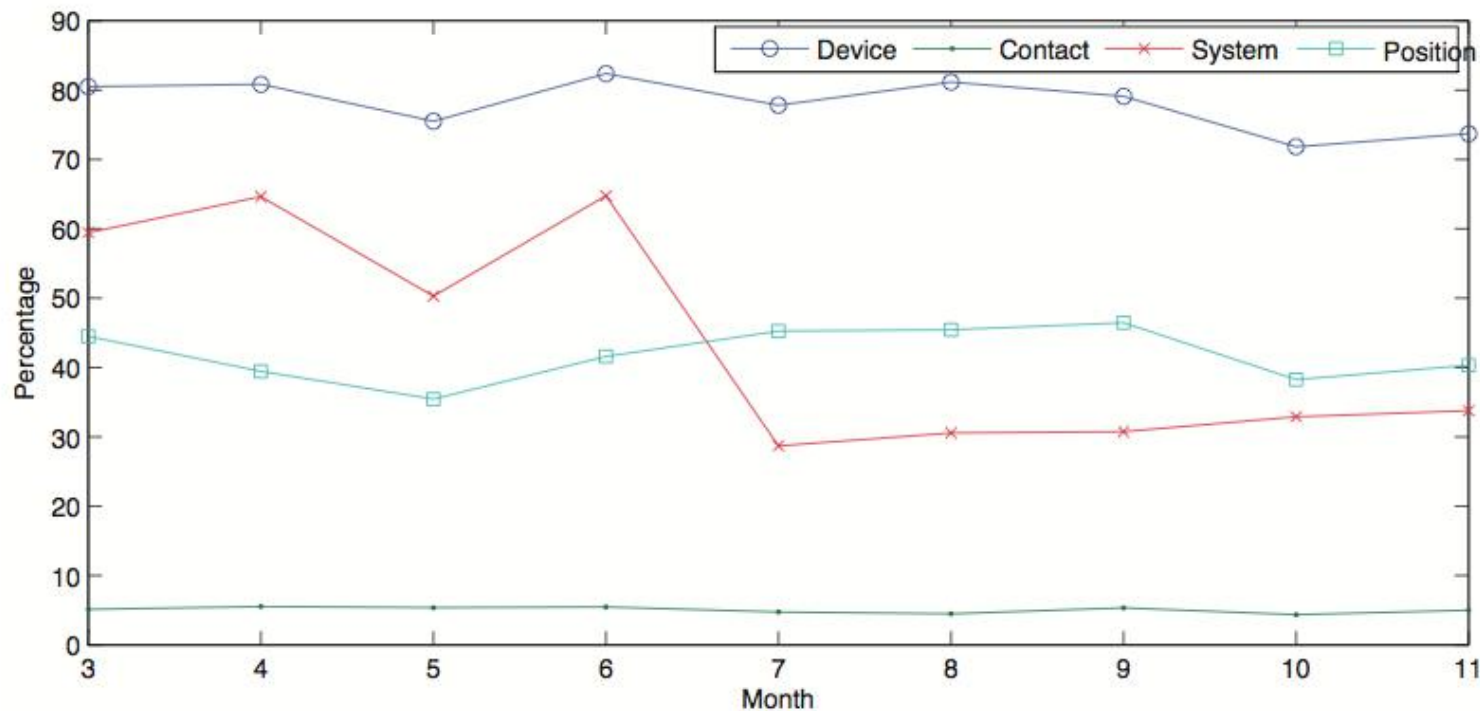
不同（国家）商城的差异



结论：

1. 不同商城的情况差别不大；
2. 中外商城差别不大 (Google Play vs. Chinese AppStore)

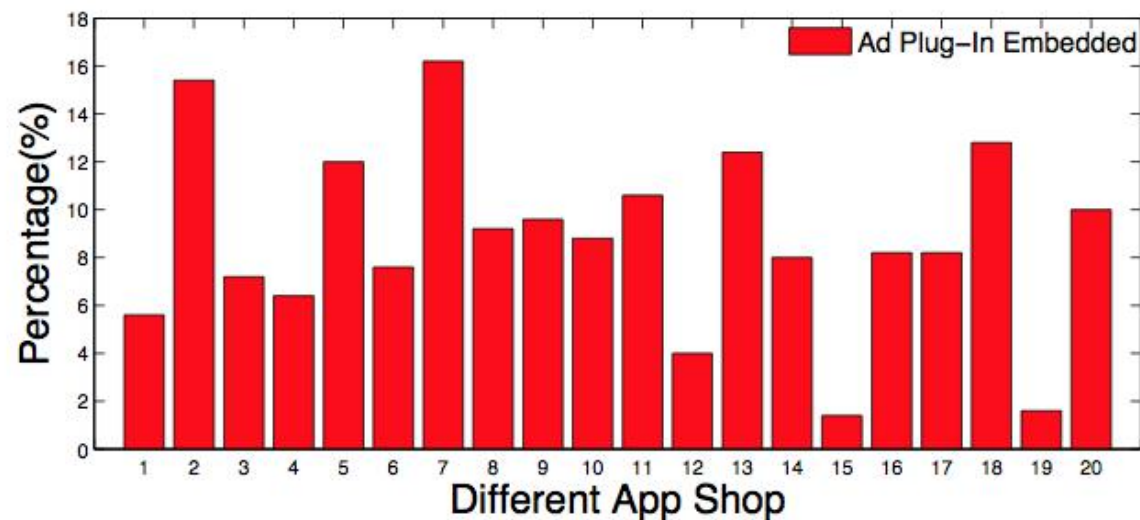
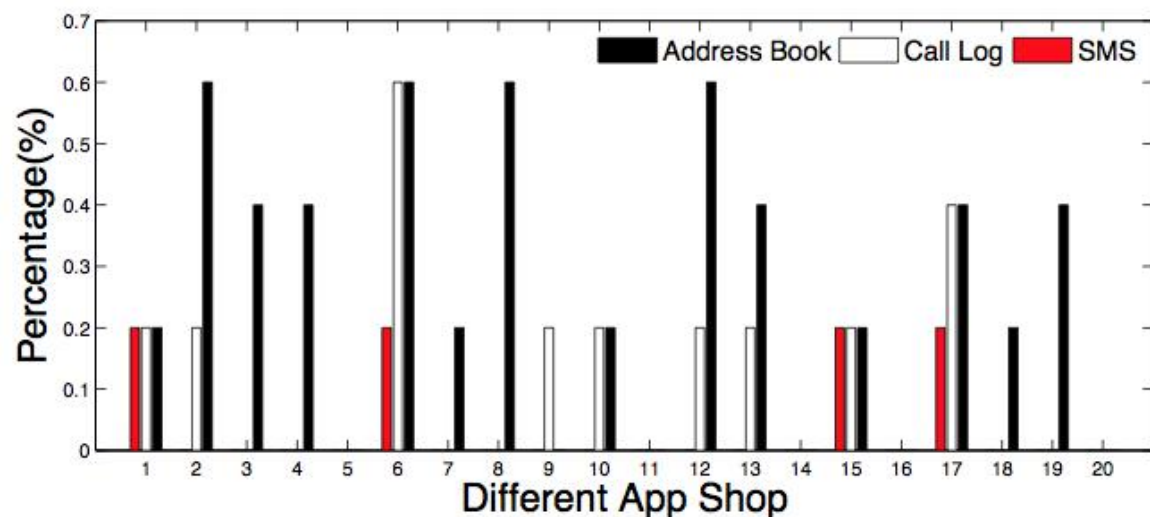
情况会逐渐改善吗？



结论：

1. 设备、通讯、位置类隐私几乎不变；
2. 系统类隐私信息在7月份后下降，Android系统更新。

恶意行为



结论:

1. 少量应用将用户的通讯录、短信、通话记录等信息上传到非法服务器;
2. 嵌入广告现象普遍。