RFID Security and Privacy

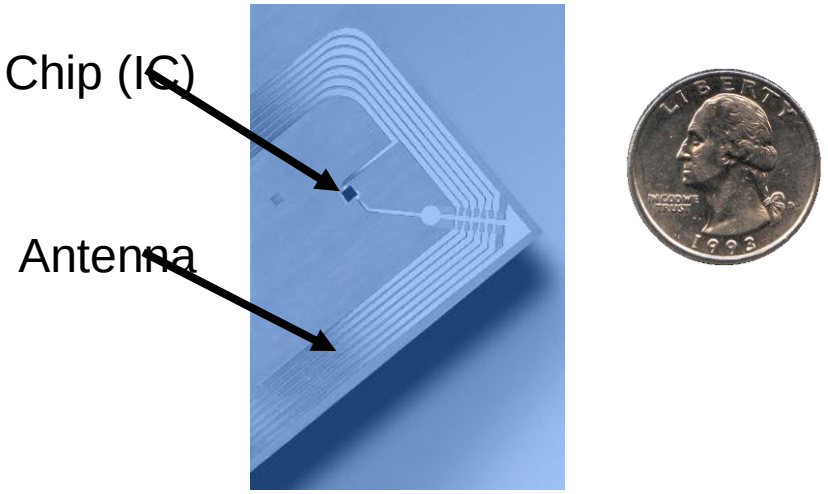
- RFID systems
- Security and Privacy Issues
- Countermeasures

Outline

- RFID systems
- Security and Privacy Issues
- Countermeasures

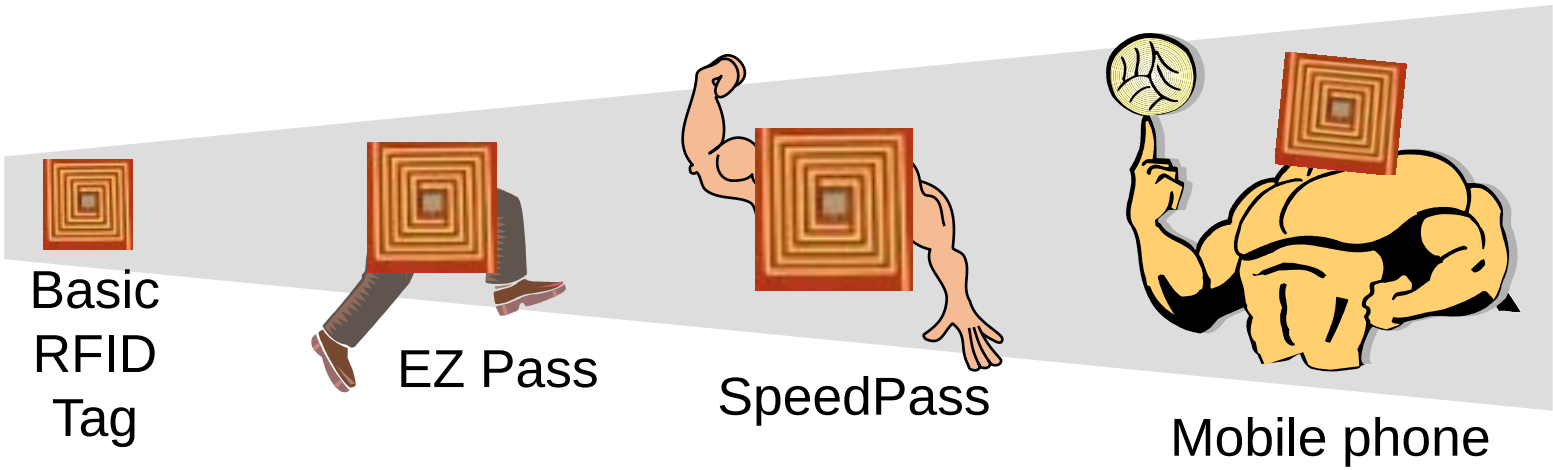
What is a **R**adio-**F**requency **Id**entification (RFID) tag?

- Miniaturized devices
  - Work passively (no battery)
  - Enable automated identification in numerous applications and circumstances
    - Through the identification information stored on tag
- In terms of appearance…



What is an RFID tag?

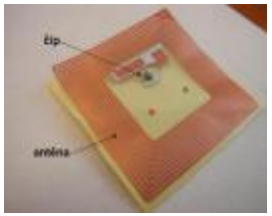
- You may own a few RFID tags…
  - Building access-card
  - RFID credit card
  - EZ Pass
  - E-passport
- RFID in fact denotes a spectrum of devices:



RFID technologies vary widely

ISO 14443 (proximity cards)
E-passports, ID cards
US$5

ISO 15693 (vicinity cards)
Library books
US$0.50



EPC
WalMart
US$0.20

3DES, RSA

sym.-key crypto

no crypto

Computation →

10cm

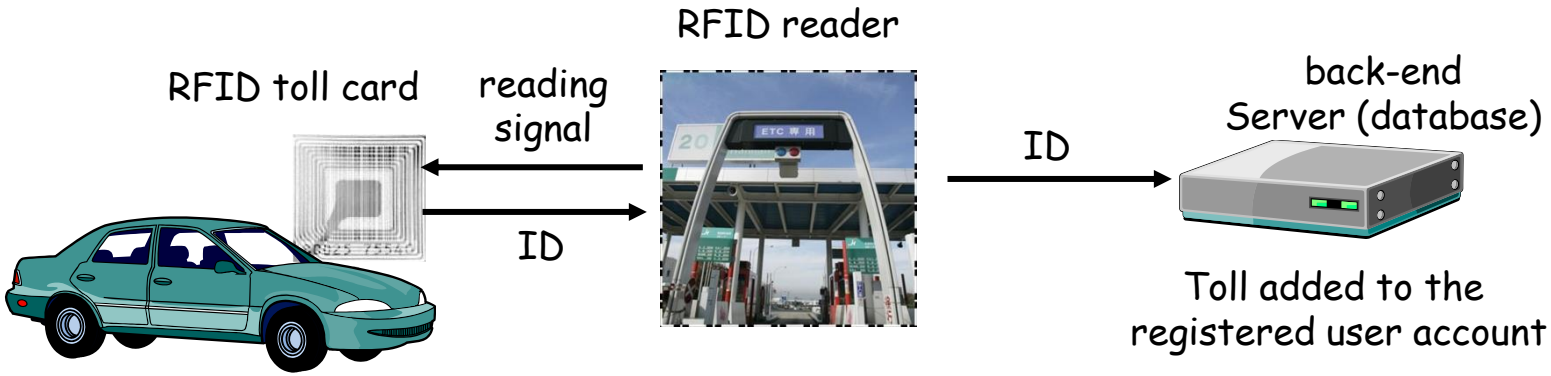
1m

3m

Intended read range →

RFID System

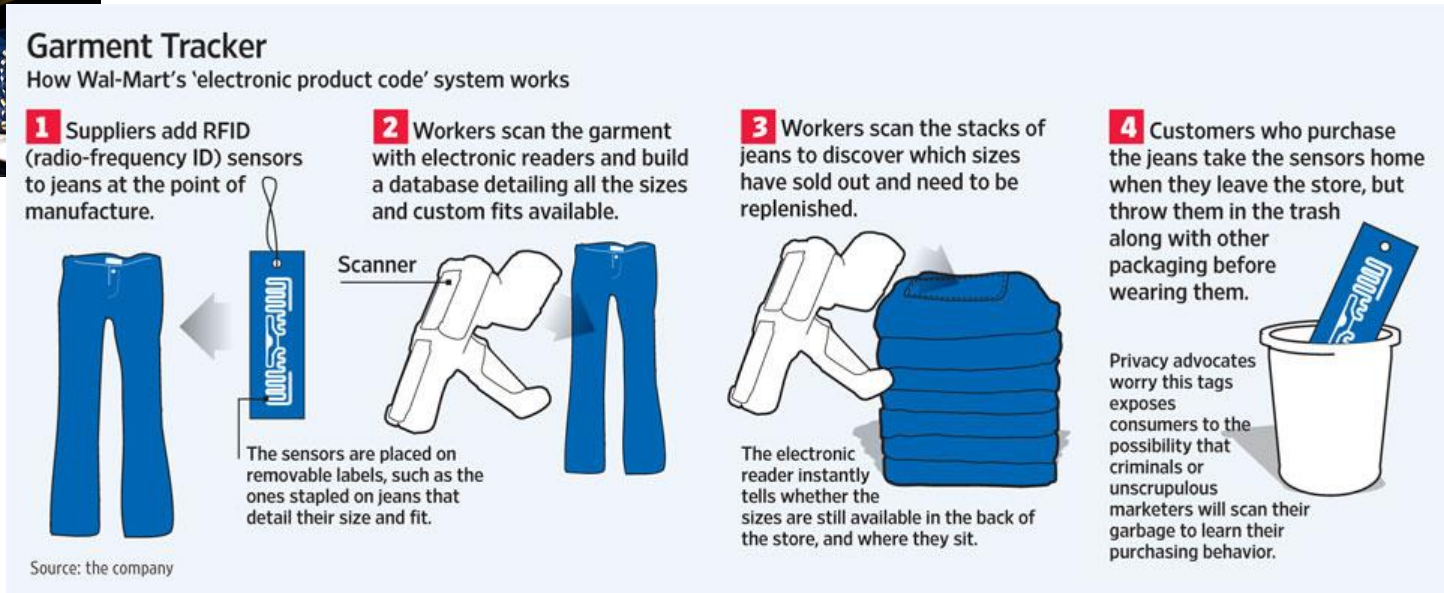
- RFID system elements
  - RFID tag, RFID reader, and/or back-end database
- Tag
  - Also called responder
  - Stores identification info about its corresponding subject
  - Powered up by reader
  - Responds to reader interrogation with the identification info
- Reader
  - Also called interrogator
  - Broadcast queries to tags for the identification info
  - Forward such info to the server
- Back-end database
  - Upon receive info from reader, process to identify the associated object
  - Make decision to take proper actions
    - Updating inventory, opening gate, charging toll, or approving transaction



Prominent RFID Applications

- Supply chain management (inventory control)

- Wall Street Journal, July 23, 2010
  - **Wal-Mart Radio Tags to Track Clothing**

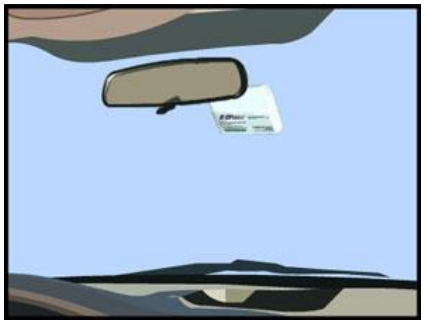


Prominent RFID Applications

- RFID Passports or e-Passport
- Stores:
  - The same data visually displayed on the data page of the passport;
  - A biometric identifier in the form of a digital image of the passport photograph, which will facilitate the use of face recognition technology at ports-of-entry;
  - The unique chip identification number; and
  - A digital signature to protect the stored data from alteration
- Allows:
  - Customs and Border inspectors to quickly access photographs and other biographical info stored in secure government databases
  - Automated terrorist watch list checks without impeding traffic flow
  - An entire car of people to be processed at once since multiple cards can be read at a distance and simultaneously

Prominent RFID Applications

- Electronic Toll Collection System
- Benefits
  - Excellent read accuracy even when vehicles are travelling at high speed
    - No need to stop at toll booth
    - Avoidance of long-queue waiting
      - Prior to ETC, for a queue of 20 vehicles, it took up 3 minutes to process
      - With ETC, virtually no queues as the processing time is only 3.6 seconds for a 1000 vph ETC lane
    - Reduction of fuel consumption
    - Increase in driver satisfiability
  - Automatic RFID identification
    - Reduce the need for employee
    - Lower the operation cost



- Worldwide deployment
- In the US
  - 26 states adopted ETC systems
  - Developed by different companies
    - E-Zpass is the most popular one
      - 24 members in 14 states

Prominent RFID Applications

- Medical Implants

- **Miniature implant monitors cardiac pressure (**http://www.gizmag.com/miniature-sensor-heart-angiography/16680/)
  - Miniature sensors are implanted into the wall of the patient's heart
  - Cardiac pressure readings can then be transmitted at any time to the attending physician
  - Readings taken "on demand" – the reader device supplies energy via induction

The IMS (Fraunhofer Institute for Microelectronic Circuits and Systems) heart sensor system involves implanting battery-free miniature sensors .

More applications

- Access control to building, transportation
- Smart car keys
- Various payment cards and credit cards
- Tagging pets
- …

Near Field Communication (NFC)

- NFC is yet another upcoming RFID technology
- An NFC-equipped device, such as a smartphone, can work as both RFID tag and reader.
- It allows a variety of applications from smart poster to mobile payments

- In particular, the use of NFC-equipped mobile devices as payment tokens (such as Google Wallet) is considered to be the next generation payment system and the latest buzz in the financial industry

30% of all sold mobile phones in 2011 are NFC-enabled

Payments using NFC will reach $670 billion by 2015

Creating NFC network effects through platforms and partnerships

Technology companies, financial institutions, and telecommunication providers have worked together and started running test programs of NFC based system in the US.

Outline

- RFID systems
- Security and Privacy Issues
- Countermeasures

RFID Security and Privacy

- RFID systems are plagued with a wide variety of security and privacy vulnerabilities due to the inherent weaknesses of the underlying wireless communication

- Tag-specific information is easily subject to eavesdropping, unauthorized reading, owner tracking, and cloning

- Providing security and privacy services are challenging
  - Partly due to constraints of tags in terms of computation, memory, and power
  - Partly due to the strict usability requirements imposed by RFID applications (originally geared for automation)

Attacks

- Eavesdropping
- Unauthorized reading
- Owner inventory checking
- Owner tracking
- Cloning

- **Relay attacks**
  - Ghost-and-Leech
  - Reader-and-leech

- Lost and theft

Pretty well addressed though in a not satisfying way

Battling ….

Not or at lest less addressed ….

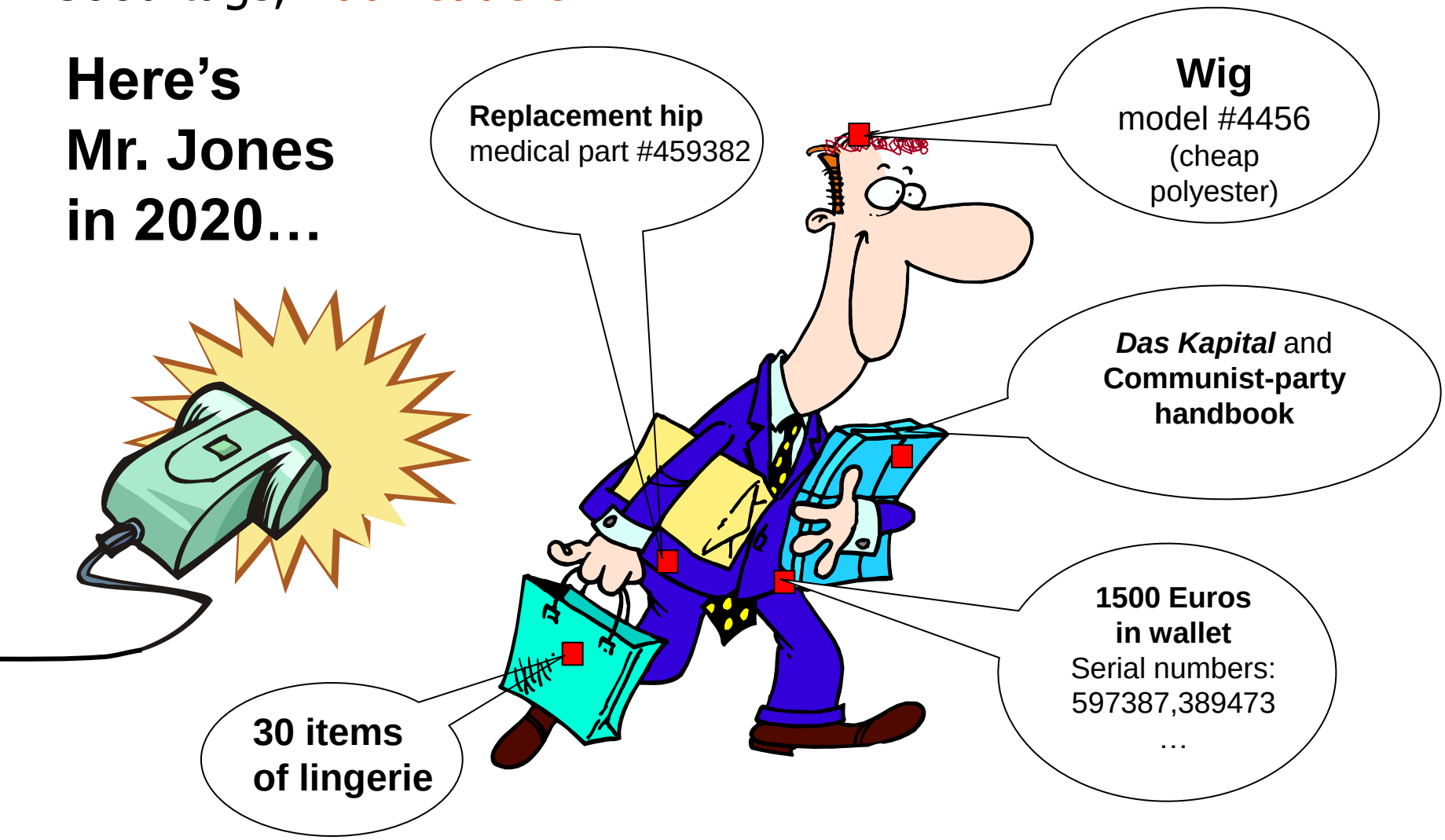
Unauthorized Reading

- RFID tags usually respond to reader queries promiscuously
  - Sensitive tag information easily subject to unauthorized reading
  - Anyone who possess a reader can get tag information
  - Tag info can be further used to track user, clone tag, and impersonate the user

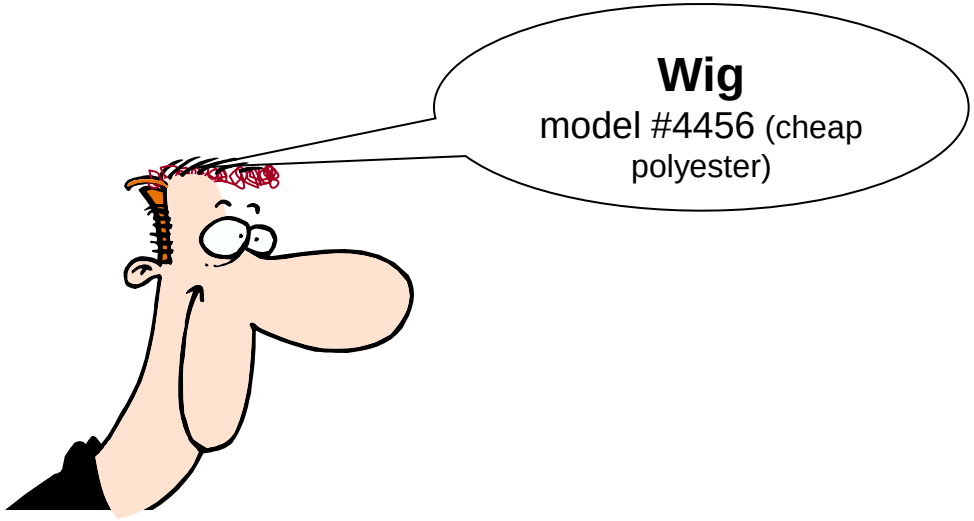
- Unauthorized reading also the ghost-and-leech relay attacks

The consumer privacy problem

Good tags, Bad readers



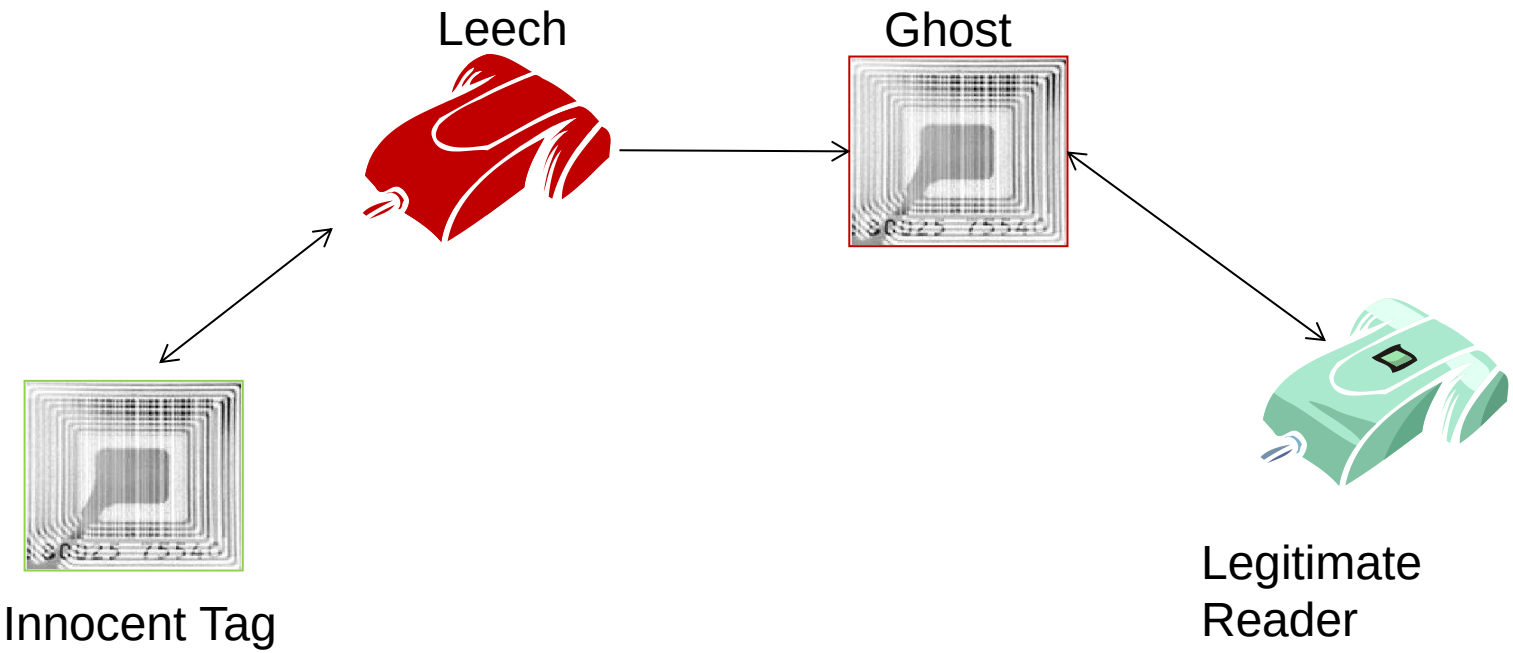
…and the tracking problem



- Mr. Jones pays with a credit card; his RFID tags now linked to his identity; determines level of customer service
  - Think of car dealerships using drivers' licenses to run credit checks…
- Mr. Jones attends a political rally; law enforcement scans his RFID tags
- Mr. Jones wins Turing Award; physically tracked by paparazzi via RFID

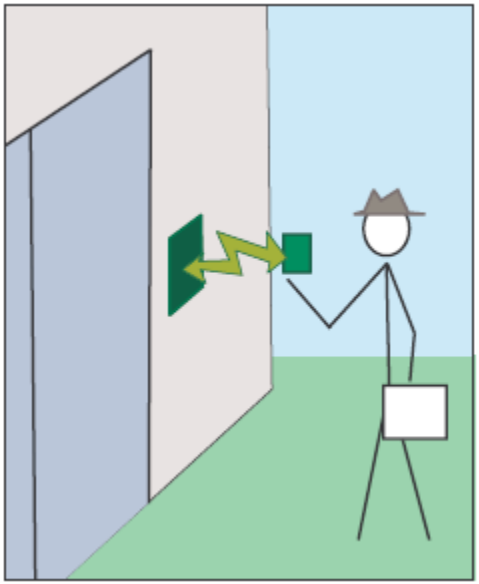
Ghost-and-Leech Relay Attack

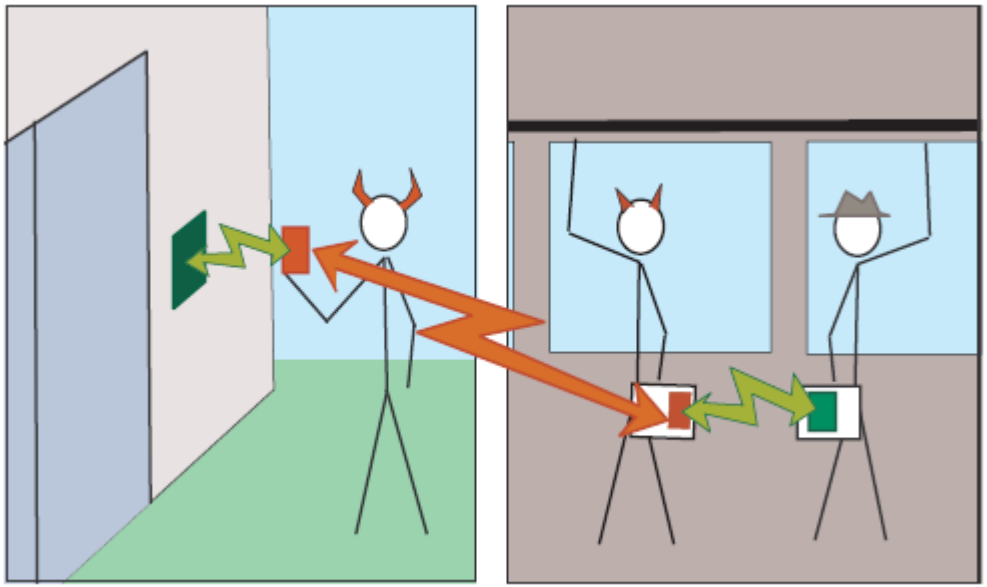
- **Leech**: acts as a malicious reader, **surreptitiously** reads info from an innocent tag and relays that info to the leech
- **Ghost**: acts as a malicious tag, receives info from Ghost and relays it to the good reader
- **Consequence**: the pair successfully impersonates the innocent tag without possessing it!!!



Ghost-and-Leech Example 1

- RFID-based access control



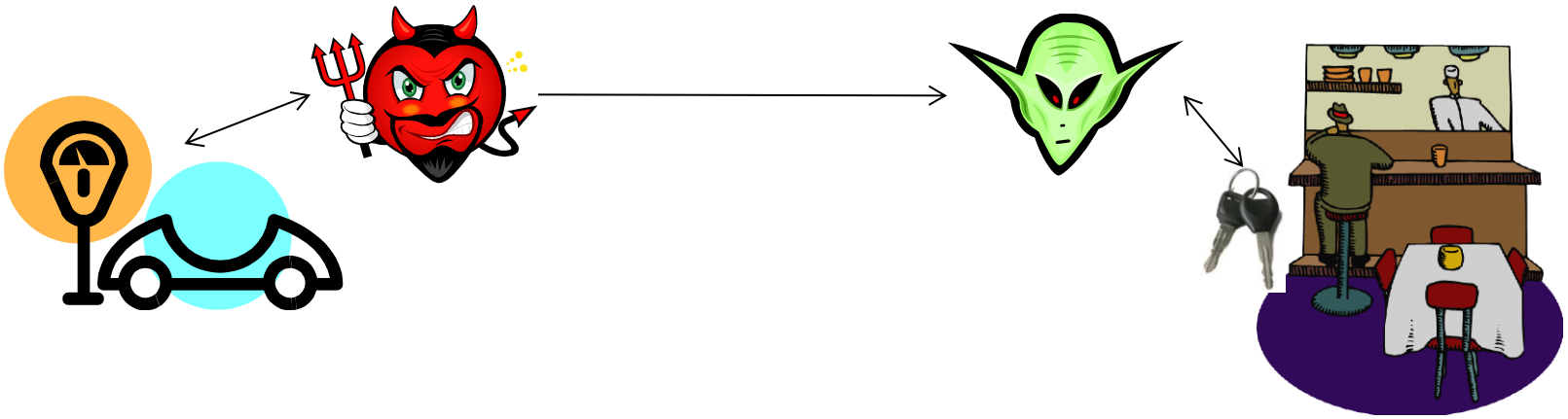


- Attacker close to the access-granting RFID tag
  - Relays signals from and to her accomplice, who obtains access

Z. Kfir and A. Wool, "Picking virtual pockets using relay attacks on contact-less smartcard," SECURECOMM "05

Ghost-and-Leech Example 2

- Passive Keyless and Start System in modern cars

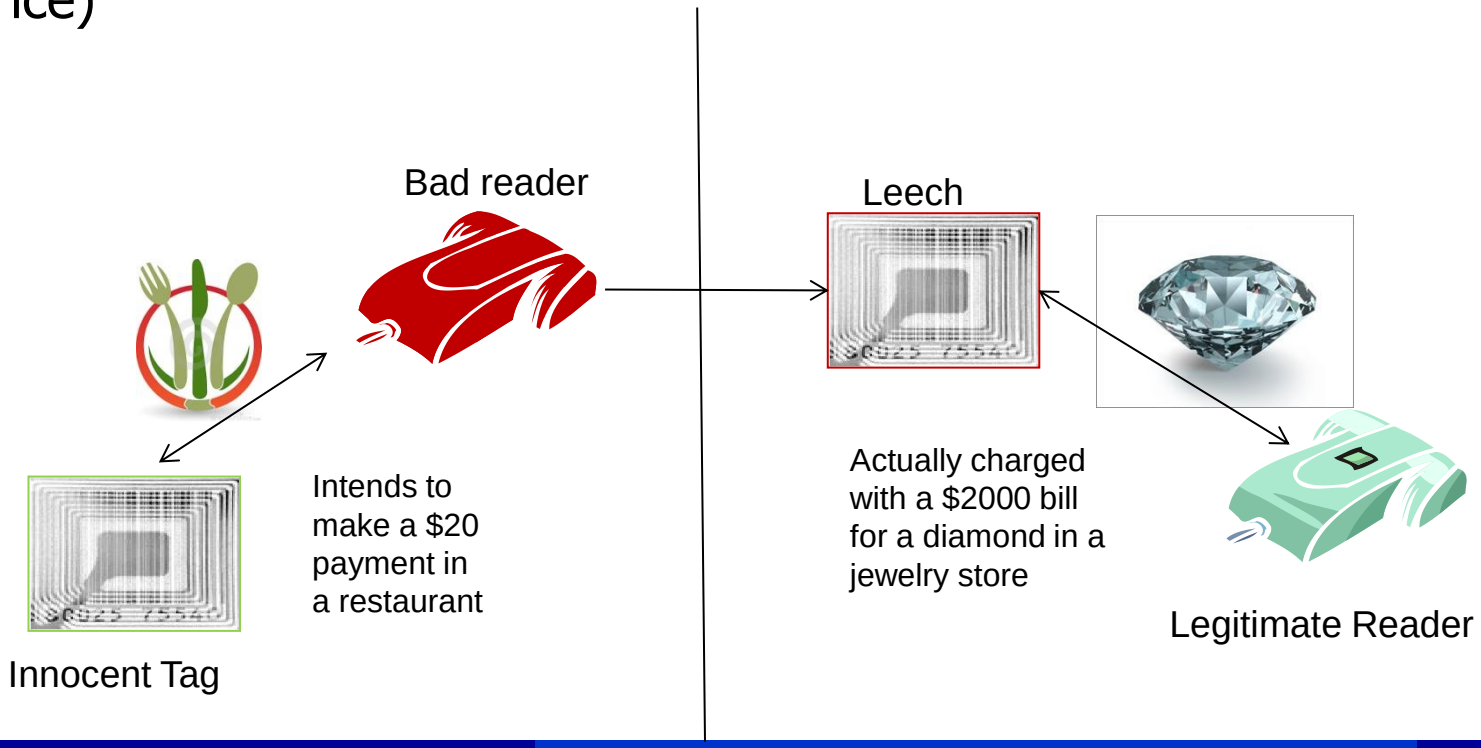


- Attacker close to key
  - Relays signals from and to her accomplice near the car to open the car door and start the car

A. Francillon and B. Danev and S. Capkun, "Relay attacks on passive keyless entry and start systems in modern cars," NDSS'11

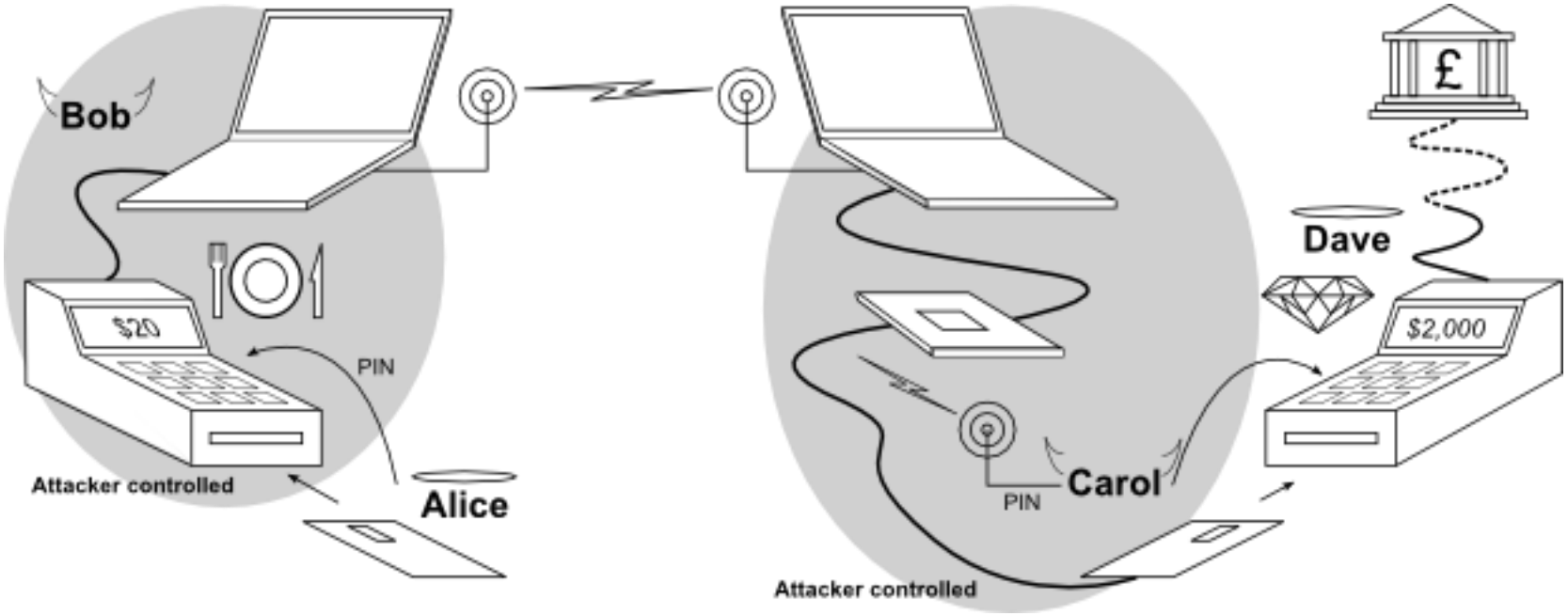
Reader-and-Ghost Relay Attack

- A more severe form of relay attacks, usually against payment cards
- Different from the normal ghost-and-leech attack, the malicious reader is the one which the innocent tag intends to make a payment with. So the innocent tag is aware of the process.
- What the innocent tag is not aware is that its response information is relayed to the leech which impersonates it to make another payment (higher price)



Reader-and-Leech Example

- Chip and Pin (EMV) credit card system (PIN is required to ensure higher security)



- Malicious reader (Bob) relays signals and PIN info to her accomplice Carol
  - Alice intends to pay a $20 bill in a restaurant. She is actually charged $2,000 for a diamond which Carol made a purchase

S. Murdoch, S. Drimer, R. Anderson, and M. Bond, "Chip and PIN is broken," S&P'10

Outline

- RFID systems
- Security and Privacy Issues
- Countermeasure
  - Countermeasure to unauthorized reading
  - Countermeasure to relay attack

Countermeasures to Unauthorized Reading

- Non-cryptographic approaches
  - protective mesh or foil
  - "kill" command
  - "sleep" command
  - renaming
  - selective unlocking

- Cryptographic approaches
  - tree-approach
  - synchronization approach
  - hash chain based approach

  (won't be discussed in the class)

Cover RFID tags with Protective Mesh or Foil

- Examples
  - Passport cover
  - ID card envelope
  - …

- Disadvantages
  - Additional cost is needed
  - User intervention
  - Good Farady Cage is expensive
    - A crumpled sleeve is ineffective for shielding purposes
  - Youtube video clip on RFID shield failure demo:

http://www.youtube.com/watch?v=-XXaqraF7pI&feature=fvw

Dead tags tell no tales

- idea: permanently disable tags with a special "kill" command
- part of the EPC specification

- advantages:
  - simple
  - effective

- disadvantages:
  - eliminates all post-purchase benefits of RFID for the consumer and for society
    - no return of items without receipt
    - no smart house-hold appliances
    - …
  - cannot be applied in some applications
    - library
    - e-passports
    - banknotes
    - …

- similar approaches:
  - put RFID tags into price tags or packaging which are removed and discarded (the Wal-Mart tags)

“Sleep” command

- idea:
  - instead of killing the tag put it in sleep mode
  - tag can be re-activated if needed
- advantages:
  - simple
  - effective
- disadvantages:
  - difficult to manage in practice
    - tag re-activation must be password protected
    - how the consumers will manage hundreds of passwords for their tags?
    - passwords can be printed on tags, but then they need to be scanned optically or typed in by the consumer

Renaming

- idea:
  - instead of not replying, responds with information unrecognizable to unauthorized readers
  - get rid of fixed names (identifiers)
  - use random pseudonyms and change them frequently
  - a bad reader won't get an idea what it reads

- requirements:
  - only authorized readers should be able to determine the real identifier behind a pseudonym
  - standard tags cannot perform computations → next pseudonym to be used must be set by an authorized reader

Renaming (cont.)

- a possible implementation
  - pseudonym = $\{R|ID\}_K$
    - R is a random number
    - K is a key shared by all authorized readers
    - $\{R|ID\}_K$ means encryption of R|ID with key K
  - authorized readers can decrypt pseudonyms and determine real ID
  - authorized readers can generate new pseudonyms
  - for unauthorized readers, pseudonyms look like random bit strings

- potential problems
  - tracking is still possible between two renaming operations
    - In between, the same pseudonym is used
  - if someone can eavesdrop during the renaming operation, then she may be able to link the new pseudonym to the old one
  - no reader authentication → rogue reader can overwrite pseudonyms in tags (tags will be erroneously identified by authorized readers)

Selective Unlocking

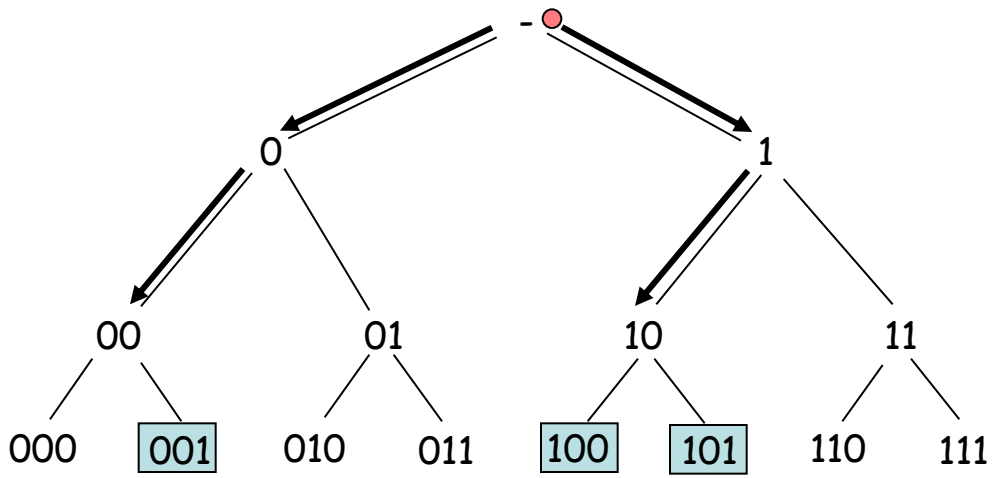
- Mechanisms used to defend against unauthorized reading
- Tags are made to respond selectively, rather than promiscuously

- Several hardware-based selective unlocking schemes exist
  - Blocking (blocker tag required) - we will talk it next
  - RFID enhancer proxy (PDA like RFID-enabled device required)
  - RFID guardian (PDA like RFID-enabled device required)

- Disadvantages
  - Specialized auxiliary device required
  - May not be available at the time of accessing RFID tags
  - Users may not willing to carry these devices

Blocking with a Blocker Tag (1/2)

- Idea: interfere the binary tree walking identification process so that tags cannot be identified
- binary tree walking
  - a mechanism to determine which tags are present (singulation procedure)
    - Recursively ask question, what's your next bit?
  - IDs are leaves of a binary tree
  - reader performs a depth first search in the tree as follows
    - reader asks for the next bit of the ID starting with a given prefix
    - if every tag's ID starts with that prefix, then no collision will occur, and the reader can extend the prefix with the response
    - if there's a collision, then the reader recursive on both possible extensions of the prefix



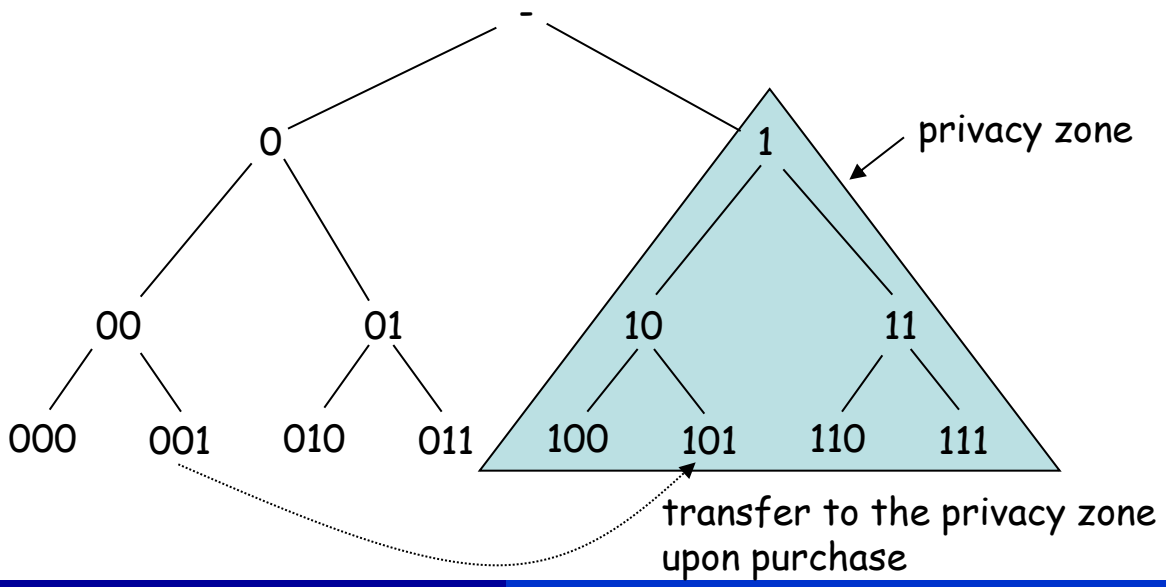
reader: prefix "-" ?
tags: collision
reader: prefix "0" ?
tags: 0
reader: prefix "00" ?
tags: 1 → 001
reader: prefix "1" ?
tags: 0
reader: prefix "10" ?
tags: collision → 100
101

Note: real tag sizes are much larger (e.g., 96 bits for EPC)

Blocking (2/2)

- privacy zone
  - tree is divided into two zones
    - privacy zone: all IDs starting with 1
  - upon purchase of a product, its tag is transferred into the privacy zone by setting the leading bit

- the blocker tag (special device carried by the user)
  - when the prefix in the reader's query starts with 1, it simulates a collision
  - when the blocker tag is present, all IDs in the privacy zone will appear to be present for the reader
  - when the blocker tag is not present, everything works normally



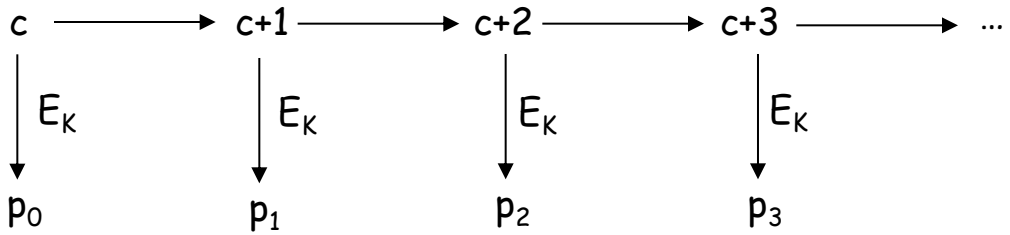
Crypto enabled tags

- assume that tags can perform some crypto operations

→ tags can compute their own pseudonyms !

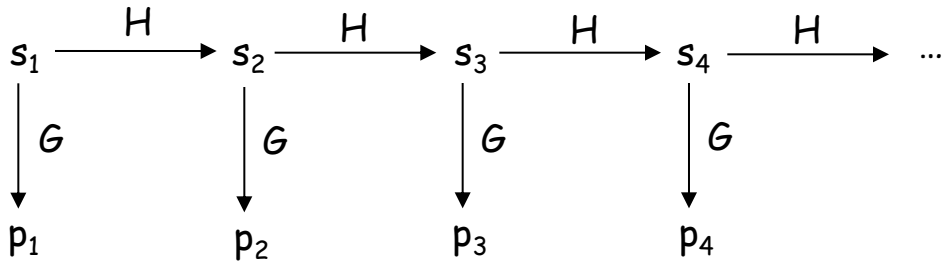
- a solution that doesn't scale:
  - next pseudonym = $\{R, S, ID\}_K$
    - R is a random number generated by the tag (ensures that pseudonyms look random and they are different)
    - S is some redundancy (ensures that the reader can determine if it used the right key to decrypt the pseudonym)
    - ID is the real identifier
    - K is a key shared by the tag and the reader
  - the reader tries all possible keys (brute-force search) until it finds the right one
  - if there are many tags, then the verification may be too slow

Synchronization approach



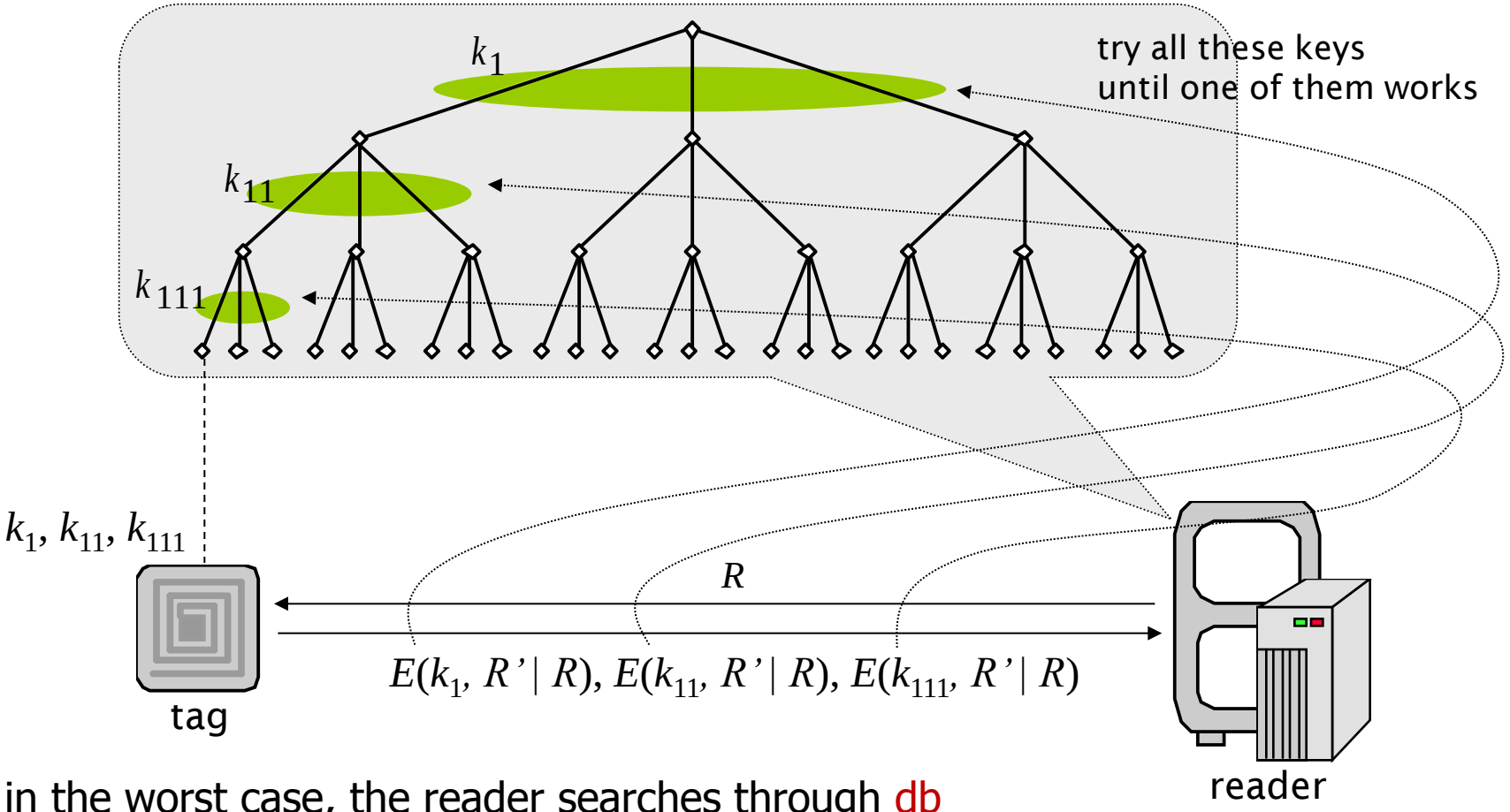
- c is a counter, K is a key shared by the tag and the reader
- operation of tag:
  - when queried by the reader, the tag responds with its current pseudonym $p = E_K(c)$ and increments the counter
- operation of the reader:
  - reader must know approximate current counter value
  - for each tag, it maintains a table with the most likely current counters and corresponding pseudonyms $(c+1, p_1)\ldots(c+d, p_d)$
  - when a tag responds with a pseudonym p, it finds p in any of its tables, identifies the tag, and updates the table corresponding to the tag
- one-wayness of $E_K()$ ensures that current counter value cannot be computed from observed pseudonym

Hash-chain based approach



- H and G are one-way functions (e.g., hash functions)
- operation of the tag:
  - current state is s_i
  - when queried the tag responds with the current pseudonym $p_i = G(s_i)$ and computes its new state $s_{i+1} = H(s_i)$
- operation of the reader is similar to the previous approach
- one-wayness of H ensures *forward secrecy* :
  - even if a disposed tag is broken and its current state is determined, previous states (and pseudonyms) cannot be computed

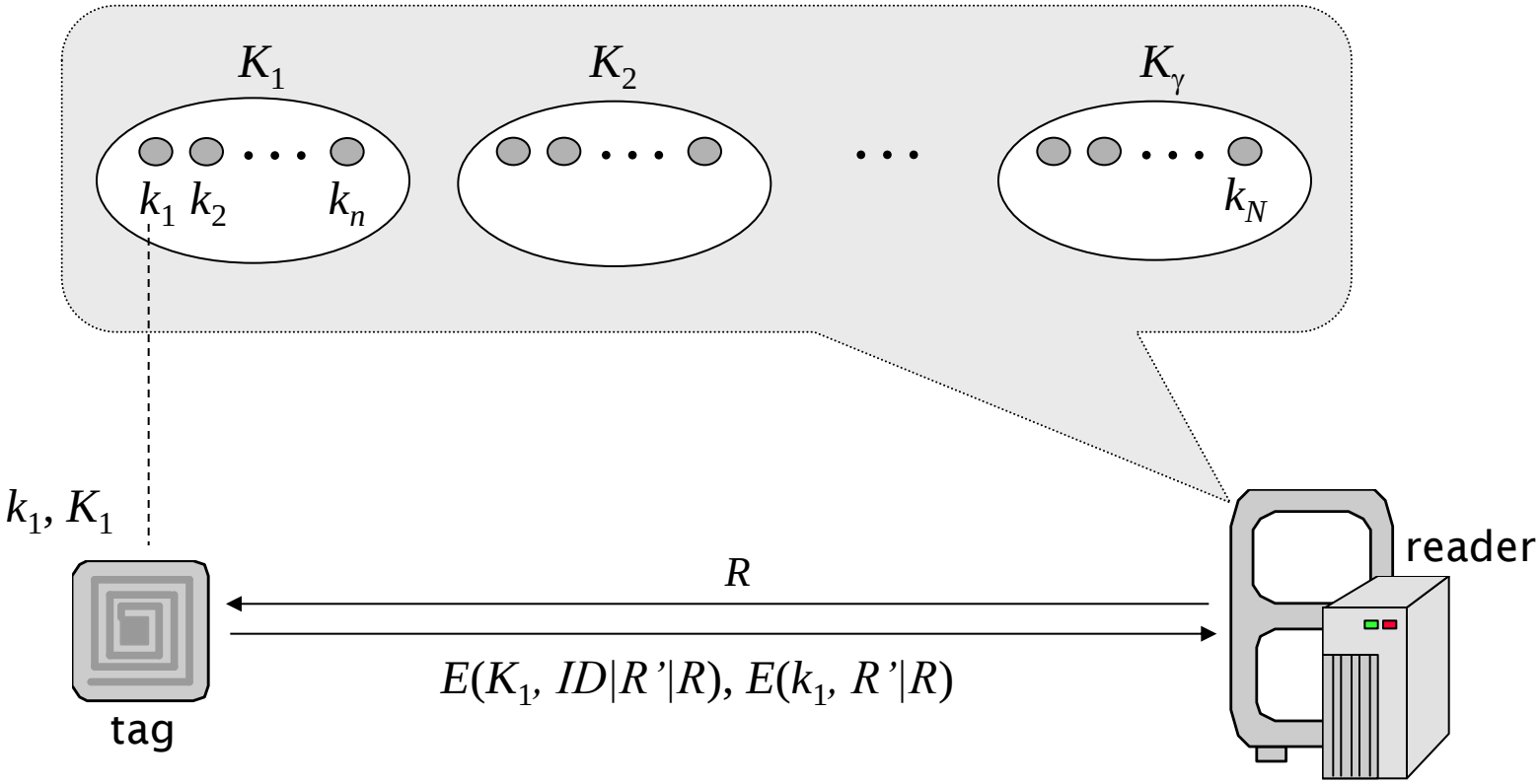
The tree-based approach



- in the worst case, the reader searches through db keys, where d is the depth of the tree, and b is the branching factor
- compare this to b^d keys, which is the total number of tags !

k_1, k_{11}, k_{111} → tag ID

The group-based approach



immediate advantage:
each tag stores and uses only only two keys

1.) try all group keys until one of them works
2.) authenticate the tag by using its individual key

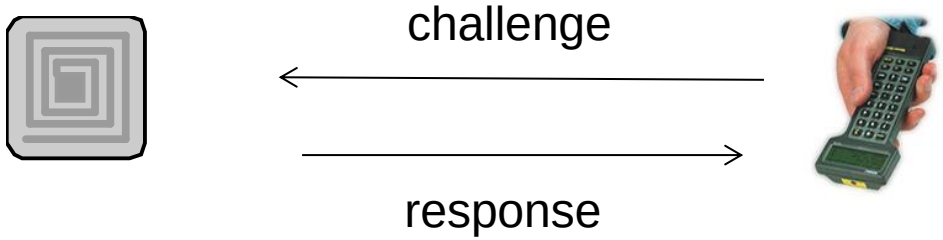
Outline

- RFID systems
- Security and Privacy Issues
- Countermeasure
  - Countermeasure to unauthorized reading
  - Countermeasure to relay attack
    - Proximity verification

Proximity Verification Using Distance Bounding Protocols

- Distance bounding protocols are the sole solution proposed as potential countermeasures to relay attacks

- They are cryptographic challenge-response protocols which allows the verifier (reader) to measure an upper-bound of its distance from the prover (tag).



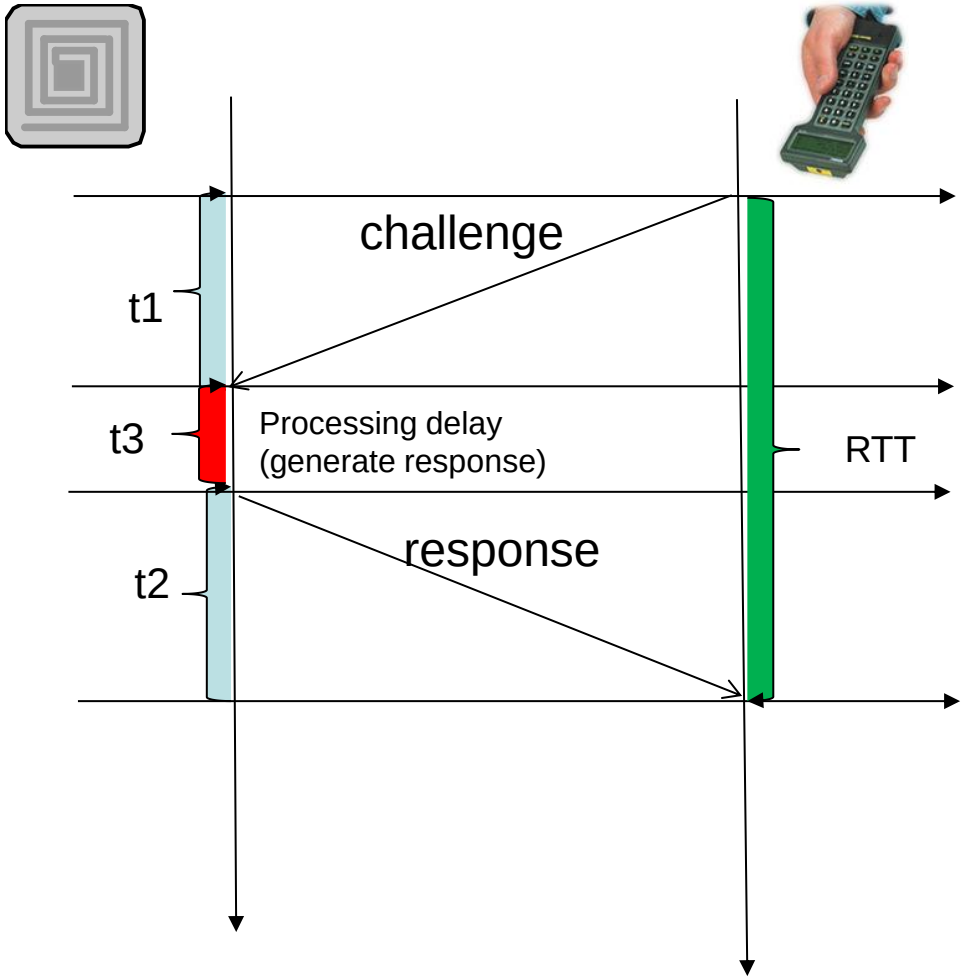
- The tag 1) verifies the response; 2) uses the round trip time (RTT) to estimate the distance between tag and reader

Distance Bounding Protocols

- The reader
  - Records RTT
  - Estimates t3 (processing time)
  - Calculates distance as:

distance = Speed-of-light * (RTT – t3)

- Accurate estimation of t3 is very important to the accuracy of distance estimation
  - Very sensitive to processing delay
  - A slight delay may result in a significant error (since the delay will be multiplied by speed-of-light)



Distance Bounding Protocols

- To prevent tag cheating, the processing delay should be as small as possible
- Even XOR- or comparison-based distance bounding protocols are not suitable for RF distance bounding since signal conversion and modulation can lead to significant delay
- A recent distance bounding protocol achieves a processing time less than 1 ns (this work will be presented later in our class) at the prover side
  - But it requires specialized hardware for channel selection (the return channel consists of two channels)
- Question: does it mean we can solve the relay attack problem with DB protocols?
  - Think about the reader-and-leech attack on the credit card

Distance Bounding Protocols

- The answer is NO, at least for the credit card relay attack case.

- Remember a distance bounding protocol is a cryptographic challenge-response authentication protocol
  - Which requires secure association between tag and reader

- How can my credit card establish secure association with readers in so many retailer stores (including overseas retailers)?

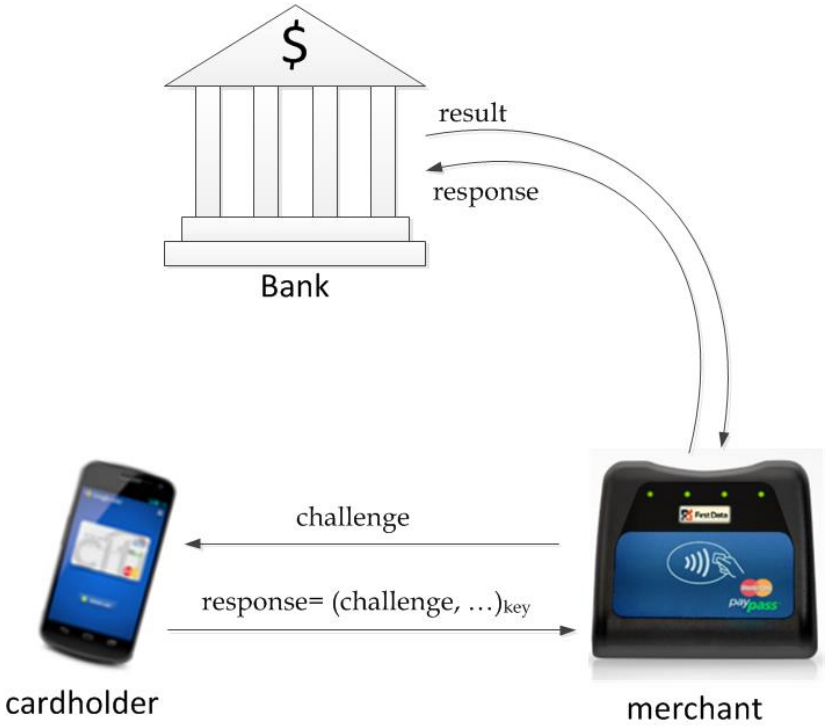
Sensing-based Co-location Verification

- Defend against Reader-and-Ghost attack targeting mobile payment service

- Use location information from both tag and reader to assist the bank server to make decision
  - Approve: when both tag and reader are from the same location
  - Reject: when the two devices are from disparate location
    - E.g., one in restaurant, one in a jewelry store.

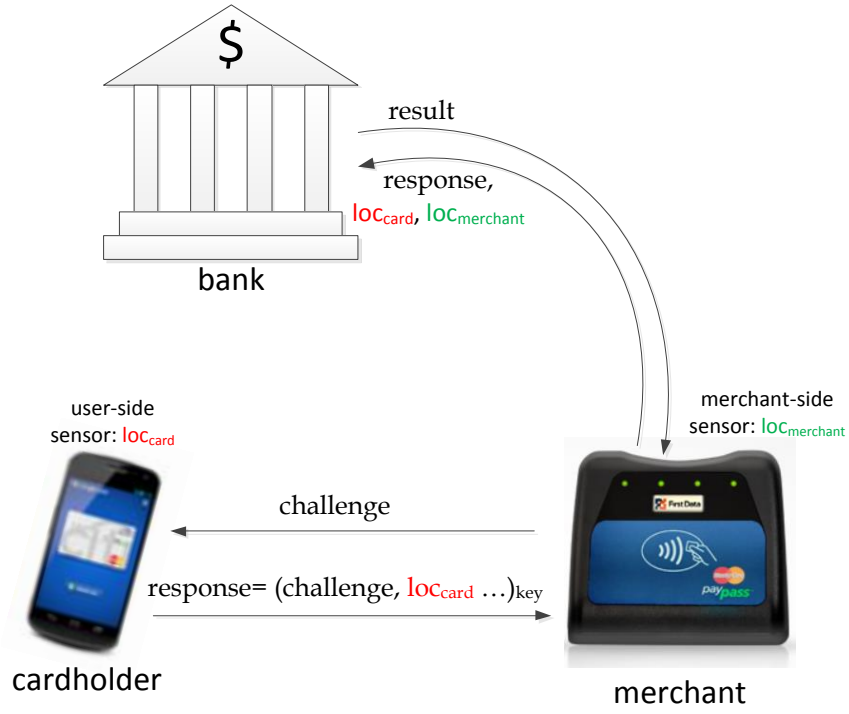
Current Mobile Payment System

- EMV
  - Stands Europay, Mastercard, and Visa
  - Global standard for credit card payment
  - Also known as ``Chip and Pin"
    - Vulnerable to the Reader-and-Ghost attack
  - Mastercard's PayPass is EMV compatible
    - Used by Google Wallet



Sensing-based Proximity Verification

- Location dependent information generated by both card and merchant
  - Card: Loc_{card}
  - Merchant: $Loc_{merchant}$
- Loc_{card} is protected by shared key with the bank
- Bank server compares Loc_{card} and $Loc_{merchant}$ to find whether they are from the same location or not



- Bank reject the transaction if card and merchant are from two different places
  - E.g., card in a restaurant while merchant is a jewelry store

Location Estimation

- Location can be obtained directly (WiSec'12)
  - GPS
- Or estimated based on ambient sensors (Esorics'12, Percom'14)
  - Ambient noise
  - Ambient light
  - WiFi
  - Bluetooth
- Intuition behind location estimation
  - Physical parameters in two places are very likely different
  - While similar in the same place

Remarks

- WiFi is better than the rest in defending against relay attacks in performance

- Fusing multiple sensor modalities improves resilience against relay attacks while retaining a high level of usability

Summary

- A brief overview of RFID systems and their security and privacy
- Studied several current countermeasures and their limitations