



张策

第10章-物联网中的信息安全与隐私保护

嵌入式系统研发中心
山东省嵌入式系统工程技术研发中心

本章内容

第一节 概述

第二节 物联网各层安全分析

第三节 RFID安全和隐私

第四节 RFID安全和隐私保护机制

第五节 位置信息与个人隐私

第六节 保护位置隐私的手段

第10章 物联网中的信息安全与隐私保护--10.1概述

一、概述

0. 物联网安全的特点

- ✗ 物联网应用和发展很快会融入我们社会和生活的方方面面。
- ✗ 据权威估计，到2020年全世界的智能物体（Smart things）有近500亿连接到网络中去，物联网通过感知与控制，将物联网融入到我们的生活、生产和社会中去，物联网的安全问题不容忽视。
- ✗ 如果忽视物联网的安全问题，我们的隐私会由于物联网的安全性薄弱而暴露无遗，从而严重影响我们的正常生活。
- ✗ 在发展物联网的同时，必须对物联网的安全隐私问题更加重视，保证物联网的健康发展。

① 与互联网不同，物联网的特点在于无处不在的数据感知、以无线为主的信息传输、智能化的信息处理。

① 从物联网的整个信息处理过程来看，感知信息经过采集、汇聚、融合、传输、决策与控制等过程，体现了与传统的网络安全不同的特点。

- 物联网的安全特征体现了：①感知信息的多样性、②网络环境的异构性、③应用需求的复杂性。
- 呈现出：①网络的规模和数据的处理量大、②决策控制复杂等特点，对物联网安全提出了新的挑战。
- 物联网除了面对：①传统TCP/IP网络、②无线网络和移动通信网络等传统网络安全问题之外，③还存在着大量自身的特殊安全问题。

第10章 物联网中的信息安全与隐私保护--10.1概述

一、概述

0. 物联网安全的特点

✎ 具体地讲，物联网的安全主要有如下特点：

① 物联网的设备、节点等无人看管，容易受到操纵和破坏

- ① 物联网的许多应用代替人完成一些复杂、危险和机械的工作，物联网中设备、节点的工作环境大都是无人监控。
- ① 因此攻击者很容易接触到这些设备，从而对设备或其嵌入其中的传感器节点进行破坏。
- ① 攻击者甚至可以通过更换设备的软硬件，对它们进行非法操控。例如，在远程输电过程中，电力企业可以使用物联网来远程操控一些变电设备。
- ① 由于缺乏看管，攻击者可轻易地使用非法装置来干扰这些设备上的传感器。如果变电设备的某些重要参数被篡改，其后果将会极其严重。

② 信息传输主要靠无线通信方式，信号容易被窃取和干扰

- ① 物联网在信息传输中多使用无线传输方式，暴露在外的无线信号很容易成为攻击者窃取和干扰的对象，对物联网的信息安全产生严重的影响。
- ① 例如攻击者可以通过窃取感知节点发射的信号，来获取所需要的信息，甚至是用户的机密信息并可据此来伪造身份认证，其后果不堪设想。
- ① 攻击者也可以在物联网无线信号覆盖的区域内，通过发射无线电信号来进行干扰，从而使无线通信网络不能正常工作，甚至瘫痪。比如在物流运输过程中，嵌入在物品中的标签或读写设备的信号受到恶意干扰，很容易造成一些物品的丢失

第10章 物联网中的信息安全与隐私保护--10.1概述

一、概述

0. 物联网安全的特点

✎ 具体地讲，物联网的安全主要有如下特点：

③ 出于低成本的考虑，传感器节点通常是资源受限的

① 物联网的许多应用通过部署大量的廉价传感器覆盖特定区域。

① 廉价的传感器一般体积较小，使用能量有限的电池供电，其能量、处理能力、存储空间、传输距离、无线电频率和带宽都受到限制，因此传感器节点无法使用较复杂的安全协议，因而这些传感器节点或设备也就无法拥有较强的安全保护能力。

① 攻击者针对传感器节点的这一弱点，可以通过采用连续通信的方式使节点的资源耗尽。

④ 物联网中物品的信息能够被自动地获取和传送

① 物联网通过对物品的感知实现物物相连，比如通过RFID(射频识别)、传感器、二维识别码和GPS定位等技术能够随时随地且自动地获取物品的信息。

① 同样这种信息也能被攻击者获取，在物品的使用者没有察觉的情况下，物品的使用者将会不受控制地被扫描、定位及追踪，对个人的隐私构成了极大威胁。

第10章 物联网中的信息安全与隐私保护--10.1概述

一、概述

1. 物联网的安全要求及安全建设

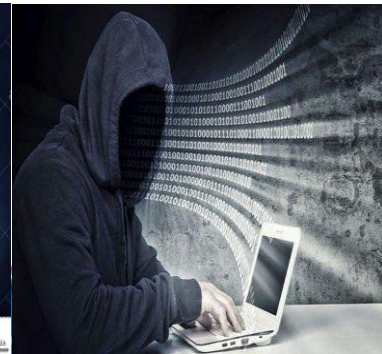
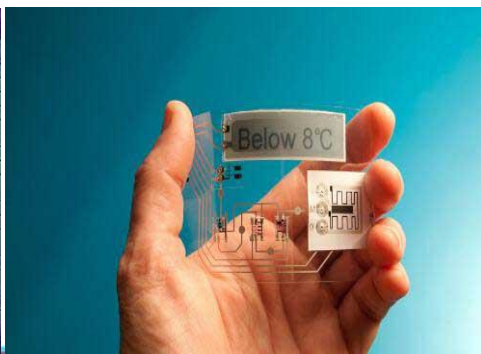
✎ 物联网安全的总体要求：

①物理安全、②信息采集的安全、③信息传输的安全和④信息处理的安全
而最终目标就是要确保信息的**机密性**、**完整性**、**真实性**和**网络的容错性**。

✎ 物联网的安全性要求：

- ①物联网中的设备自己必须是安全可靠的，不仅要可靠地完成设计规定的功能，更不能发生故障危害到人员或者其他设备的安全；
- ②另一方面，它们必须有能力防护自己，在遭受黑客攻击和外力破坏的时候仍然能够正常工作。

✎ 物联网的信息安全建设是一个**复杂的系统工程**，需要从**政策引导**、**标准制定**、**技术研发**等等多方面向前推进，提出坚实的信息安全保障手段，保障物联网的健康、快速的发展。



第10章 物联网中的信息安全与隐私保护--10.1概述

一、概述

2. 物联网各层的安全问题

综合而言，物联网从安全上讲涉及到：①信息安全感知、②可靠感知数据传输和③安全信息操控。从层面上讲，如图所示，涉及到①感知层、②网络层、③信息处理层和④应用层四个层面。

应用层	智能交通、环境监测、内容服务等	网络 管理 与 安全
支持层	数据挖掘、智能计算、并行计算、云计算等	
传输层	WIMAX、GSM、3G通信网、卫星网、互联网等	
感知层	RFID、二维码、传感器、红外感应等	

第10章 物联网中的信息安全与隐私保护--10.1概述

一、概述

2. 物联网各层的安全问题

✎ 对于物联网的安全，可以参照互联网所设计的安全防范体系，在**传感层、网络传输层和应用层**分别设计相应的**安全防范体系**，如下图所示。

应用环境安全技术
可信终端、身份验证、访问控制、安全审计等

网络环境安全技术
无线网安全、虚拟专用网、传输安全、安全路由、防火墙、安全域策略、安全审计等

信息安全防御关键技术
攻击监测、内容分析、病毒防治、访问控制、应急响应、战略预警等

信息安全基础核心技术
密码技术、高速密码芯片、PKI公钥基础设施、信息系统平台安全等

二、安全分析

1. 感知层的安全问题

- ✎ 感知层处于物联网的最底层，是物联网的原始数据来源地，也是许多物联网应用层控制硬件实现端。
- ✎ 物联网感知层要实现感知和控制的功能，一旦感知层的节点受到攻击，不仅可以破坏数据的正确来源，还会造成控制的失败，从而破坏物联网的正常工作。

(1) 感知层的基本情况

- ① 物联网在感知层采集数据时，其信息传输方式主要采用无线网络传输，对这种暴露在公共场所中的信号如果缺乏有效保护措施的话，很容易被非法监听、窃取、干扰；
- ① 物联网中的物品设备大多都是部署在无人监控的地点完成任务的，那么攻击者就会比较容易地接触到这些设备，从而可以对这些设备或其承载的传感器进行破坏，甚至通过破译传感器通信协议，对它们进行非法操控。
- ① 感知节点的另外一个问题是功能单一、能量有限、数据传输和消息也没有特定的标准，为提供统一的安全保护体系带来障碍。
- ① 在感知层，一般感知信息要通过一个或多个与外界网连接的网关节点（Sink或Gateway）作为感知层和通信层的联系渠道，但一旦网关节点被破坏，感知层的信息将无法传递到网络层。

二、安全分析

1. 感知层的安全问题

(2) 感知层的信息安全问题

- ① 传感网的普通节点被敌手捕获，为入侵者对物联网发起攻击提供了可能性；
- ② 传感网的网关节点（Sink或 Gateway）被敌手控制，安全性全部丢失；
- ③ 尽管现有的互联网具备相对完整的安全保护能力，但由于物联网中存在的数量庞大的节点，将会导致大量的数据同时发送，使得传感网的节点（普通节点或网关节点）受到来自于网络的拒绝服务（DOS）攻击；
- ④ 接入到物联网的超大量传感节点的标识、识别、认证和控制问题。

二、安全分析

1. 感知层的安全问题

(3) 物联网感知层的信息安全防护

① 加强对传感网机密性的安全控制

- 在传感网内部，需要有效的**密钥管理机制**，用于保障传感网内部通信的安全，**机密性**需要在通信时建立一个**临时会话密钥**，确保数据安全。例如在物联网构建中选择射频识别系统(RFID)，应该根据实际需求考虑是否选择有**密码和认证功能**的系统。

② 加强节点认证

- 个别传感网（特别当传感数据共享时）需要**节点认证**，确保非法节点不能接入。**认证性**可以通过**对称密码或非对称密码**方案解决。使用对称密码的认证方案需要预置节点间的共享密钥，在效率上比较高，消耗网络节点的资源较少，许多传感网都选用此方案；而使用非对称密码技术的传感网一般具有较好的计算和通信能力，并且对安全性要求更高。**在认证的基础上完成密钥协商**是建立会话密钥的必要步骤。

③ 加强入侵监测

- 一些重要传感网需要**对可能被敌手控制的节点行为进行评估**，以降低敌手入侵后的危害。敏感场合，节点要设置**封锁或自毁程序**，发现节点离开特定应用和场所，启动封锁或自毁，使攻击者无法完成对节点的分析。

④ 加强对传感网的安全路由控制

- 几乎所有传感网内部都需要不同的安全路由技术。传感网的安全需求所涉及的密码技术包括**轻量级密码算法**、**轻量级密码协议**、**可设定安全等级的密码技术**等。

二、安全分析

2. 网络传输层的安全问题

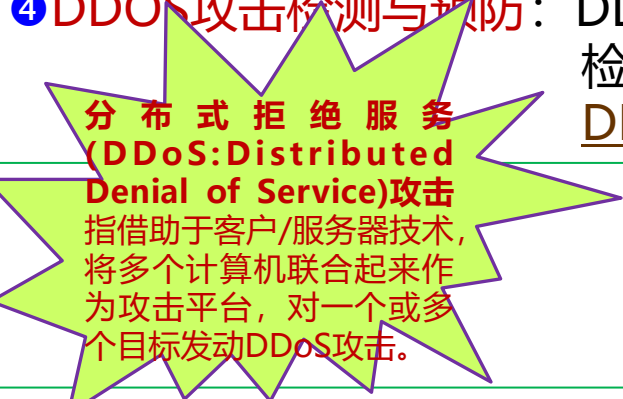
(1) 网络传输层的基本情况

- ① 处于网络末端的节点的传输如感知层的问题一样，节点功能简单，能量有限，使得它们无法拥有复杂的安全保护能力，对网络传输层的安全保障带来困难。
- ② 物联网的传输层主要用于把感知层收集到的信息安全可靠地传输到信息处理层，然后根据不同的应用需求进行信息处理，而网络层是一个高度异构的网络。
- ③ 物联网传输层的异构网络信息交换的安全性是其中的脆弱点，特别在网络认证方面，难免存在“中间人攻击”和其他类型的攻击。这需要有更高的安全防护措施。
- ④ 对于核心承载网络而言，虽然它具有相对完整的安全保护能力，但由于物联网中节点数量庞大，且常以集群方式存在。对于事件驱动的应用，大量数据的同时发送可以致使网络拥塞，产生拒绝服务攻击。
- ⑤ 在传输层会带来更加复杂的网络安全问题。大量节点的数据传输需求会导致网络拥塞，产生拒绝服务攻击。此外，现有通信网络的安全架构都是以人通信的角度设计的，对以物为主体的物联网需要建立新的传输与应用安全架构。

二、安全分析

2. 网络传输层的安全问题

(2) 对于传输层的安全要求

- ① **数据机密性**：要保证数据在传输过程中不泄露内容；
- ② **数据完整性**：要保证数据在传输过程中不被非法篡改，并且被篡改的数据容易被检测出；
- ③ **数据流机密性**：对数据流量进行保密，防止数据流量信息被非法窃取
- ④ **DDOS攻击检测与预防**：DDOS是网络中常见的攻击现象，在物联网中要能及时检测到DDOS攻击的发生，并能对脆弱节点如网关的DDOS攻击进行防护


分布式拒绝服务 (DDoS: Distributed Denial of Service) 攻击
指借助于客户/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。
- ⑤ **移动网络中认证与密钥协商 (AKA: Authentication and Key Agreement) 机制**的一致性或兼容性、跨越认证和跨网认证等，比如不同无线网络所使用的不同**AKA**机制对跨网认证不利。

二、安全分析

2. 网络传输层的安全问题

(3) 传输层的信息安全问题

✎ 传输层的信息安全问题主要有以下几个方面：

- ① DOS攻击(Denial of Service的简称，即**拒绝服务**)、DDOS攻击
- ② 假冒攻击、“中间人”攻击(**Man-in-the-Middle Attack, MITM**)等
- ③ 跨异构网络的网络攻击

二、安全分析

2. 网络传输层的安全问题

(4) 物联网传输层的信息安全防护

✎ 传输层的安全机制分为：端到端的机密性和节点到节点的机密性。

① 端到端的机密性的安全机制可以保证数据完整性，主要安全机制包括：端到端的认证机制；端到端的密钥协商机制；端到端的密钥管理机制；端到端的机密性算法选取机制等。

① 对于节点到节点的安全性机制主要包括节点的认证和密钥协商机制。

✎ 对于跨网络的安全形式需要建立不同网络环境的认证衔接机制。

✎ 网络传输可以根据需要分为单播通信、组播通信和广播通信，针对不同类型的通信模式要有相应的认证机制和机密性保护机制。

二、安全分析

2. 网络传输层的安全问题

(5) 传输层的安全架构

综合以上情况，传输层的安全架构主要包括一些几个方面：

- ① 节点认证、数据机密性、完整性、数据流机密性、DDOS攻击的检测与预防
- ② 移动网中AKA(认证与密钥协商, AKA: Authentication and Key Agreement)机制的一致性或兼容性、跨域认证和跨网认证
- ③ 密钥管理、端到端加密和节点到节点加密、密码算法和协议等
- ④ 组播和广播通信的认证性、机密性和完整性机制等。

二、安全分析

3. 网络处理层的安全问题

(1) 处理层的基本情况

✎ 物联网的处理层是**信息技术与行业应用**紧密结合的产物，涉及到**业务管理、中间件、云计算、分布式系统、海量信息处理**等部分。

① 上述这些支撑平台要为上层服务管理和大规模行业应用建立起一个高效、可靠和可信的系统，而**大规模、多平台、多业务类型使物联网业务层次的安全面临新的挑战**，比如针对不同的行业应用建立相应的安全策略，还是建立一个相对独立的安全架构。

② 考虑到物联网涉及多领域多行业，**海量数据信息处理和业务控制策略将在安全性和可靠性方面面临巨大挑战**，特别是**业务控制、管理和认证机制、中间件以及隐私保护**等安全问题显得尤为突出。

二、安全分析

3. 网络处理层的安全问题

(2) 处理层的安全挑战

✎ 物联网的处理层的安全挑战包括如下几个方面：

挑战

- ① 来自于超大量终端的海量数据的识别和处理
- ② 智能变为低能
- ③ 自动变为失控（可控性是信息安全的重要指标之一）
- ④ 灾难控制和恢复
- ⑤ 非法人为干预（内部攻击）
- ⑥ 设备（特别是移动设备）的丢失

二、安全分析

3. 网络处理层的安全问题

(3) 处理层的安全机制

✎ 物联网智能处理层的基本安全需求，需要如下的安全机制：

攻克

- ① 可靠的认证机制和密钥管理方案
- ② 高强度数据机密性和完整性服务
- ③ 可靠的密钥管理机制，包括PKI(Public Key Infrastructure, 公钥基础设施)和对称密钥的有机结合机制
- ④ 可靠的高智能处理手段
- ⑤ 入侵检测和病毒检测
- ⑥ 恶意指令分析和预防，访问控制及灾难恢复机制
- ⑦ 保密日志跟踪和行为分析，恶意行为模型的建立
- ⑧ 密文查询、秘密数据挖掘、安全多方计算、安全云计算技术等
- ⑨ 移动设备文件（包括秘密文件）的可备份和恢复
- ⑩ 移动设备识别、定位和追踪机制

二、安全分析

4. 应用层的安全问题

(1) 应用层的基本情况

- ✎ 物联网应用层是**综合的或有个体特性的具体应用业务**，它所涉及的某些安全问题通过前面几个逻辑层的安全解决方案可能仍然无法解决。
- ✎ 在这些问题中，**隐私保护**就是典型的一种。无论感知层、传输层还是处理层，都不涉及隐私保护的问题，但它却是一些特殊应用场景的实际需求，即**应用层的特殊安全需求**。
- ✎ 物联网的数据共享有多种情况，涉及到不同权限的数据访问。此外，在应用层还将涉及到**知识产权保护、计算机取证、计算机数据销毁**等安全需求和相应技术。

二、安全分析

4. 应用层的安全问题

(2) 需要隐私保护的应用

✎ 一般认为需要隐私保护的应用至少包括以下几种：

- ① 移动用户既需要知道（或被合法知道）其**位置信息**，又不愿意非法用户获取该信息
- ② 用户既需要证明自己合法使用**某种业务**，又不想让别人知道自己在使用某种业务，如在线游戏
- ③ 病人急救时需要及时获得该病人的**电子病历信息**，但又要保护该病历信息不被非法获取，包括病历数据管理员。事实上，电子病历数据库的管理人员可能有机会获得电子病历的内容，但**隐私保护采用某种管理和技术手段使病历内容与病人身份信息在电子病历数据库内无关联**
- ④ 许多业务需要**匿名性**，很多情况下，**用户信息**是认证过程的必须信息，如何对这些信息提供隐私保护，是一个具有挑战性的问题，但又是必须要解决的问题

二、安全分析

4. 应用层的安全问题

(3) 应用层的安全挑战和安全需求

✎ 应用层的安全挑战和安全需求主要有以下几个方面：

挑战

- ① 如何根据不同访问权限对同一数据库内容进行**筛选**
- ② 如何提供用户**隐私信息保护**，同时又能**正确认证**
- ③ 如何解决**信息泄露追踪**问题
- ④ 如何进行**计算机取证**
- ⑤ 如何**销毁**计算机数据
- ⑥ 如何保护电子产品和软件的**知识产权**

二、安全分析

4. 应用层的安全问题

(4) 应用层需要的安全机制

挑战

✎ 基于物联网综合应用层的安全挑战和安全需求，需要如下的安全机制：

① 有效的数据库访问控制和内容筛选机制

② 不同场景的隐私信息保护技术

③ 叛逆追踪和其他信息泄露追踪机制

④ 有效的计算机取证技术

⑤ 安全的计算机数据销毁技术

⑥ 安全的电子产品和软件的知识产权保护技术

✎ “**同态加密**”是指2009年9月，IBM公司的**克雷格·金特里**（Craig Gentry）发表了一篇文章，公布了一项关于密码学的全新发现：一项真正的突破。他发现，对经过同态加密的数据进行处理得到一个输出，将这一输出进行解密，其结果与用同一方法处理未加密的原始数据得到的输出结果是一样的。

✎ 即在明文上的某种运算对应于密文上的某种运算。

✎ 针对这些**安全架构**，需要发展相关的**密码技术**，包括访问控制、匿名签名、匿名认证、密文验证（包括**同态加密**）、门限密码、叛逆追踪、数字水印和指纹技术等。

三、信息安全和隐私保护

✍ 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。

1. 网络信息安全的一般性指标

- ①**可靠性**：三种测度标准（抗毁、生存、有效）
- ②**可用性**：用正常服务时间和整体工作时间之比衡量
- ③**保密性**：常用的保密技术（防侦听、防辐射、加密、物理保密）
- ④**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。
- ⑤**不可抵赖性**：参与者不能抵赖已完成的操作和承诺的特性
- ⑥**可控性**：对信息传播和内容的控制特性

三、信息安全和隐私保护

✎ 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。

2. 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**

❶ 不当使用会侵害隐私

❶ 恰当的技术可以保护隐私



台湾高校学生抵制多功能学生卡

- 持卡輕觸感應區即可通行。
- 可用金額即將用畢前，請再加值繼續使用。
- 請勿折損或接近高溫。
- 服務電話：0800-02-8880
- 本證於每學期註冊時蓋章方為有效。

台北智慧卡票證公司
Taipei Smart Card Corporation

學年/班級	/	/	/	/
上學期				
下學期				

RFID世界网

悠遊卡 EASYCARD | 學生卡 | www.rfidworld.com.cn
104 091868 1

一、RFID安全现状概述

1. RFID安全隐私标准规范和建议

✎ EPCglobal(EPCglobal是国际物品编码协会EAN和美国统一代码委员会(UCC)一个合资公司) 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：

- ① 物品级标签协议要求文档
- ① ISO/IEC: RFID数据安全准则



✎ 欧盟：《RFID隐私和数据保护的若干建议》

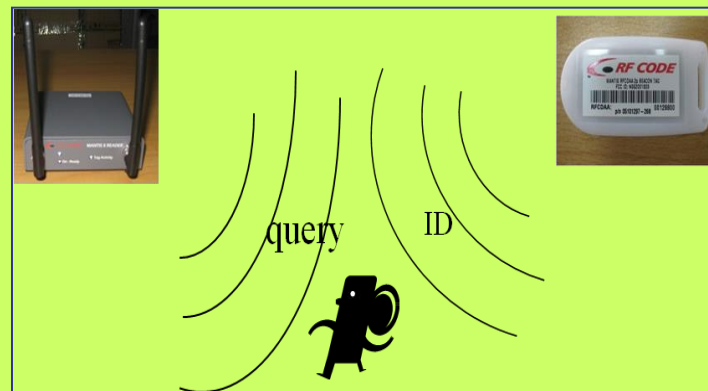


第10章 物联网中的信息安全与隐私保护--10.3 RFID安全和隐私

二、主要安全隐患

1. 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



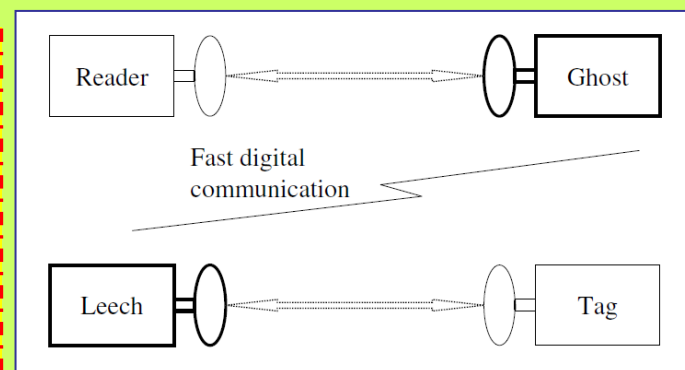
2. 中间人攻击(man-in-the-middle attack, MITM)

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

① 一种“间接”的入侵攻击，通过各种技术手段将受入侵者控制的一台计算机虚拟放置在网络连接中的两台通信计算机之间，这台计算机就称为“中间人”。

② 即通过拦截正常的网络通信数据，并进行数据篡改和嗅探（窃取），而通信的双方却毫不知情。

③ 曾经猖獗一时的SMB会话劫持、DNS欺骗等技术都是典型的MITM攻击手段。MITM攻击成为对网银、网游、网上交易等最有威胁并且最具破坏性的一种攻击方式。



第10章 物联网中的信息安全与隐私保护--10.3 RFID安全和隐私

二、主要安全隐患

3. 欺骗、重放、克隆

- ✎ **欺骗(spoofing)**: 攻击者用已掌握的标签数据发给阅读器, 进而**欺骗阅读器**
- ✎ **重放(replaying)**: 将标签的回复记录下来, 然后在阅读器询问时**播放以欺骗阅读器**
- ✎ **克隆(cloning)**: 将一个RFID标签中的内容记录下来, 并写入另一个标签, 以形成原来标签的一个副本

4. 拒绝服务攻击(Denial-of-service attack, DoS)

- ✎ 通过不完整的交互请求 (蓄谋的构造出来) 消耗系统资源, 如对阅读器的DoS:
 - ① 产生标签冲突 (多个标签发生通信冲突), 影响正常读取
 - ① 发起认证消息, 消耗系统计算资源 (一个特别设计的用于消耗阅读器资源的标签发送数据时)
- ✎ 对标签的DoS
 - ① 消耗有限的标签内部状态(例如, 随机二进制树算法(一种**基于二进制树的防冲突算法**)), **使之无法被正常识别** (一个特别设计的标签可以打乱识别过程, 使阅读器无法正确识别所有标签)

二、主要安全隐患


5. 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
 - ① 推测此标签之前发送的消息内容
 - ① 推断其他标签的秘密

6. 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 

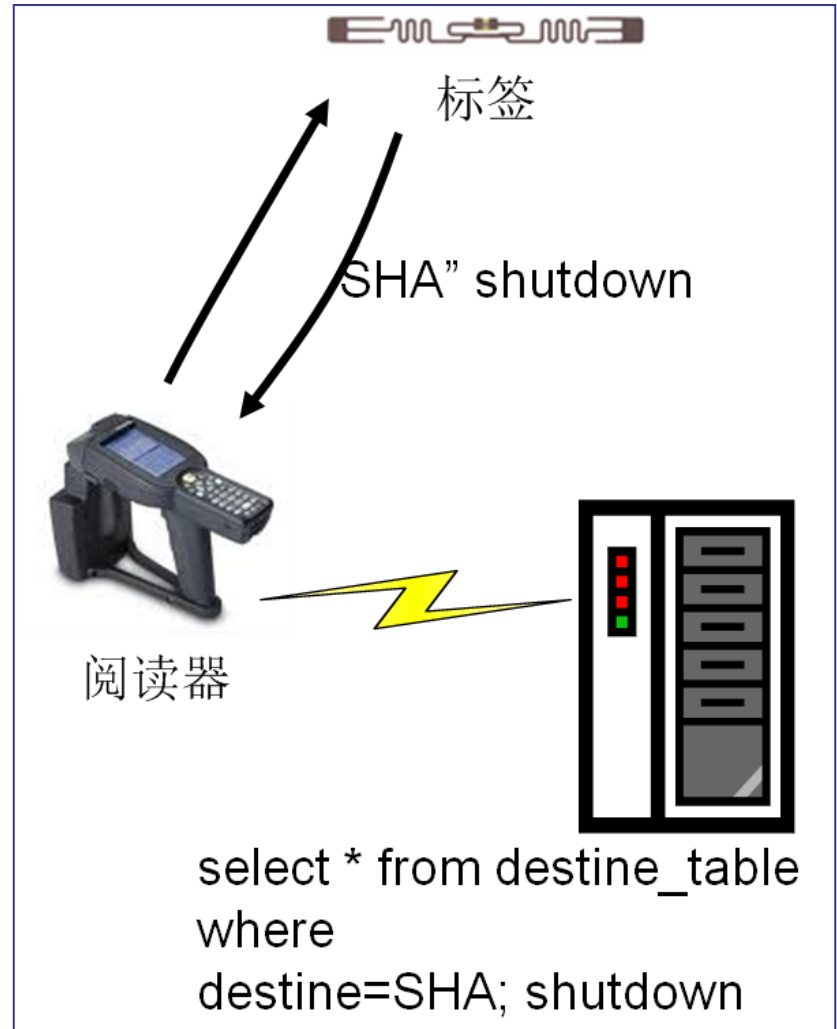
二、主要安全隐患

7. RFID病毒(virus, malware恶意软件)

- ✎ 标签中可以写入一定量的代码
- ✎ 读取tag时, 代码被注入系统
- ① SQL注入

8. 其他隐患

- ✎ 电子破坏
- ✎ 屏蔽干扰
- ✎ 拆除
- ✎ ...



三、主要隐患问题

1. 隐私信息泄露

- ✎ 姓名、医疗记录等个人信息

2. 跟踪

- ✎ 监控，掌握用户行为规律和消费喜好等。
- ✎ 进一步攻击

3. 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



一、安全机制

1. 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非法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。

一、安全机制

2. 基于密码学的安全机制(都需要查找)

① 哈希锁(hash-lock)(协议)



① 优点：初步访问控制

① 威胁：偷听，跟踪假冒(由于是固定的不会更新的metaID)

标签平时是【锁定】状态，通信前需要【解锁】

一、安全机制

2. 基于密码学的安全机制(都需要查找)

② 随机哈希锁 (randomized hash-lock)



① 优点：增强的安全和隐私

① 线性复杂度key-search: $O(M)$

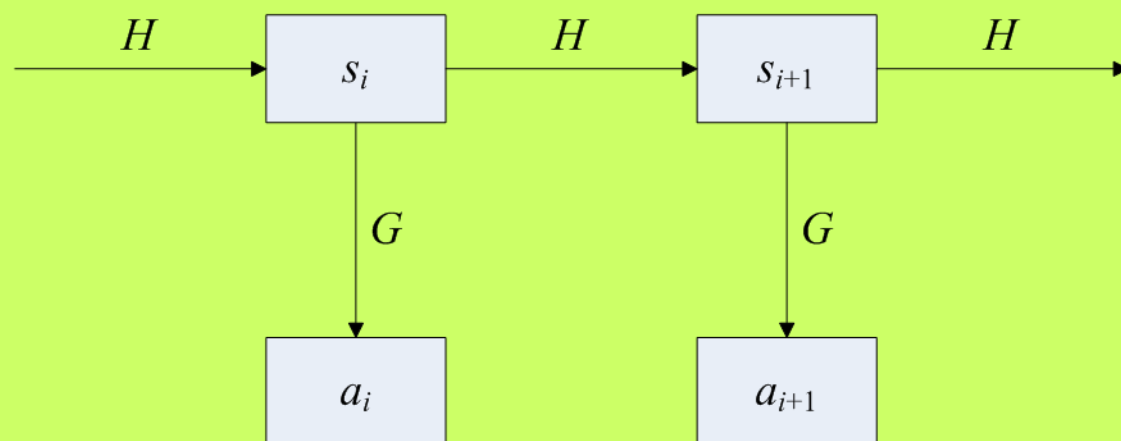
① 能抵抗重放(回放)攻击? **No!(伪装标签)**

标签平时是【锁定】状态，通信前需要【解锁】

一、安全机制

2. 基于密码学的安全机制(都需要查找)

③ 哈希链(hash chain)



- ❖ 阅读器和标签共享一个初始的随机化标识符 s
- ❖ 阅读器第 i 次阅读时, 标签返回 s_i 的哈希值 $a_i = G(s_i)$, 同时标签更新标识符为 $s_{i+1} = H(s_i)$
- ❖ 阅读器第 $i+1$ 次阅读时, 标签返回 s_{i+1} 的哈希值 $a_{i+1} = G(s_{i+1})$, 同时标签更新标识符为 $s_{i+2} = H(s_{i+1})$

① 优点: 前向安全性

① 威胁: DoS

每次查询后, 标签的标识符都使用了单向密码学哈希函数进行了更新 (这还需要标签和数据库内部的标识符保持同步)

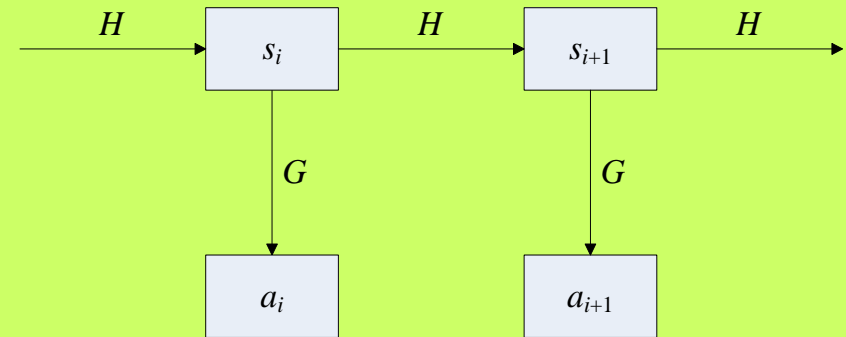
一、安全机制

2. 基于密码学的安全机制(都需要查找)

④同步方法(synchronization approach)

- ✎ 预计算并存储标签的可能回复;
- ✎ 例如：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**

实现快速认证
(识别)标签



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

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

① 高效key-search: $O(1)$

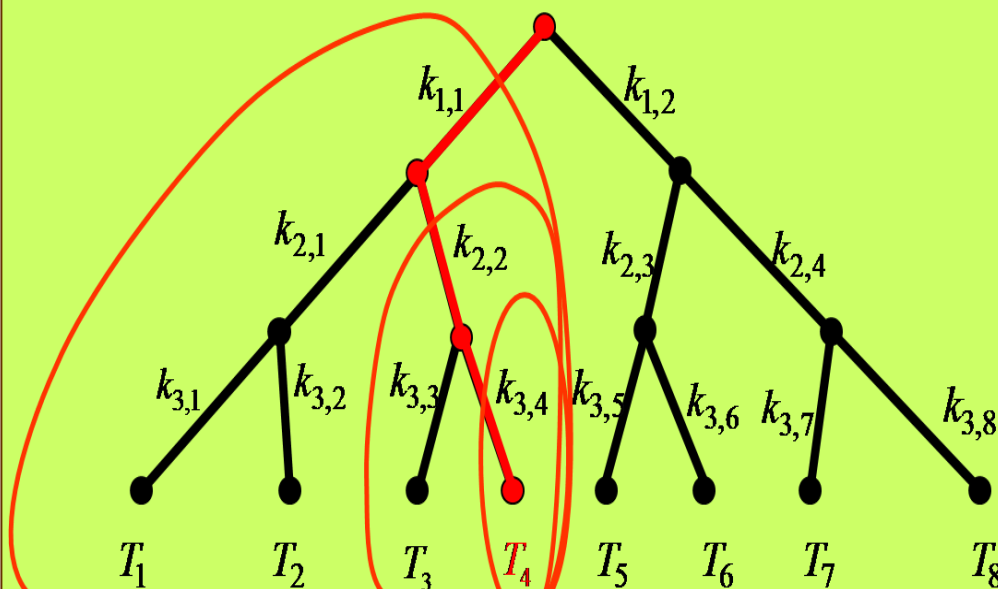
① 威胁：回放(欺骗), DoS

“同步方法”旨在在“哈希链”方法的基础上，降低后者中的阅读器需要采用“穷尽”的方法来计算复杂度(“使用所有标签的(所有)标识符计算哈希值来与收到的信息进行匹配”)，而直接在数据库中搜索“事先存储的标签回复”即可定位到哪个标签。

一、安全机制

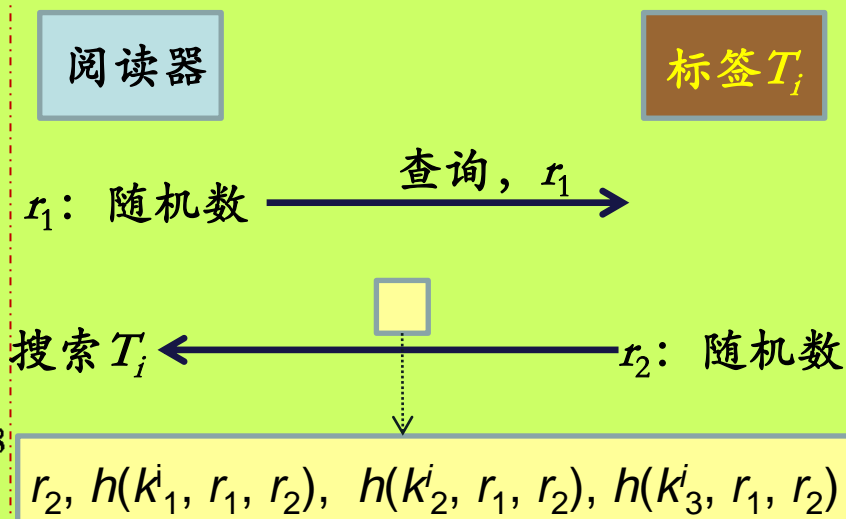
2. 基于密码学的安全机制(都需要查找)

⑤ 树形协议(tree-based protocol)



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

- ❖ 每个标签有**多个**密钥，这些密钥被组织在一个树形结构中；
- ❖ 阅读器和标签共享哈希函数 $H(\cdot)$ ，并记录所有标签的密钥。



- ❖ 阅读器利用标签发来的回复信息，在树中进行深度优先**遍历(查找)**，找出被认证的**标签在树中叶节点的位置**。

一、安全机制

2. 基于密码学的安全机制

⑥ 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上一层掩码来保护通信内容(偷听者无法得知阅读器或标签发出的具体信息, 而接收者可以利用网络编码原理得到发送者发送的信息)。
- ✎ 可拆卸天线
- ✎ 带方向的标签



二、如何面对安全和隐私挑战？

1. 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。

2. 与其他技术结合

- ✎ 生物识别
- ✎ 近场通信(Near field communication, **NFC**)

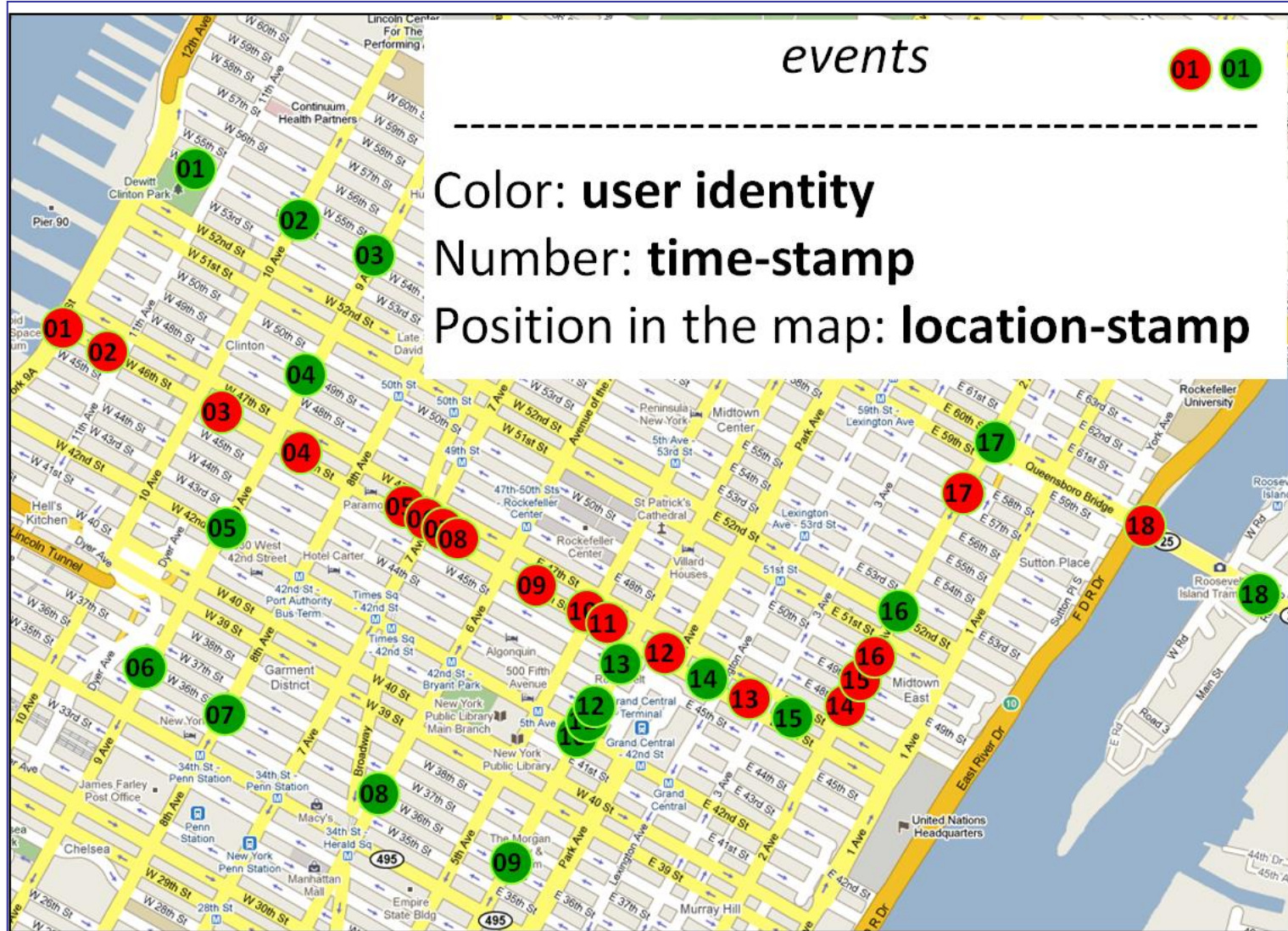
3. 法律法规

- ✎ 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。



第10章 物联网中的信息安全与隐私保护--10.5 位置信息与个人隐私

一、位置信息与个人隐私



位置信息与基于位置的服务 (LBS)

一、位置信息与个人隐私

1. 位置隐私的定义

✎ 用户对自己位置信息的掌控能力，包括：

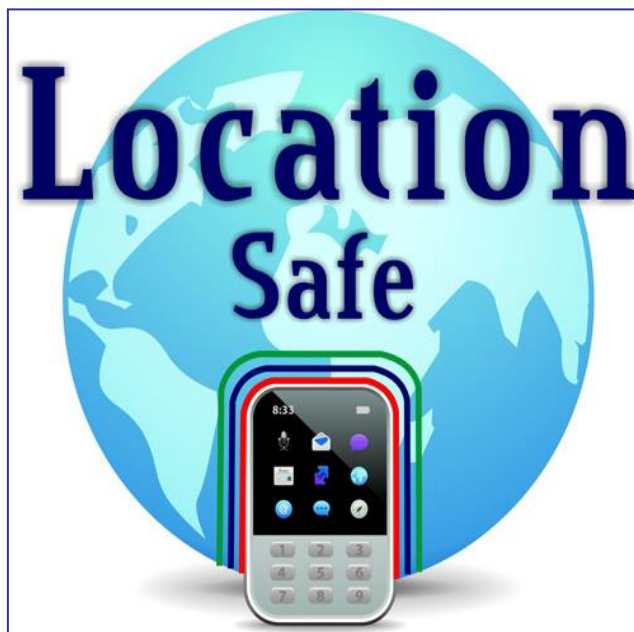
- ① 是否发布
- ① 发布给谁
- ① 详细程度

2. 保护位置隐私的重要性

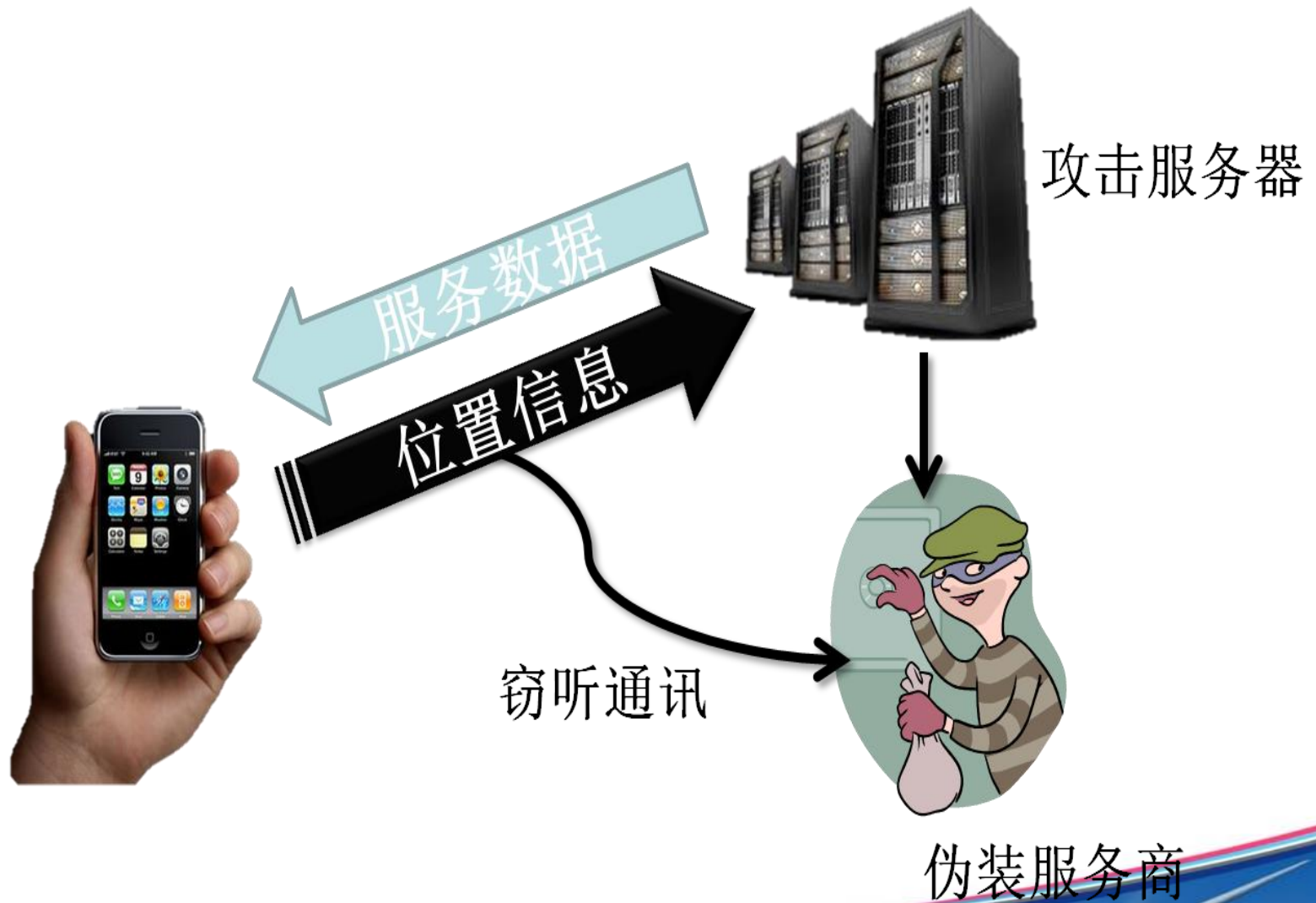
- ① 三要素：时间、地点、人物
- ① 人身安全
- ① 隐私泄露

3. 位置隐私面临的威胁

- ① 通信
- ① 服务商
- ① 攻击者



一、位置信息与个人隐私



一、保护位置隐私的手段

1. 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

- ① 一切隐私保护的基础
- ① 有强制力确保实施

✎ 缺点

- ① 各国隐私法规不同，为服务跨区域运营造成不便
- ① 一刀切，难以针对不同人不同的隐私需求进行定制
- ① 只能在隐私被侵害后发挥作用
- ① 立法耗时甚久，难以赶上最新的技术进展

一、保护位置隐私的手段

2. 隐私方针 (定制的针对性隐私保护)

✎ 分类

- ① 用户导向型, 如PIDF (Presence Information Data Format)
- ① 服务提供商导向型, 如P3P (Privacy Preferences Project)

✎ 优点

- ① 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

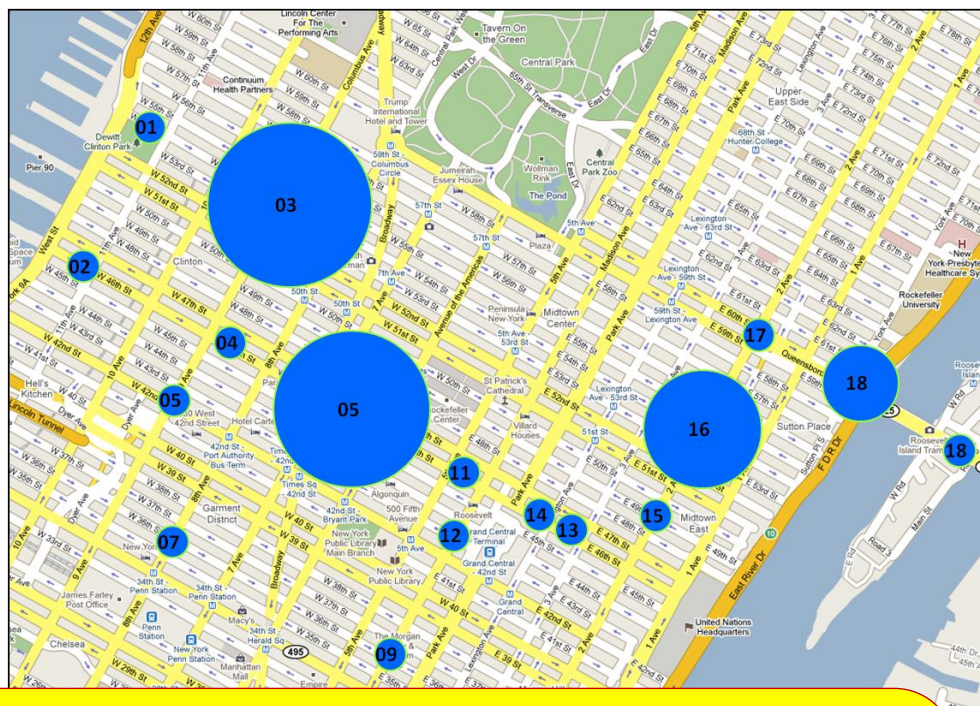
- ① 缺乏强制力保障实施
- ① 对采用隐私方针机制的服务商有效, 对不采用该机制的服务商无效

第10章 物联网中的信息安全与隐私保护--10.6 保护位置隐私的手段

一、保护位置隐私的手段

3. 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



优点

- ① 不需要强制力保障实施
- ① 对任何服务商均可使用
- ① 在隐私被侵害前保护用户隐私

缺点

- ① 牺牲服务质量
- ① 通常需要借助“中间层”保障隐私
- ① 无法应用于需要身份信息的服务

一、保护位置隐私的手段

4. 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**

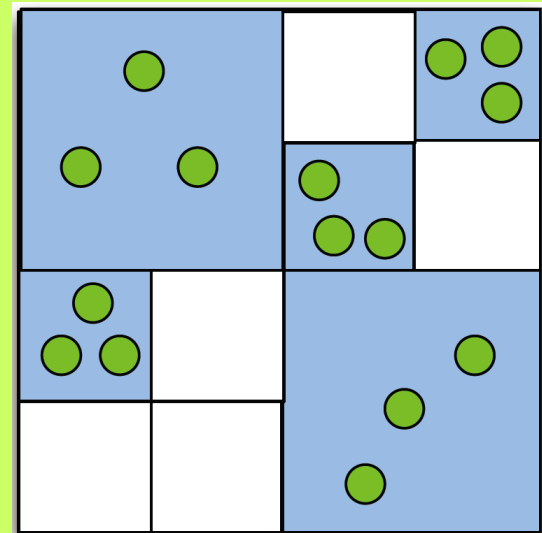
① 空间上：扩大位置信息的覆盖范围

① 时间上：延迟位置信息的发布

✎ **例：3-匿名**

① 绿点：用户精确位置

① 蓝色方块：向服务商汇报的位置信息



一、保护位置隐私的手段

5. 数据混淆

➤ **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

- ① **模糊范围：**精确位置->区域
- ① **声东击西：**偏离精确位置
- ① **含糊其辞：**引入语义词汇，例如“附近”

✍ 优点

- ① 服务质量损失相对较小
- ① 不需中间层，可定制性好
- ① 支持需要身份信息的服务

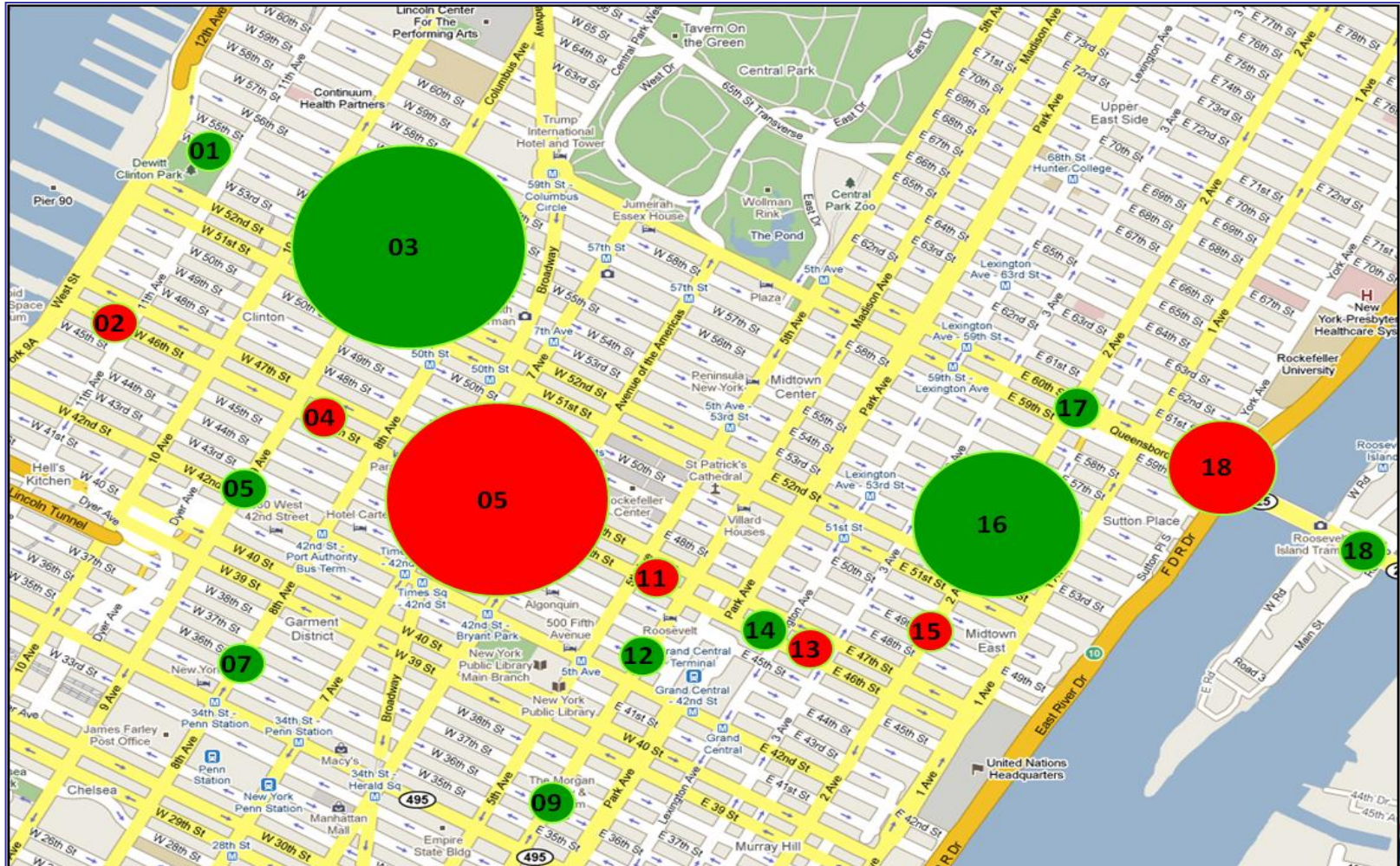
✍ 缺点

- ① 运行效率低
- ① 支持的服务有限

第10章 物联网中的信息安全与隐私保护--10.6 保护位置隐私的手段

一、保护位置隐私的手段

5. 数据混淆：模糊范围



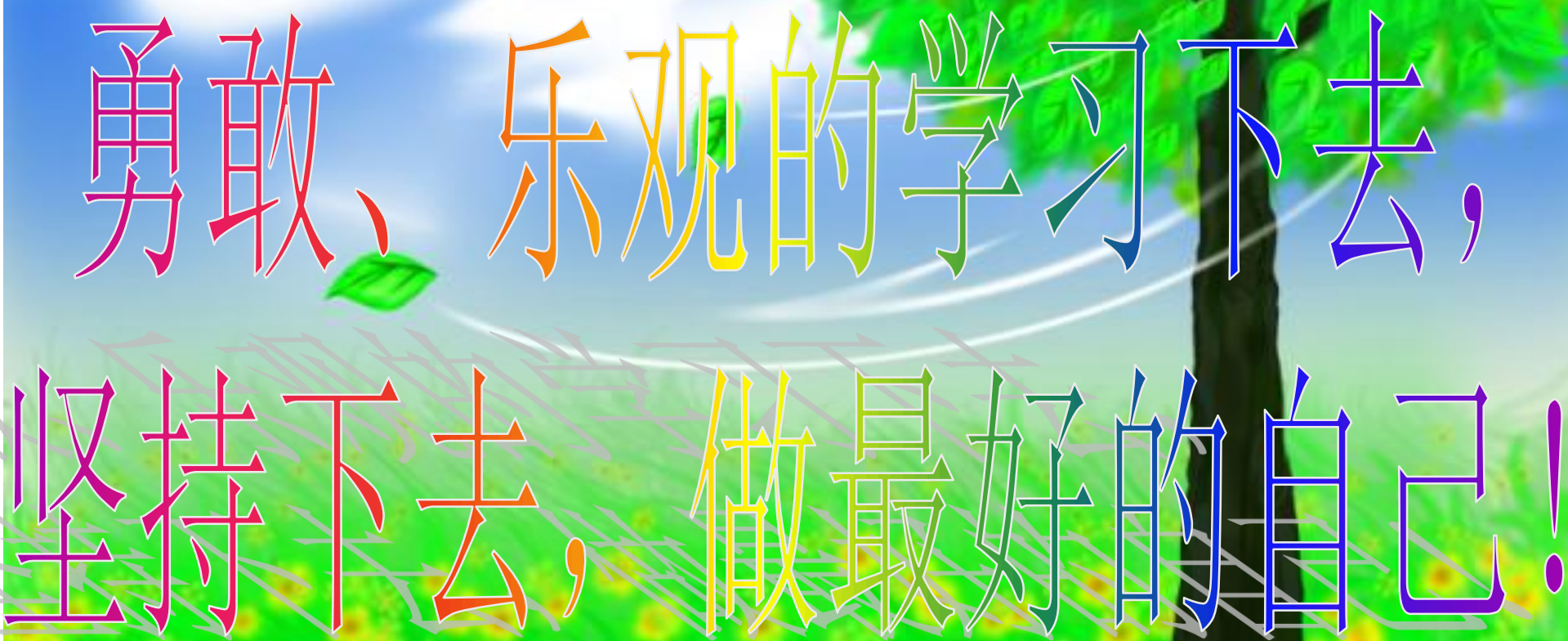
本章结束

感谢.....

祝大家：

成绩优异，身体健康；
天天愉快，阖家欢乐！





勇敢、乐观的学习下去，
坚持下去，做最好的自己！

考试时间

考试安排

课程名称	学号	任课教师	考试日期	考试时间	考场	考试形式
物联网实用技术	1811101	张策	2020年12月24日	10:05-12:05	M楼-104	期末
物联网实用技术	1811102	张策	2020年12月24日	10:05-12:05	M楼-203	期末
物联网实用技术	1811103	张策	2020年12月24日	10:05-12:05	M楼-203	期末
物联网实用技术	1811104	张策	2020年12月24日	10:05-12:05	M楼-204	期末
物联网实用技术	1811105	张策	2020年12月24日	10:05-12:05	M楼-204	期末
物联网实用技术	1811106	张策	2020年12月24日	10:05-12:05	M楼-105	期末

纵容是伤害



严格是大爱

