RFID Tags: Privacy and Security without Cryptography

Ari Juels

ajuels@rsasecurity.com

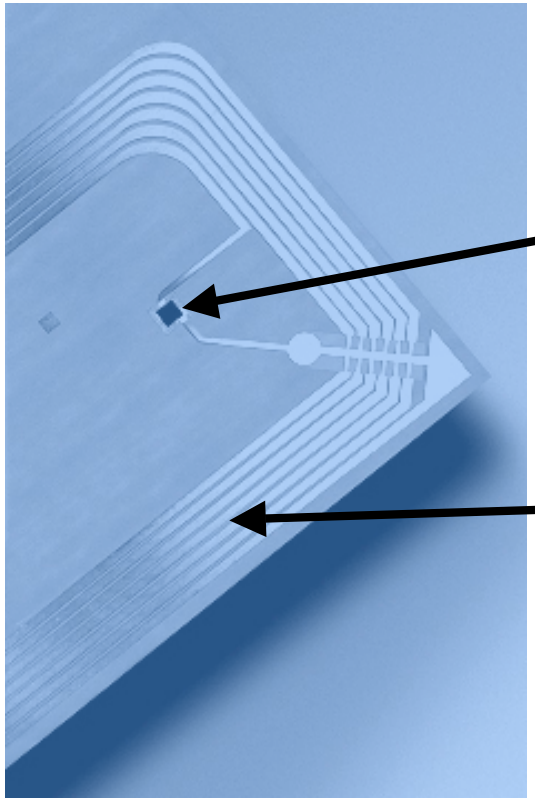
RFID-Privacy Workshop at MIT

15 November 2003

RSA LABORATORIES

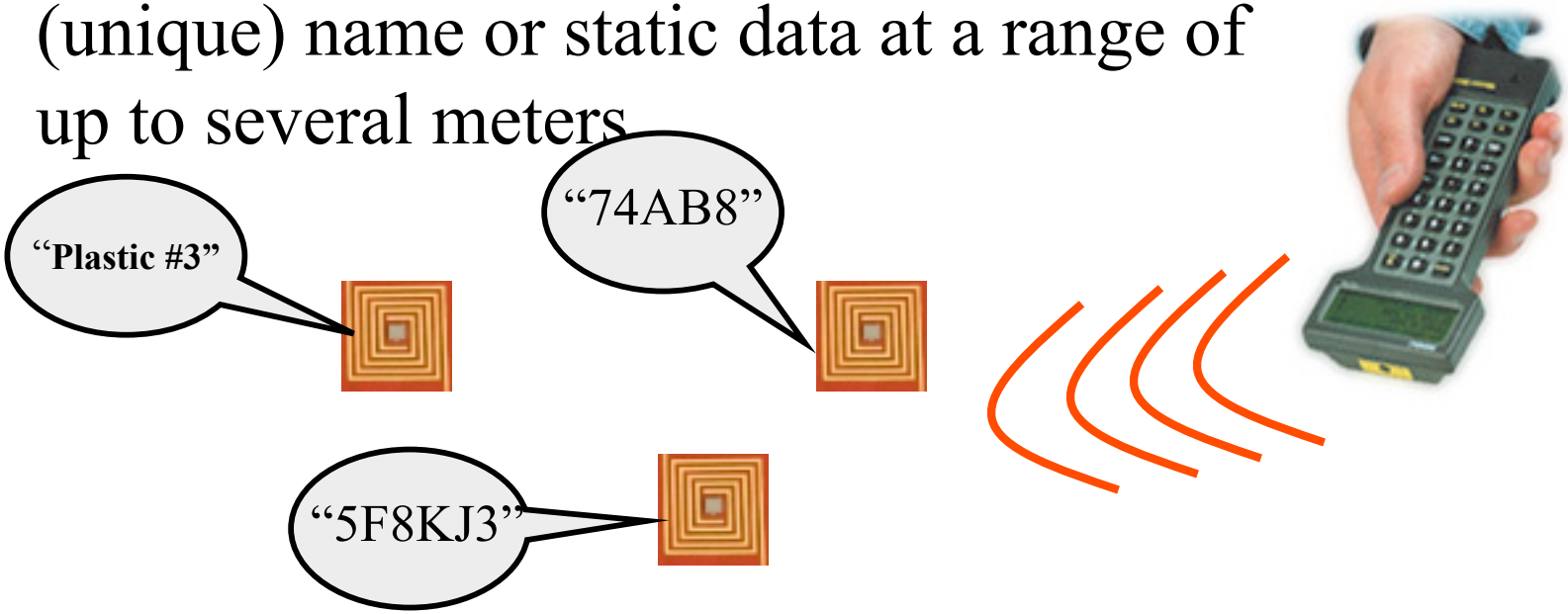
What is a **R**adio-**F**requency **Id**entification (RFID) tag?

- In terms of appearance…



What is an RFID tag?

- You may own a few RFID tags…
  - Contactless physical-access cards
  - Automated toll payment
  - Inventory tags
- At present, an RFID tag simply calls out its (unique) name or static data at a range of up to several meters



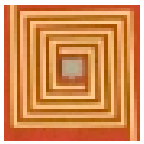
The capabilities of basic RFID tags

- No power
  - Receives power from reader
  - Range a few meters
- Little memory
  - Static 64-to-128-bit identifier in current ultra-cheap generation (five cents / unit)
  - Hundreds of bits soon
- Little computational power
  - A few thousand gates
  - ***No* cryptographic functions available**
  - Static keys for read/write permission

The grand vision:
RFID as next-generation barcode

Barcode

RFID tag



Line-of-sight — **Radio contact** — ***Fast, automated scanning***

Specifies object type — **Uniquely specifies object** — ***Provides pointer to database entry for every object***

Commercial applications

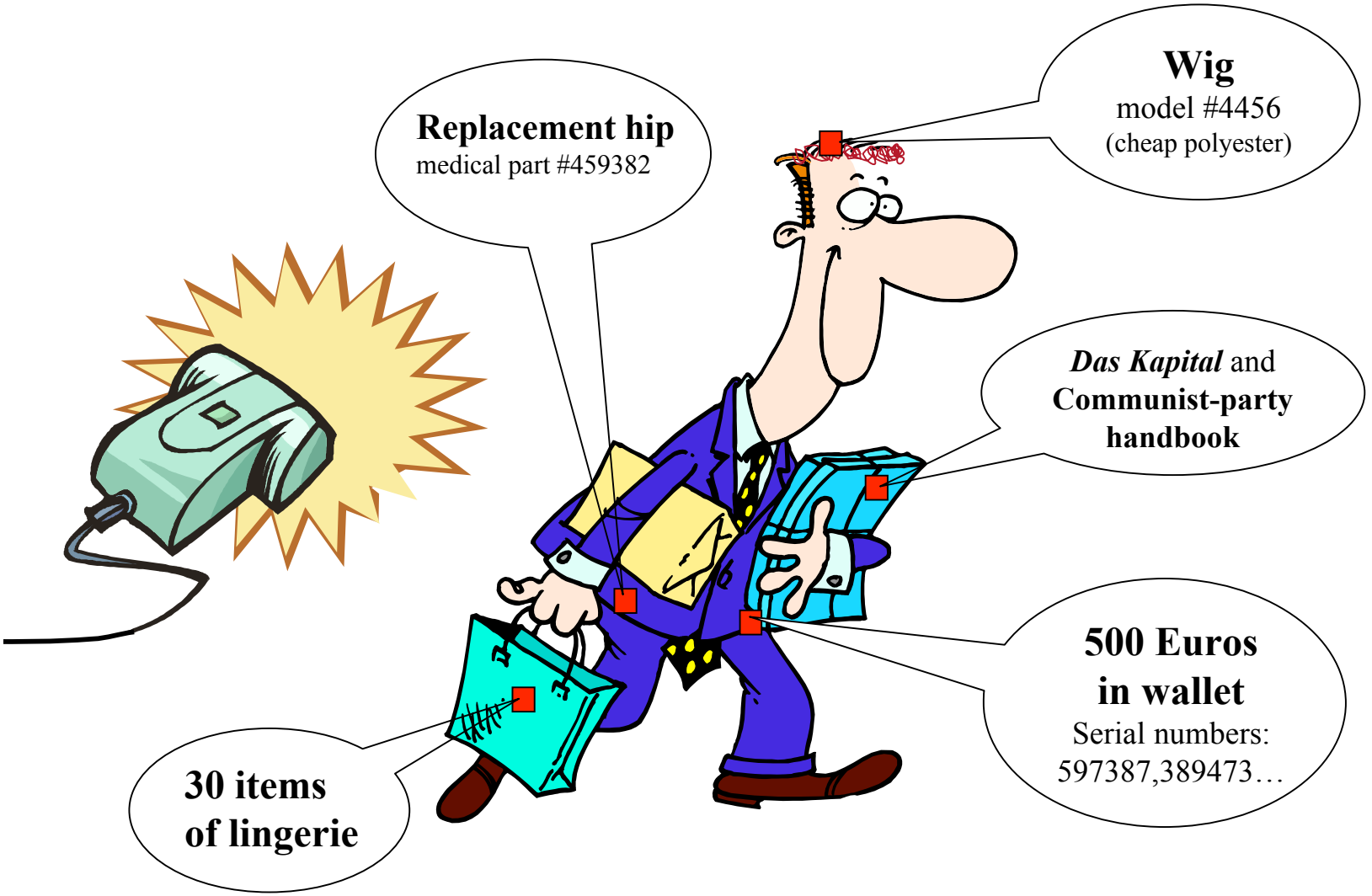
- Smoother inventory tracking
  - Military supply logistics
    - Gulf War I: Placement of double orders to ensure arrival
    - Gulf War II: RFID renders supply chain much more reliable
  - Procter & Gamble: Elimination of dock bottleneck -- fast loading of pallets onto trucks
- Product recalls
- Anti-counterfeiting
- Maintaining shelf stocks in retail environments
  - Gillette Mach3 razor blades
- Parenting logistics
  - Water park uses RFID bracelets to track children

There is an impending explosion in RFID-tag use

- Wal-Mart requiring top 100 suppliers to deploy RFID at pallet level by 2005
- Gillette announced order of 500,000,000 RFID tags
- Auto-ID Center at MIT
  - Wal-Mart, Gillette, Procter & Gamble, etc.
  - Spearheading EPC (electronic product code) data standard for tags
  - Developing cheap manufacturing techniques
  - Handing over standards to Uniform Code Council
- Estimated costs
    - 2005: $0.05 per tag; $100 per reader
    - 2008: $0.01 per tag; several dollars per reader (?)
- RFID realm sometimes called *"Extended Internet"*

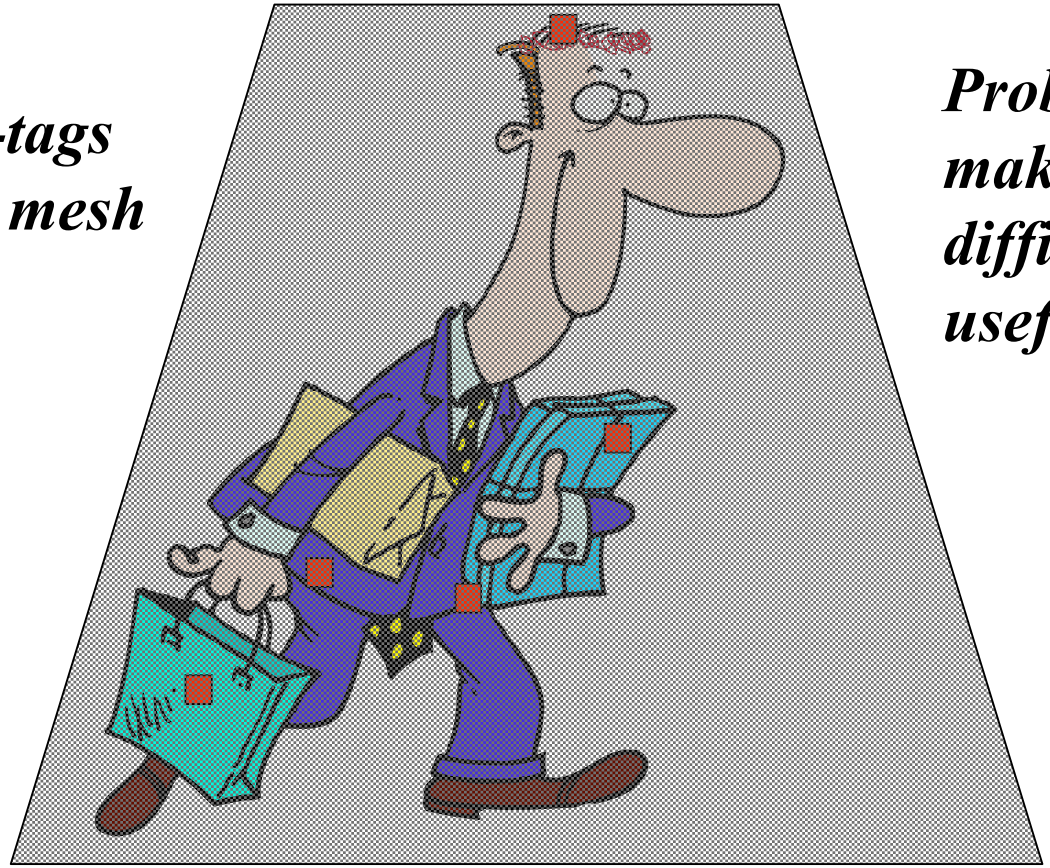
The Consumer-Privacy Problem

RFID tags will be *everywhere*…



Simple approaches to consumer privacy

Method 1:
Place RFID-tags
in protective mesh
or foil



Problem:
makes locomotion
difficult… perhaps
useful for wallets

Simple approaches to consumer privacy

Method 2:
"Kill" RFID tags

Problem:
RFID tags are
much too useful…

Some consumer applications today

- Prada, Soho NYC
  - Personalization / accessorization
- House pets

- Building access (HID)
- ExxonMobil Speedpass
- Benetton
  - Clothing – anti-forgery, supply-chain

Consumer applications tomorrow

- "Smart" appliances
  - Refrigerators that automatically create shopping lists
  - Closets that tell you what clothes you have available, and search the Web for advice on current styles, etc.
  - Ovens that know how to cook pre-packaged food
- "Smart" products
  - Clothing, appliances, CDs, etc. tagged for store returns
- "Smart" paper
  - Airline tickets that indicate your location in the airport
  - Library books
  - Business cards
- Recycling
  - Plastics that sort themselves

Another future application: Euro banknotes

- European Central Bank rumored to plan implanting RFID tags in banknotes by 2005

- Uses?
  - Anti-counterfeiting
  - Tracking of illicit monetary flows

Other possible uses

- More efficient mugging

- Fairly easy tracking of people and transactions by *anyone!*
  - Law-enforcement snooping capabilities made freely available

Why might power to track be freely accessible?

- Simple static identifiers are the most naïve
- How about encrypting ID?
  - Creates new static identifier, i.e., “meta-ID”
- How about a law-enforcement access key?
  - Tag-specific keys require initial release of identity
  - Universal keys subject to interception / reverse-engineering
- Tags readable only at short range, e.g., 1 cm?
  - Protects privacy, but is RFID cost effective?
- Anti-counterfeiting?

Early examples of consumer backlash

- 42% of Google results on “RFID” include word “privacy”
- CASPIAN **(Consumers Against Supermarket Privacy Invasion and Numbering)**
  - Diatribes on RFID at:
    - NoCards.org
    - BoycottGillette.com
    - BoycottBenetton.com
  - National news coverage: *NY Times*, *Time*, etc.
- Wal-Mart “smart-shelf project” cancelled
- Benetton RFID plans withdrawn

The two messages of this talk

1. Deployed naïvely, embedding of RFID tags in consumer items presents a serious danger to privacy.

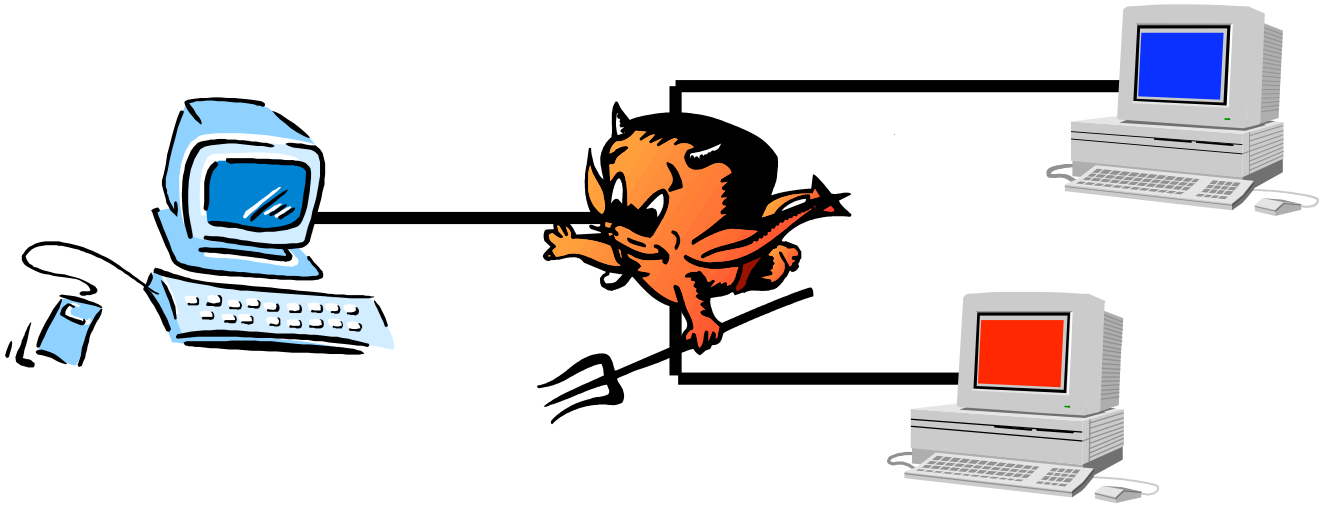
2. The danger can be mitigated: It is possible to strike a balance between privacy and convenience.

Two Technical Approaches to Enhancing RFID Privacy

First approach [Juels '03]: Minimalist cryptography

Standard, e.g., Internet "adversarial" model

- System components simultaneously accessible by adversary
- Adversary may interact in unlimited way



First approach:
Minimalist cryptography

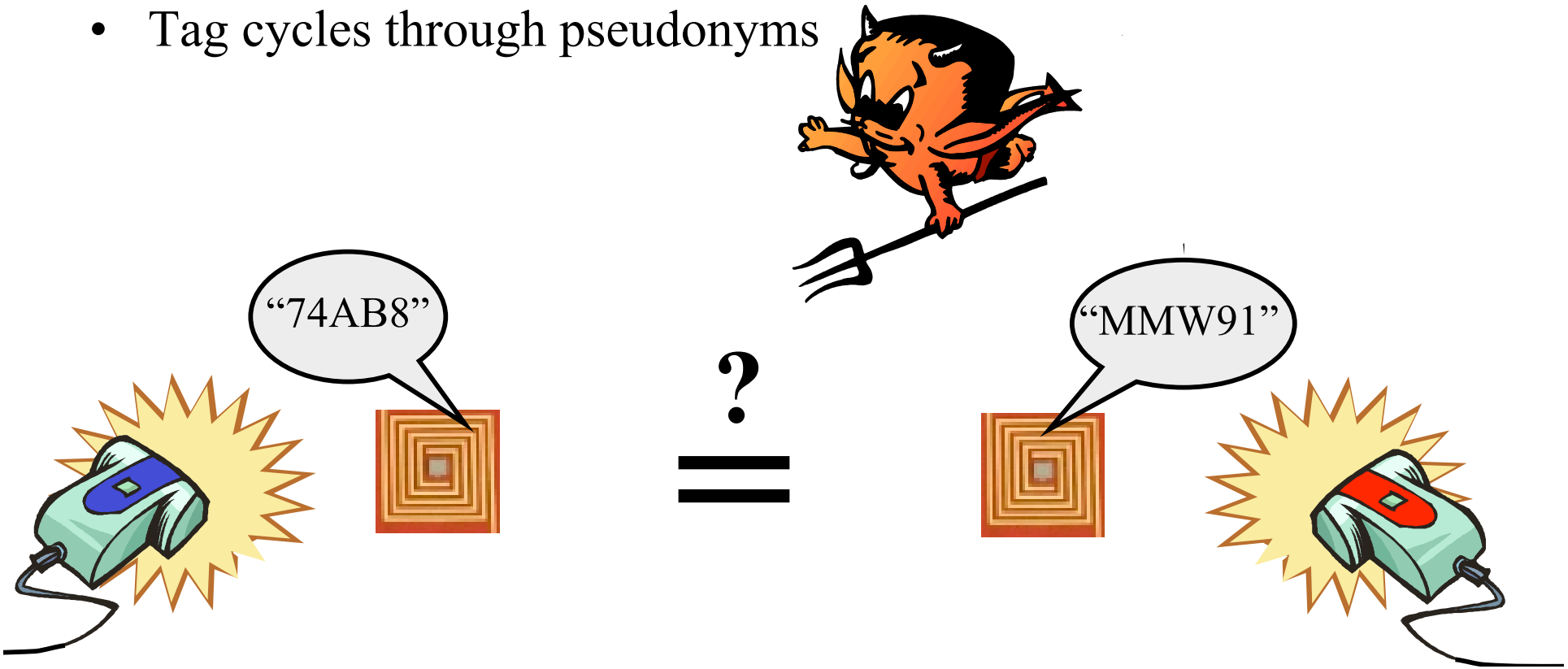
- RFID adversarial model is different:
  - Adversary with full system access can easily break it
    - Without cryptography, tags cannot survive attack!
  - In real world, adversary must have physical proximity to tags to interact with them

A couple of scenarios

- Example: Building access
  - Adversary may make limited queries of tags in parking lot before employees authenticate to door readers
- Example: Readers scattered around city
  - Adversary may performed limited scanning of pedestrians

Pseudonym rotation

- Set of cryptographically unlinkable pseudonyms *computed externally* by trusted verifier
- Pseudonyms stored on tag
  - Limited storage means at most, e.g., 10 pseudonyms
- Tag cycles through pseudonyms



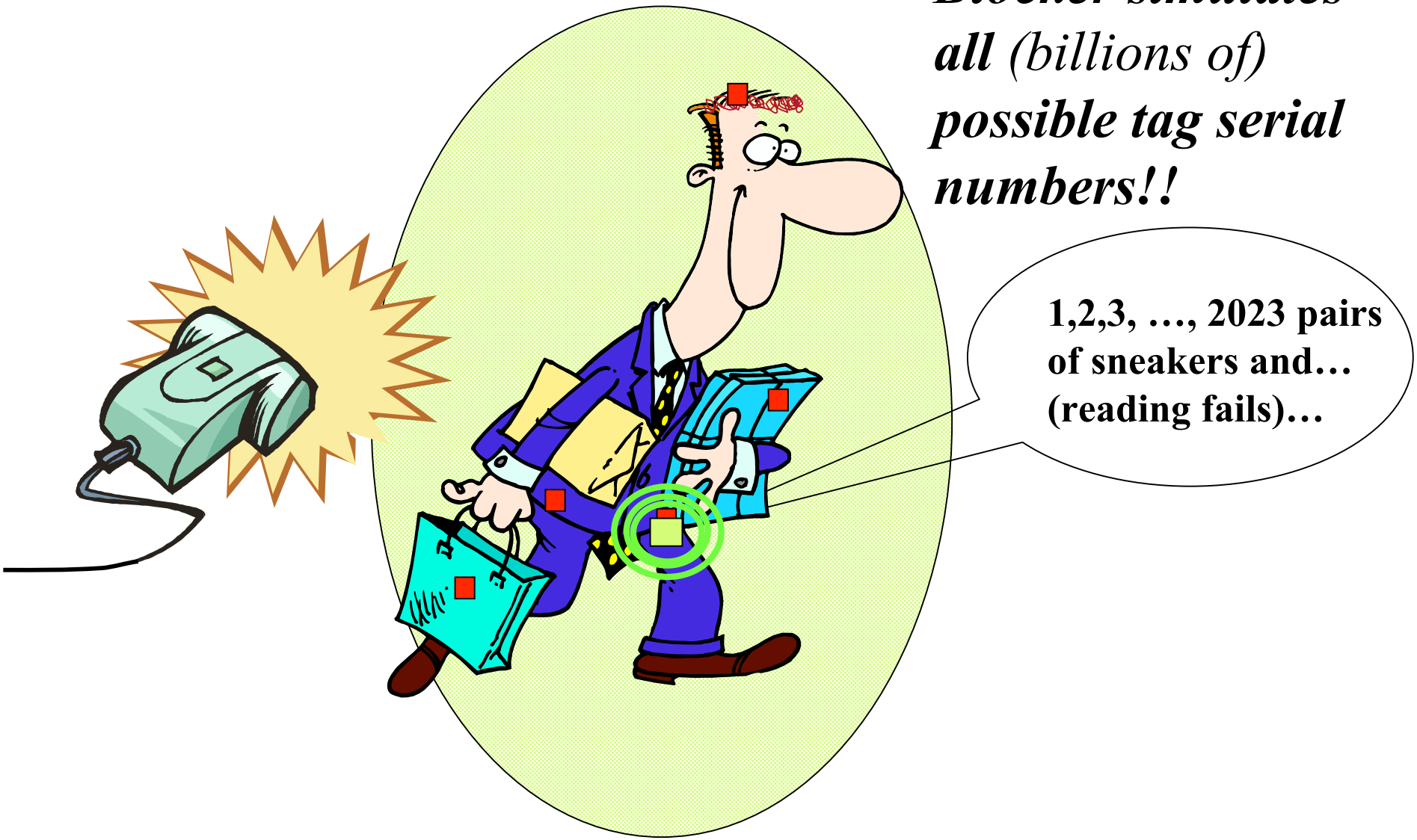
Are several pseudonyms enough?

- Strengthen restriction on adversarial queries using "throttling"
  - Tag enforces pattern of query delays
- Pseudonym refresh
  - Valid reader provides new pseudonyms
  - Pseudonyms must be protected against eavesdropping and tampering using encryption, but tags cannot do standard cryptography!
  - Pseudonyms encrypted using special interleaving of one-time pads
- Getting good model is difficult

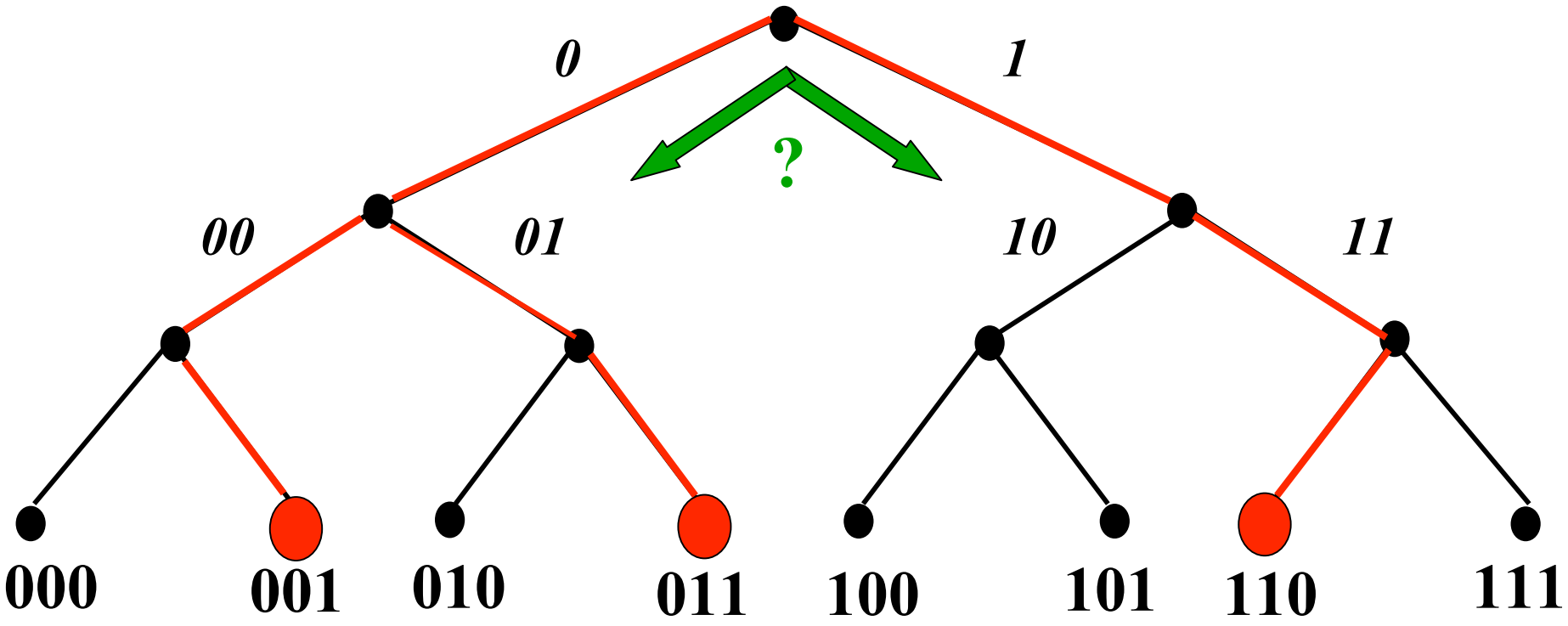
Second Approach [Juels, Rivest, & Szydlo '03]: The "Blocker" Tag

“Blocker” Tag

Blocker simulates all** (billions of) **possible tag serial numbers!!



“Tree-walking” anti-collision protocol for RFID tags



In a nutshell

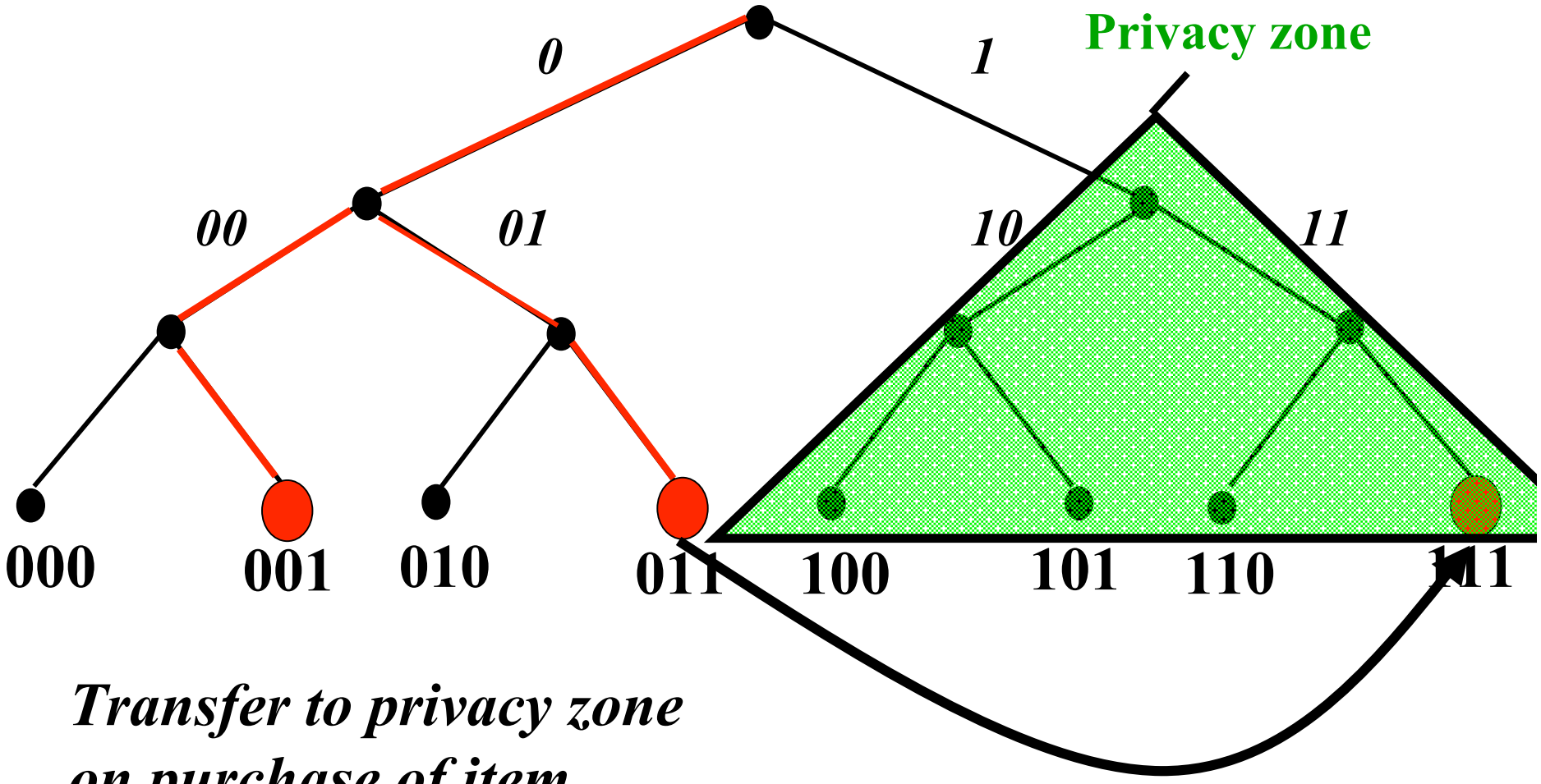
- "Tree-walking" protocol for identifying tags recursively asks question:
  - "What is your next bit?"
- Blocker tag always says ***both '0' and '1'***!
  - Makes it seem like *all* possible tags are present
  - Reader cannot figure out which tags are actually present
  - Number of possible tags is *huge* (at least a billion billion), so reader stalls

Blocker tag system should protect privacy but still avoid blocking unpurchased items

Consumer privacy + commercial security

- Blocker tag can be ***selective:***
  - *Privacy zones:* Only block certain ranges of RFID-tag serial numbers
  - *Zone mobility*: Allow shops to move items into privacy zone upon purchase
- Example:
  - Blocker blocks all identifiers with leading ‘1’ bit
  - Items in supermarket carry leading ‘0’ bit
  - On checkout, leading bit is flipped from ‘0’ to ‘1’
    - PIN required, as for “kill” operation

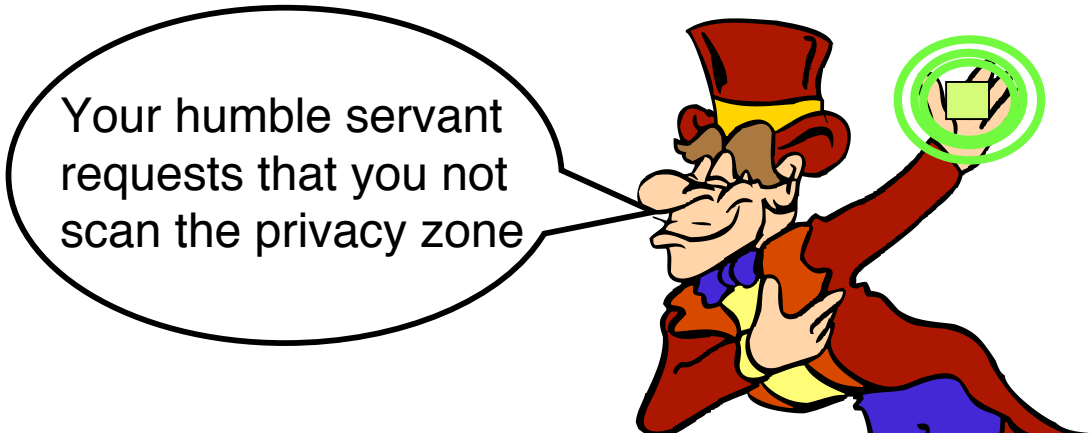
Blocking with privacy zones



Transfer to privacy zone on purchase of item

Polite blocking

- We want reader to scan privacy zone when blocker is not present
  - Aim of blocker is to keep functionality active – when desired by owner
- But if reader attempts to scan when blocker is present, it will stall!
- Polite blocking: Blocker informs reader of its presence



More about blocker tags

- Blocker tag can be cheap
  - Essentially just a “yes” tag and “no” tag with a little extra logic
  - Can be embedded in shopping bags, etc.
- With multiple privacy zones, sophisticated, e.g., graduated policies are possible
- Standards integration would be quite helpful
  - AutoID Center (UCC) may support this

Application of pseudonyms and blockers

- Privacy isn't just a consumer issue!
  - RFID tags make industrial espionage easier in supply chains
- *Pseudonym management* good for supply chains
- *Pseudonym management* helps provide anti-cloning
- *Blocker* most appropriate for privacy protection for consumers

Final remarks

- Contrast dystopian visions with physical reality of RFID tags:
  - Manufacturers struggling with reliability, e.g., UHF tags hard to read near human body!
- RFID tags vs. mobile phones
  - Infrastructure ownership
  - Nature of information leakage
  - Control of on/off
  - RFID tags like physical cookies
- Spectrum of RFID devices
  - $0.05 vs. $1.00
- Legislation and technology most effective in concert
- Privacy is just one of many RFID-related security issues!
  - As “Extended Internet”, RFID represents extension of traditional security perimeter