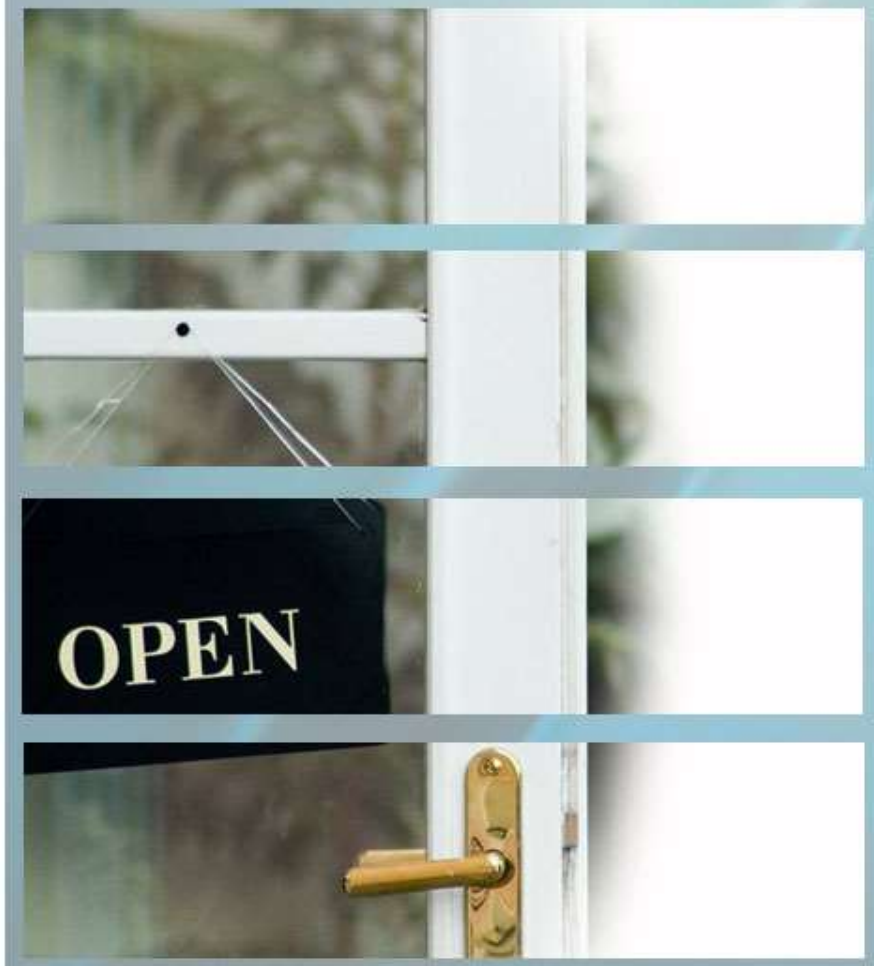
Chapter 14

Information security and privacy protection



From the perspective of **Information security and Privacy protection**, the widespread introduction of Internet of things terminals (RFID, sensors, intelligent information devices) not only provides richer information, but also increases the risk of exposing such information.

This chapter will focus on RFID security and location privacy two major security privacy issues.

内容提要

Review

Chapter 13 introduces the intelligent decision - data mining technology of Internet of things.

- Basic process of data mining
- Typical data mining algorithms
- The extensive application of data mining technology in Internet of things

This chapter focuses on RFID security and location privacy hazards in the Internet of things and typical security mechanisms.

Content

14.1 Overview

14.2 RFID security and privacy

14.3 RFID security and privacy protection mechanism

14.4 location information and personal privacy

14.5 measures to protect location privacy

What are the general indicators of network security?


General index of network information security

Reliability: three measures (destruction resistance, survival and effectiveness)
Availability: measured as the ratio of normal service hours to total working hours
Confidentiality: common security technologies (anti-interception, radiation protection, encryption, physical security)
Integrity: information cannot be changed without authorization; The difference between confidentiality and confidentiality: confidentiality requires information not to be disclosed to unauthorized persons, and integrity requires information not to be damaged for various reasons.
Non-repudiation: participants cannot repudiate the features of the completed operations and commitments
Controllability: the characteristic of controlling the dissemination and content of information

What is privacy?

Privacy right: the right to make decisions about personal information, including personal information, body, property or decision.

Internet of things and privacy

Improper use can invade privacy

The right technology can protect privacy

Content

14.1 Overview

14.2 RFID security and privacy

14.3 RFID security and privacy protection mechanism

14.4 location information and personal privacy

14.5 measures to protect location privacy

What is the status of RFID security?

What are the major security and privacy concerns?

Overview of RFID security status

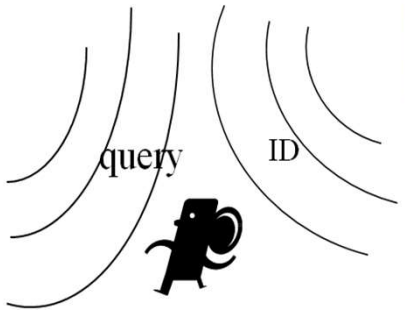
RFID security privacy standard specification and recommendations

- EPCglobal describes the functional components to be supported by RFID tags in the uhf category I and second generation tag air interface specification, and its security requirements are as follows:
  - ✓ Article level labeling protocol requirements document
  - ✓ ISO/IEC: RFID data safety standards
- Eu: *recommendations on RFID privacy and data protection*

Main safety hazard

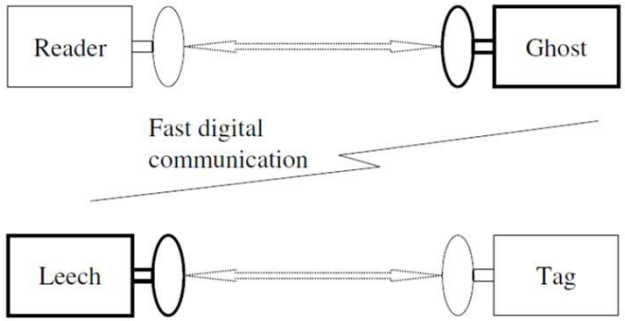
Hacking (eavesdropping)

- Rfid communication between the tag and the reader
- Attackers can eavesdrop on messages from a set distance



Man-in-the-middle attack (MITM)

- Passes, intercepts, or modifies communication messages to a reader(tag) disguised as a tag(reader)
- Pickpocket system



Main safety hazard

Cheat, replay, clone

- Spoofing: tags are spoofing via the reader based on the data you already know
- Replaying: record and play back the tag's response
- Cloning is a process in which a copy of the original tag is formed

Denial-of-service attack (DoS)

- Consuming system resources through incomplete interaction requests, such as:
  - ✓ Tag conflict, affecting normal reading
  - ✓ Initiate authentication messages and consume system computing resources
- DoS for tags
  - ✓ Consumes a limited amount of internal label state, making it impossible to recognize properly

Main safety hazard

Physical cracking (corrupt)

- Tags are easy to get
- Labels can be cracked: through techniques such as reverse engineering
- After cracking, you can launch further attacks
- Infer the content of the message sent before this tag
- Infer the secrets of other labels

Modification of information

- Unauthorized modification or erasure of label data

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

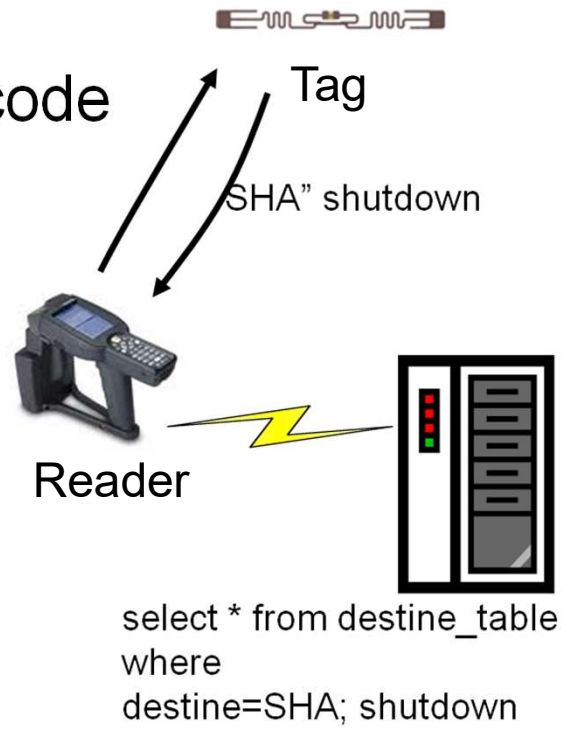
Main safety hazard

RFID virus (malware)

- Tag can write a certain amount of code
- When the tag is read, the code is injected into the system
- SQL injection

Other hazards

- Electronic destruction
- Shielding interference
- demolition
- ...



Main safety hazard

Privacy information disclosure

- Personal information such as name, medical record, etc

Tracking

- Monitor and master user behavior rules and consumption preferences.
- Further attack

Efficiency versus privacy

- Label identity confidentiality
- To quickly verify a tag, you need to know the tag's identity to find the information you need
- Balance: appropriate, available security and privacy

Content

What are the general indicators of network security?

14.3 RFID security and privacy protection mechanism

Early physical security mechanisms

- Kill: kill the tag to disable the function of the tag and make it unable to respond to the scan of the attacker.
- Faraday screen: shields electromagnetic waves and prevents tags from being scanned.
- Active jamming: the user actively broadcasts the wireless signal to prevent or destroy the reading of the RFID reader.
- Block tags: a special tag collision algorithm prevents unauthorized readers from reading tags that prevent the tags from being protected.

The physical security mechanism satisfies the requirements of privacy protection by sacrificing some functions of labels.

14.3 RFID security and privacy protection mechanism

Security mechanism based on cryptography

Hash (hash - lock lock)

Advantages: initial access control

Threats: eavesdropping, stalking

14.3 RFID security and privacy protection mechanism

Security mechanism based on cryptography

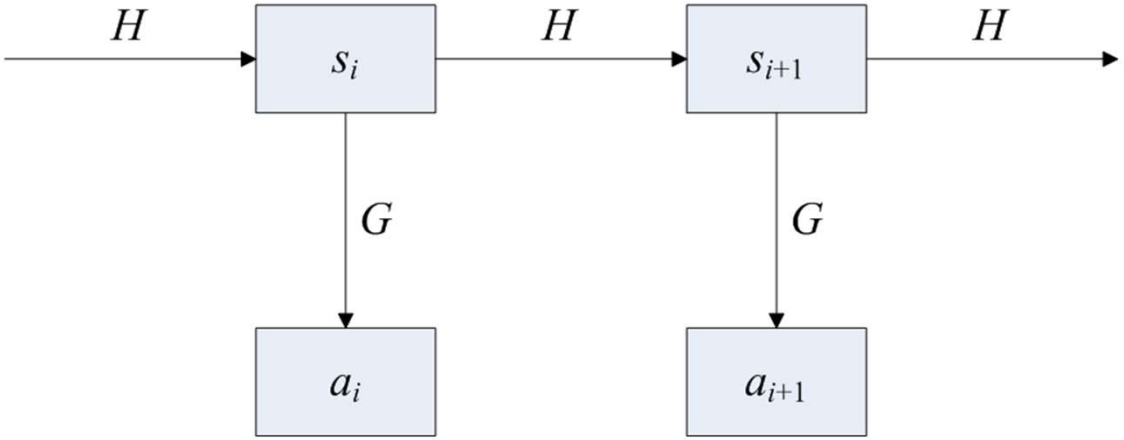
Randomized hashed -lock

Advantages: enhanced security and privacy
Linear complexity key-search: O(N)

14.3 RFID security and privacy protection mechanism

Security mechanism based on cryptography

Hash chain



Advantages: forward security

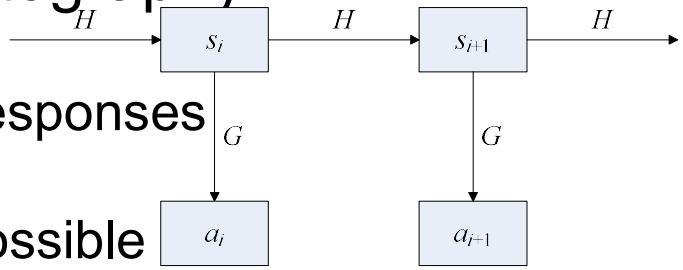
Threat: DoS

14.3 RFID security and privacy protection mechanism

Security mechanism based on cryptography

Synchronization approach

- Anticipate and store possible responses to labels, such as:
- In the hash chain method, m possible replies can be stored for each tag, and the tag response is directly looked up in the database



Efficient key - search: O (1)

Threat: playback, DoS

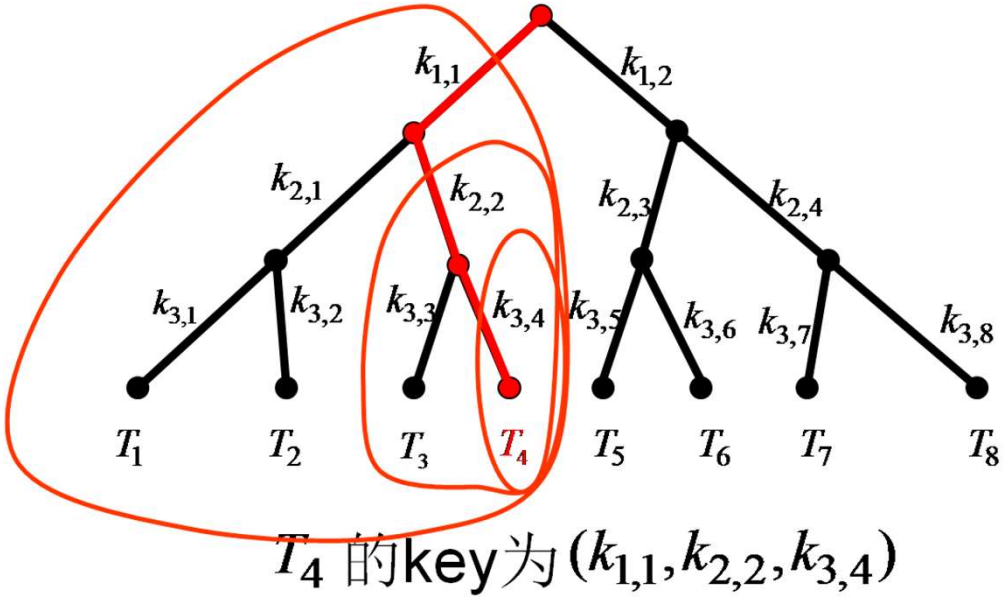
$$s_{i+k} = H^k(s_i), (0 \leqq k \leqq m\text{-}1)$$

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

14.3 RFID security and privacy protection mechanism

Security mechanism based on cryptography

Tree-based protocol



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

14.3 RFID security and privacy protection mechanism

Security mechanism based on cryptography

Tree-based protocol

Log-complexity key-search: O(logN), threatened by cracking attacks, attack success rate:

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} tag, δ: Branch number K_o tags are broken (Avoine, SAC'05)

14.3 RFID security and privacy protection mechanism

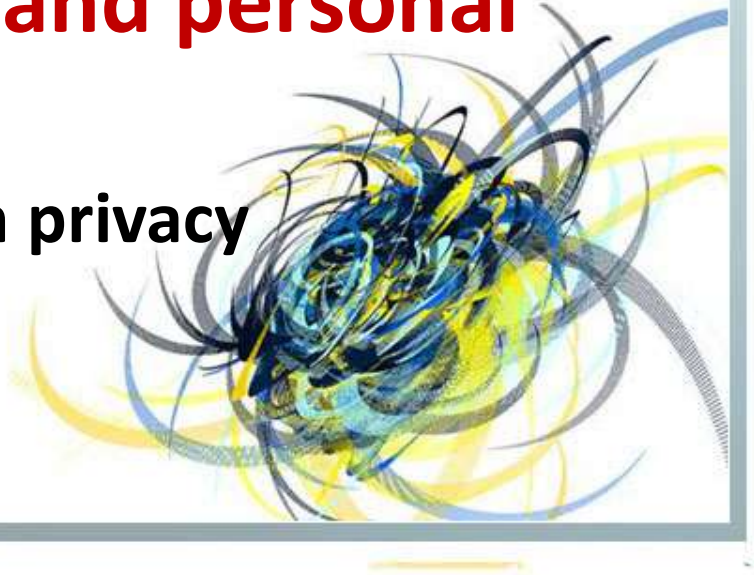
Other methods

- Physical unclonable function, (PUF) : implement the function with Physical properties by making use of the randomness that is expected in the manufacturing process. It is easy to calculate and difficult to characterize.
- Mask: use an external device to add additional protection to the communication between the reader and the tag.
- Information is obtained through network coding principle
- Detachable antenna
- Label with direction

How to face security and privacy challenges?

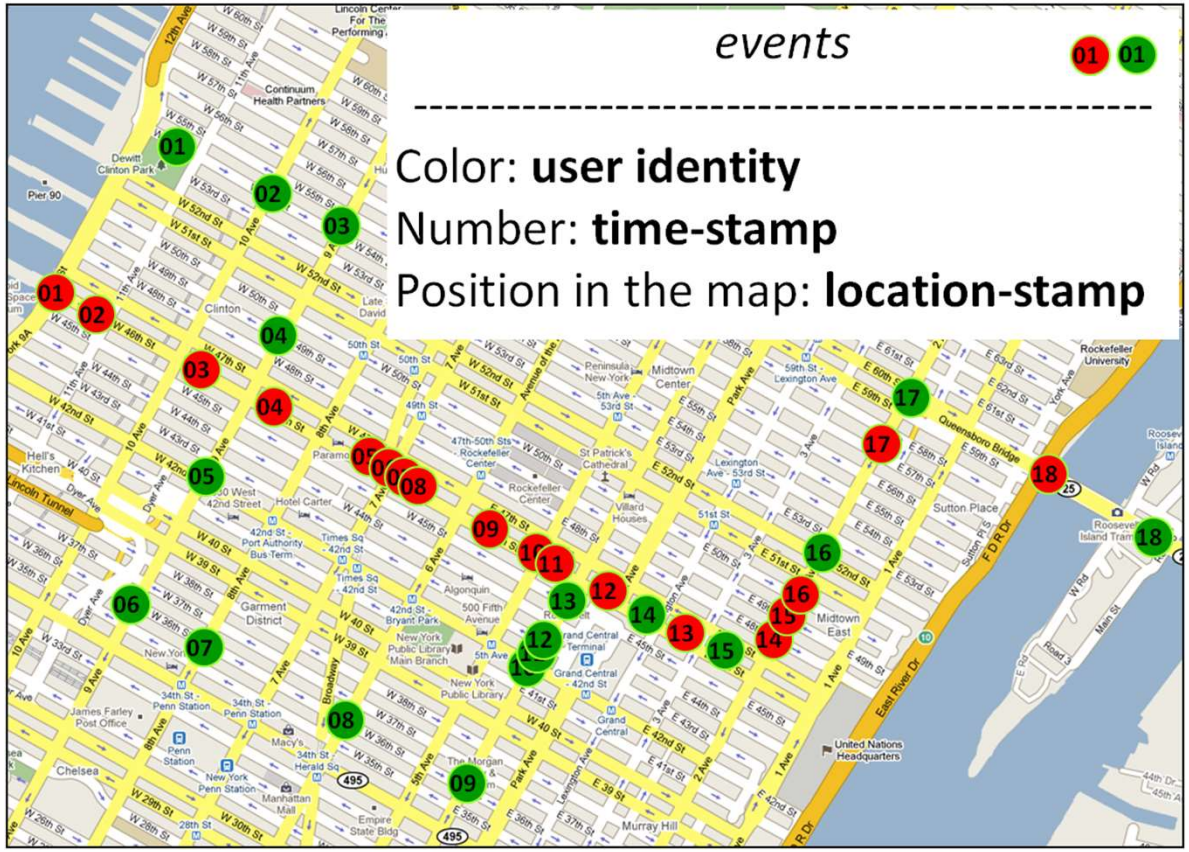
- **Unity of usability and security**
  There is no need to provide security and privacy protection for all information and hierarchical management of information.
- **With other technologies**
  - ✓ biometric
  - ✓ Near field communication (NFC)
- **Laws and regulations**
  From the perspective of laws and regulations increase the harm to users through RFID technology
  The costs of security and privacy, and how do you define them
  Guidance.

Content



What is location privacy?

14.4 Location information and personal privacy



Location information and location-based services (LBS)

14.4 Location information and personal privacy

Definition of location privacy

Users' ability to control their location information, including:

- ✓ Whether issued
- ✓ Release to who
- ✓ How detailed

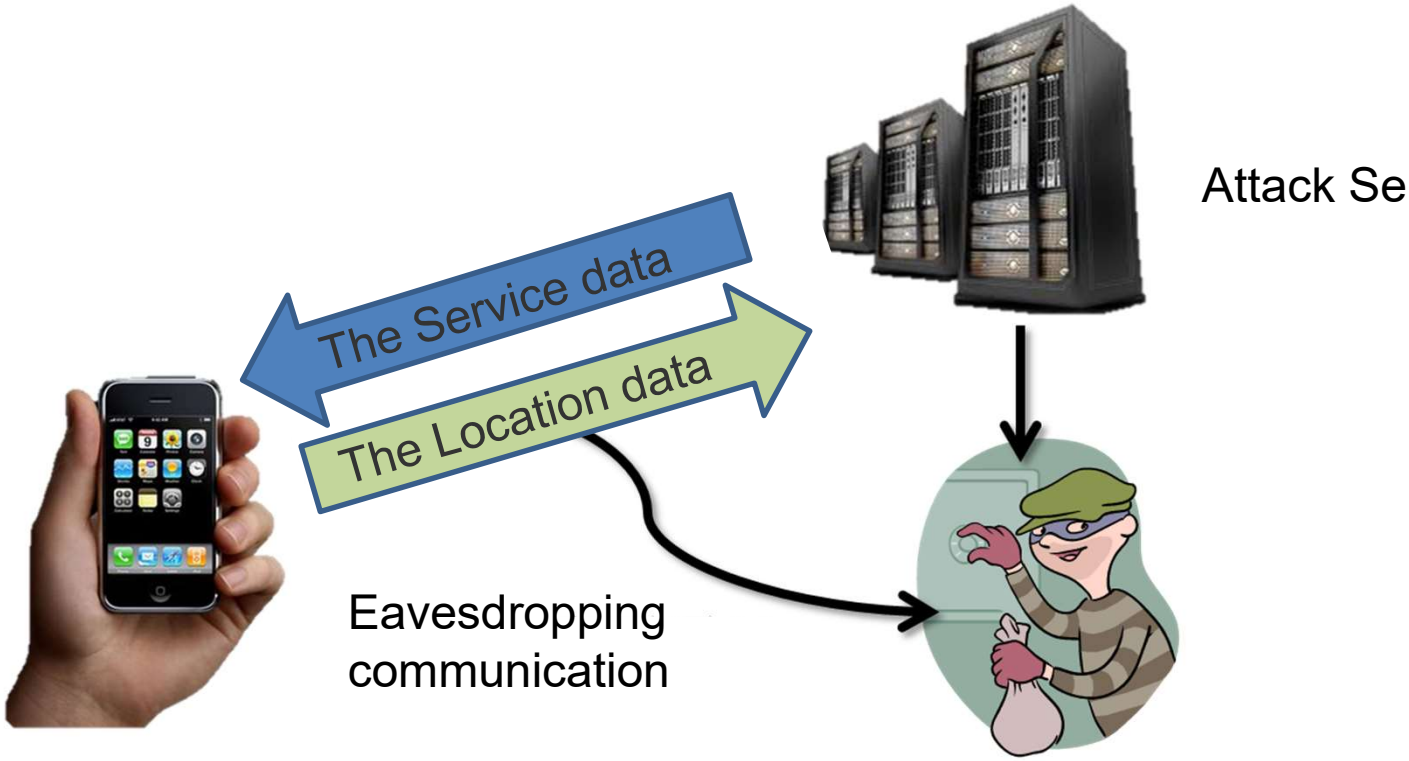
The importance of protecting location privacy

- Three elements: time, place and people
- The personal safety
- privacy

Threats to location privacy

- communication
- Service providers
- The attacker

14.4 Location information and personal privacy



Content

14.1 Overview
14.2 RFID security and privacy
14.3 RFID security and privacy protection mechanism
14.4 location information and personal privacy
14.5 measures to protect location privacy

What are ways to protect location privacy?

14.5 Methods to protect location privacy

Institutional constraints

- 5 principles (right to know, right to choose, right to participate, collector, mandatory)
- **Advantages**
  - ✓ The basis of all privacy protection
  - ✓ Enforce the law
- **Disadvantages**
  - ✓ Privacy laws vary from country to country, making it inconvenient for services to operate across regions
  - ✓ One-size-fits-all, it is difficult to customize for different privacy needs of different people
  - ✓ Only when privacy is compromised
  - ✓ Legislation takes too long to keep up with the latest technological advances

14.5 Methods to protect location privacy

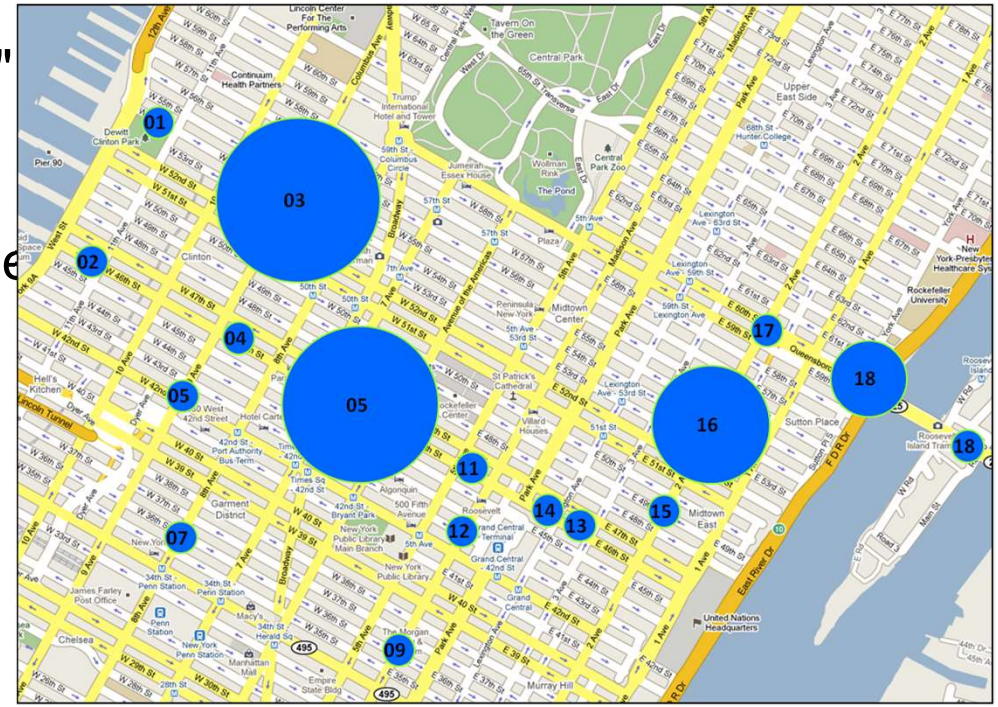
Privacy policy: customized targeted privacy protection

- **Classification**
  User oriented, such as PIDF (Presence Information Data Format)
  Service provider oriented, such as P3P (Privacy Preferences Project)
- **Advantages**
  Customizable, users can set different privacy levels according to their own needs
- **Disadvantages**
  Lack of coercive force to ensure implementation
  It is valid for service providers that adopt the privacy policy mechanism and invalid for those that do not

14.5 Methods to protect location privacy

Anonymous:

- Thinking "all service providers are suspicious"
- Hiding "identities" in location information
- Service providers can use location information to provide services, but cannot infer a user's identity from location information
- Common technique: K anonymity



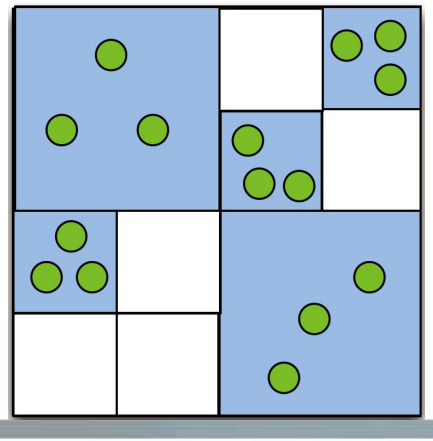
14.5 Methods to protect location privacy

Anonymity (continued)

- Advantages
  - ✓ It does not require coercive force
  - ✓ Available to any service provider
  - ✓ Protect users' privacy before it is violated
- Disadvantages
  - ✓ Sacrifice quality of service
  - ✓ Often a "middle tier" is needed to protect privacy
  - ✓ Cannot be applied to services that require identity information

K Anonymous

- **Basic idea:** make the location information of K users indistinguishable
- **Two ways**
  - ✓ Spatially: expand the coverage of location information
  - ✓ Time: delay the release of location information
- **Example: 3- anonymity**
  - ✓ Green dot: user exact location
  - ✓ Blue square: location information reported to service providers

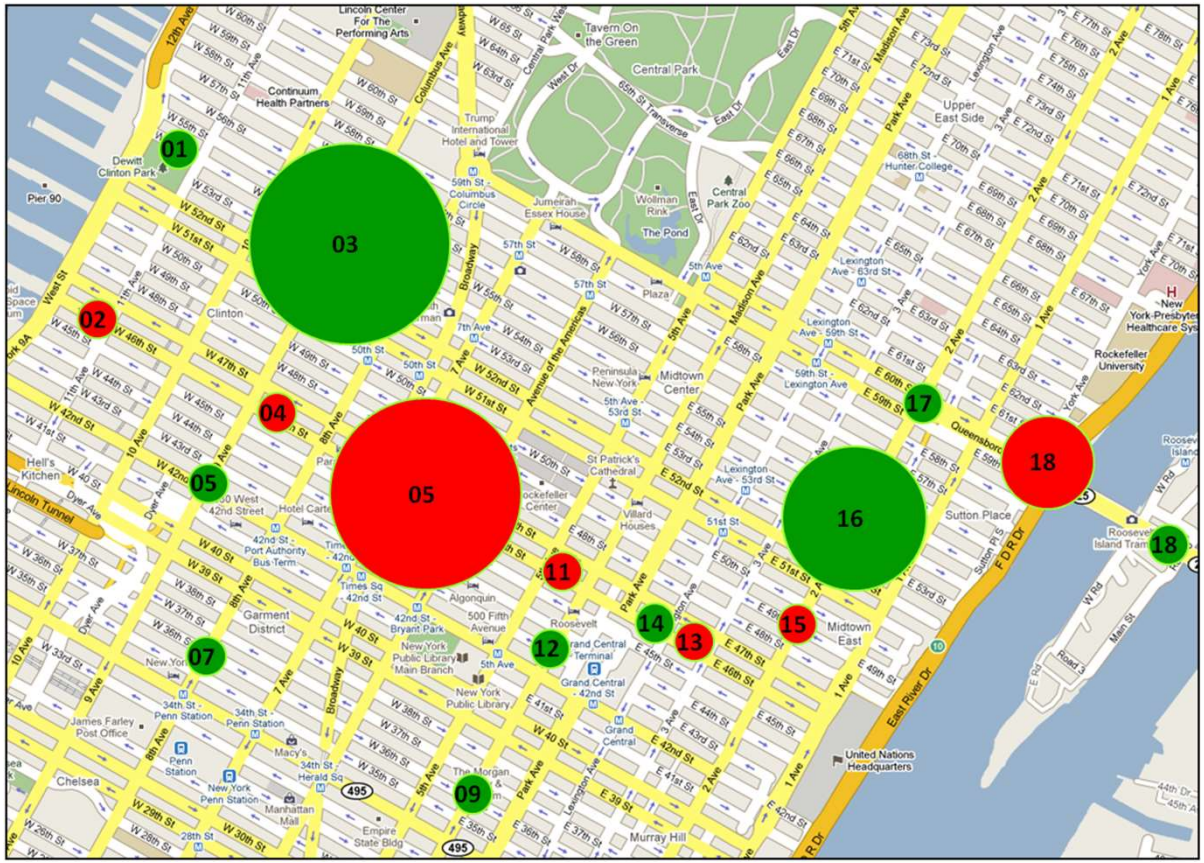


14.5 Methods to protect location privacy

Data obfuscation: preserving identity and obfuscating other parts of location information so that an attacker cannot know the exact location of a user

- Three methods
  - ✓ Fuzzy range: precise location -> region
  - ✓ Diversion: deviation from precise position
  - ✓ Ambiguity: introducing semantic words, such as "nearby"
- Advantages
  - ✓ The loss of service quality is relatively small
  - ✓ No middle layer, good customization
  - ✓ Support services that require identity information
- Disadvantages
  - ✓ Low operating efficiency
  - ✓ Support services are limited

Data obfuscation: Fuzzy range



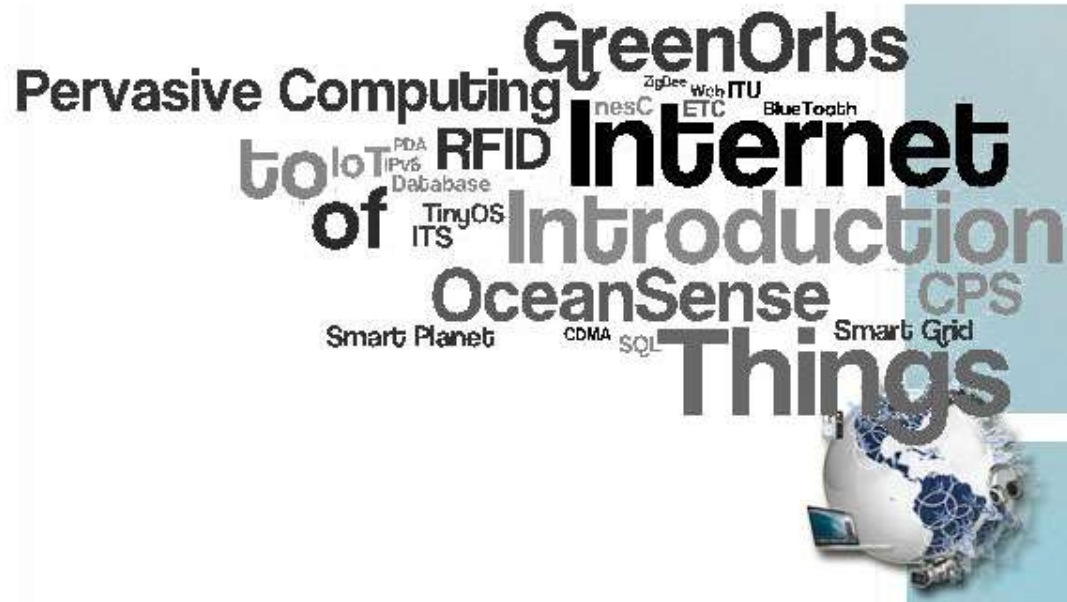
Conclusion

Review

This chapter introduces RFID security and typical security mechanisms, as well as location privacy risks and corresponding protection measures.

Key Points

- Understand the general index of network information security.
- Master major RFID security risks.
- Understand RFID security protection mechanism, focus on the security mechanism based on cryptography.
- Understand the definition of location information and illustrate the means to protect location information.



Thank you!

Internet of Things