Information Security Engineering

2017.11.15

物理安全

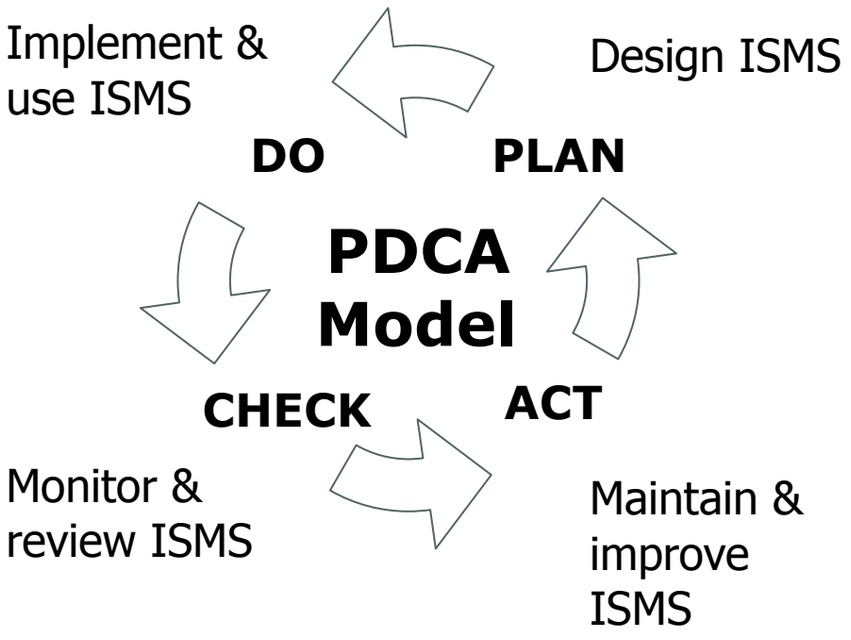
北京大学 软件与微电子学院
School of Software and Microelectronics, Peking University

Huiping Sun(孙惠平)
sunhp@ss.pku.edu.cn

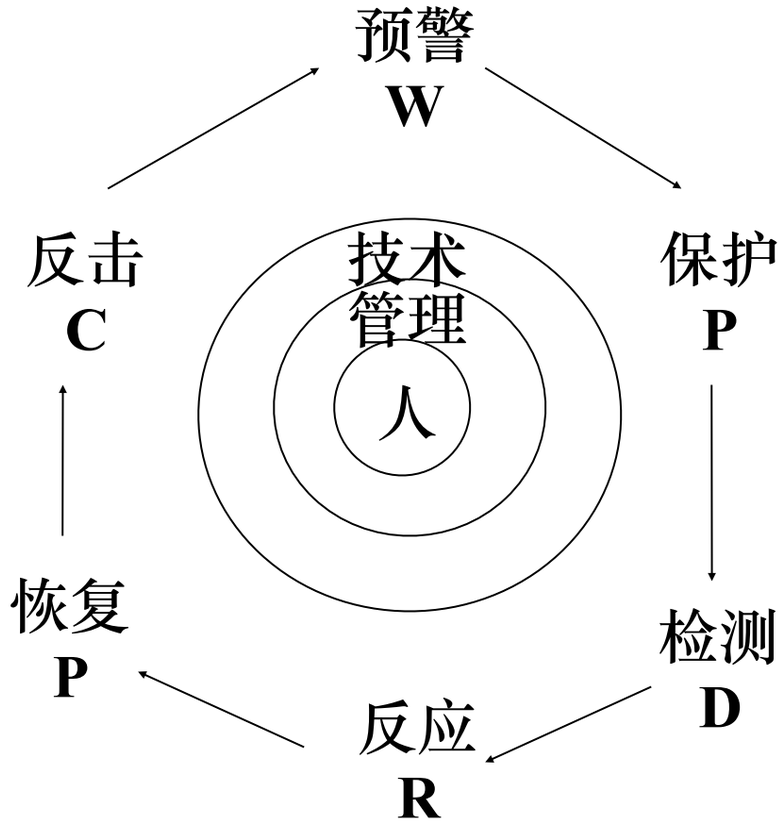
信息安全管理中的物理安全

信息安全管理

- 加强信息安全管理被普遍认为是解决信息安全问题的重要途径。
- 由于管理的复杂性与多样性，信息安全管理制度的制定和实施往往与决策者的个人思路有很大关系，随意性较强，因此信息安全管理需要一定的标准来指导



- BS7799
- ISO 17799
- ISO 13335



信息安全管理

标准	目的	内容
安全方针	为信息安全提供管理方向和支持。	建立安全方针文档
安全组织	建立组织内的管理体系以便安全管理。	组织内部信息安全责任；信息采集设施安全；可被第三方利用的信息资产的安全；外部信息安全评审；外包合同的安全。
资产分类与控制	维护组织资产的适当保护系统。	利用资产清单，分类处理，信息标签等对信息资产进行保护。
人员安全	减少人为造成的风险。	减少错误，偷窃，欺骗或资源误用等人为风险；保密协议；安全教育培训；安全事故与教训总结；惩罚措施。
物理与环境安全	防止对关于IT服务的未经许可的介入，损伤和干扰服务。	阻止对工作区与物理设备的非法进入；业务机密和信息非法的访问、损坏、干扰；阻止资产的丢失，损坏或遭受危险；桌面与屏幕管理阻止信息的泄漏。
通信与运营管理	保证通讯和操作设备的正确和安全维护。	确保信息处理设备的正确和安全的操作；降低系统失效的风险； 保护软件和信息的完整性；维护信息处理和通讯的完整性和可用性；确保网络信息的安全措施和支持基础结构的保护； 防止资产被损坏和业务活动被干扰中断；防止组织间的交易信息遭受损坏，修改或误用。
访问控制	控制对业务信息的访问。	控制访问信息；阻止非法访问信息系统；确保网络服务得到保护；阻止非法访问计算机；检测非法行为； 保证在使用移动计算机和远程网络设备时信息的安全。
系统开发与维护	保证系统开发与维护的安全	确保信息安全保护深入到操作系统中； 阻止应用系统中的用户数据的丢失，修改或误用；确保信息的机密性，可靠性和完整性；确保IT项目工程及其支持活动在安全的方式下进行；维护应用程序软件和数据的安全。
业务持续性管理	防止商业活动中断和灾难事故的影响。	防止商业活动的中断；防止关键商业过程免受重大失误或灾难的影响。
符合性	避免任何违反法令、法规、合同约定及其他安全要求的行为。	避免违背刑法、民法、条例，遵守契约责任以及各种安全要求； 确保组织系统符合安全方针和标准；使系统审查过程的绩效最大化，并将干扰因素降到最小。

Physical Security

安全区域

- 目标
  - 防止未经授权的访问，预防对业务基础和业务信息的破坏以及干扰
- 内容
  - 把关键的和敏感的业务信息处理设备放在安全区域，受到确定的安全范围的保护，并有适当的安全屏障和接入控制。对他们从实体上加以保护，以防未经授权的访问并免于干扰和破坏

- 自身人员管理
- 第三方人员管理
- 最小信息原则
- 任何行为可监督
- 最小授权原则
- 附加屏障和界线
- 摄影、录像、录音

Physical Security

物理访问控制

- 设立安全屏障、建立安全界线
- 墙、前台、门禁等
- 进入受控，访问受限
- 相应的管理机制与规章
- 人防＋技防
- 屏障的设立和界线的划分，乃至保护力度取决于风险评估的结果

物理安全界线

- 进入须授权，操作须认证
- 监控区域内人员、记录出入时间
- 使用身份认证管理
- 佩戴相关标识、盘查无标识人员
- 定期检查和更新对安全区域的访问权限
- 保存出入记录，保证可审查追踪

物理进入控制

环境安全

- 水、火等灾难
- 门窗上锁，外部保护
- 安装入侵者监控系统
- 注意危险品与易燃物品
- 注意备份介质和备份设备的放置和存储

Physical Security

设备安全

- 目标
  - 防止资产流失、被损坏或者破坏，防止对业务活动的破坏
- 内容
  - 对设备加以实体上的保护，使其免于安全风险和环境灾难
  - 为减少对数据未经授权访问所造成的危险并保护其免受损失或破坏

- 设备应当得到正确的维护，以确保其持续有效性和完整性
- 按时维护、专人维护
- 记录事故与故障、记录处理方法
- 外送维修应注意保密

Physical Security

设备安全

- 妥善安置设备，把对工作区不必要的访问降低到最低限度
- 处理敏感数据的信息处理和存储设备应当妥善放置以减少其使用期间忽视对其监督的风险。
- 应当把需要特殊保护的物品隔离开，以降低所用保护等级
- 组织应当考虑对在信息处理设施附近就餐、饮水和吸烟的政策规定

- 应当采取措施降低潜在风险内容
- 应当监测那些可能对信息处理设备有负面影响的环境条件
- 应当为工业化环境中的设备而采用专门的保护方法，比如键盘保护膜
- 应当考虑到在房屋附近发生灾难所产生的影响，例如邻近建筑物的火灾、屋顶或者地表的渗水或者街道上发生的爆炸

Physical Security

设备安全

- 个人电脑、手机、文件
- 有人看管、正常使用
- 评估风险、采取对策

设备转移

- 敏感信息的存储介质
- 完全删除内容
- 设备检测
- 风险评估

设备处理

- 防止对信息和信息处理设备的损坏和盗窃
- 清洁桌面
  - 纸张
  - 可移动存储
- 清洁屏幕

一般性措施

电力

- 应当对设备加以保护使其免于电力中断或者其它电力异常的影响
- 有多路供电途径以避免单点电力供应发生故障的危险
- 不间断电源（*UPS*）
- 备用发电机

电力供应

- 应当保护传输数据和辅助信息服务的电缆和通讯线路，使其免于截取或者破坏
- 埋入地下、足够的选择性保护、专门管线
- 把供电线路与通讯线路隔离
- 安装包皮的管线并将房间或者箱子上锁
- 使用光纤

电缆

信息安全工程中的物理保护

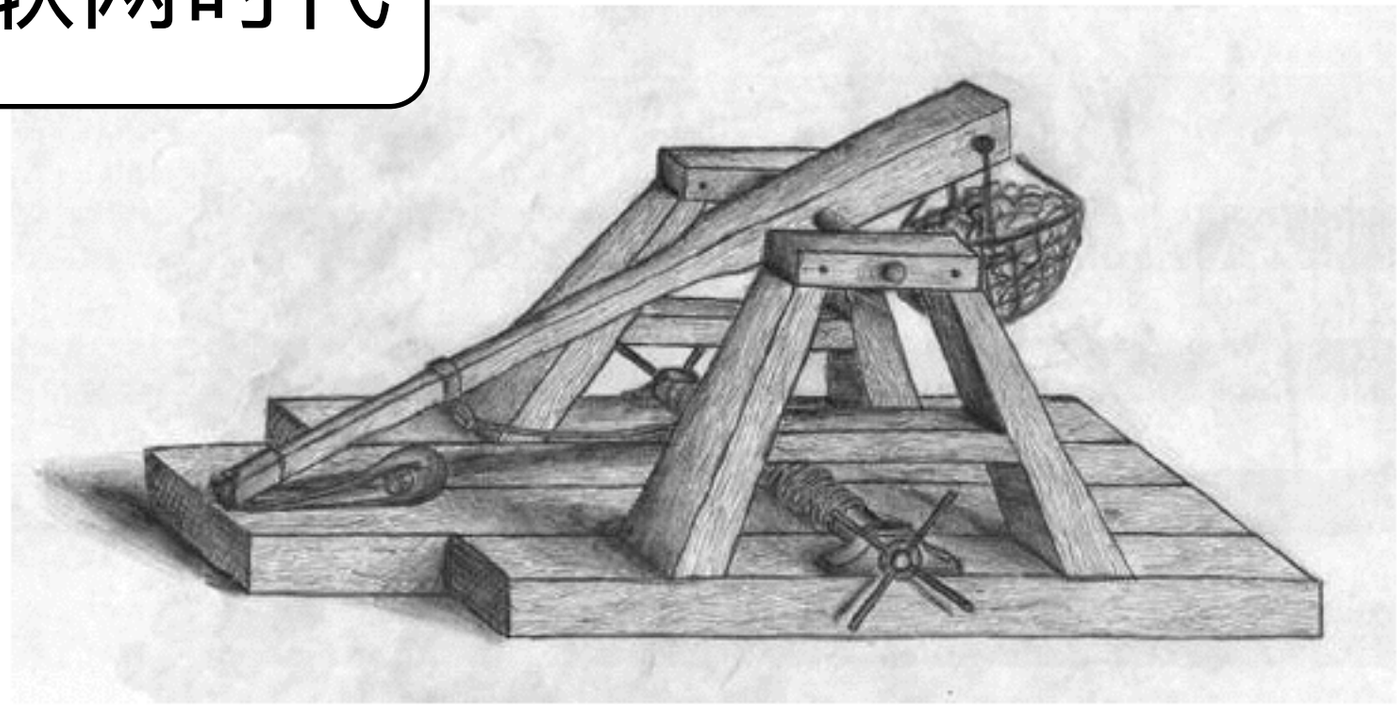
主要内容

- *Security Engineering (Second Edition). Chapter 11: Physical Protection.*
- *Security Engineering (Second Edition). Chapter 14: Security Printing and Seals.*
- *Security Engineering (Second Edition). Chapter 16: Physical Tamper Resistance.*
- *Security Engineering (Second Edition). Chapter 17: Emission Security.*

Physical Protection

墙是一种物理保护

互联网时代



访问控制

- 对于一个资源和地点的选择性的访问限制
- 物理安全 *vs* 信息安全
- 访问可以是消费、进入、使用、退出等
- 分配存取资源的允许，授权
- 验证：人 *vs* 机器

Who Where When	Key Credential

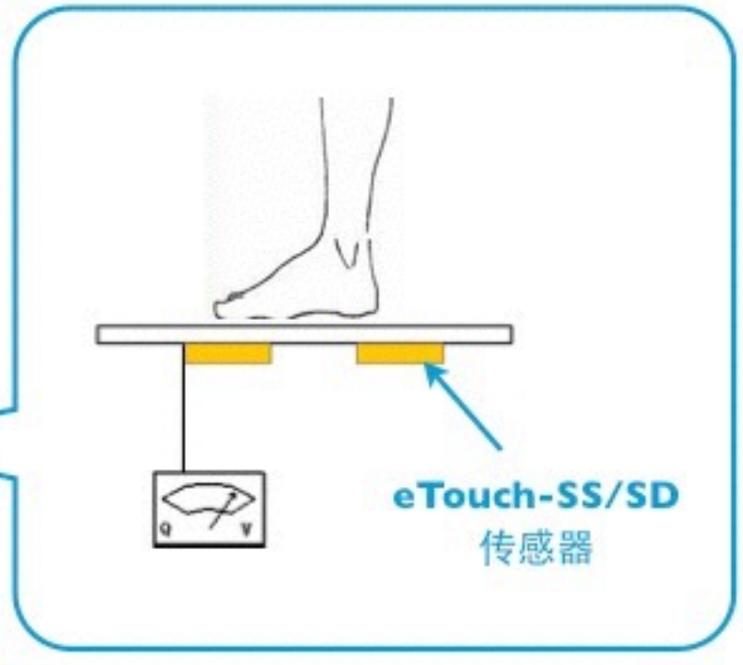
- 授权每个员工可以进入自己房间，但不能进入其他人房间，但是保洁员可以访问所有人房间

Physical Protection

物理防护手段和威胁

- 振动探测
- 红外检测
- 运动监测

- 拒绝服务攻击
- 围墙和安全
- 威慑作用
- 错误警报



攻击者能力 vs 手段

- 无目标、无知识、无能力
- 有“专业知识”
- 有目标、有知识
- 内部人员
- 有资助、有支持

- 威慑
- 检测
- 报警
- 延迟
- 响应

威慑和障碍

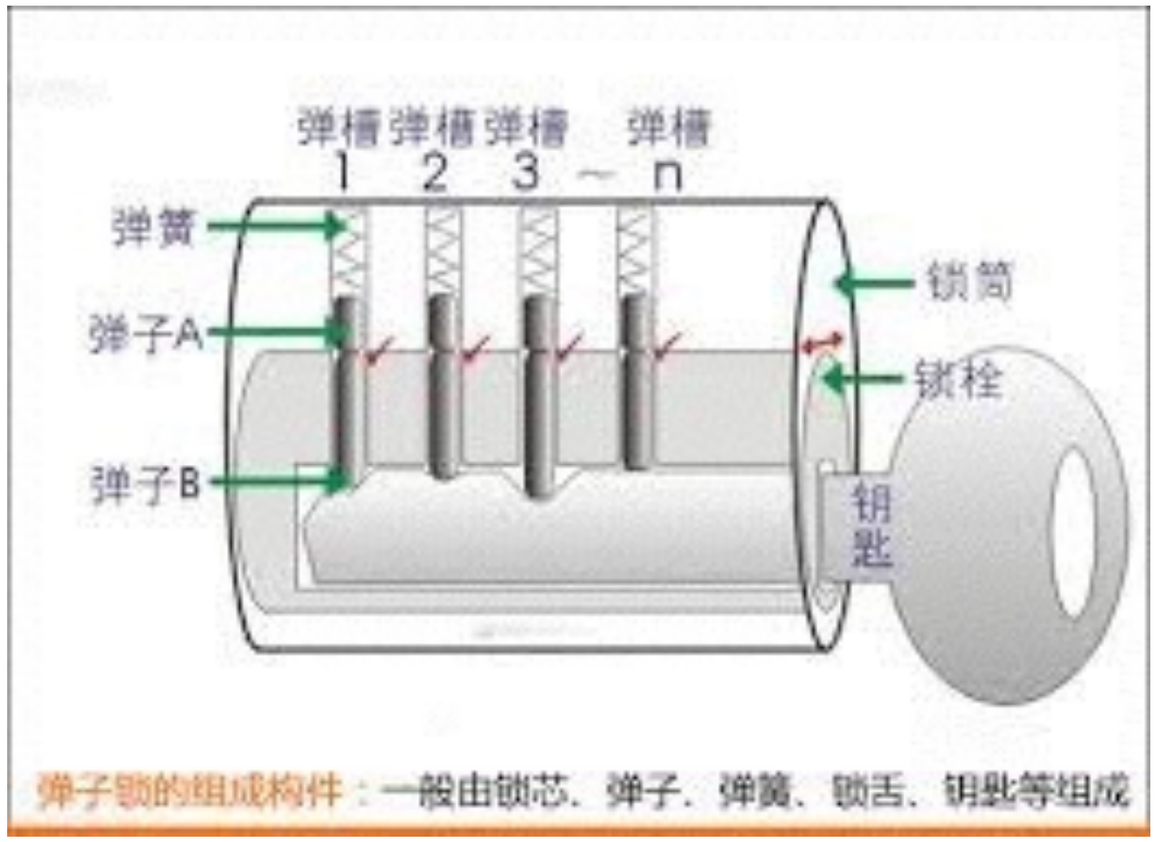
- 默默无闻
- 环境设计
- 保护目标
- 安全边界
- 报警器
- 通信系统

- 好区 vs 坏区
- 可防卫空间
- 破窗理论

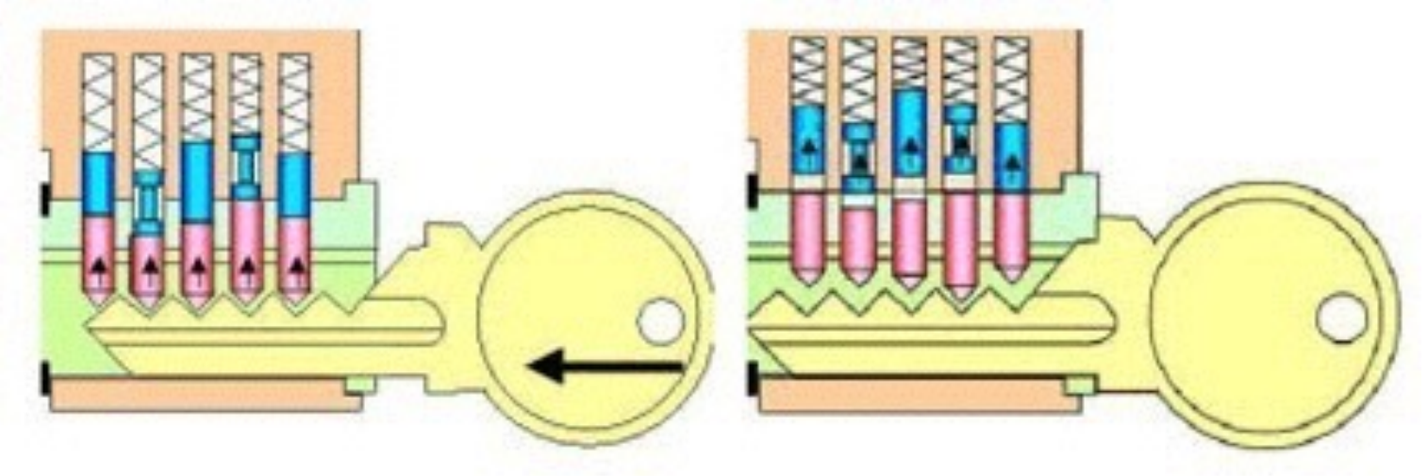
- 银行
- 核电站

- 传感器失灵
- 误报
- 人为破坏

存在万能钥匙



撞匙开锁枪



撞钥攻击

主钥攻击

电子锁

封印

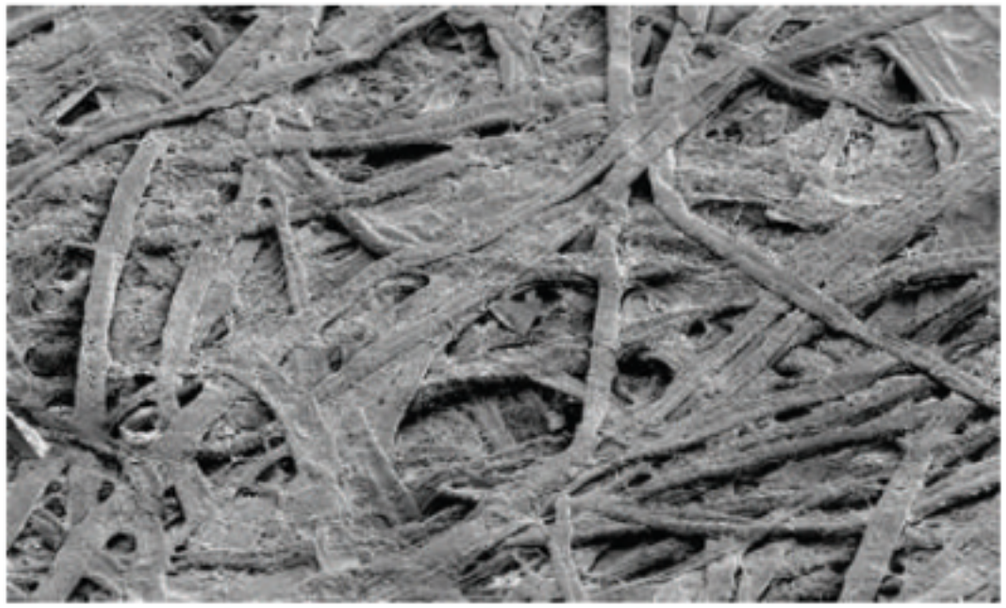

新版
2015年版 第5套
人民币
那些事...
中国人民银行
100
壹佰圆
样币
AA00000000
钞票正面
钞票背面
ZHONGGUO RENMIN YINHANG
100
YUAN
2015年
样币禁止流通
多一份金融了解
多一份财富保障
2015年版第5套人民币100元纸币在保持2005年版第五套人民币100元纸币规格、正背面主图案、主色调、“中国人民银行”行名、国徽、盲文和汉语拼音行名、民族文字等不变的前提下，对部分图案做了调整，对整体防伪性能进行了提升。
① 光变镂空开窗安全线
② 雕刻凹印
③ 胶印对印图案
④ 光彩光变数字
⑤ 白水印
⑥ 人像水印
⑦ 横纵双号码
广发银行
CGB

Security Printing and Seals

封印

Security Printing and Seals

安全打印



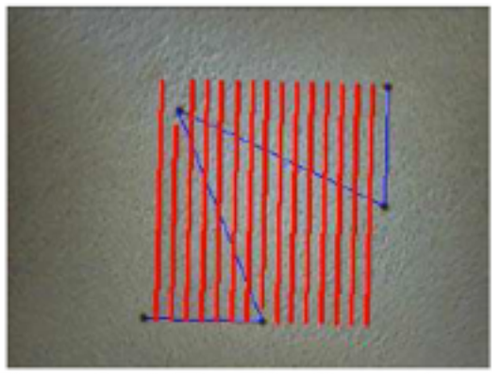
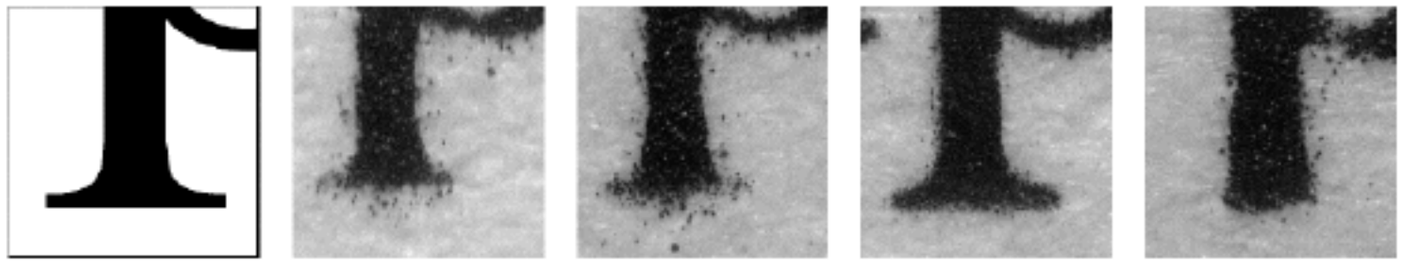
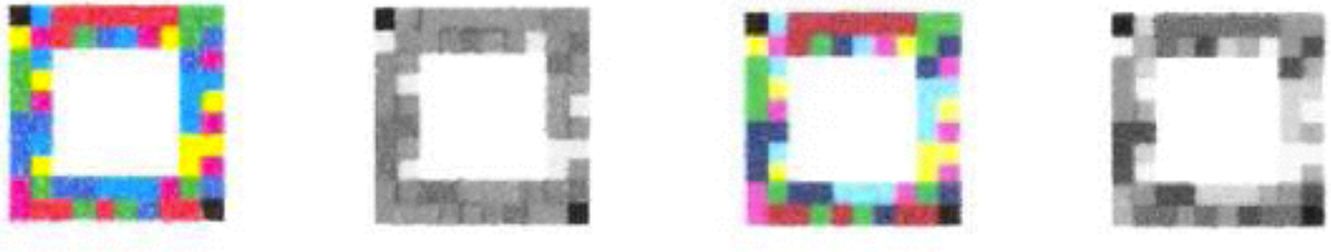
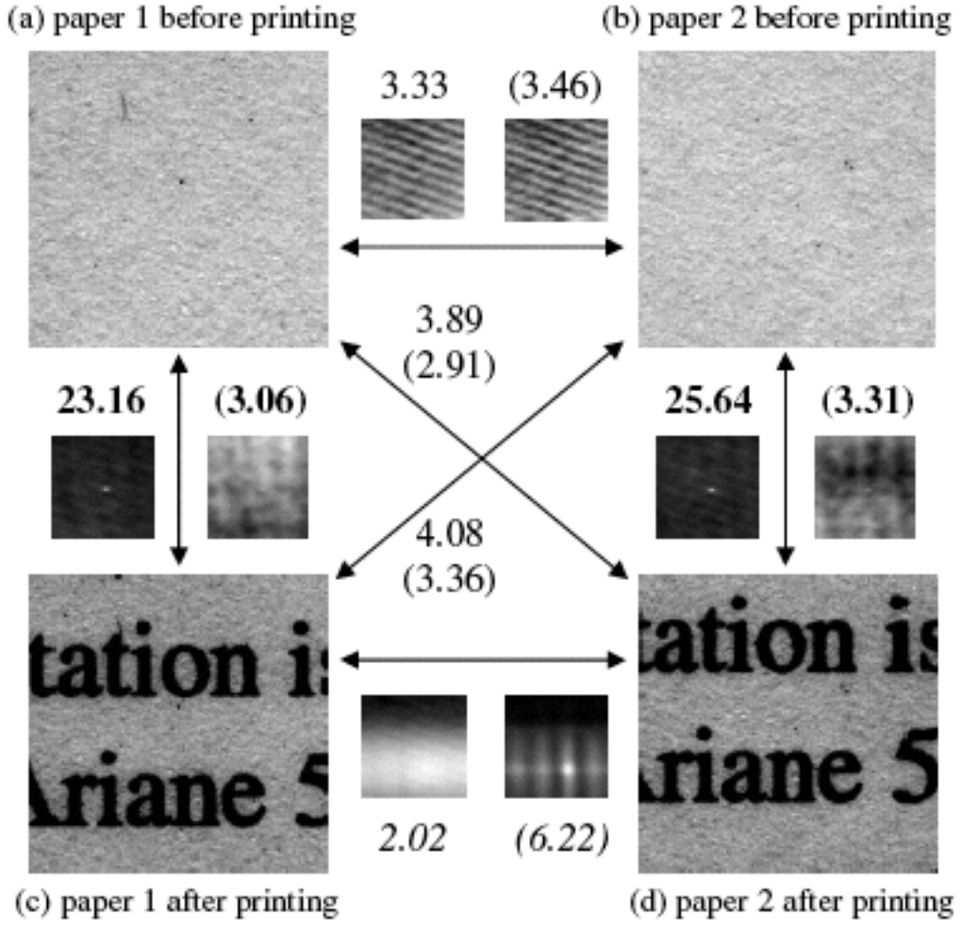


Figure 3: a) The Fiberfingerprint method; b) Verification device used to extract the substrate individualities (Source: Metois et al. (2002))







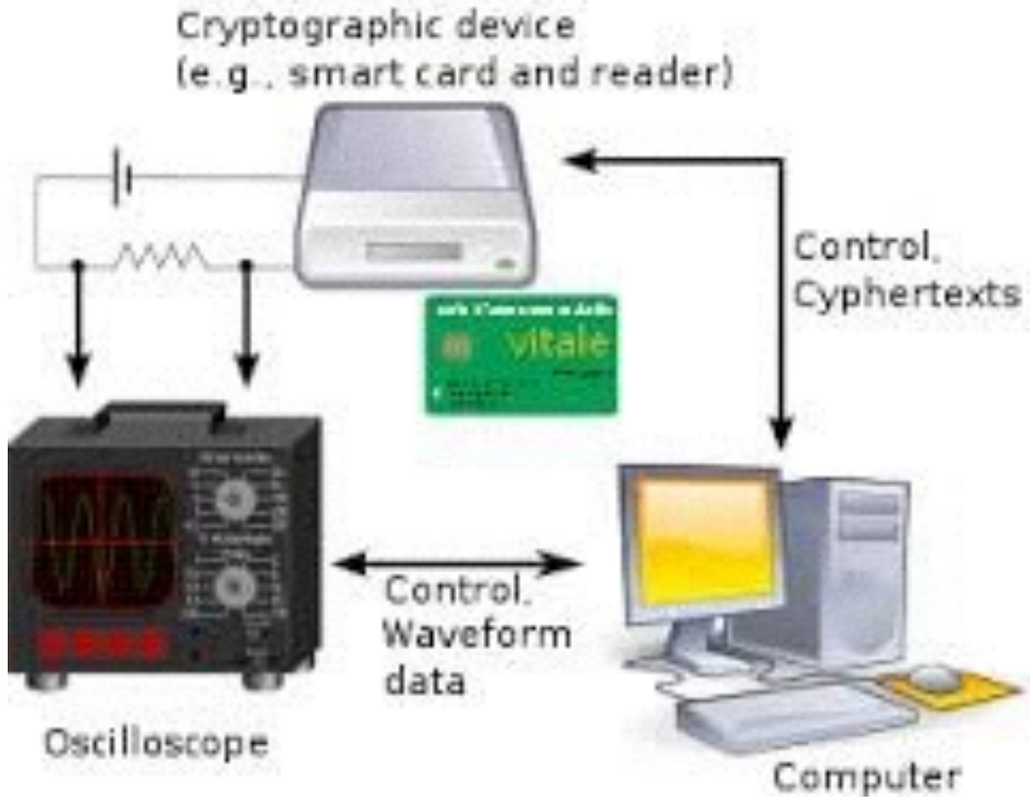
攻击安全处理器

- 偷取密钥
- 外壳切割
- 探针攻击
- 剩磁攻击
- 冷冻攻击
- 电磁泄漏
- 接口攻击
- … ….
- 协议分析
- 光学探测
- 冗余监测
- 柠檬市场

Physical Tamper Resistance

物理防篡改 vs 物理攻击

IBM 4758

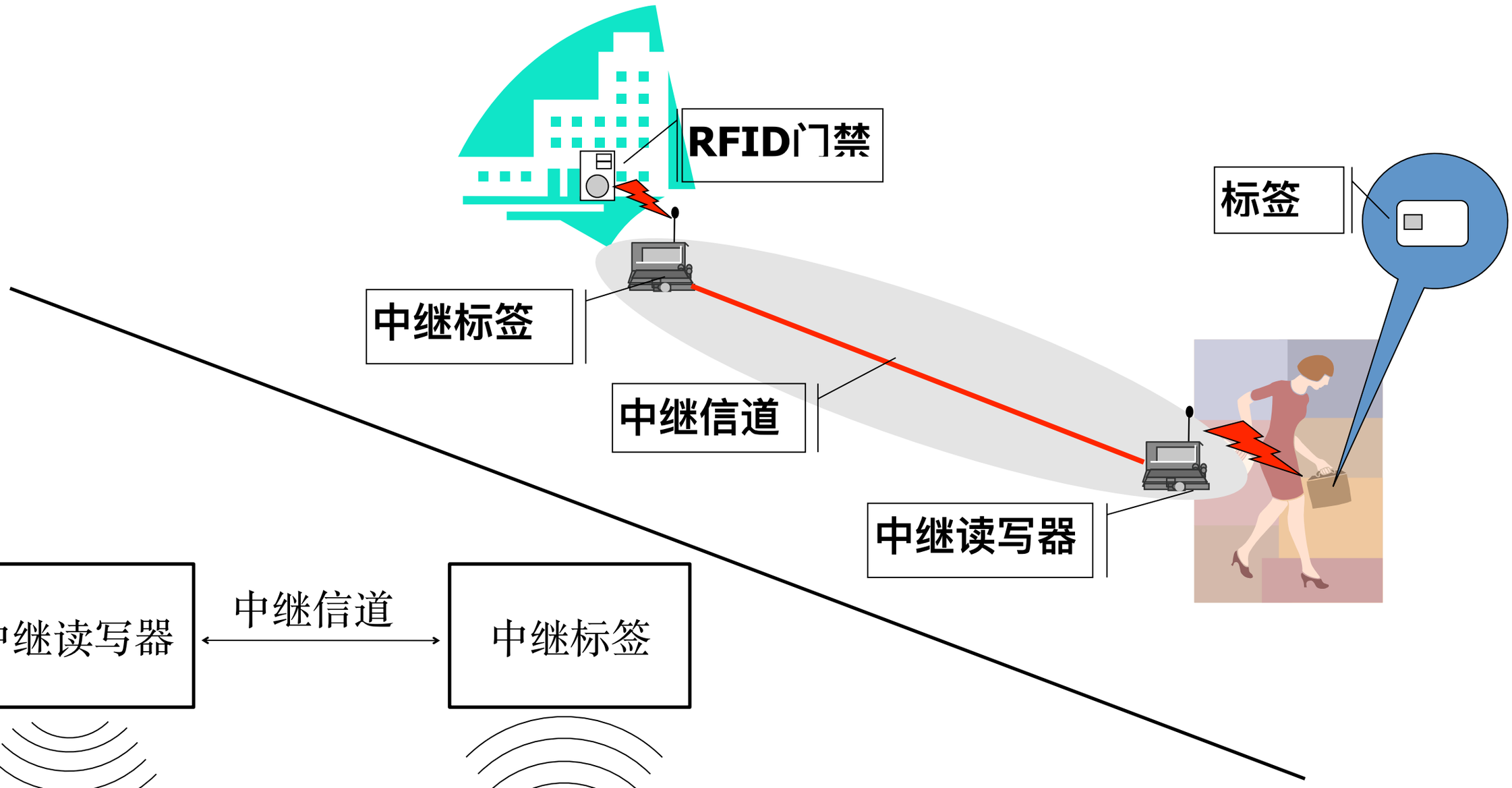


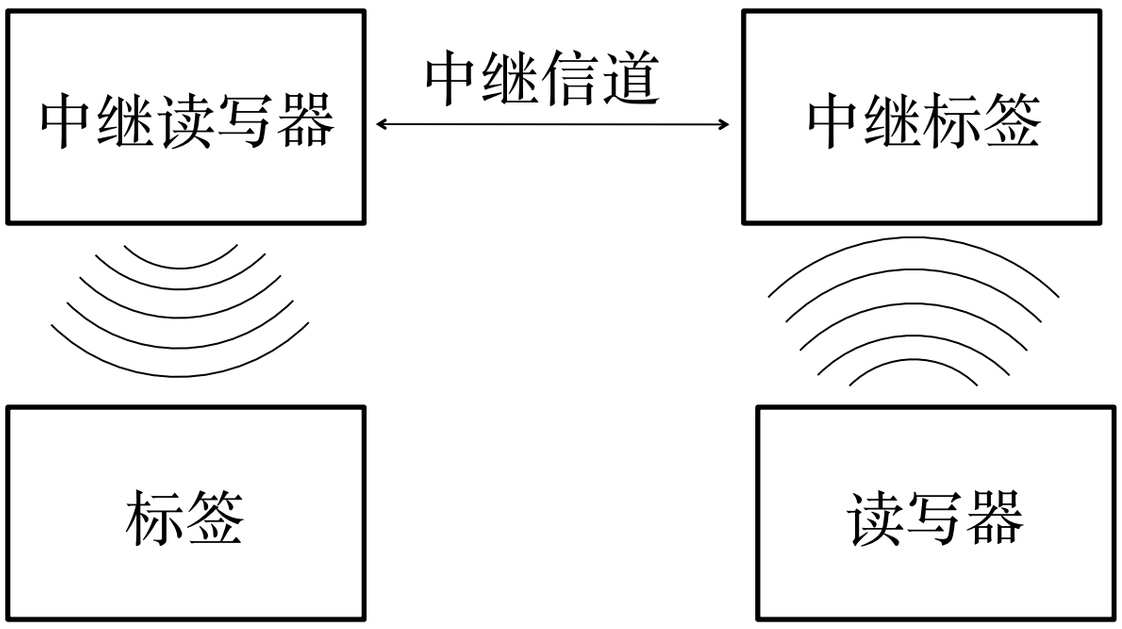
Emission Security

发射安全

- 电话窃听
- 功耗分析
- 电磁泄漏
- 光学旁路
- 声学旁路
- … ….

中继攻击





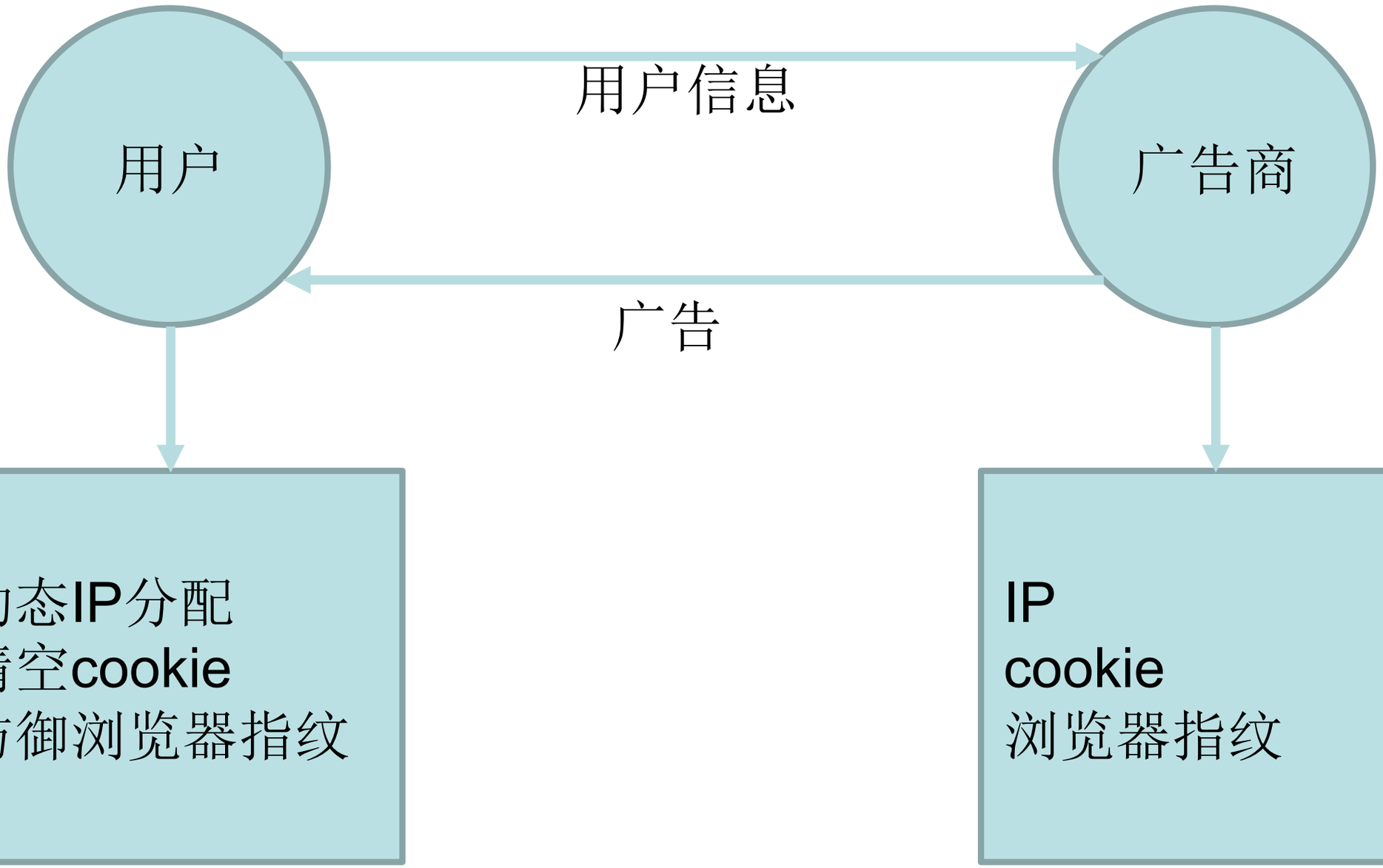
浏览器指纹

浏览器指纹

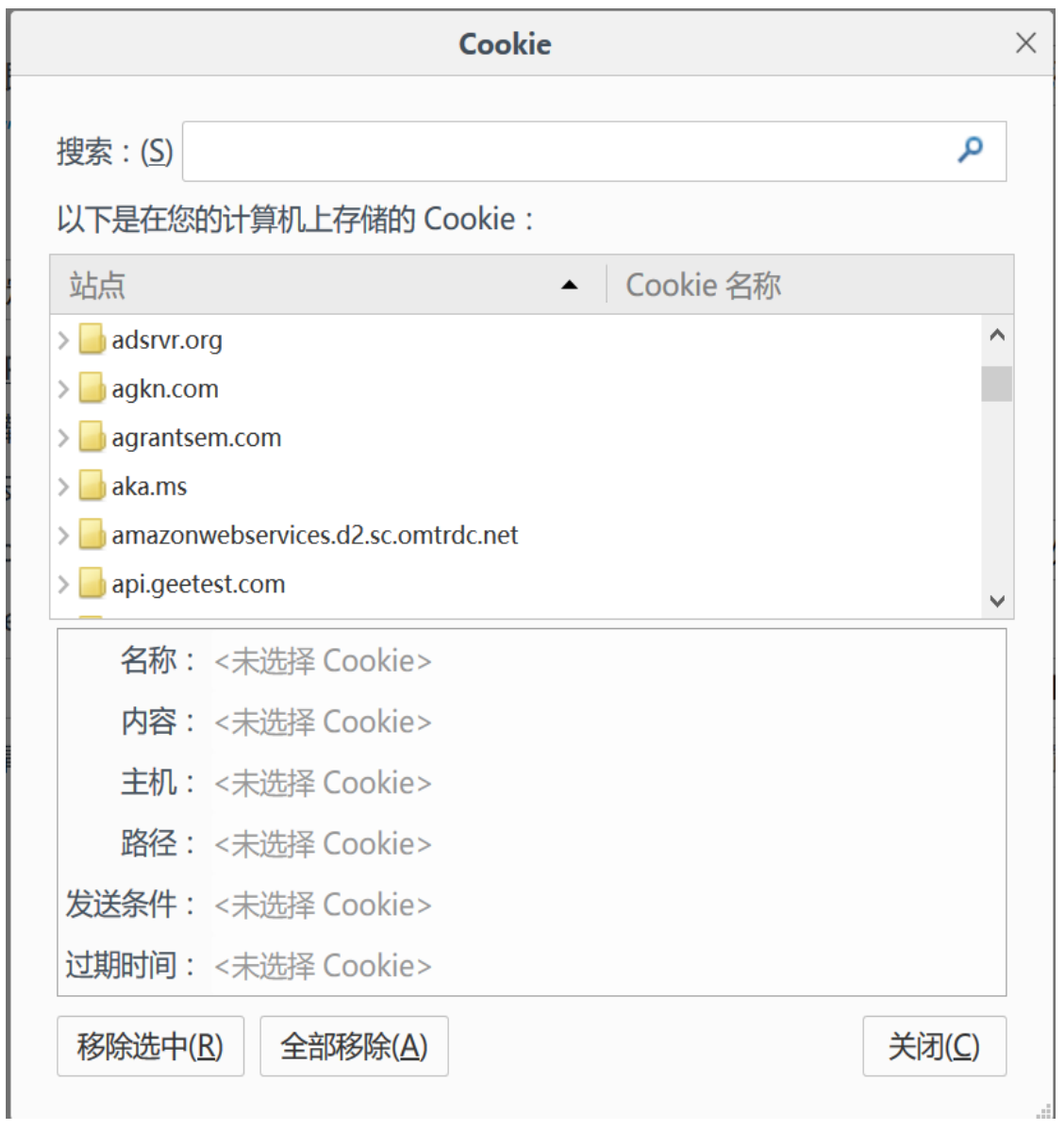
当你使用浏览器访问某个网站的时候，浏览器【必定会暴露】某些信息给这个网站。为什么强调“必定”呢？因为这些信息中，有些是跟 *HTTP* 协议相关的。只要你基于 *HTTP* 协议访问网站，浏览器就【必定】会传输这些信息给网站的服务器。只要你通过浏览器访问 *Web*，必定是基于 *HTTP* 协议的。因此，*Web* 网站的服务器必定可以获取到跟你的浏览器相关的某些信息。

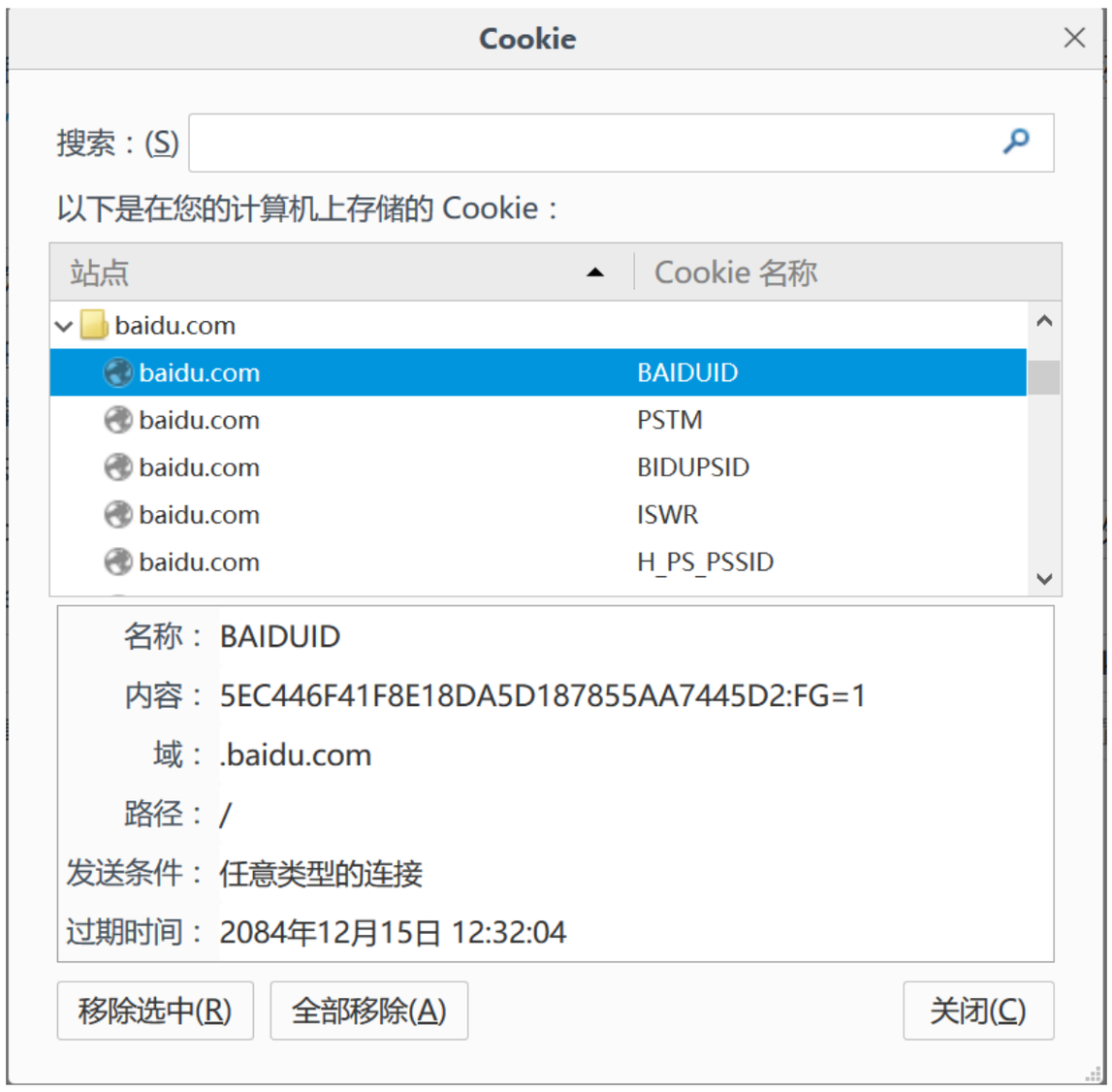
- 更互动的网络（例如，*JavaScript*库的繁荣，*HTML5*的每周创新）
- 更可用的网络（例如，移动设备的爆炸）
- 更安全的网络（例如，*Flash*正在消失，*NPAPI*插件正在被弃用）
- 更私人的网络（例如，增加立法反对*cookies*，扩展的巨大成功，如*Ghostery*和*AdBlock*）。

背景



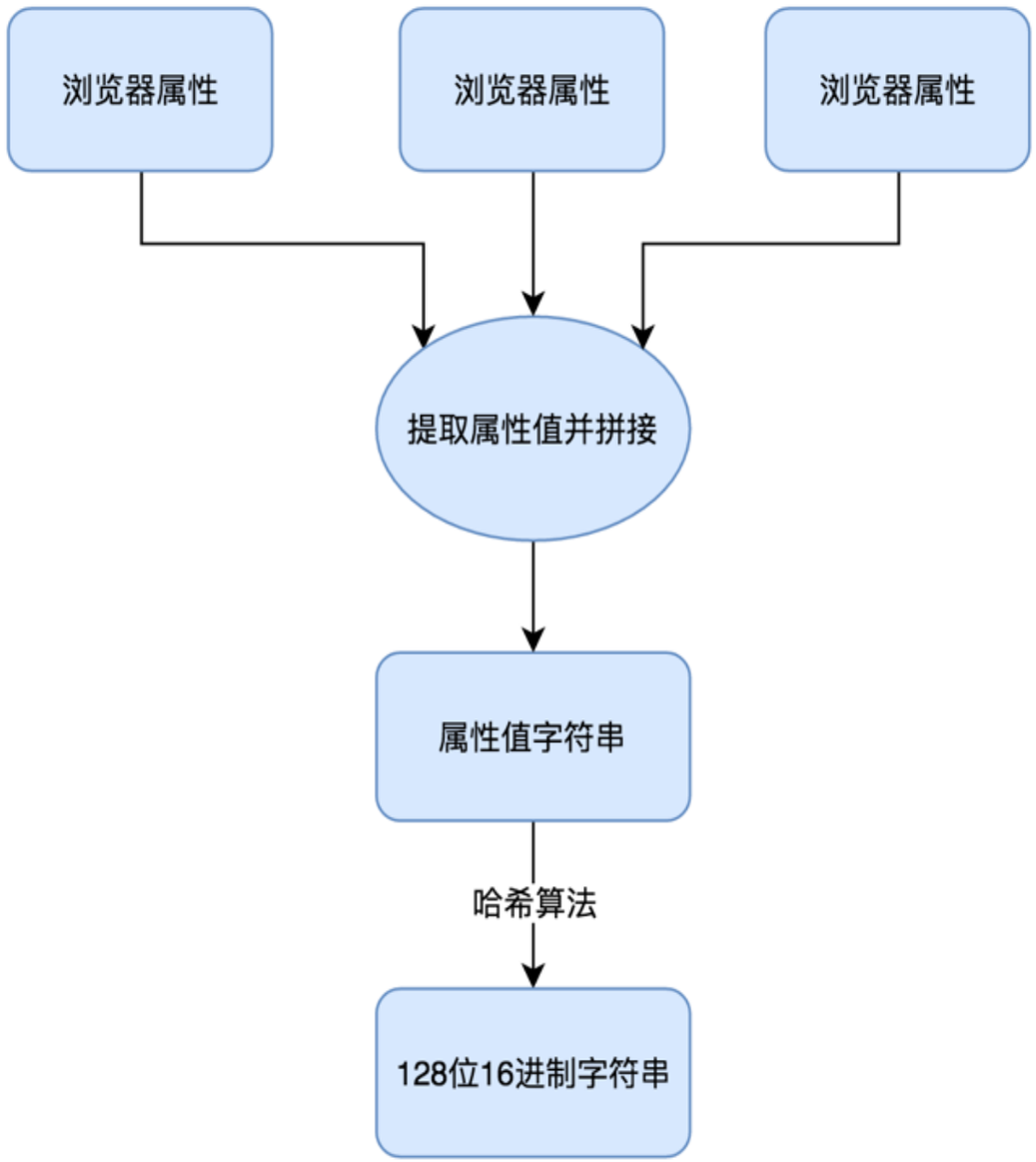
Cookie

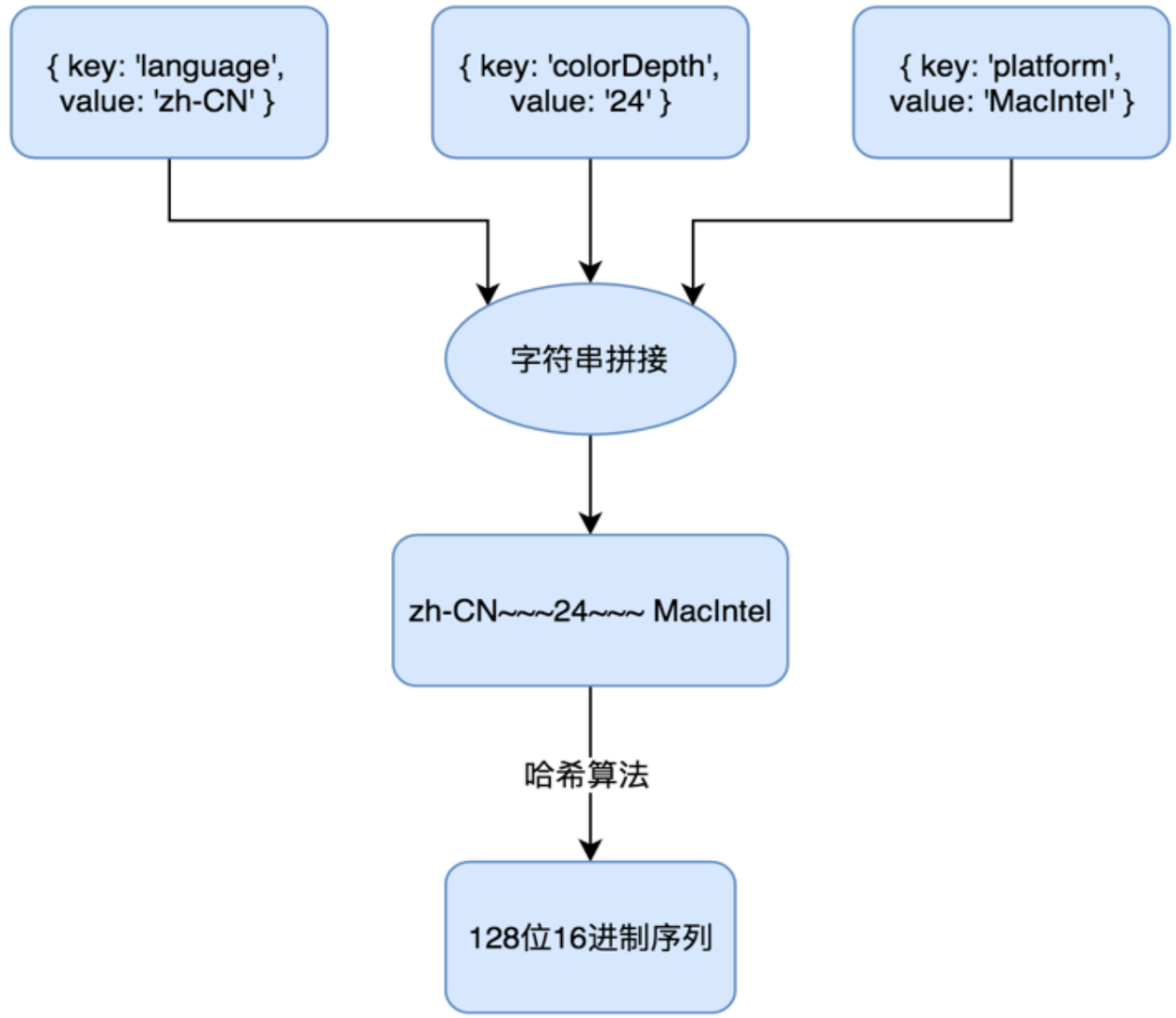

Cookie
搜索：(S)
以下是在您的计算机上存储的 Cookie：
站点
Cookie 名称
adsrvr.org
agkn.com
agrantsem.com
aka.ms
amazonwebservices.d2.sc.omtrdc.net
api.geetest.com
名称： <未选择 Cookie>
内容： <未选择 Cookie>
主机： <未选择 Cookie>
路径： <未选择 Cookie>
发送条件： <未选择 Cookie>
过期时间： <未选择 Cookie>
移除选中(R)
全部移除(A)
关闭(C)


Cookie
搜索：(S)
以下是在您的计算机上存储的 Cookie：
站点
Cookie 名称
baidu.com
baidu.com BAIDUID
baidu.com PSTM
baidu.com BIDUPSID
baidu.com ISWR
baidu.com H_PS_PSSID
名称： BAIDUID
内容： 5EC446F41F8E18DA5D187855AA7445D2:FG=1
域： .baidu.com
路径： /
发送条件： 任意类型的连接
过期时间： 2084年12月15日 12:32:04
移除选中(R)
全部移除(A)
关闭(C)

Browser Fingerprinting

浏览器指纹提取





浏览器属性分类

可以通过浏览器提供的接口或对象直接获取值的属性	User Agent、屏幕分辨率、可用屏幕分辨率、平台、语言、时区、色深度、色素率、会话存储、本地存储、索引数据库、开放数据库、CPU种类、触感支持，禁止追踪、插件
需要通过JavaScript做一些判断，才能确定值的属性	是否安装了广告屏蔽插件，用户是否修改了语言、用户是否修改了分辨率、用户是否修改了操作系统、用户是否修改了浏览器
通过Canvas、WebGL获取到的浏览器属性	Canvas、WebG

HTML 5 Canvas

- 当用户访问一个包含*canvas*的指纹脚本，他会被要求绘制一个隐蔽的图形。不同浏览器会有不同的图像处理引擎、导出选项、压缩等级。相同的*JavaScript*代码在不同的平台上执行最终的结果会不同（*OS*，*OS Version*，*Browser*，*Browser Version*，*GPU*）。由于，绘制出的图形会有差别，根据这些差别为用户分配唯一的编号（指纹）。

- 持续性；用户透明
- 易获得；*High-Entropy*

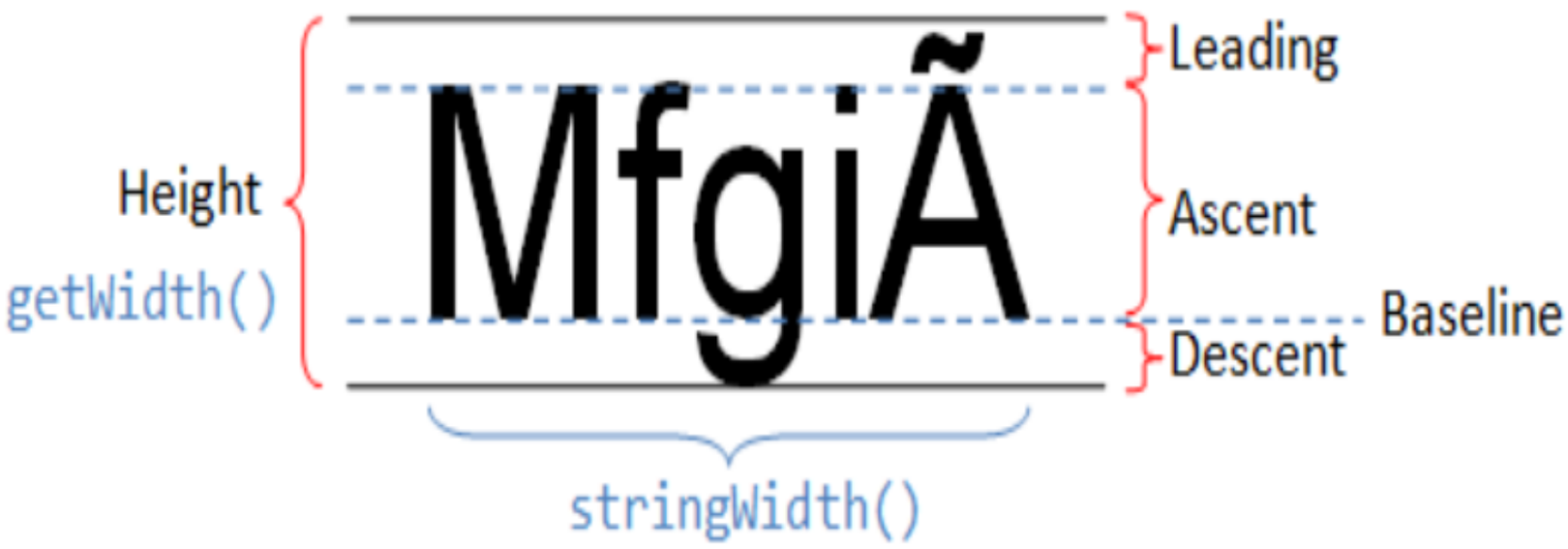
```
<canvas id="myCanvas"></canvas>

<script type="text/javascript">

var canvas=document.getElementById('myCanvas');
var ctx=canvas.getContext('2d');
ctx.fillStyle='#FF0000';
ctx.fillRect(0,0,80,100);

</script>
```

Font Metrics

- 包含*JavaScript*的*Web*页面，将*code points(*码点*)*插入*DOM*,测量相应字体的维度。将每个码点放入空盒子*(bounding box)*，通过测量盒子的尺寸。

- 变量类型：*browser;browser version;*

- 安装的字体类型；字体的设置；



Font Metrics

Table 2. Code points with the most and least individual entropy.

rank	individual entropy (bits)	code point	name
#1	4.908178	U+20B9	INDIAN RUPEE SIGN
2	4.798824	U+20B8	TENGE SIGN
3	4.698577	U+FBEE	ARABIC LIGATURE YEH WITH HAMZA ABOVE WITH WAW ISOLATED FORM
4	4.698577	U+FBF0	ARABIC LIGATURE YEH WITH HAMZA ABOVE WITH U ISOLATED FORM
5	4.698577	U+FBF2	ARABIC LIGATURE YEH WITH HAMZA ABOVE WITH OE ISOLATED FORM
6	4.698577	U+FBF4	ARABIC LIGATURE YEH WITH HAMZA ABOVE WITH YU ISOLATED FORM
7	4.657576	U+F002	*Private Use Area*
8	4.652798	U+F001	*Private Use Area*
9	4.646632	U+FD3D	ARABIC LIGATURE ALEF WITH FATHATAN ISOLATED FORM
10	4.640043	U+FBF8	ARABIC LIGATURE YEH WITH HAMZA ABOVE WITH E INITIAL FORM
11	4.640043	U+FBFB	ARABIC LIGATURE UIGHUR KIRGHIZ YEH WITH HAMZA ABOVE WITH ALEF MAKSURA INITIAL FORM
⋮	⋮	⋮	
125,766	2.573742	U+202A	LEFT-TO-RIGHT EMBEDDING
125,767	2.573742	U+202B	RIGHT-TO-LEFT EMBEDDING
125,768	2.573742	U+202D	LEFT-TO-RIGHT OVERRIDE
125,769	2.573742	U+202E	RIGHT-TO-LEFT OVERRIDE
125,770	2.481283	U+202C	POP DIRECTIONAL FORMATTING
125,771	2.462760	U+000C	FORM FEED (FF)
125,772	2.462760	U+000D	CARRIAGE RETURN (CR)
125,773	0.156341	U+00AD	SOFT HYPHEN
125,774	0.000000	U+0009	CHARACTER TABULATION
125,775	0.000000	U+000A	LINE FEED (LF)
125,776	0.000000	U+0020	SPACE

例子

您的浏览器指纹是:

93a23be01b82930c37707a264def73b9

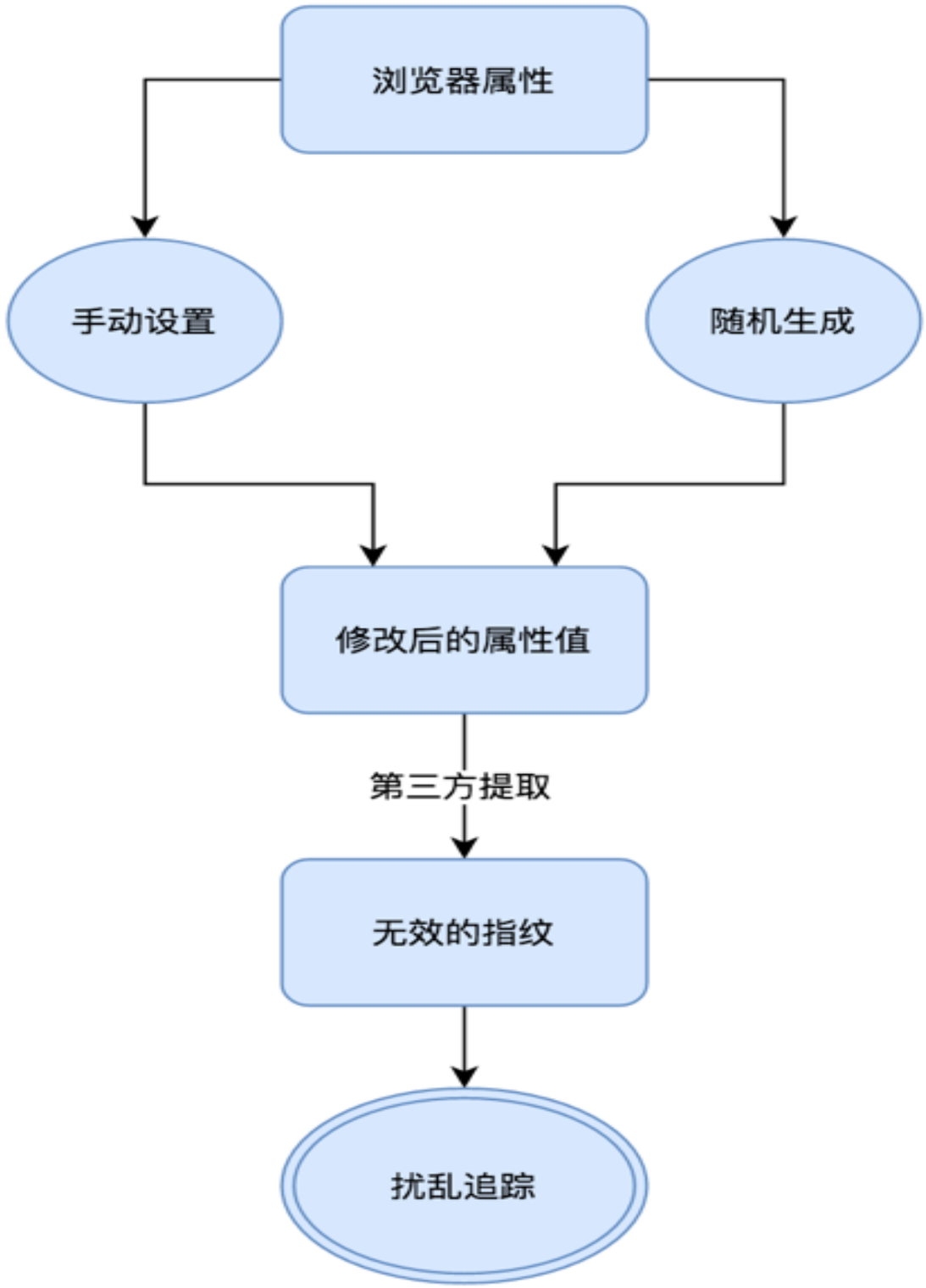
这是您第 **1** 次访问。

计算浏览器指纹耗时:**168** ms

1. **user_agent** : Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.110 Safari/537.36
2. **resolution** : 1440,900
3. **available_resolution** : 1440,873
4. **navigator_platform** : MacIntel
5. **language** : en-US
6. **timezone_offset** : -480
7. **color_depth** : 24
8. **pixel_ratio** : 2
9. **session_storage** : 1
10. **local_storage** : 1
11. **indexed_db** : 1
12. **open_database** : 1
13. **cpu_class** : unknown
14. **do_not_track** : unknown
15. **regular_plugins** : Widevine Content Decryption Module::Enables Widevine licenses for playback of

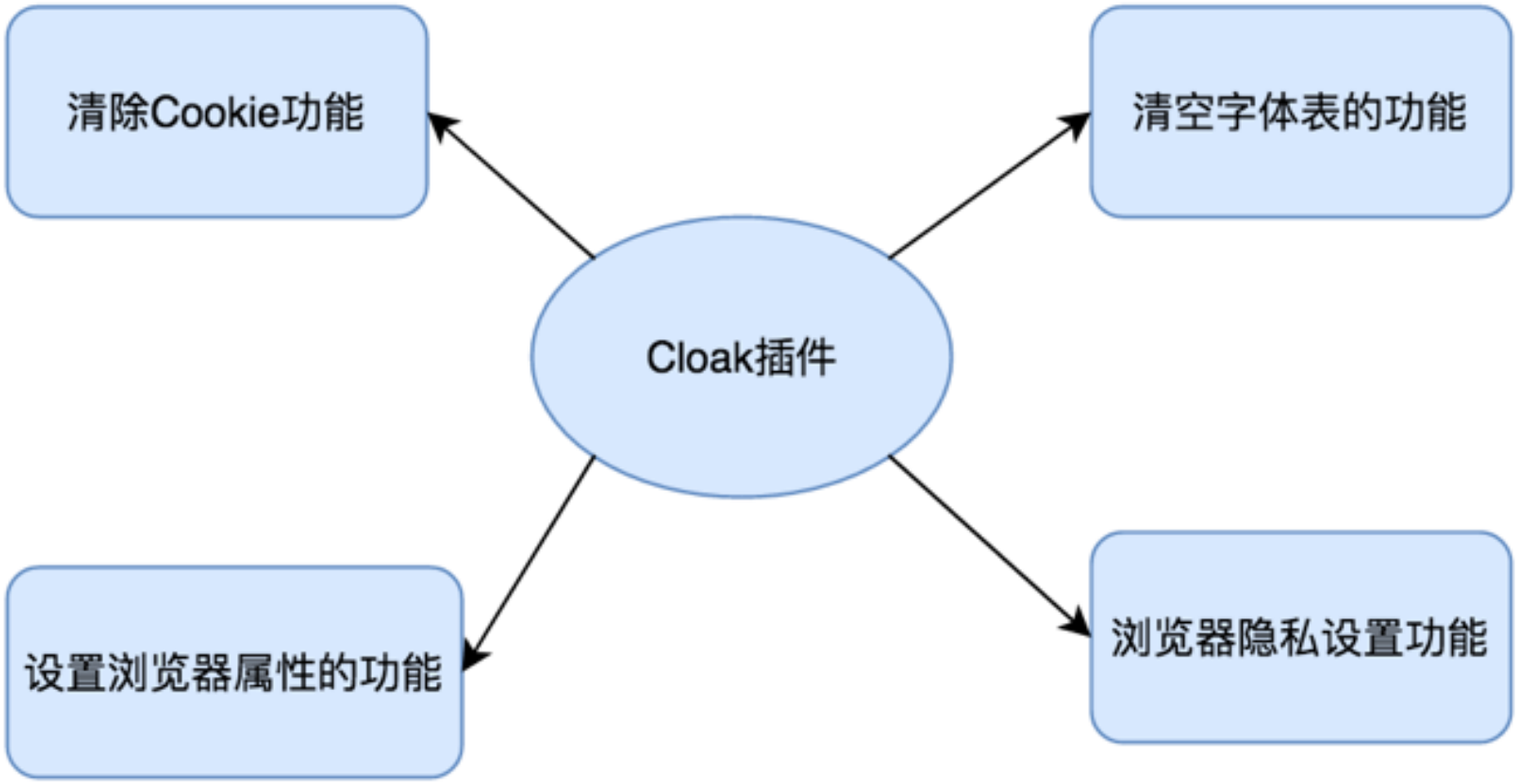
浏览器指纹提取防范

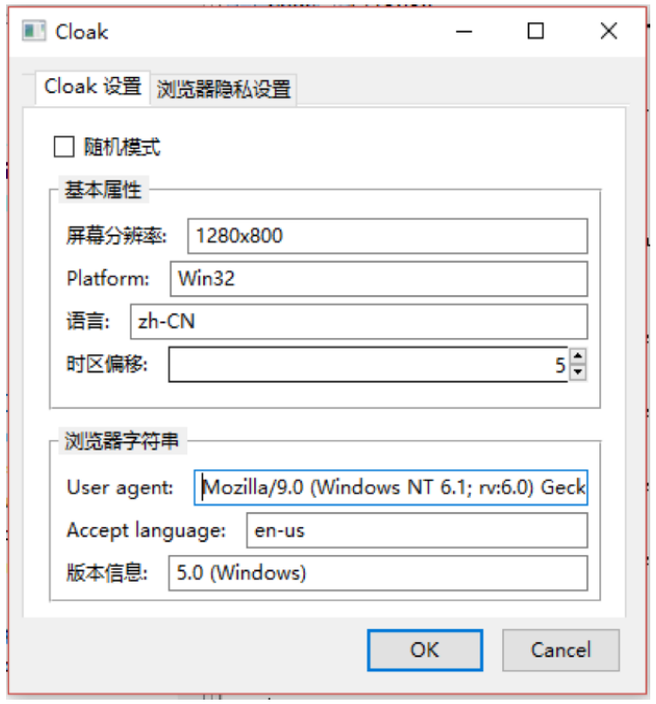
- **手动设置或随机生成某些浏览器属性的值，这样当第三方追踪软件想要提取我们浏览器属性的值时，获取到的就是经过修改或随机生成的值，从而生成无效的浏览器指纹。**

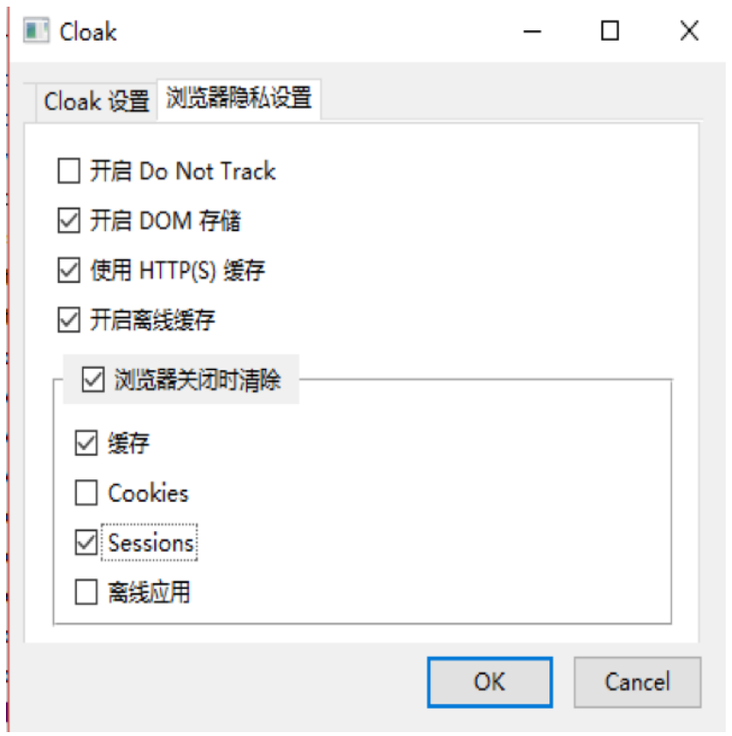


Browser Fingerprinting

浏览器指纹提取防范系统







Homework 课后作业

- 要求阅读如下论文：

➡ *Beauty and the Beast: Diverting Modern Web Browsers to Build Unique Browser Fingerprints. IEEE S&P 2016.*

下次上课测试！

谢谢！

孙惠平

sunhp@ss.pku.edu.cn