High-Power Proxies for Enhancing RFID Privacy and Utility

PETs Workshop
June 1, 2005

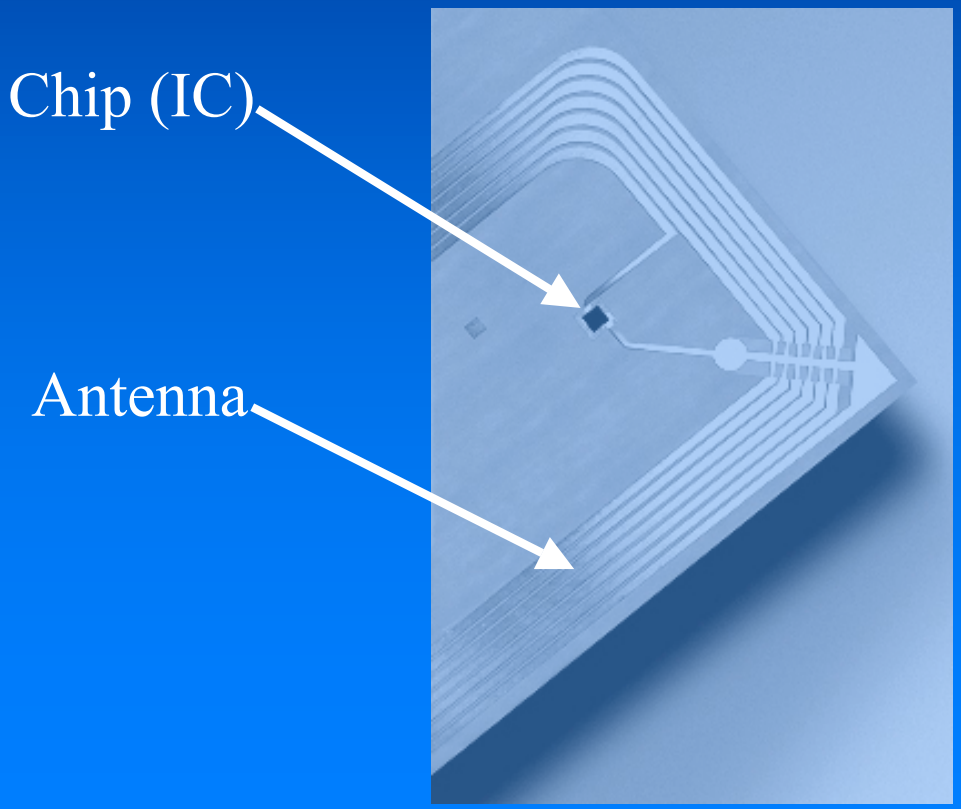
Paul Syverson
Naval Research Laboratory
Joint work with
Ari Juels, Dan Bailey
RSA Labs

Presentation Outline

- Background on RFID
- Security and privacy problems
- Prior technical approaches
- RFID Enhancer Proxy (REP)
  - Overview
  - Four components of REP managing an RFID tag
  - Preventing swapping attacks
- Conclusions

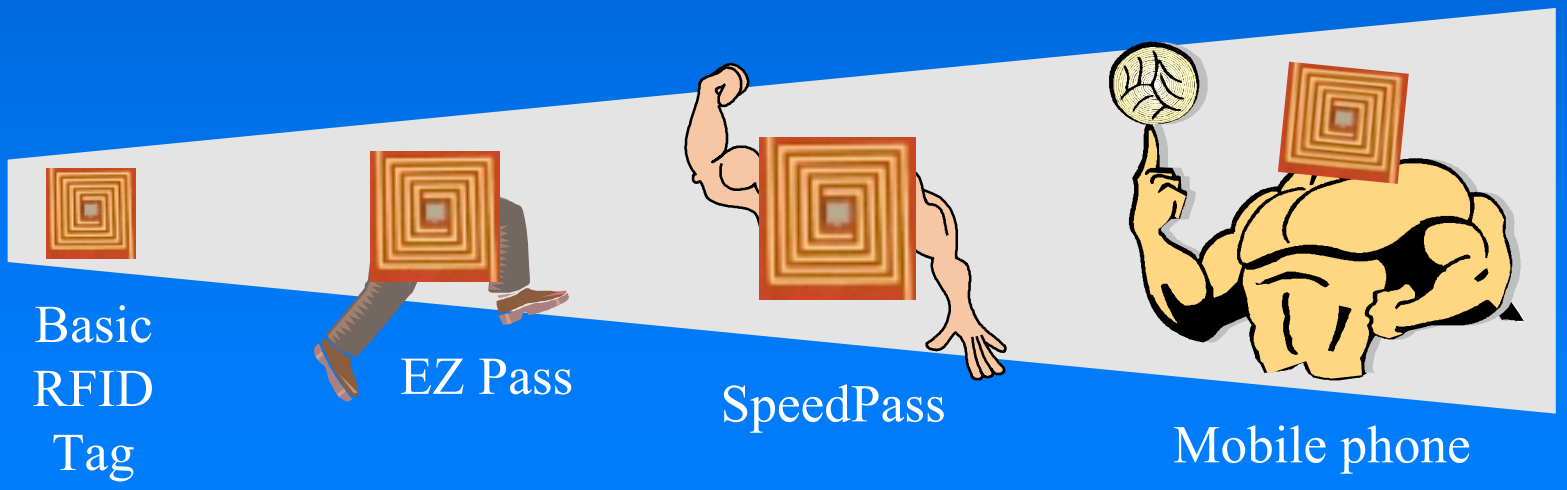
What is a Radio-Frequency Identification (RFID) tag?

- In terms of appearance…



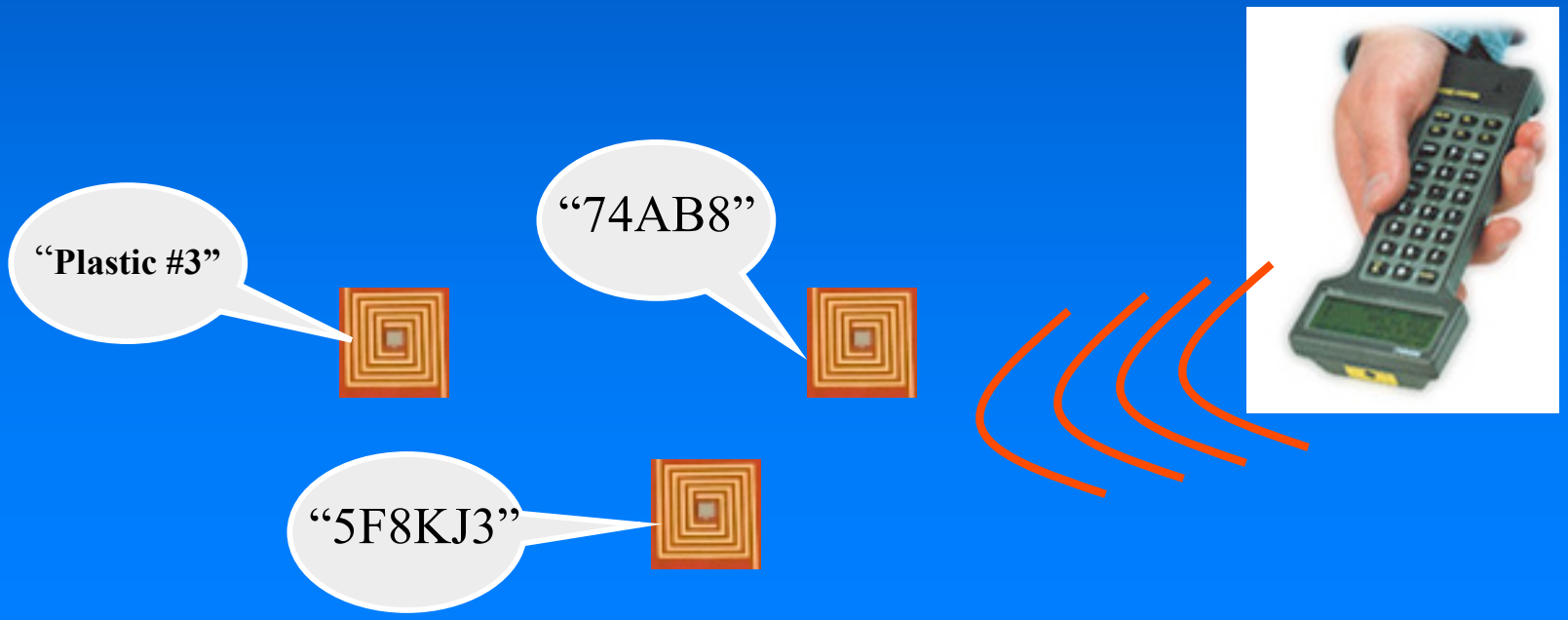
What is an RFID tag?

- You may own a few RFID tags…
  - –Proximity cards (contactless physical-access cards)
  - –ExxonMobil Speedpass
  - –EZ Pass
- RFID in fact denotes a spectrum of devices:



What is a basic RFID tag?

- Characteristics:
  - Passive device – receives power from reader
  - Range of up to several meters
  - In effect a "smart label": simply calls out its (unique) name and/or static data



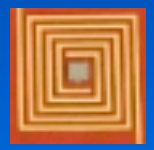
Capabilities of a basic RFID tag

- Little memory
  - Static 64-to-128-bit identifier in current ultra-cheap generation (five cents / unit)
  - Hundreds of bits soon
  - Maybe writeable under good conditions
- Little computational power
  - A few thousand gates
  - Static keys for read/write permission
  - **No real cryptographic functions available**

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, i.e., unique, detailed history. Possibly rewritable.

Some applications

- Better supply-chain visibility -- #1 commercial app
- Theft prevention
- Govt.uses: DHS: Passports, FDA: Pharmaceuticals, Defense: Badging, Inventory, Supply (ordinary materials, munitions, hazardous materials).
- Libraries
- Housepets – approx. 50 million

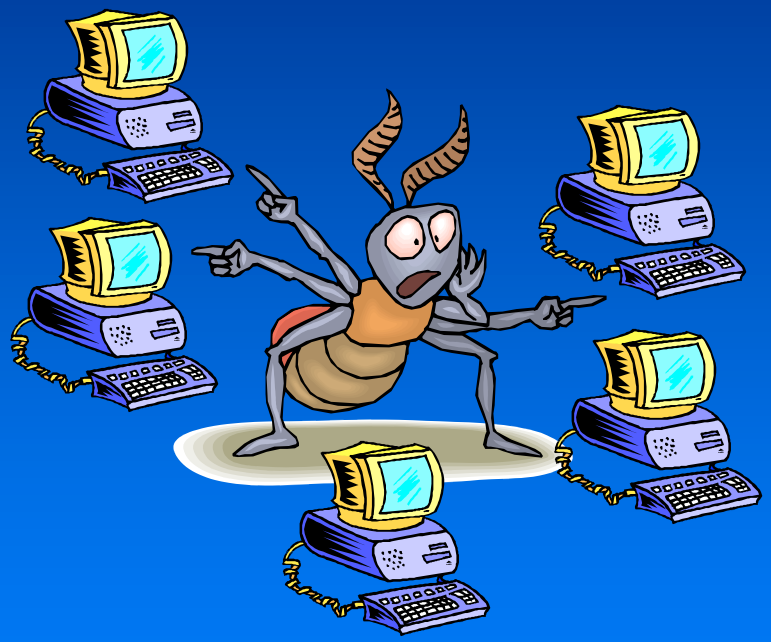
- Parenting logistics
  - Water-park with tracking bracelet
- RFID in Euro banknotes (?)

There is an impending explosion in RFID-tag use

- Wal-Mart requiring top 100 suppliers to start deploying RFID in 2005
- Other retailers and US DoD following Wal-Mart lead
- Pallet and case tagging first -- item-level retail tagging seems years away
- Estimated costs
  - 2005: $0.05 per tag; hundreds of dollars per reader
  - 2008: $0.01 per tag; several dollars per reader (?)
- A broader vision: *"Extended Internet"*

RFID means a world with billions of ant-sized, five-cent computers

- Highly mobile
- Contain personal and/or sensitive information
- Subject to surreptitious scanning
- Again, no cryptography…
  - Access control difficult to achieve
  - Data privacy difficult to achieve



Presentation Outline

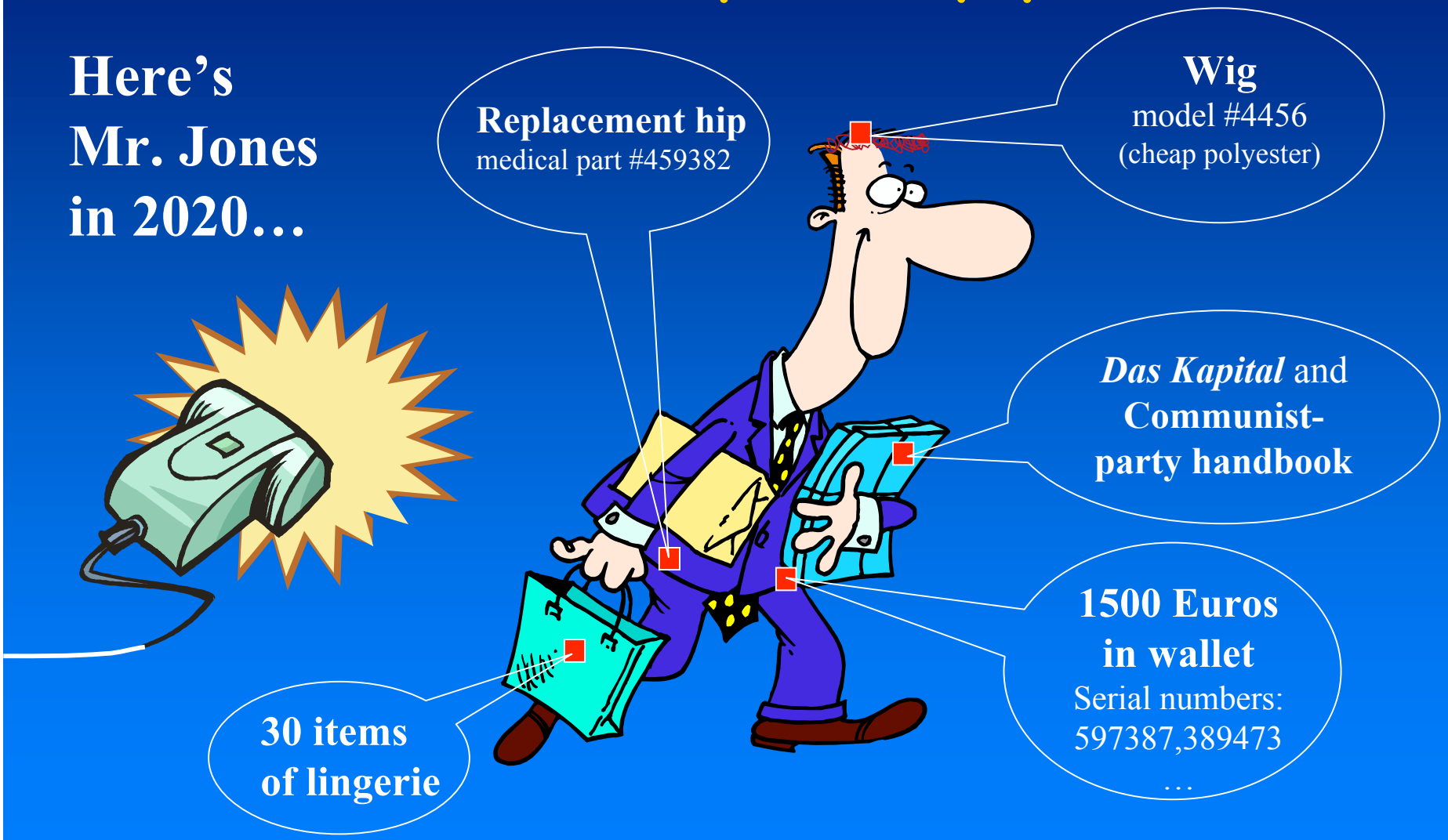
- Background on RFID
- Security and privacy problems
- Prior technical approaches
- RFID Enhancer Proxy (REP)
  - Overview
  - Four components of REP managing an RFID tag
  - Preventing swapping attacks
- Conclusions

The consumer privacy problem

Here's Mr. Jones in 2020…

The consumer privacy problem

Here's Mr. Jones in 2020…



Government and Corporate Security Problems

- Espionage: Privacy is not just a consumer issue
  - Eavesdropping on warehouse transmissions
  - Scanning of shelves for turnover rates
- Tag counterfeiting
  - Automation means dependence!
- Special demands of U.S. Department of Defense
  - "DoD would be like Wal-Mart… if Christmas were a random event every five years, and a stockout meant that everyone in the store could die…" ***-Nicholas Tsougas, DoD***
  - Even that is a logistics view, not a security view.
  - Actually, it's more like Santa's elves spy to see when your stock is low and schedule Christmas then.

Some proposed solutions to the privacy problem

Approach 1: Cover RFID tags with protective mesh or foil

Problem:
Makes locomotion difficult

Approach 2: "Kill" RFID tags

Problem: RFID tags are much too useful in "live" state…

We already have SpeedPass, etc., and then…

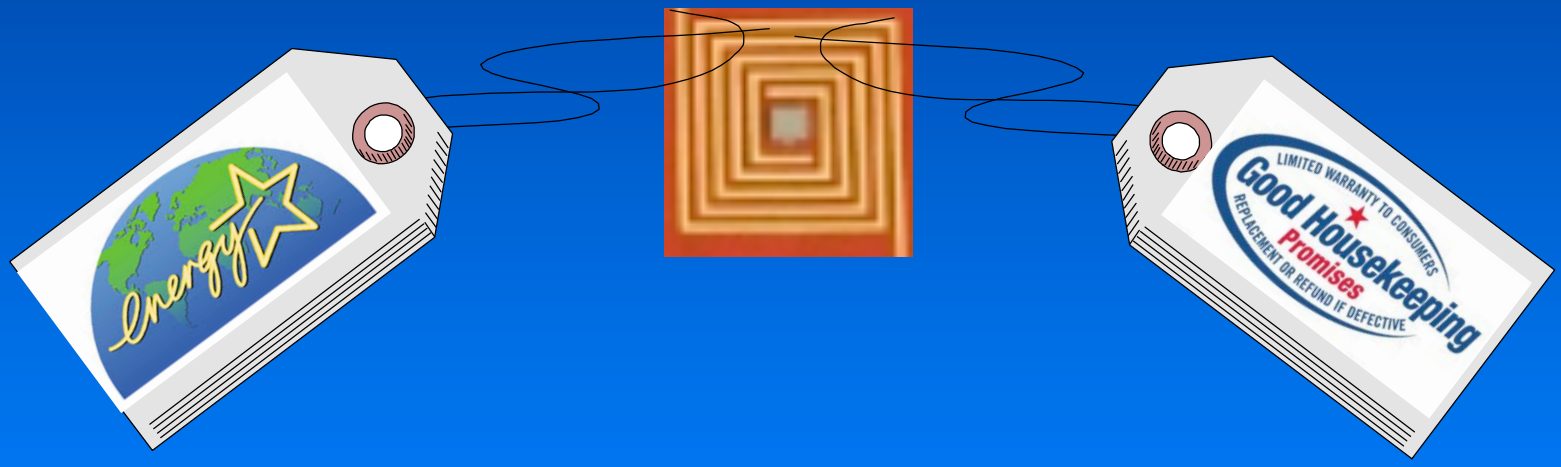
Tomorrow's consumer applications

- Tagged products
  - Clothing, appliances, CDs, etc. tagged for store returns, locatable in house (lost your keys, cordless phone, etc.), replacement parts
- "Smart" appliances
  - Refrigerators: auto create shopping lists, say when milk expires
  - Washing machines that detect proper wash cycle
- "Smart" print
  - Airline tickets that indicate your location in the airport
  - Business cards
- Aids for cognitively impaired, e.g., "smart" medicine cabinets
  - Project at Intel
- Recycling
  - Plastics that sort themselves

Consumers will not want their tags "killed," but should still have a right to privacy!

Approach 3: Policy and legislation

- Undoutedly helpful if thought through well, but…
- "Good Housekeeping" seal



- Retailer's guarantee means little: tags may be read by anyone!
- FTC Section 5 ("Deceptive practices") and the like are similarly limited

Another possible use of RFID

More efficient mugging

Another possible use of RFID

More efficient mugging

"Just in case you want to know, she's got 700 Euro and a Rolex…"

***"and* a US govt. 'Official' Passport"**

Whom will the FTC prosecute now?

And won't help for national security issues

Presentation Outline

- Background on RFID
- Security and privacy problems
- Prior technical approaches
- RFID Enhancer Proxy (REP)
  - Overview
  - Four parts of a REP managing an RFID tag
  - Preventing swapping attacks
- Conclusions

Cryptographers' view of device security – emphasis on "oracle" access

A basic RFID tag cannot survive…

For RFID, can have different and weakened adversarial assumptions

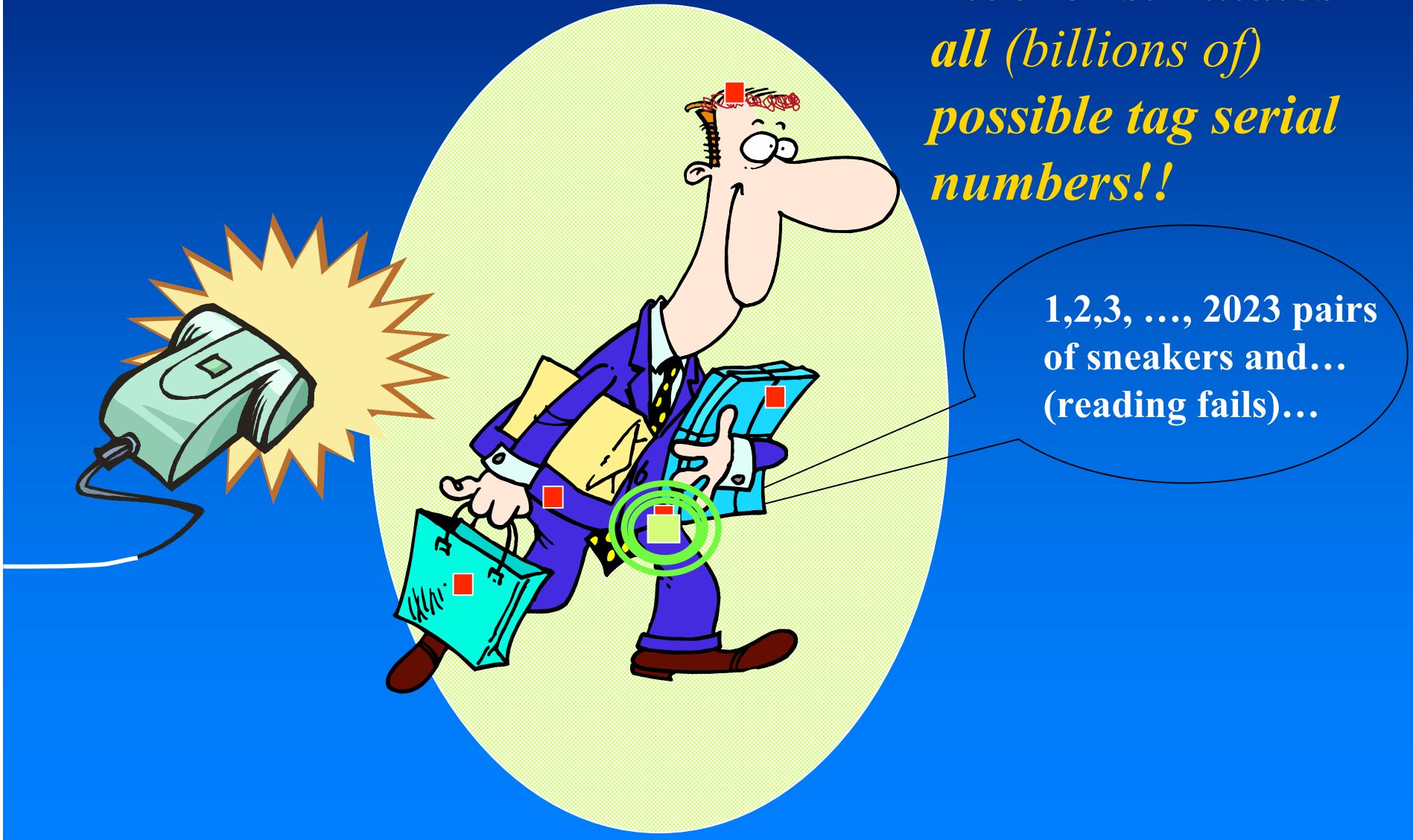
- Adversary is not present 24 hours a day
  - Adversary must be physically close to tag to scan it
- We can deploy security protocols on physical channels – not just logical ones
- External, higher-capability devices can help protect tags

Will not discuss,,,

- Minimalist Crypto [Juels SCN04]
- Approaches using even lightweight hashing or MACs [Juels PerSec04]
- Encryption (except perhaps XOR)
- Basically, anything that assumes tags that are more powerful than today (even at the same cost)

"Blocker" Tag [Juels, Rivest, & Szydlo CCS '03]:

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



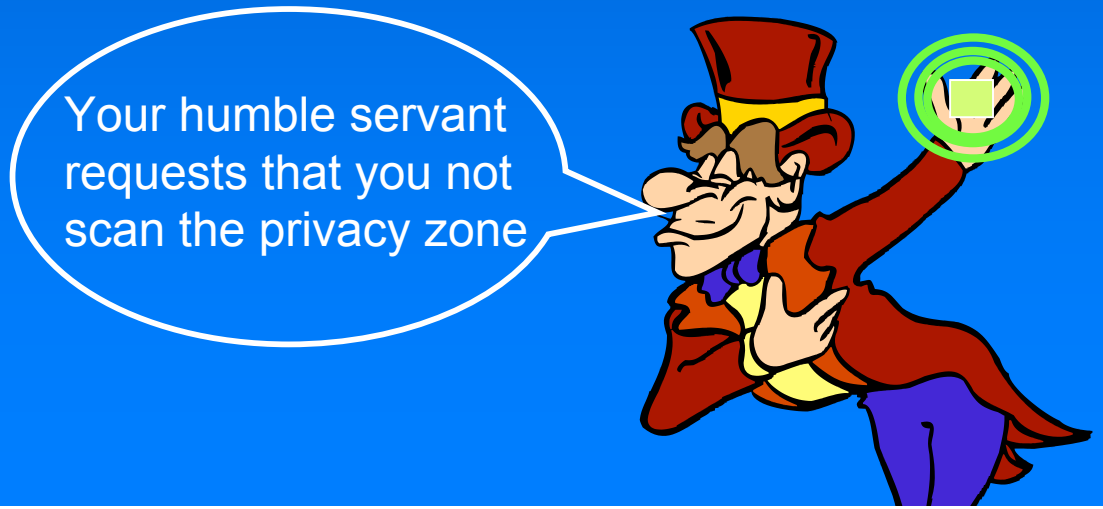
Blocker tag system should protect privacy but still avoid blocking unpurchased items

Selective Blocking

- *Privacy zones:* Only block certain ranges of RFID-tag serial numbers
- *Zone mobility*: Allow shops to move items into privacy zone upon purchase

Polite blocking

- Requests that the reader not scan in the privacy zone



"Soft" Blocking [Juels and Brainard WPES '04]

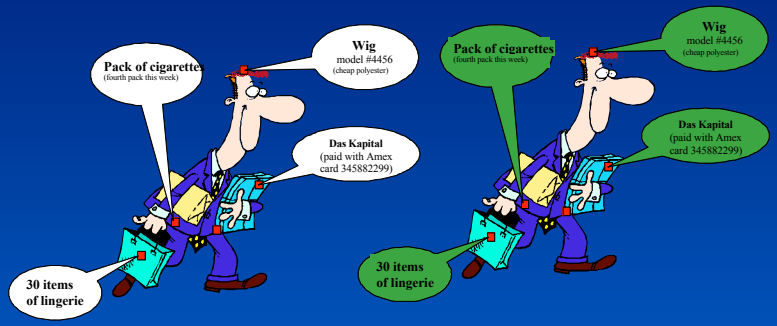
- **Idea**: Implement polite blocking only – no hardware blocking
  - A little like P3P…
- **Advantages**:
  - "Soft blocker" tag is an ordinary RFID tag
  - Flexible policy:
    - "Opt-in" now possible
    - e.g., "Medical deblocker" now possible
- Weaker privacy, but can combine with "hard" blocker

Universal Re-encryption

[Golle, Jakobsson, Juels, Syverson, CT-RSA04]

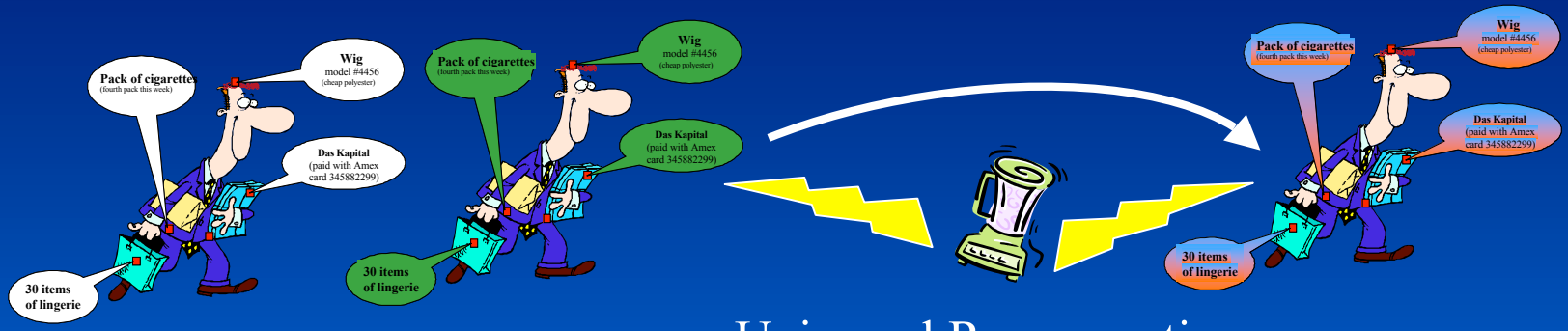
Recall Mr. Jones

Privacy via Universal Re-encryption



Universal encryption with public key at stores

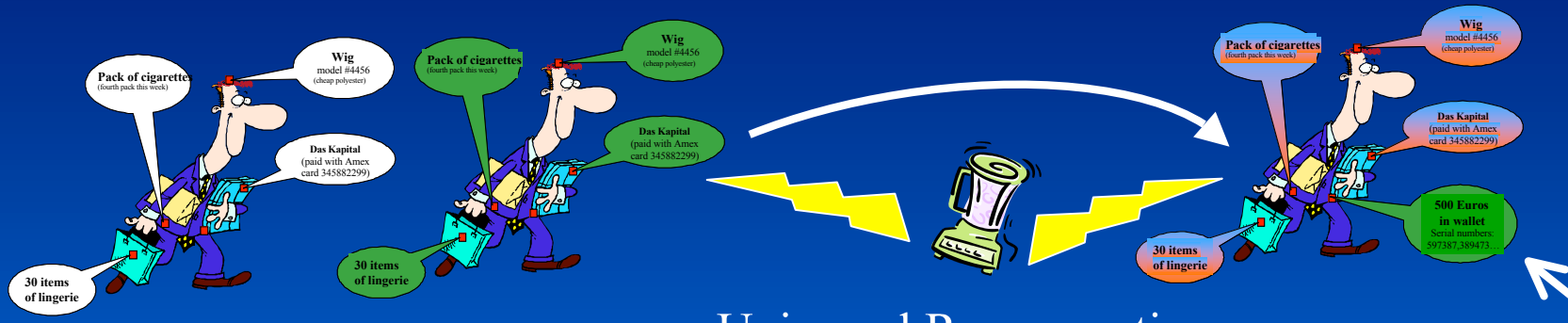
Privacy via Universal Re-encryption



Universal encryption with public key at stores

Universal Re-encryption walking past RF mix

Privacy via Universal Re-encryption



Universal encryption with public key at stores

Universal Re-encryption walking past RF mix

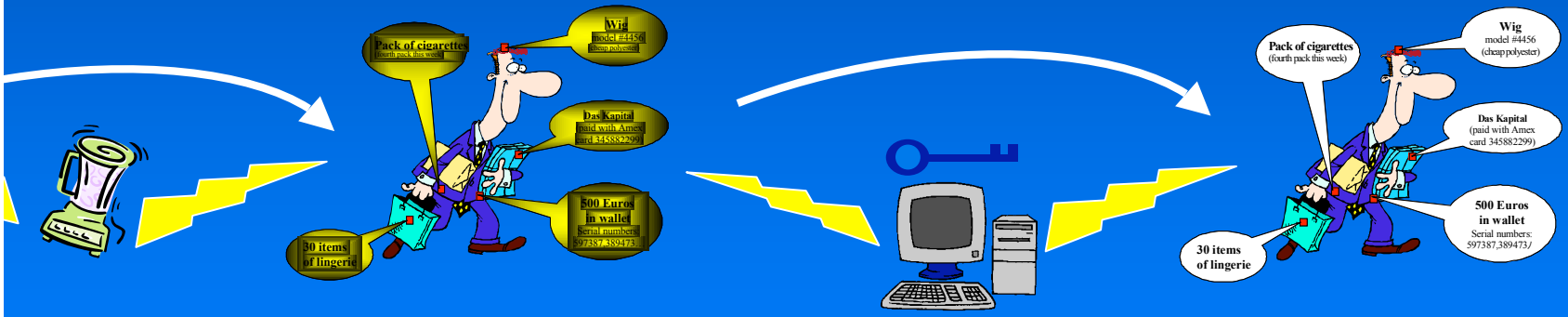
New Purchase (after encryption)

Privacy via Universal Re-encryption

Universal encryption with public key at stores

Universal Re-encryption walking past RF mix

New Purchase (after encryption)



Decryption with private key
(Returning home or as needed)

Limitations of Previous Approaches

- Blocker Tag:
  - Prevents reading of all tags in area irrespective of owner
- Polite/Soft Blocking:
  - Does not protect against "impolite" readers
  - Requires specialized modified readers
  - Does not protect against tracking
- Universal Re-encryption:
  - Does not protect against unauthorized modification such as Swapping Attacks

Presentation Outline

- Background on RFID
- Security and privacy problems
- Prior technical approaches
- RFID Enhancer Proxy (REP)
  - Overview
  - Four parts of a REP managing an RFID tag
  - Preventing swapping attacks
- Conclusions

REP (RFID Enhancer Proxy)

- Main Idea: REP *represents* the tag in interactions with readers
  - Small high-power device, often carried on your person
  - Hides tag values
  - Changes tag appearance to prevent tracking
  - Simulates and enhances tag signal for weak or distant readers
  - Basically all the functionality of previous approaches (and more) without the drawbacks

Your personal REP

- Could be incorporated in other devices
- Nokia offers mobile phone RFID kits since 2004
- Example applications quoted from Nokia RFID kit site
  - **Service Professional:** Touch the item to be serviced and you will get up to date service information.
  - **Security:** Attach tags to sites that are visited by security guards. Get accurate time stamps and proof of work done.
  - **Visual Phone Directories:** Attach a tag behind a person's photo to initiate a call to them. Simplify making phone calls for those not used to mobile phones or those who have physical limitations. Create personal directory for children or the elderly.
  - **Distress Assistance:** Touch a tag on your clothing such as a belt, and the phone initiates an emergency call.

REP Actions

- Tag Acquisition
- Tag Relabeling
- Tag Simulation
- Tag Release

REP Actions: Tag Acquistion

- Tag data transferred directly to REP
  - At shop checkout via Bluetooth
  - In supply chain via IrDA, Bluetooth, ZigBee
- Tag data could be acquired out of band on authenticated channels
  - Keys could be barcoded on tag for optical scan
  - Resurrected Duckling paradigm (physical contact restores acquired state)

REP Actions: Tag Relabeling

- During time interval t REP assigns k-bit pseudonym $p_{t,i}$ to tag i
- Integrity Problem: Anyone can relabel tag to any value
- Can authenticate writes with pseudonym:

  REP $\rightarrow$ i: $p_{t-1,\,i}$

Attacking Integrity of Tag Relabeling

- Adversary Eve can eavesdrop on high power signal from REP to tag (forward channel)
- Could, e.g., use PIN exchanged during tag acquisition to protect new writes

  During interval $t-1$, REP $\rightarrow$ i: $p_{t-1,\,i}$ XOR PIN

  During interval t, REP $\rightarrow$ i: $p_{t-1,\,i}$
- Eve in forward range during $t-1$, t learns PIN

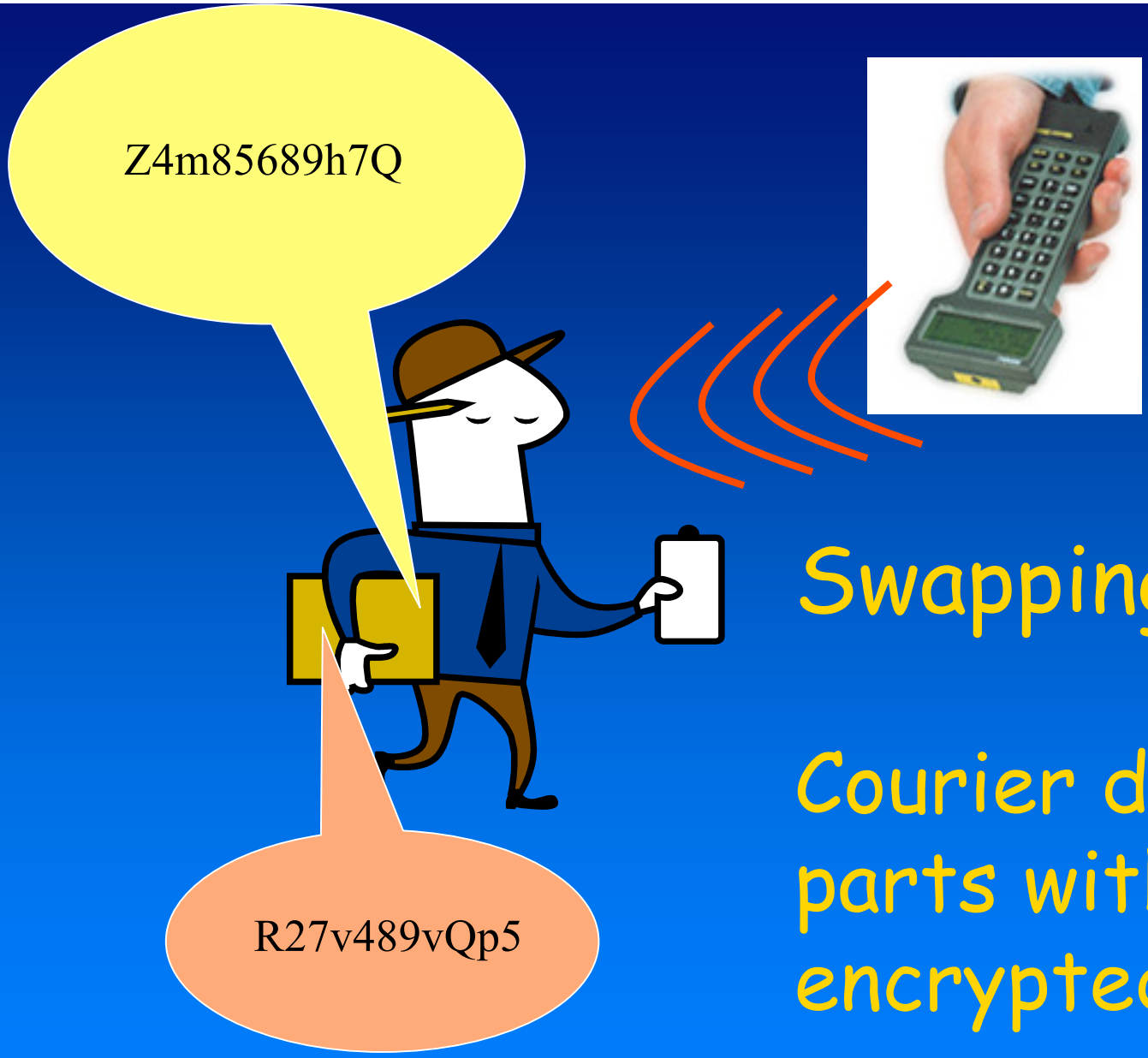
Attacking Integrity of Tag Relabeling (2)

- Can play games with only sending PIN in clear on lower power back channel (tag to REP)
- Eve in forward channel range for two intervals and back channel range for one gets PIN and/or pseudonym

Attacking(?) Integrity of Tag Relabeling

- So what?
- At worst the result is Denial of Service,
  - No confidential information is leaked to attacker

- Tags are no longer being relabeled: trackable
- Beeper or light on REP can alert owner to acquisition loss
- Owner can reaquire the tag by inspection



Swapping Attack:

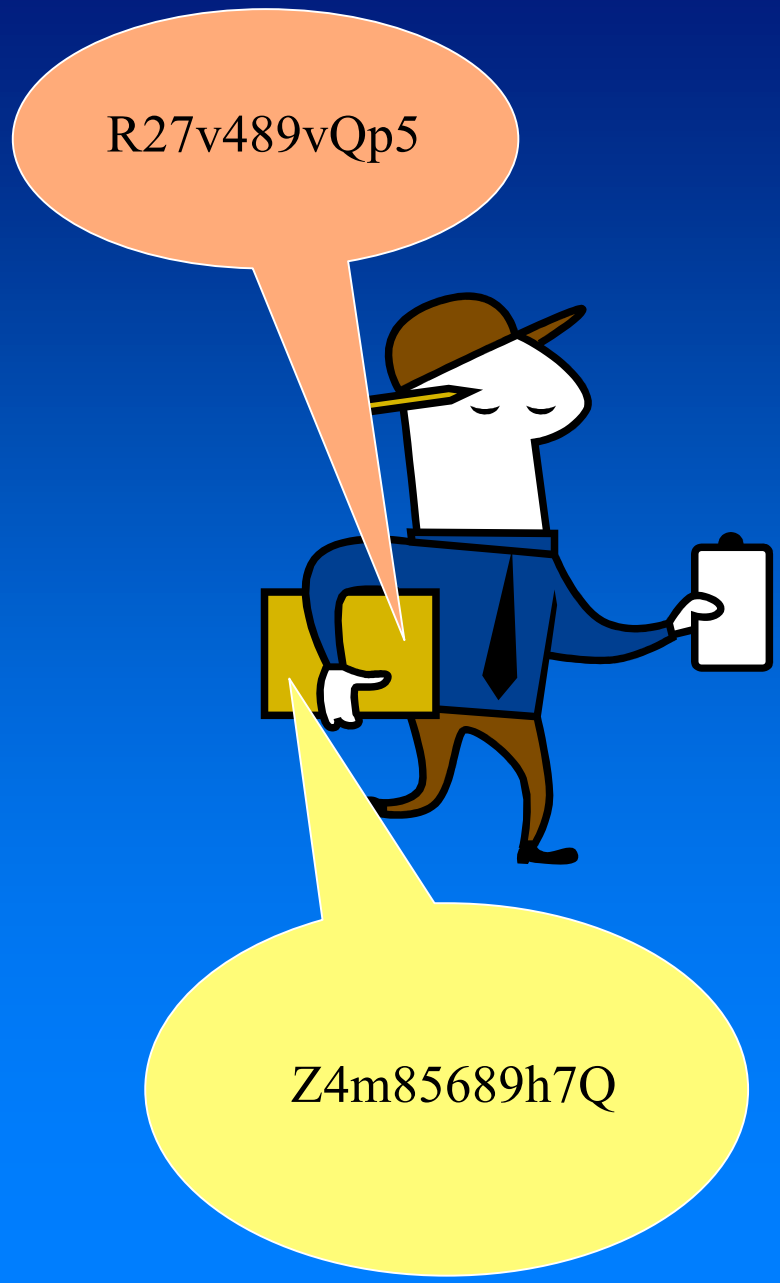
Courier delivering parts with encrypted tags

Swapping Attack:

Courier delivering parts with encrypted tags

Swapping Attack

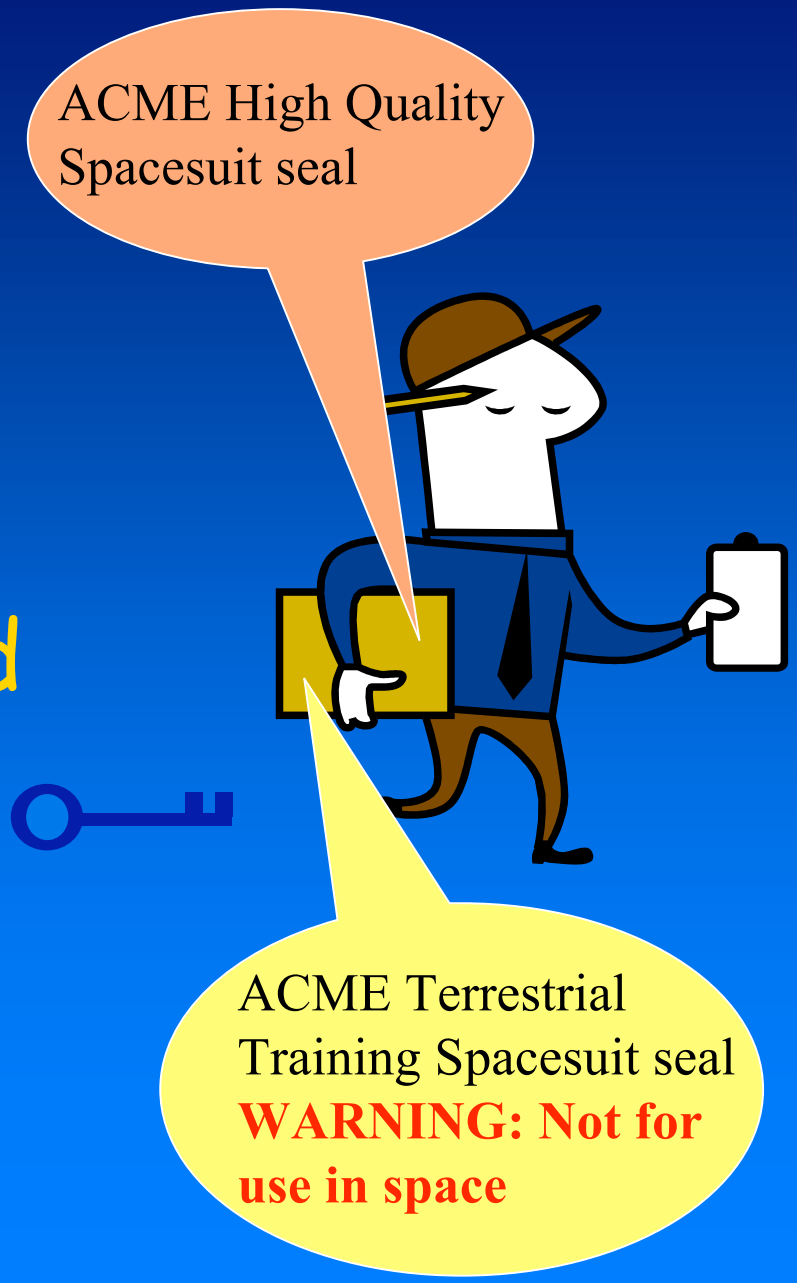
- Courier arrives at supply depot



Swapping Attack

- Courier arrives at supply depot

- Tags are decrypted




Houston, we
have a problem


BOOM!!

Preventing Swapping

- Tags can generate small amount of randomness
- Tags can dictate (part of) their next pseudonym
- Only accept a pseudonym that matches on the tag generated part
- Will that work?

Example

- Suppose a pallet with 100 tags
- Tags relabeled once per minute
- Suppose tag can generate 32-bit nonce
- Adversary attacking persistently for a day (1440 minutes) has probability of successful swapping attack =

  $(1- (1 - 99/2^{32}) \times 1440 < 0.000034$

Tag simulation

- REP has higher send/receive power than tags
- Can simulate tags in unfavorable environments
  - warehouse with metal drums of liquid, etc.
  - what is inside shipping container it is on outside of
- Can communicate with farther readers
- Can communicate with different type devices

Tag simulation (2)

- REP has higher computational power than tags
  - REP can store and manage much more information about items than tags
  - REP can have much more sophisticated policy for managing item information

Tag simulation examples

- Tag can simulate Patek Philippe watch while in upscale shops, otherwise it's a Timex
- Can easily acquire and carry info about your fridge to get parts or match pattern, color at appliance store
- Can simulate nonexistent inventory or not simulate present inventory to complicate stock espionage
- Could become a blocker tag or dynamically obfuscatory if it detects unauthorized activity,
  - e.g., readers should do inventory at some known (secret?) schedule

Tag release

- When item is left home, sold to customer, etc. REP will release tag, restore state
- May want to restore "property bits", but not unique identifier bits
  - E.g., 100g bar of Toblerone chocolate, but not candy bar # 3e84a7c25,
- May want to restore identity bits
  - E.g., a specific copy of a book returned to library
  - E.g., if an item's warranty is tied to serial number

How to know when to release Tags

- Environmental cues:
  - House system tells REP "You're home now REP. Lay down your burden and release your tags."
- Item is sold:
  - Cashier touches it to/waves it near release device
- Detect loss of control:
  - By varying power, REP can determine that item is moving away and release it while it can

Conclusions

- RFIDs are coming… with big privacy/security problems
- Introduced REP: a device that renders RFID tags effectively dormant and simulates them to other devices
  - Improves security and privacy of RFID tag use
  - Requires no specialized tags or tag readers
- First effective mechanism against swapping attacks on writable simple tags