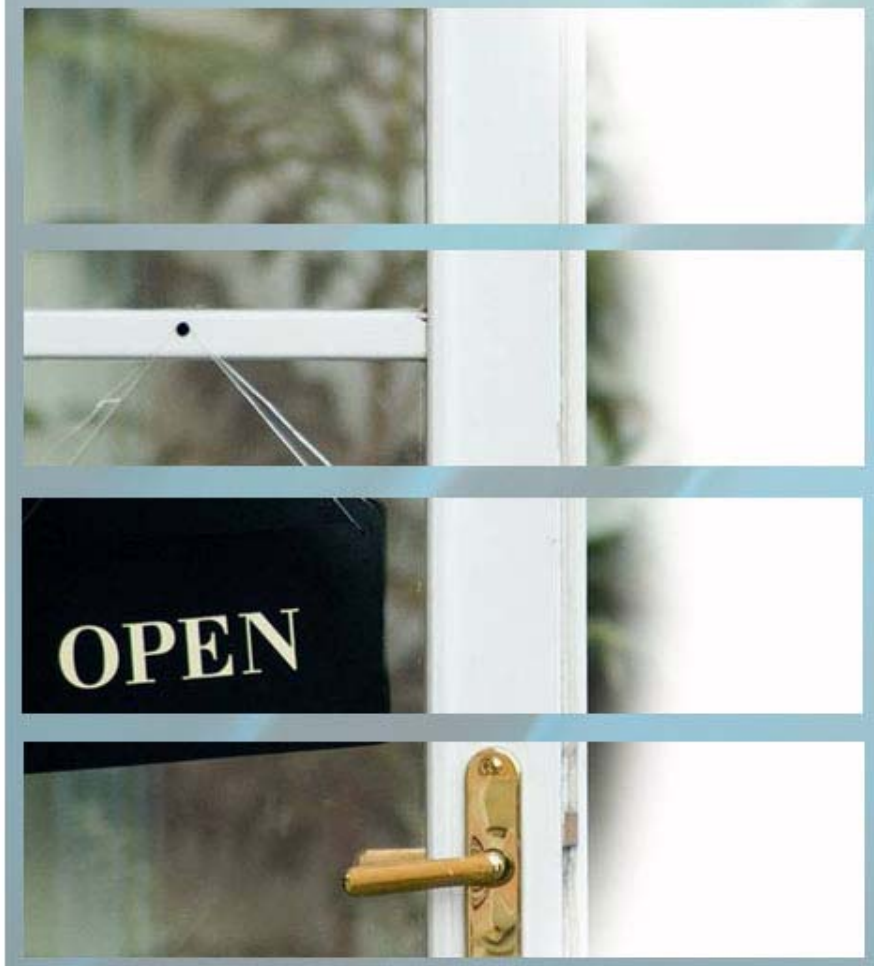
第14章

物联网中的信息安全与隐私保护

物联网导论

Introduction to Internet of Things



从**信息安全和隐私保护**的角度讲，物联网终端（RFID, 传感器，智能信息设备）的广泛引入在提供更丰富信息的同时也增加了暴露这些信息的危险。

本章将重点讨论RFID安全和位置隐私两大安全隐私问题。

内容提要

内容回顾

- 第13章介绍了物联网的智能决策——数据挖掘技术。
  - 数据挖掘的基本流程
  - 典型的数据挖掘算法
  - 物联网中数据挖掘技术的广泛应用

- 本章重点介绍物联网中RFID安全和位置隐私隐患以及典型的安全机制。

本章内容

14.1 概述
14.2 RFID安全和隐私
14.3 RFID安全和隐私保护机制
14.4 位置信息与个人隐私
14.5 保护位置隐私的手段

网络安全的一般性指标有哪些？



网络信息安全的一般性指标

可靠性： 三种测度标准（抗毁、生存、有效）

可用性： 用正常服务时间 和整体工作时间之比衡量

保密性： 常用的保密技术（防侦听、防辐射、加密、物理保密）

完整性： 未经授权不能改变信息；与保密性的区别：保密性要求信息不被泄露给未授权的人，完整性要求信息不受各种原因破坏。

不可抵赖性： 参与者不能抵赖已完成的操作和承诺的特性

可控性： 对信息传播和内容的控制特性

什么是隐私？

隐私权：个人信息的自我决定权，包含个人信息、身体、财产或者自我决定等。

物联网与隐私

- 不当使用会侵害隐私
- 恰当的技术可以保护隐私

本章内容

14.1 概述

14.2 **RFID安全和隐私**

14.3 RFID安全和隐私保护机制

14.4 位置信息与个人隐私

14.5 保护位置隐私的手段

RFID安全的现状如何？有哪些主要安全和隐私隐患？

RFID安全现状概述

RFID安全隐私标准规范和建议

•EPCglobal在超高频第一类第二代标签空中接口规范中说明了RFID标签需支持的功能组件，其安全性要求有：

✓物品级标签协议要求文档

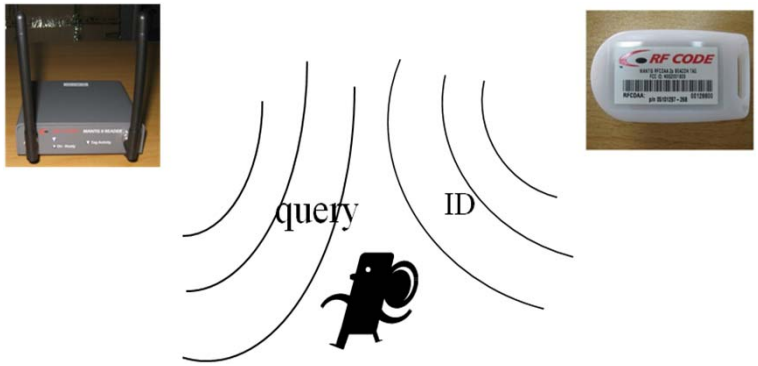
✓ISO/IEC：RFID数据安全准则

•欧盟：《RFID隐私和数据保护的若干建议》

主要安全隐患

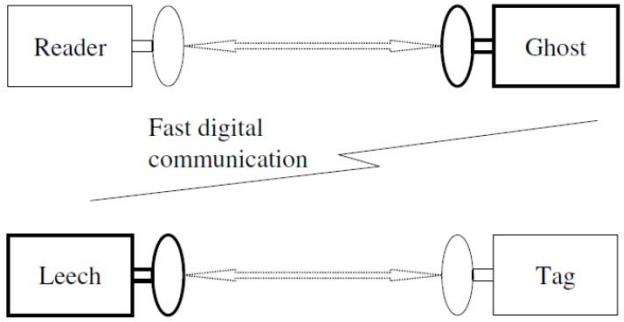
窃听(eavesdropping)

- 标签和阅读器之间通过无线射频通信
- 攻击者可以在设定通信距离外偷听信息



中间人攻击(man-in-the-middle attack, MITM)

- 对reader(tag)伪装成tag(reader)，传递、截取或修改通信消息
- “扒手”系统



主要安全隐患

欺骗、重放、克隆

- **欺骗(spoofing)**：基于已掌握的标签数据通过阅读器
- **重放(replaying)**：将标签的回复记录并回放
- **克隆(cloning)**：形成原来标签的一个副本

拒绝服务攻击(Denial-of-service attack, DoS)

- 通过不完整的交互请求消耗系统资源，如：
  - ✓产生标签冲突，影响正常读取
  - ✓发起认证消息，消耗系统计算资源
- 对标签的DoS
  - ✓消耗有限的标签内部状态，使之无法被正常识别

主要安全隐患

物理破解(corrupt)

- 标签容易获取
- 标签可能被破解：通过逆向工程等技术
- 破解之后可以发起进一步攻击
  - ✓推测此标签之前发送的消息内容
  - ✓推断其他标签的秘密

篡改信息(modification)

- 非授权的修改或擦除标签数据

Two RFID researchers created a video showing how an RFID reader attached to an improvised explosive device could theoretically identify a U.S. citizen walking past the reader and set off a bomb. They haven't yet tested the theory on a real U.S. passport since the documents have yet to be distributed. The still here shows an attack using a prototype passport with RFID chip placed in the pocket of the victim. As the chip passes the reader, the reader detonates an explosive device placed in the trash can. View Slideshow

主要安全隐患

RFID病毒(virus, malware)

- •标签中可以写入一定量的代码
- •读取tag时，代码被注入系统
  - ✓SQL注入

其他隐患

- •电子破坏
- •屏蔽干扰
- •拆除
- •...

主要隐私问题

隐私信息泄露

- 姓名、医疗记录等个人信息

跟踪

- 监控，掌握用户行为规律和消费喜好等。
- 进一步攻击

效率和隐私保护的矛盾

- 标签身份保密
- 快速验证标签需要知道标签身份，才能找到需要的信息
- **平衡：** 恰当、可用的安全和隐私

本章内容

14.1 概述
14.2 RFID安全和隐私
14.3 **RFID安全和隐私保护机制**
14.4 位置信息与个人隐私
14.5 保护位置隐私的手段

典型的隐私保护机制有哪些？

14.3 RFID安全和隐私保护机制

早期物理安全机制

- 灭活(kill)：杀死标签，使标签丧失功能，不能响应攻击者的扫描。
- 法拉第网罩：屏蔽电磁波，阻止标签被扫描。
- 主动干扰：用户主动广播无线信号阻止或破坏RFID阅读器的读取。
- 阻止标签(block tag)：通过特殊的标签碰撞算法阻止非授权阅读器读取那些阻止标签预定保护的标签。

物理安全机制通过牺牲标签的部分功能满足隐私保护的要求。

14.3 RFID安全和隐私保护机制

基于密码学的安全机制

哈希锁(hash-lock)

优点：初步访问控制
威胁：偷听，跟踪

14.3 RFID安全和隐私保护机制

基于密码学的安全机制

随机哈希锁(randomized hash-lock)

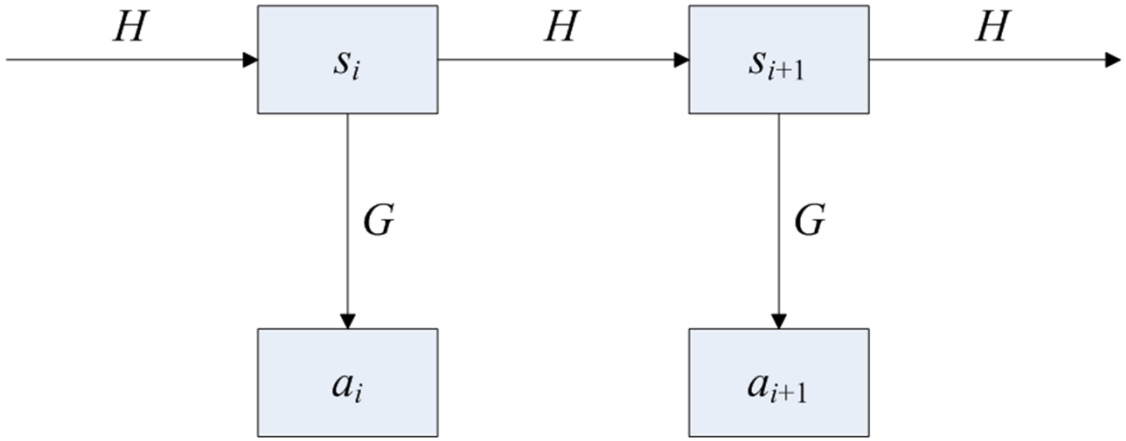
优点：增强的安全和隐私

线性复杂度key-search: $O(N)$

14.3 RFID安全和隐私保护机制

基于密码学的安全机制

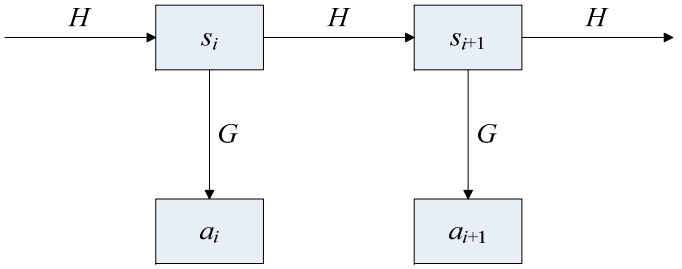
哈希链(hash chain)



优点：前向安全性
威胁：DoS

14.3 RFID安全和隐私保护机制

基于密码学的安全机制



同步方法(synchronization approach)

- 预计算并存储标签的可能回复，如：
- 在哈希链方法中，可以为每个标签存储m个可能的回复，标签响应时直接在数据库中查找

高效key-search: O(1)

威胁：回放，DoS

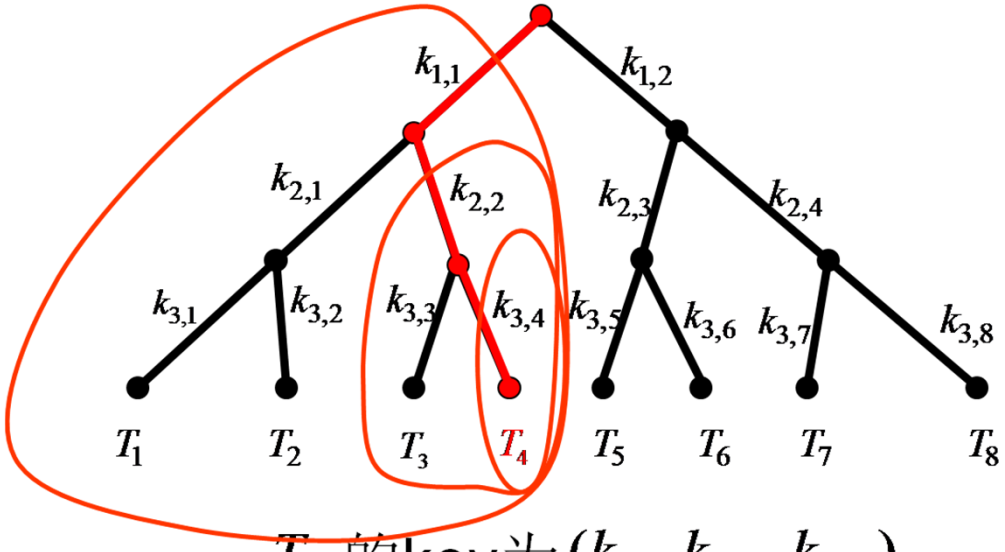
$$s_{i+k} = H^k(s_i), (0 \leqq k \leqq m\text{-}1)$$

$$a_{i+k} = G(H^k(s_i)), (0 \leqq k \leqq m\text{-}1)$$

14.3 RFID安全和隐私保护机制

基于密码学的安全机制

树形协议(tree-based protocol)



T_4 的key为 $(k_{1,1}, k_{2,2}, k_{3,4})$

14.3 RFID安全和隐私保护机制

基于密码学的安全机制

树形协议(tree-based protocol)（续）

对数复杂度key-search: O(logN)，受破解攻击威胁，攻击成功率：

K_0 \ δ	2	20	100	500	1000
1	66.6%	9.5%	1.9%	0.3%	0.1%
20	95.5%	83.9%	32.9%	7.6%	3.9%
50	98.2%	94.9%	63.0%	18.1%	9.5%
100	99.1%	95.4%	85.0%	32.9%	18.1%
200	99.5%	96.2%	97.3%	55.0%	32.9%

2^{20}个tag，δ:分枝数，K_0个tag被破解 (Avoine, SAC'05)

14.3 RFID安全和隐私保护机制

其他方法

- Physical unclonable function, (PUF)：利用制造过程中必然引入的随机性，用物理特性实现函数。具有容易计算，难以特征化的特点。
- 掩码：使用外加设备给阅读器和标签之间的通信加入额外保护。
- 通过网络编码(network coding)原理得到信息
- 可拆卸天线
- 带方向的标签

如何面对安全和隐私挑战？

•可用性与安全的统一

无需为所有信息提供安全和隐私保护，信息分级别管理。

•与其他技术结合

✓生物识别

✓近场通信(Near field communication, NFC)

•法律法规

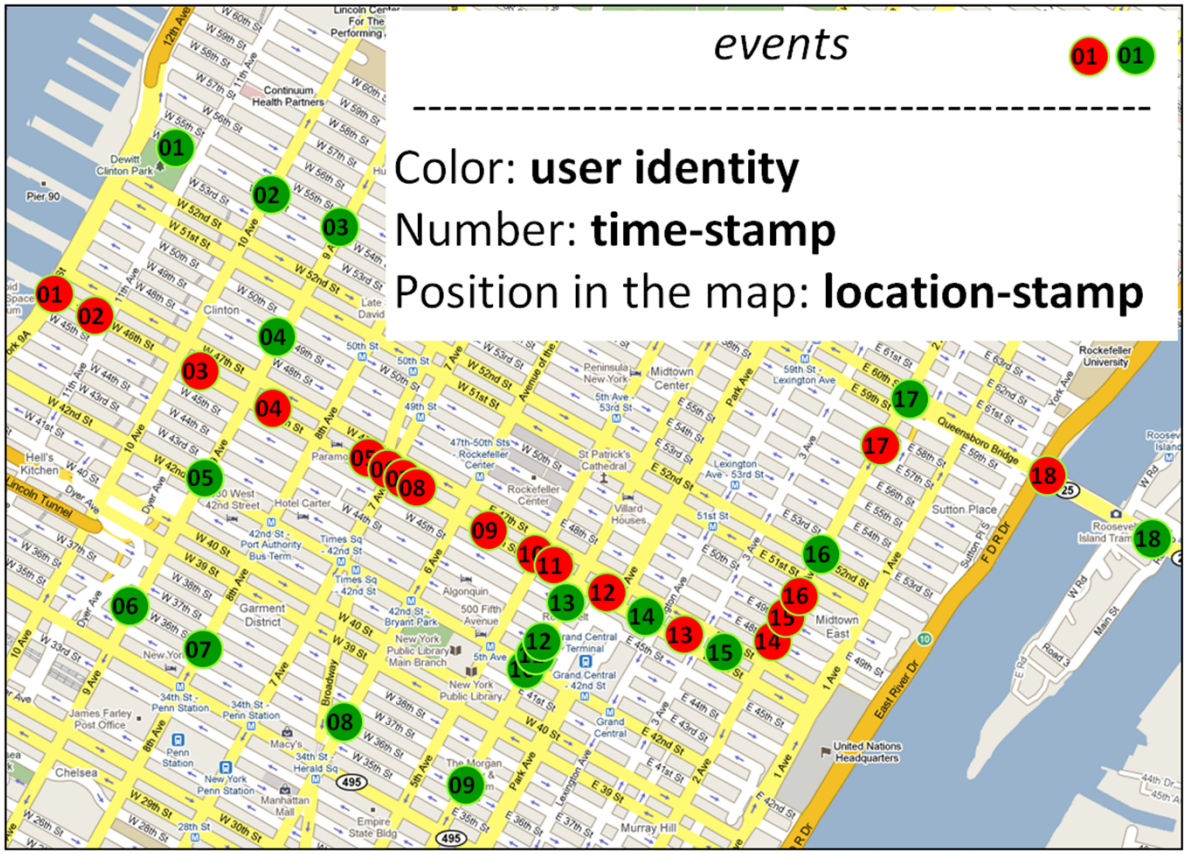
从法律法规角度增加通过RFID技术损害用户安全与隐私的代价，并为如何防范做出明确指导。

本章内容

14.1 概述
14.2 RFID安全和隐私
14.3 RFID安全和隐私保护机制
14.4 位置信息与个人隐私
14.5 保护位置隐私的手段

什么是位置隐私？

14.4 位置信息与个人隐私



位置信息与基于位置的服务（LBS）

14.4 位置信息与个人隐私

位置隐私的定义

- 用户对自己位置信息的掌控能力，包括：
  - ✓是否发布
  - ✓发布给谁
  - ✓详细程度

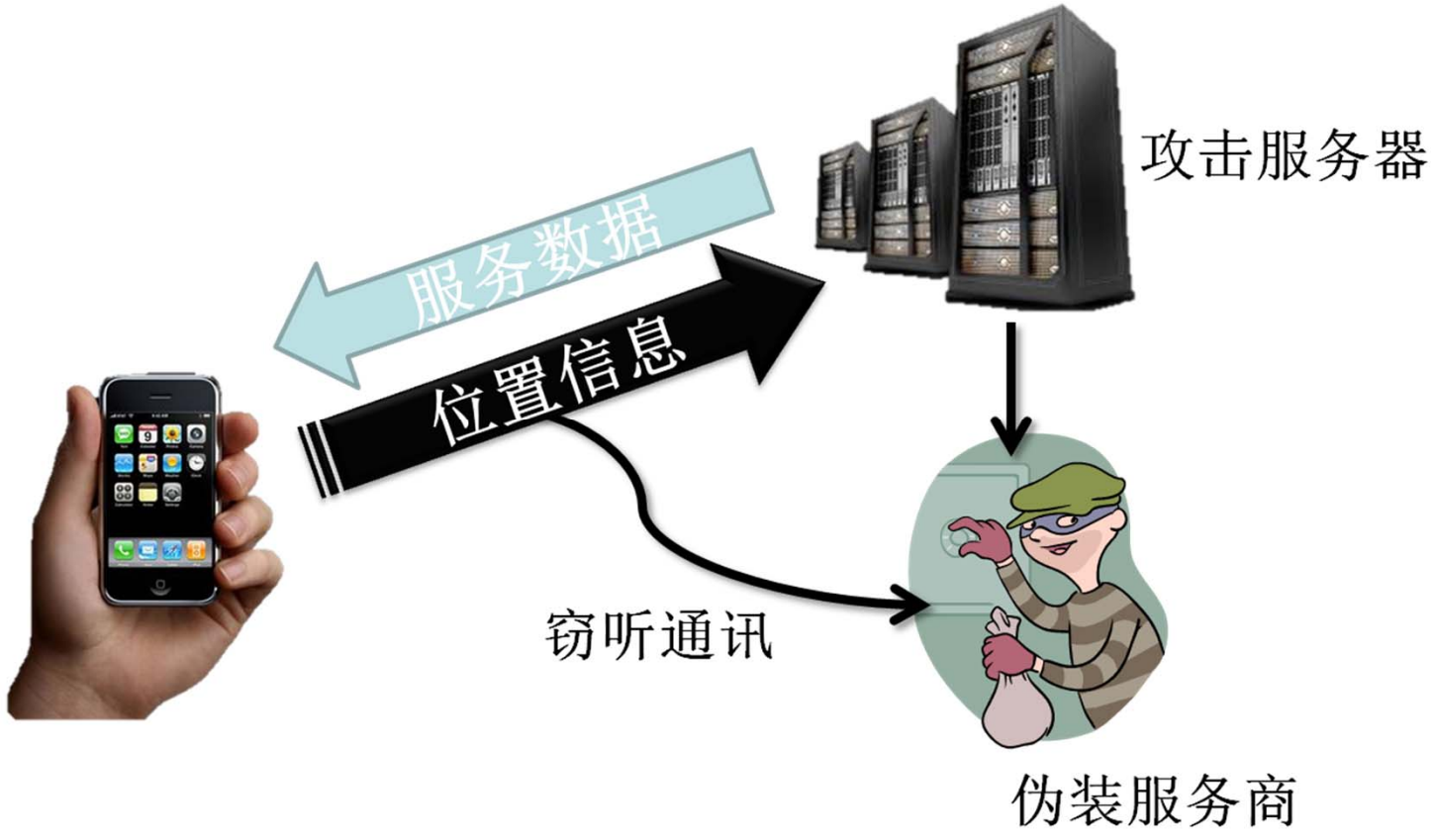
保护位置隐私的重要性

- 三要素：时间、地点、人物
- 人身安全
- 隐私泄露

位置隐私面临的威胁

- 通信
- 服务商
- 攻击者

14.4 位置信息与个人隐私



本章内容

14.1 概述
14.2 RFID安全和隐私
14.3 RFID安全和隐私保护机制
14.4 位置信息与个人隐私
14.5 保护位置隐私的手段

保护位置隐私的手段有哪些？

14.5 保护位置隐私的手段

制度约束

- 5条原则（知情权、选择权、参与权、采集者、强制性）
- 优点
  - ✓一切隐私保护的基础
  - ✓有强制力确保实施
- 缺点
  - ✓各国隐私法规不同，为服务跨区域运营造成不便
  - ✓一刀切，难以针对不同人不同的隐私需求进行定制
  - ✓只能在隐私被侵害后发挥作用
  - ✓立法耗时甚久，难以赶上最新的技术进展

14.5 保护位置隐私的手段

隐私方针： 定制的针对性隐私保护

- **分类**

  用户导向型，如PIDF（Presence Information Data Format）

  服务提供商导向型，如P3P（Privacy Preferences Project）

- **优点**

  可定制性好，用户可根据自身需要设置不同的隐私级别

- **缺点**

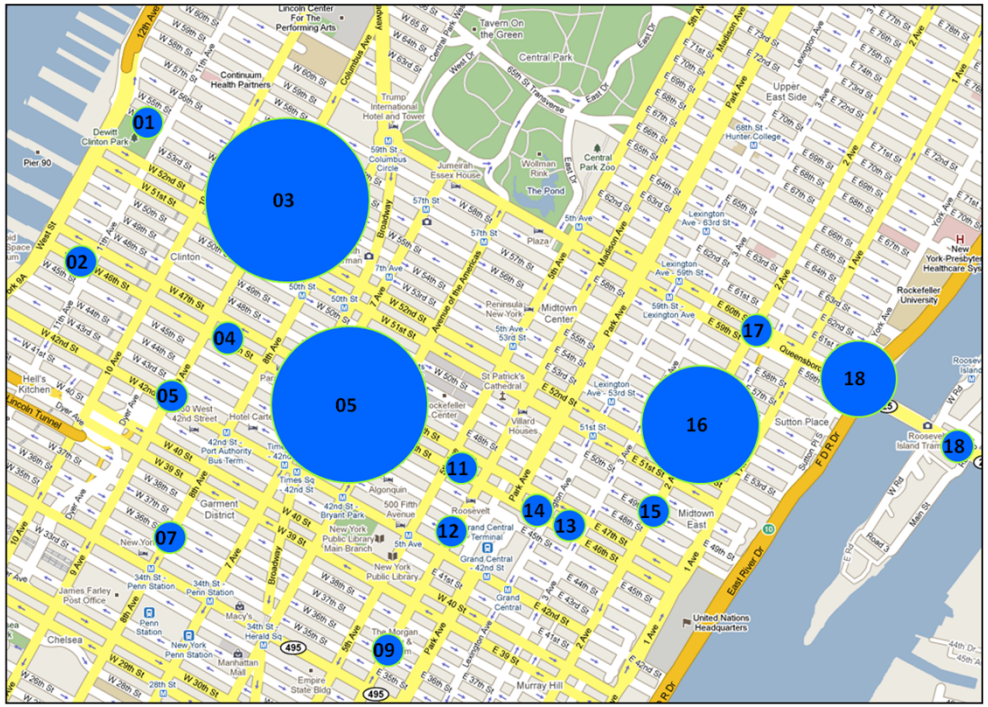
  缺乏强制力保障实施

  对采用隐私方针机制的服务商有效，对不采用该机制的服务商无效

14.5 保护位置隐私的手段

身份匿名：

- 认为“一切服务商皆可疑”
- 隐藏位置信息中的“身份”
- 服务商能利用位置信息提供服务，但无法根据位置信息推断用户身份
- 常用技术：K匿名



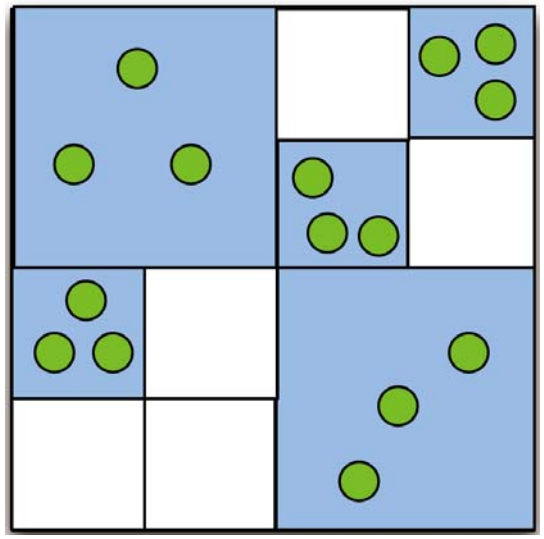
14.5 保护位置隐私的手段

身份匿名（续）

- 优点
  - ✓不需要强制力保障实施
  - ✓对任何服务商均可使用
  - ✓在隐私被侵害前保护用户隐私
- 缺点
  - ✓牺牲服务质量
  - ✓通常需要借助“中间层”保障隐私
  - ✓无法应用于需要身份信息的服务

K匿名

- **基本思想：** 让K个用户的位置信息不可分辨
- **两种方式**
  - ✓空间上：扩大位置信息的覆盖范围
  - ✓时间上：延迟位置信息的发布
- **例：3-匿名**
  - ✓绿点：用户精确位置
  - ✓蓝色方块：向服务商汇报的位置信息

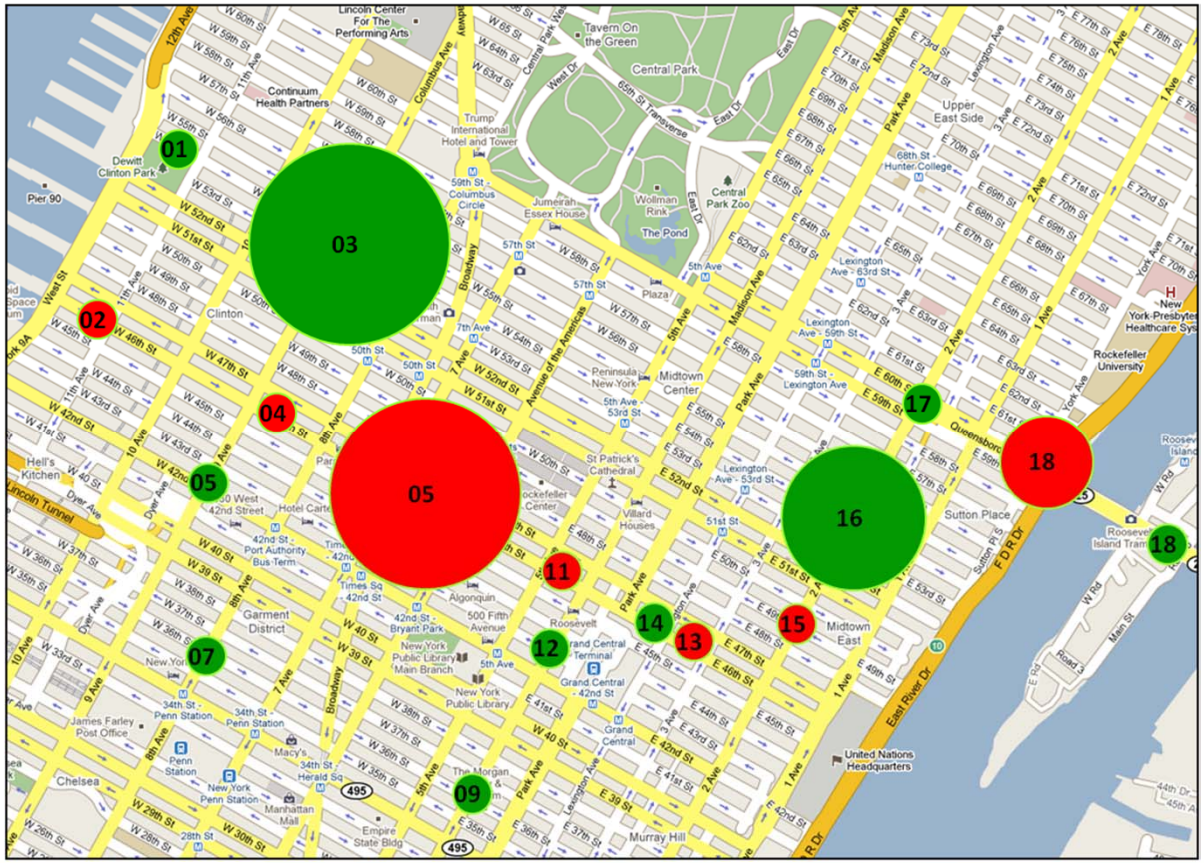


14.5 保护位置隐私的手段

数据混淆：保留身份，混淆位置信息中的其他部分，让攻击者无法得知用户的确切位置

- 三种方法
  - ✓模糊范围：精确位置->区域
  - ✓声东击西：偏离精确位置
  - ✓含糊其辞：引入语义词汇，例如“附近”
- 优点
  - ✓服务质量损失相对较小
  - ✓不需中间层，可定制性好
  - ✓支持需要身份信息的服务
- 缺点
  - ✓运行效率低
  - ✓支持的服务有限

数据混淆：模糊范围





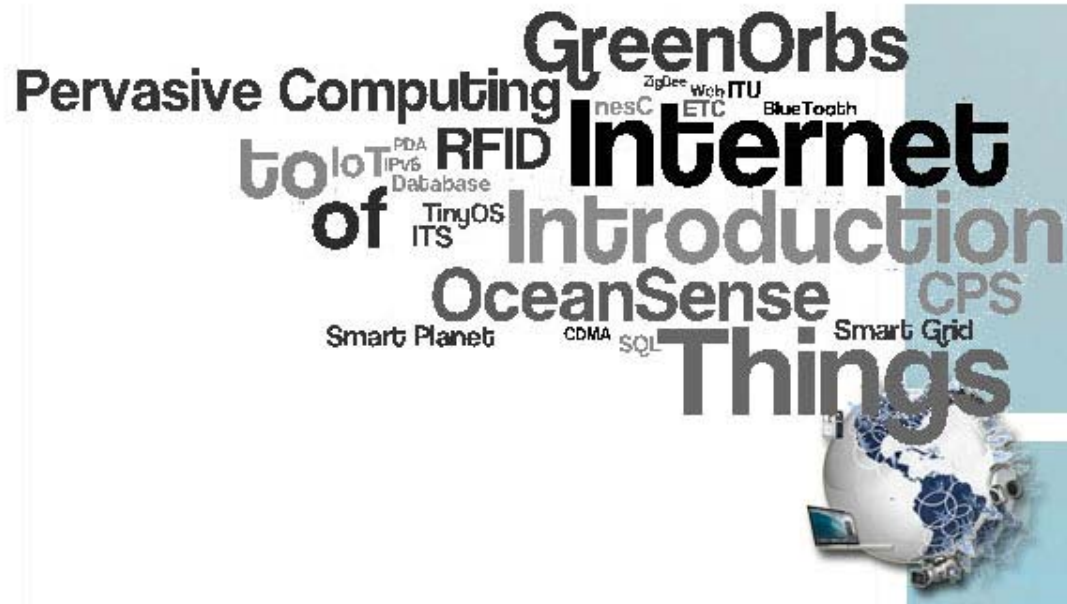
本章小结

内容回顾

本章介绍了RFID安全和典型的安全机制，以及位置隐私隐患和相应的保护手段。

重点掌握

- 了解网络信息安全的一般性指标。
- 掌握主要的RFID安全隐患。
- 了解RFID安全保护机制，重点掌握基于密码学的安全机制。
- 理解位置信息的定义，举例说明保护位置信息的手段。



Thank you!

Internet of Things