The Blocker Tag:
Selective Blocking of RFID Tags for Consumer Privacy

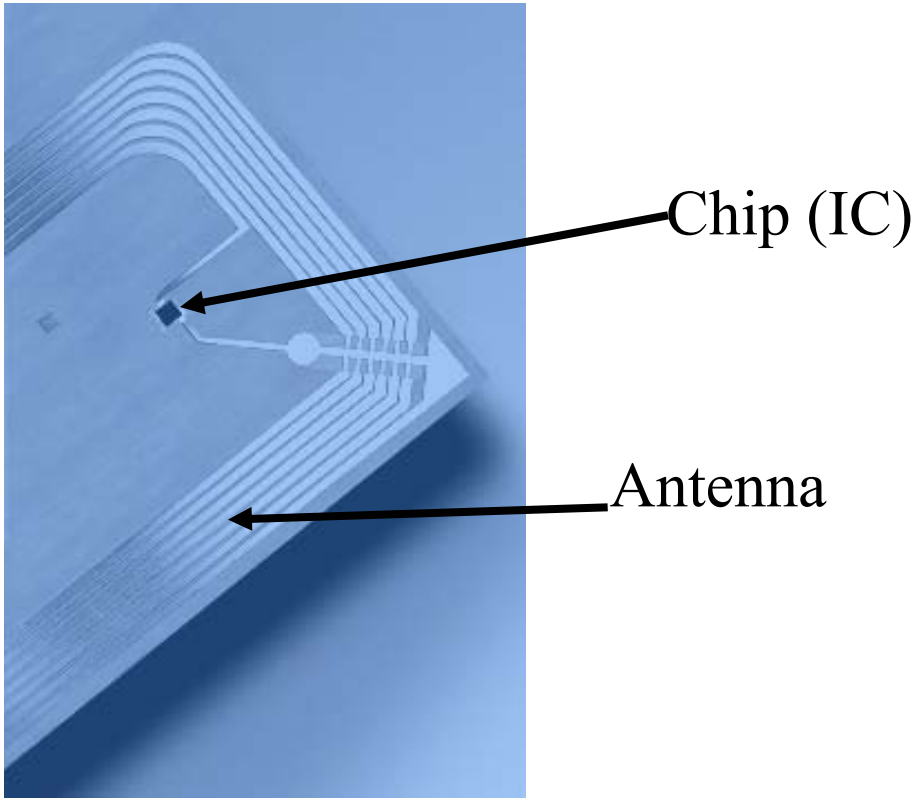
Ari Juels
RSA Laboratories

Ron Rivest
MIT CSAIL

Mike Szydlo
RSA Laboratories

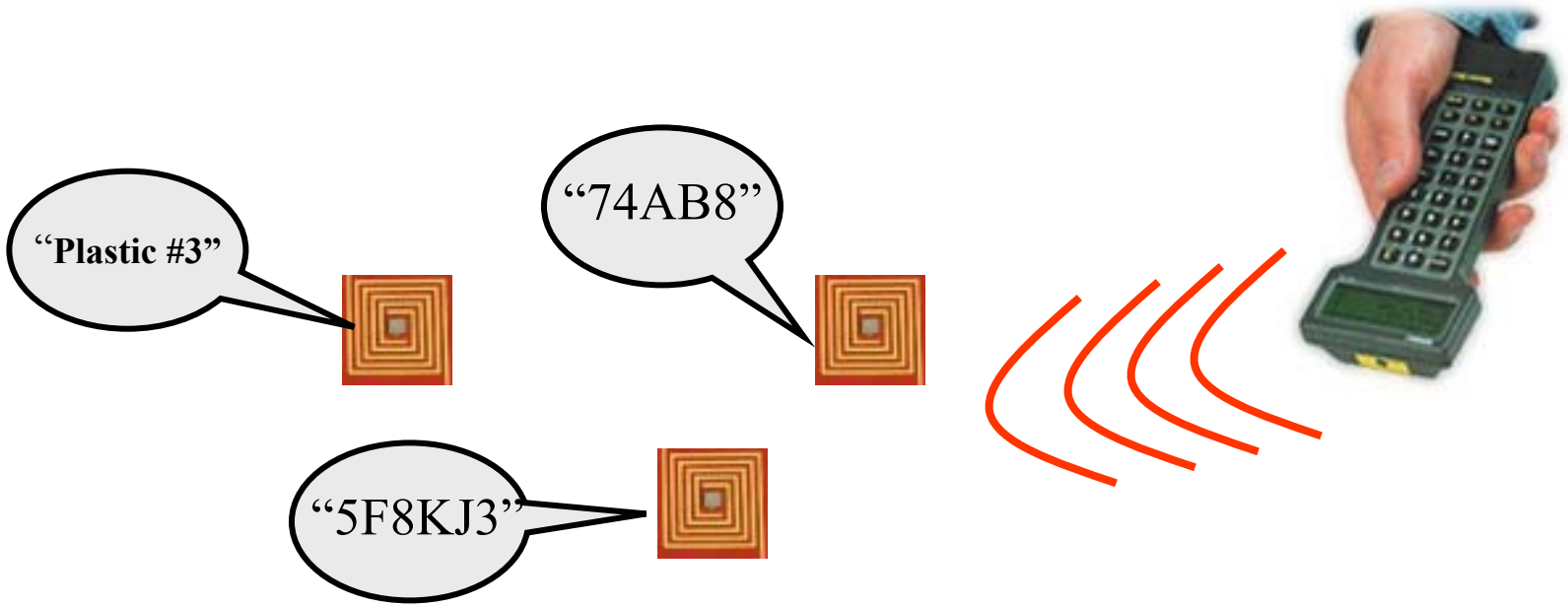
What is a **R**adio-**F**requency **Id**entification (RFID) tag?

- In terms of appearance…



What is an RFID tag?

- You may own a few RFID tags…
  - Contactless physical-access cards
  - Automated toll payment
- At present, an RFID tag simply calls out its (unique) name or static data over a short distance



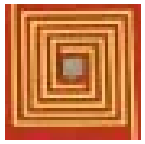
The capabilities of basic RFID tags

- 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

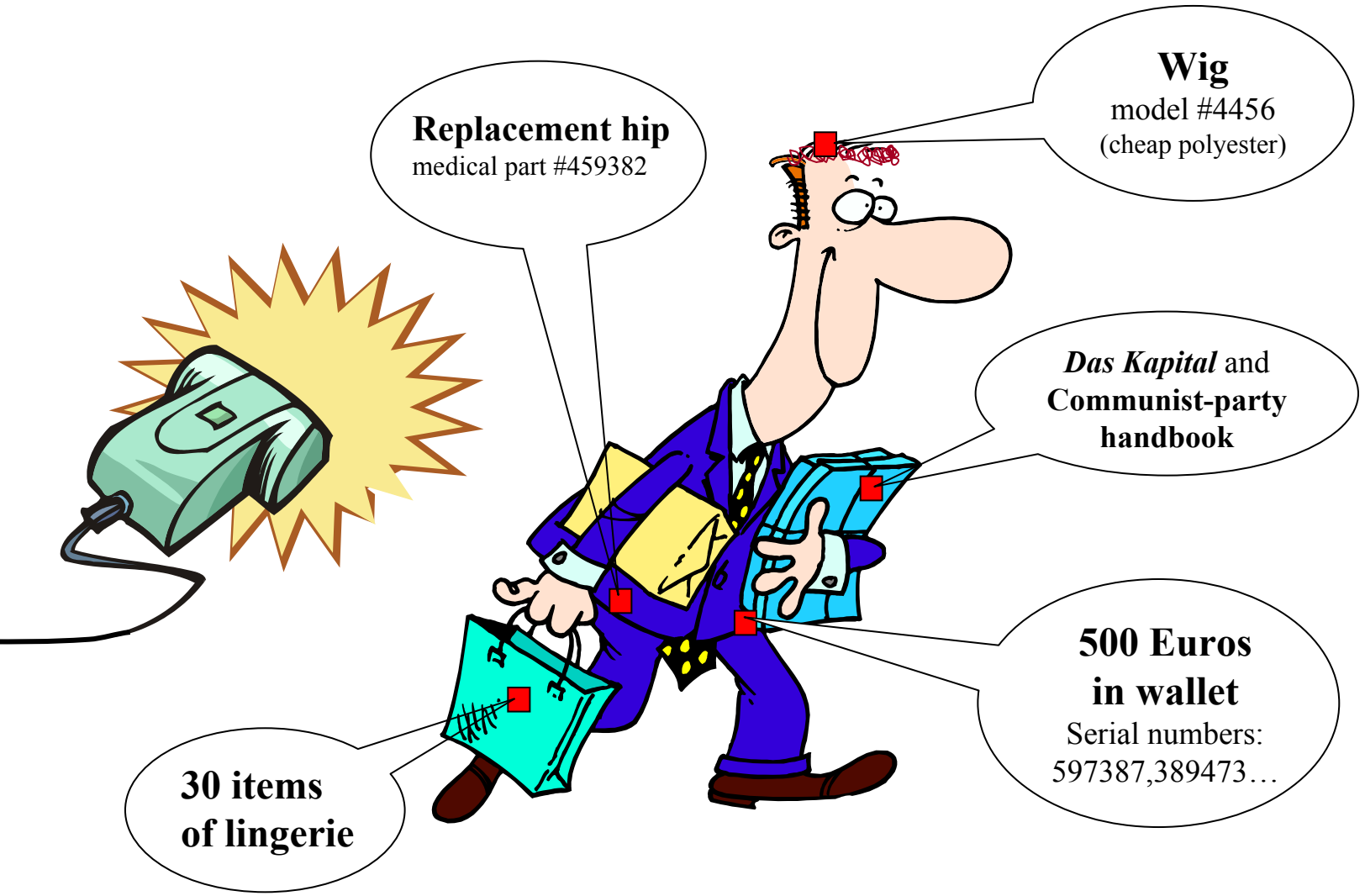
- Smoother inventory tracking
  - Military supply logistics
    - Gulf War I: Placement of double orders to ensure arrival
    - Gulf War II: RFID renders supply chain much more reliable
- Product recalls
- Anti-counterfeiting
- Maintaining shelf stocks in retail environments
  - Gillette Mach3 razor 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 (?)

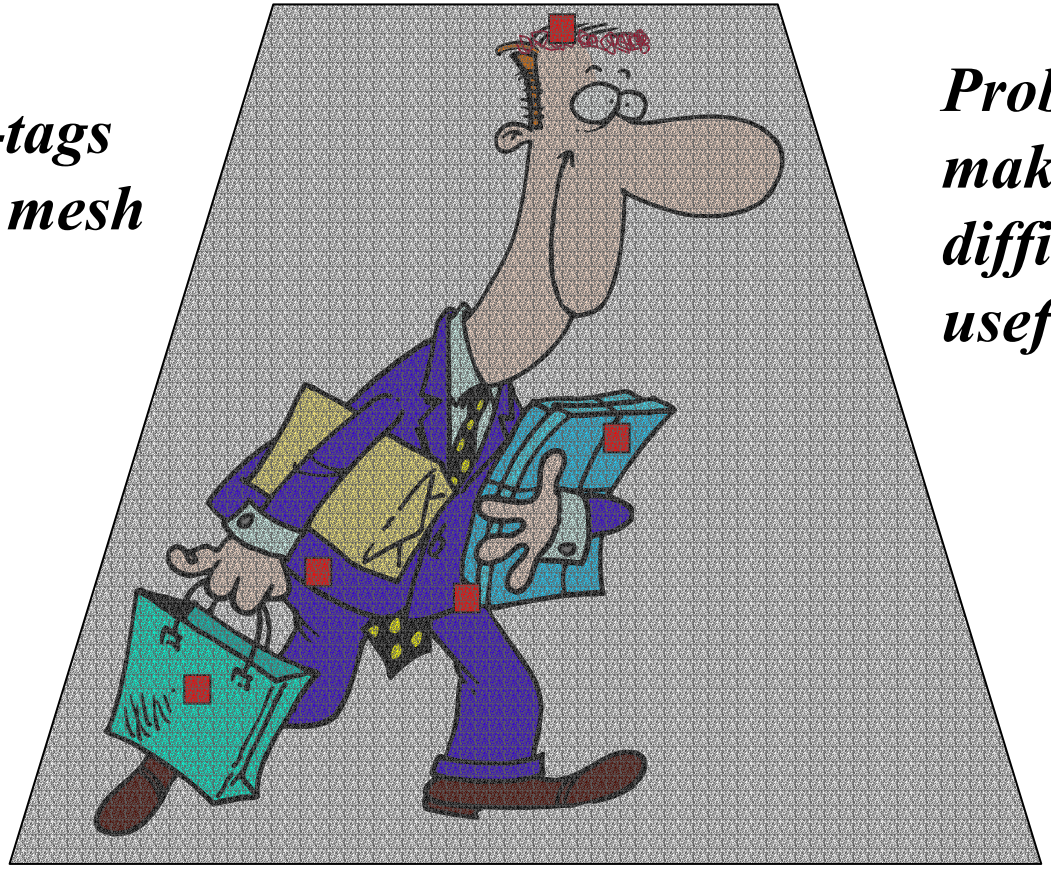
The Consumer-Privacy Problem

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

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

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

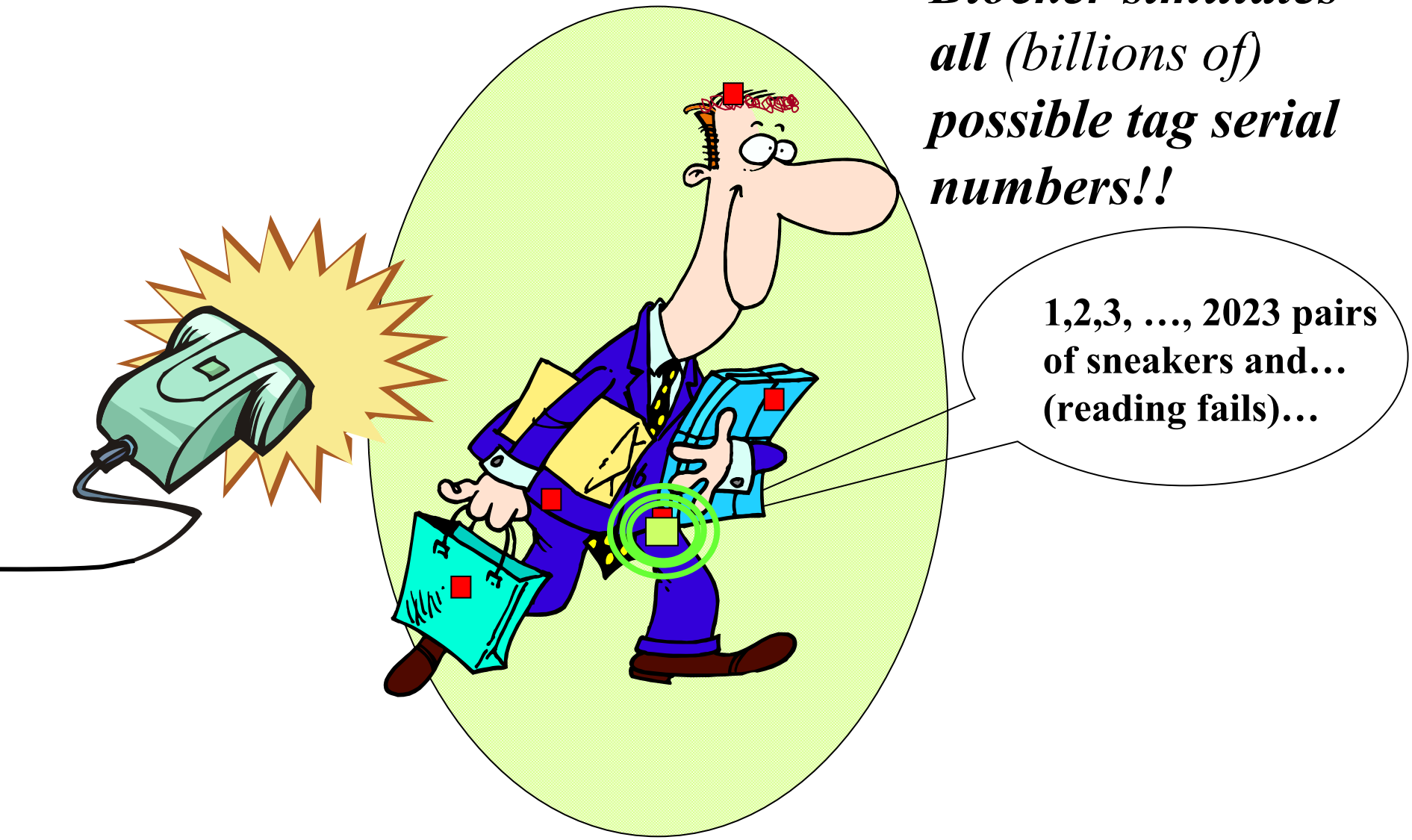
1. Deployed naïvely, embedding of RFID tags in consumer items presents a serious danger to privacy.

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

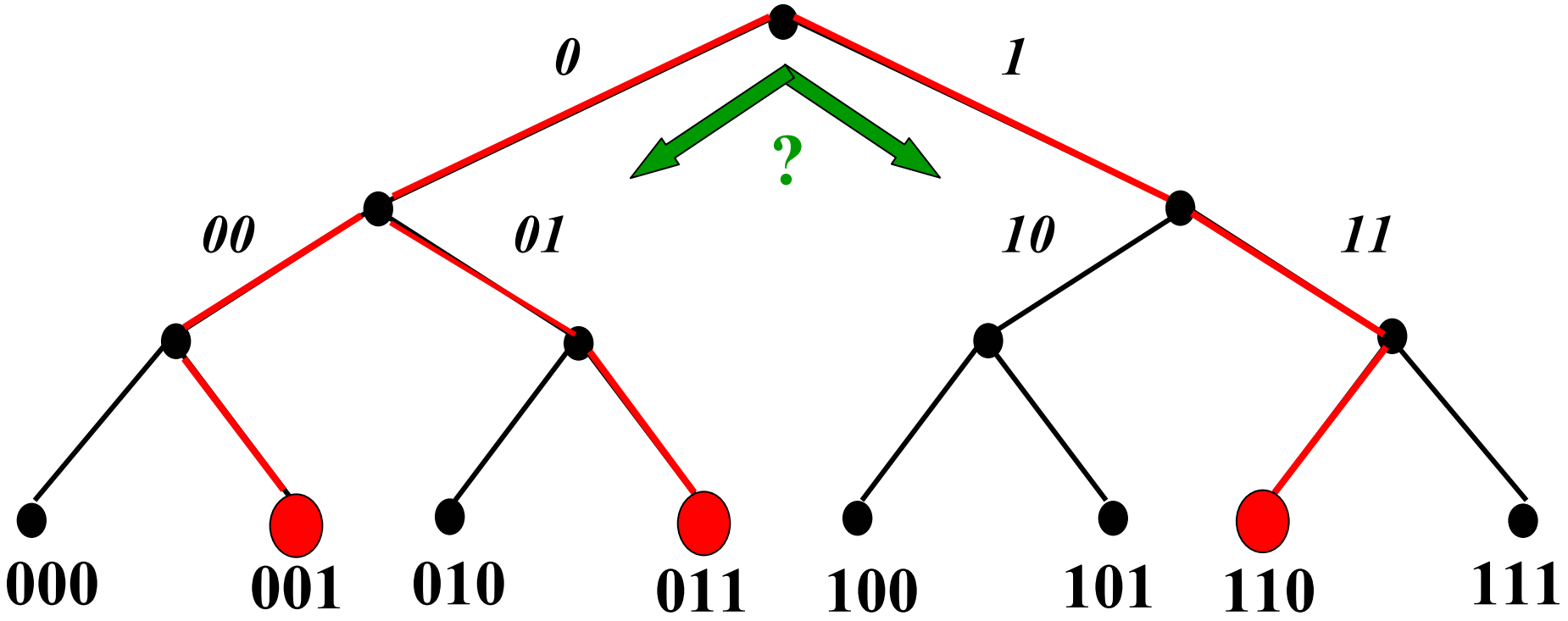
The “Blocker” Tag

“Blocker” Tag

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



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



In a nutshell

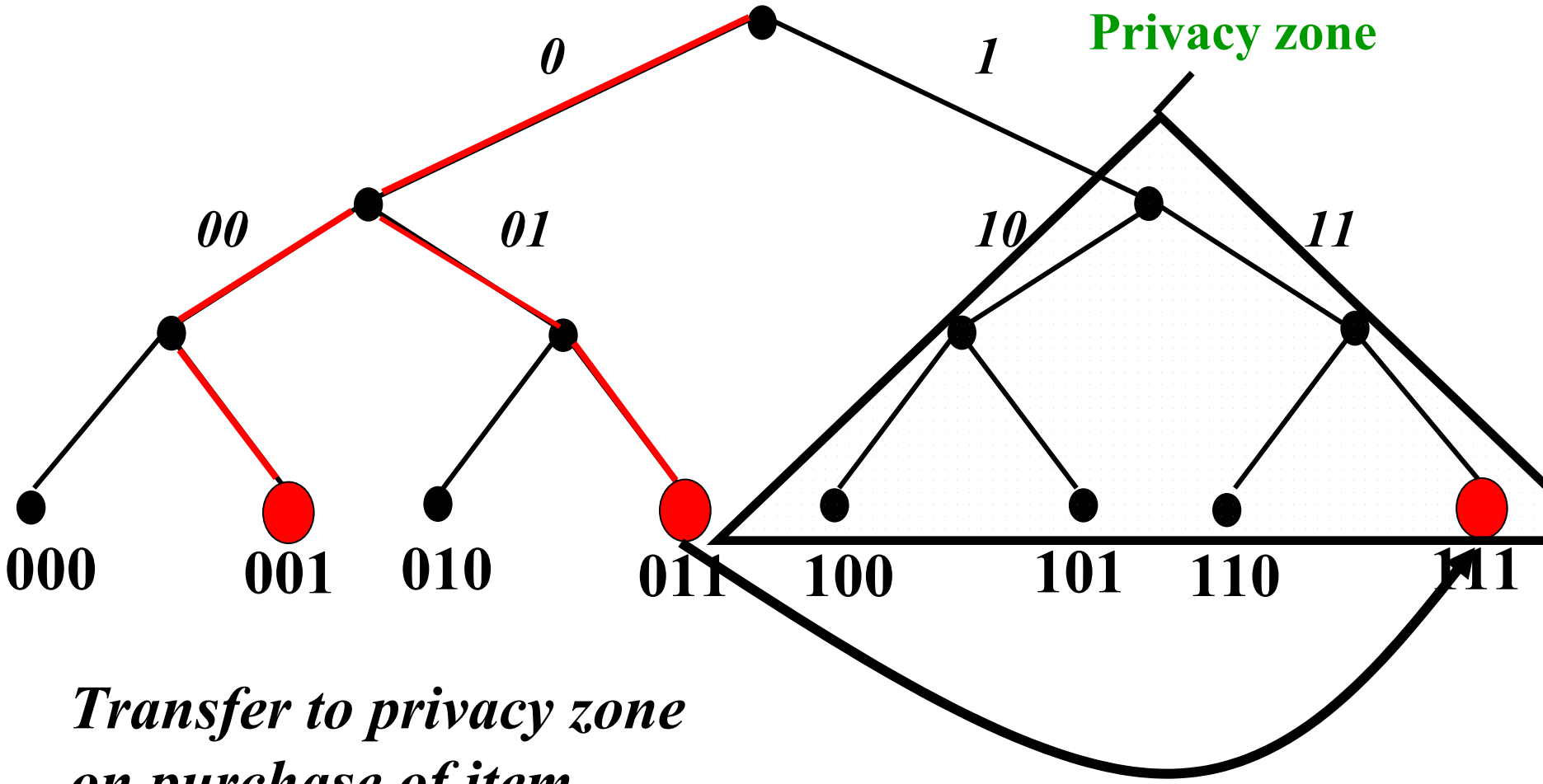
- "Tree-walking" protocol for identifying tags recursively asks question:
  - "What is your next bit?"
- Blocker tag always says ***both '0' and '1'***!
  - Makes it seem like *all* possible tags are present
  - Reader cannot figure out which tags are actually present
  - Number of possible tags is *huge*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

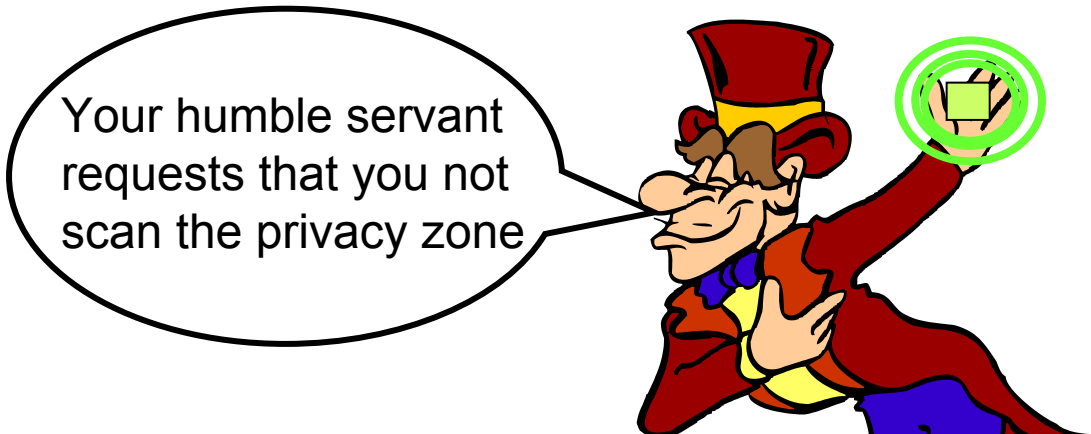
Blocking with privacy zones



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

Final remarks

- Spectrum of RFID devices
  - $0.05 vs. $1.00
- Privacy is not just a consumer issue – it's also a corporate issue
- Privacy is just one of many RFID-related security issues!
  - As "Extended Internet", RFID represents extension of traditional security perimeter
- Legislation and technology most effective in concert

- **"Proponents [of RFID] envision a pervasive global network of millions of receivers along the entire supply chain -- in airports, seaports, highways, distribution centers, warehouses, retail stores, and in the home. This would allow for seamless, continuous identification and tracking of physical items as they move from one place to another, enabling companies to determine the whereabouts of all their products at all times."**
- Contrast a physical reality of RFID tags:
  - Manufacturers struggling with reliability, e.g., UHF tags hard to read near human body!

More about RFID work

- **See ari-juels.com for "blocker" info**
- **Also see:**
  - **MIT RFID Privacy Workshop, 15 November 2003**
    - **www.rfidprivacy.org**
  - **AutoID center: www.autoidcenter.org**
  - **Master's thesis of Steve Weis**
  - **"Bill of Rights" of Simson Garfinkel**
  - **Electronic Privacy Information Center Web site (URL: www.epic.org/privacy/rfid/)**
  - **CASPIAN (yellow journalism) (URL: www.nocards.org)**