# Today's Lecture - RFID

Part I: Technology and applications.

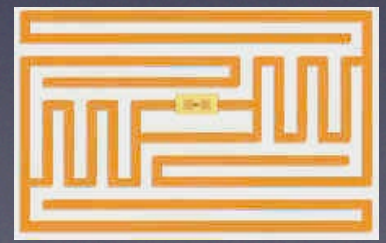
Part II: Security and privacy aspects.

# Barcode

- Automatic identification system.
- Components:
  1. Tag
  2. Reader.
- Universal product code (UPC):
  1. Product associated with code.
  2. Code linked with data record.

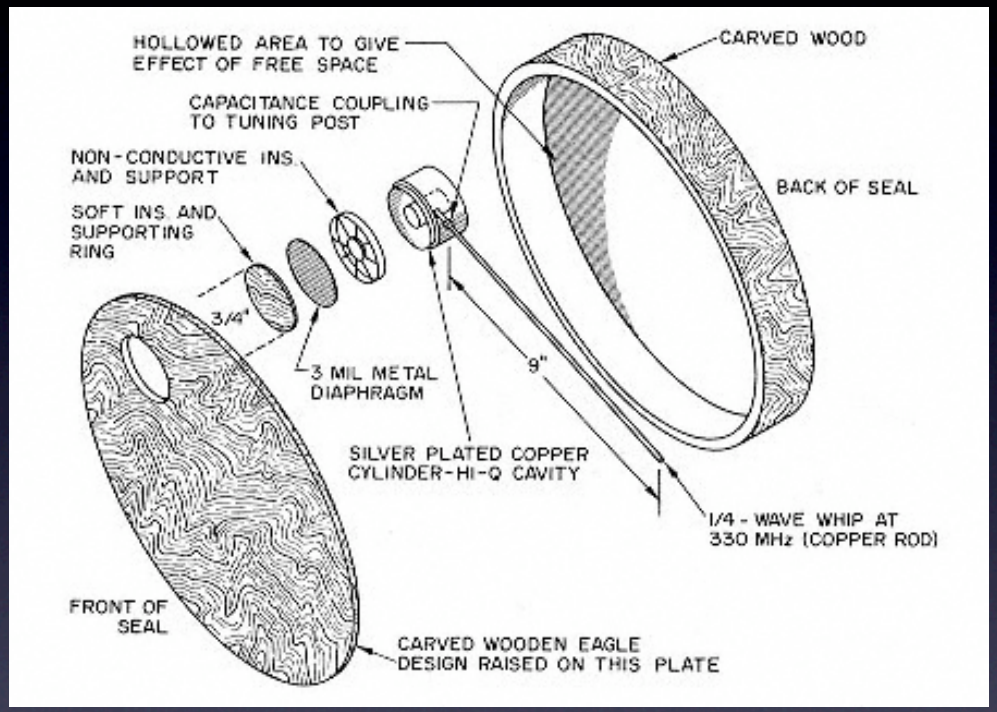

# RFID (Radio Frequency Identification)

- "Wireless" *identification system.*
- Tags
  1. Small transponders - attached to physical objects.
  2. May become most pervasive microchip in history.
- Readers
  1. Transceivers - read (write) data from tags.
  2. Data associated with arbitrary data records.



*Foil Inlay Tag*

# “The Great Seal Bug”



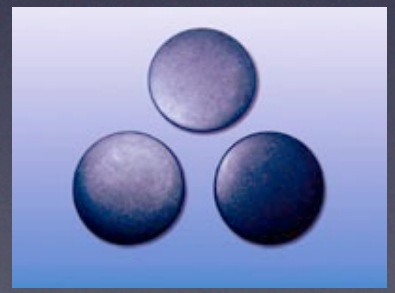

- Wooden replica of the great seal of US.
- 1946 - Given to US ambassador in moscow.
- Contained microphone and resonant cavity.
- Could be stimulated from outside radio signal.

# RFID History

- 40's - WW II Identify Friend or Foe (IFF), 1st paper
- 70's - Theft prevention (EAS), agriculture (cattle), 1st patent
- 80's - EZ-Pass, ski-passes, gasoline-pass...
- 1999 - Auto-ID center.
    1. 2003 - Auto-ID labs and EPCGlobal Inc.
    2. Electronic Product Code (EPC) development.
- 2000's- dramatic increase in deployment...

# Why Now?

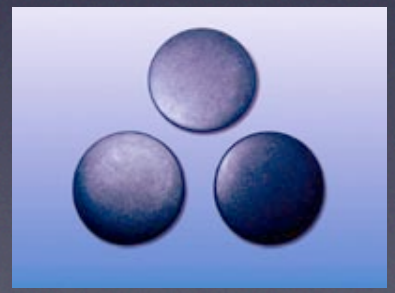
- RFID has been around for 60 years.
- So why now?



*Laundry Tags*

# Why Now?

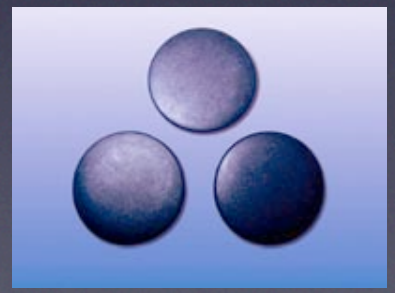
- RFID has been around for 60 years.
- So why now?
- Advances in chip technology:
  1. Cheap.
  2. Small.



*Laundry Tags*

# Why Now?

- RFID has been around for 60 years.
- So why now?
- Advances in chip technology:
  1. Cheap.
  2. Small.
- Vigorous standardization.



*Laundry Tags*

# RFID vs. Barcode

- RFID offers unique identification:
  1. Electronic Product Code (EPC).
  2. Records *serial number* of individual items.
  3. Can track transaction history of any item.
- RFID enables automation:
  1. Barcode requires human intervention.
  2. RFID does not require line of sight contact.
  3. Can scan hundreds of items per second.


# RFID or Barcode?

# The "Promise" of RFID

- RFID has the potential to revolutionize:
  1. Supply Chain Management
  2. Inventory Control
  3. Retail Systems
  4. Payment systems
  5. Access Control


- But progress is slower than predicted:
  1. Logistical complications.
  2. Tag cost.

# Economic Barriers

- Many kinds of RFID systems.
- Inverse correlation between:
  1. Price.
  2. Size/Functionality.
- Wide deployment requires low cost:
  1. The threshold is 5c per tag - not there yet.
  2. Currently readers cost 1000K+ - too much.

*Keychain Tag*


# Privacy

# Privacy Concerns

- Past applications - in closed systems
- New applications - affect individuals more
- Not clear what countermeasures should be incorporated into RFID systems
- Main concerns?

*Implantable Tag*

# Privacy Concerns

- Past applications - in closed systems
- New applications - affect individuals more
- Not clear what countermeasures should be incorporated into RFID systems
- Main concerns?
  1. Ability to read tag remotely
  2. Ability to link specific products/data to individuals
  3. May enable clandestine *tracking* and *inventorying*

*Implantable Tag*

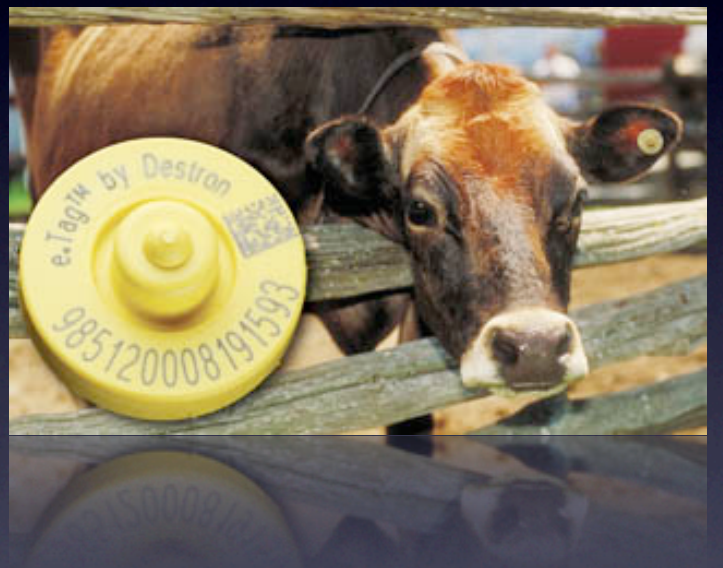
# Over-hype and Backlash

- Late 90's - "RFID will solve everything."
- Early 2000's - "RFID is the source of all evil."
- Truth is NOT somewhere in the middle.
  1. RFID capabilities over-estimated by everybody.
  2. Probably neither sinister or glamorous.
- The challenge: tell apart facts from fiction...

# Applications

# Tracking and Identification

- Large assets (railway cars, containers).
- Livestock (rugged tags).
- Pets (implanted tags).
- Supply-chain management (EPC)
- Inventory control (EPC)
- Retail checkout (EPC)
- Recycling and waste disposal



# Payment/Stored-Value Systems

- Electronic toll systems
- Conctact-less credit cards (e.g. Amex Blue Card)
- Stored value systems (e.g. Exxon-Mobil Speedpass)
- Subway and bus passes
- Casino tokens and concert tickets

# Access Control

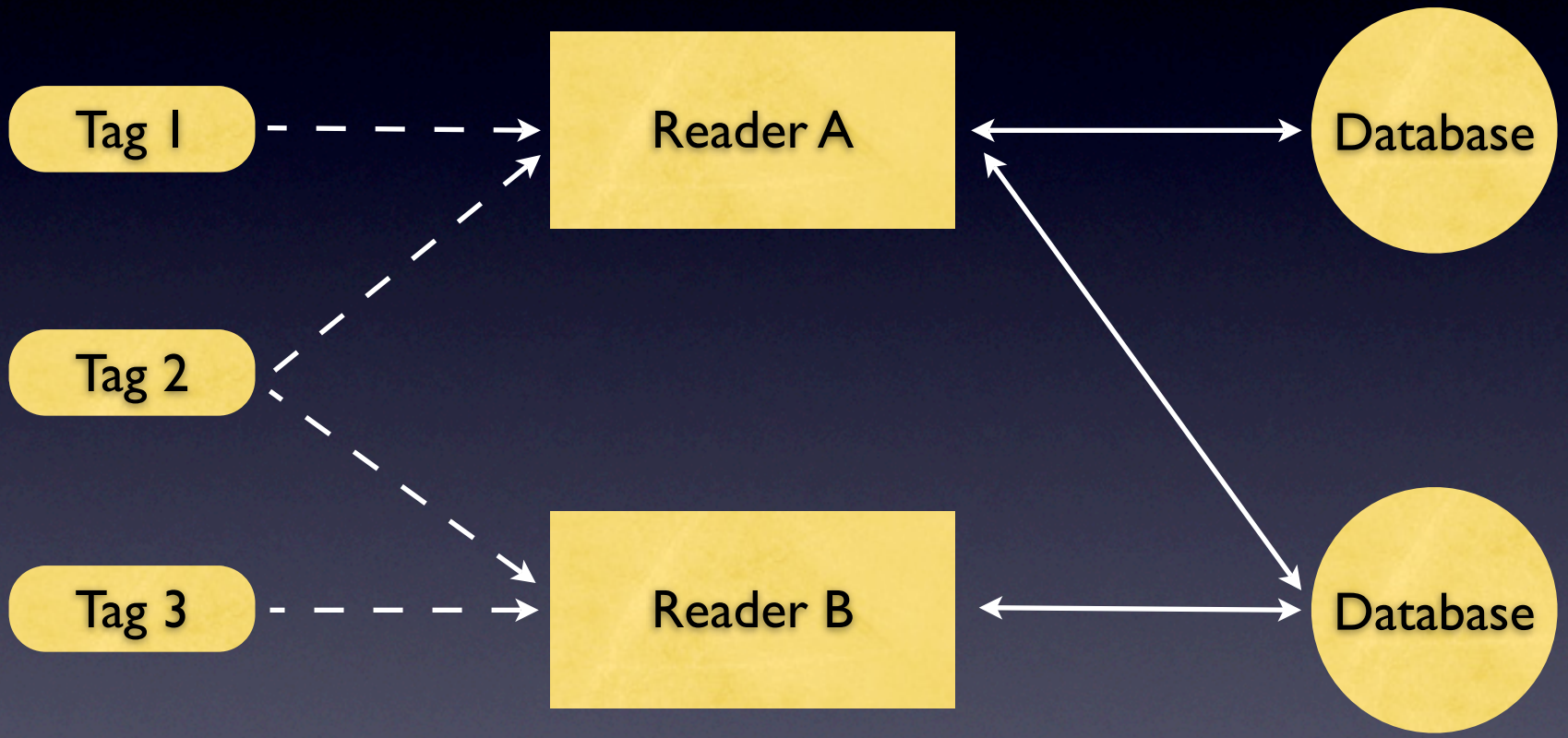
- Building access with proximity cards
- Ski-lift passes
- Concert tickets
- Automobile ignition systems

# Anti-Counterfeiting

- Casino tokens (e.g. Wynn Casino, Las Vegas)
- High-denomination currency notes
- Luxury goods, e.g. Prada
- Prescription drugs

# Principles

# RFID System Components



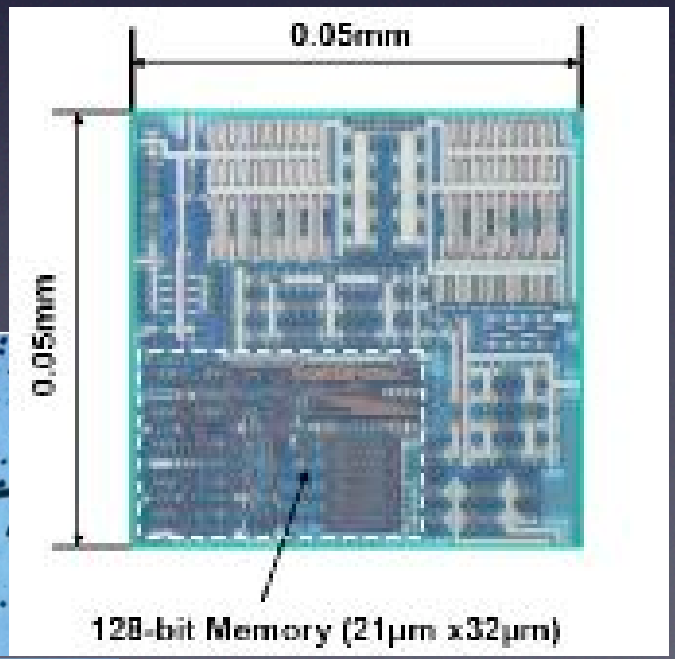
# Tags

- Antenna + integrated circuitry
- Many variants:
  1. different power sources
  2. radio frequencies
- Three classes of tags:
  1. **active** - battery, may initiate communication
  2. **semi-passive** - battery, may not initiate comm.
  3. **passive** - no battery, may not initiate comm.

*Active Tags*

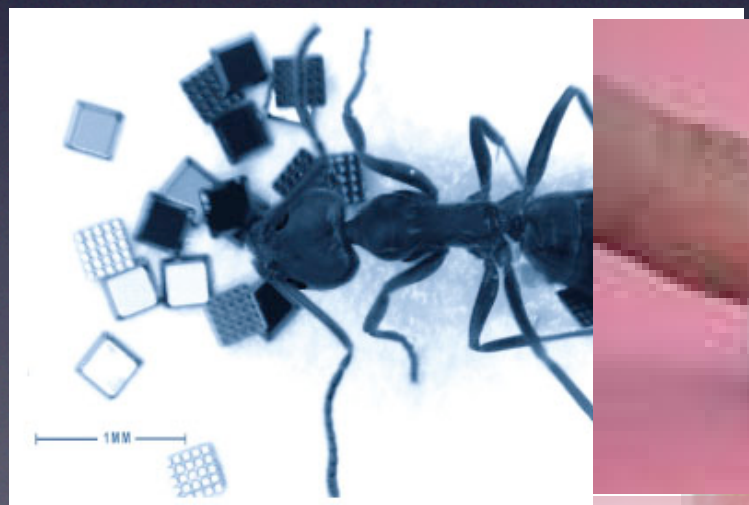
# Tags Can be Very Small

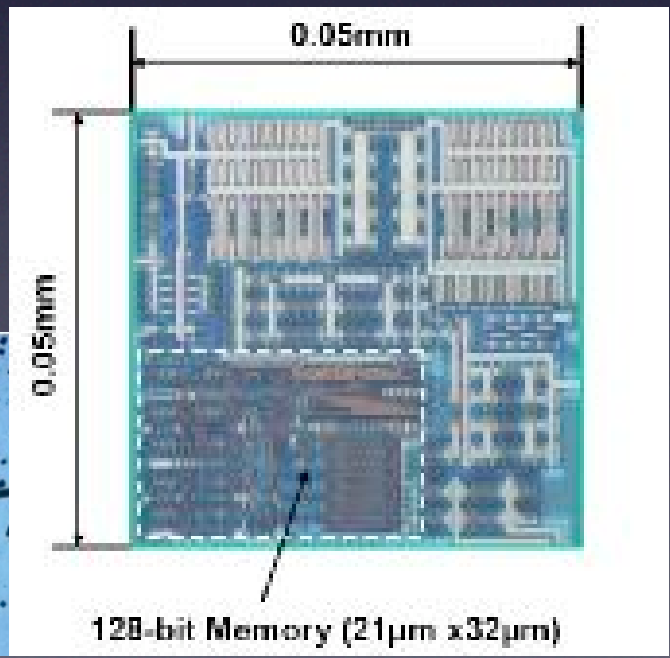
- As small as 0.05x0.05 mm
- But price per tag is still high
- Does not include antenna (6cm)...

# Tags Can be Very Small

- As small as 0.05x0.05 mm
- But price per tag is still high
- Does not include antenna (6cm)...





# Tag Comparison

| Tag Type | Passive | Semi-Passive | Active |
|---|---|---|---|
| **Power Source** | Harvesting | Battery | Battery |
| **Communication** | Response only | Response only | Respond/Initiate |
| **Max Range** | 10 M | > 100 M | > 100 M |
| **Relative Cost** | Least | More | Most |
| **Example Applications** | EPC<br>Prox. Cards | Electronic Tolls<br>Pallet tracking | Large-asset tracking<br>Livestock tracking |

# Readers

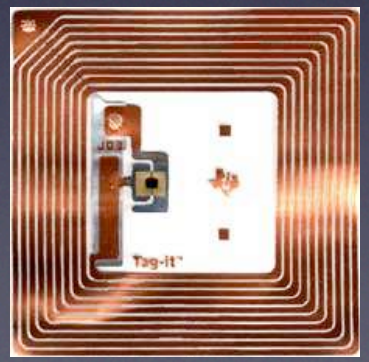
- Ping or multi-round protocol.
- “Anti collision” protocols - communicate with many tags in serial order
- Power passive tags w/ RF signal
  1. induction
  2. capacitance
- Still very expensive (US$1000+)

# Databases

- May contain:
  1. Product info - tracking logs/sales data/exp. dates
  2. Aggregated information about you...
- Object Naming Service (ONS):
  1. Find database w/ some tag identification value
  2. Analogous to DNS

# Operating Frequencies

- Various ranges of radio frequencies
- Each range determines:
  - operating range, power requirement, performance
  - physical dimensions of tag/antenna
  - regulations/restrictions




*Foil Inlay Tag*

# Read Ranges

| Frequency Range | Frequencies | Passive Read Distance |
|---|---|---|
| Low Frequency (LF) | 120-140 KHz | 10-20 cm |
| High Frequency (HF) | 13.56 MHZ | 10-20 cm |
| Ultra-High Frequency (UHF) | 868-928 MHz | 3 meters |
| Microwave | 2.45 & 5.8 GHz | 3 meters |
| Ultra-Wide Band (UWB) | 3.1-10.6 GHz | 10 meters |

# Features

| Frequency | The good | The bad | Liquids /metals | Price |
|---|---|---|---|---|
| **LF** | • short range | • low read rate<br>• short range | not affected | US$1 |
| **HF** | • higher read rate<br>• longer range | • heavily regulated | affected | US$0.50 |
| **UHF** | • high read rate<br>• longest range | • high reader cost<br>• interferes with medical equip. | severely affected | < US$0.15 |
| **Microwave** | • smaller size<br>• higher read rate | • energy consumption<br>• interference w/ WiFi | | US$25 |
| **UWB** | • longest range (line of sight) | • active or semi-passive | not affected | US$5 |

# Functionality

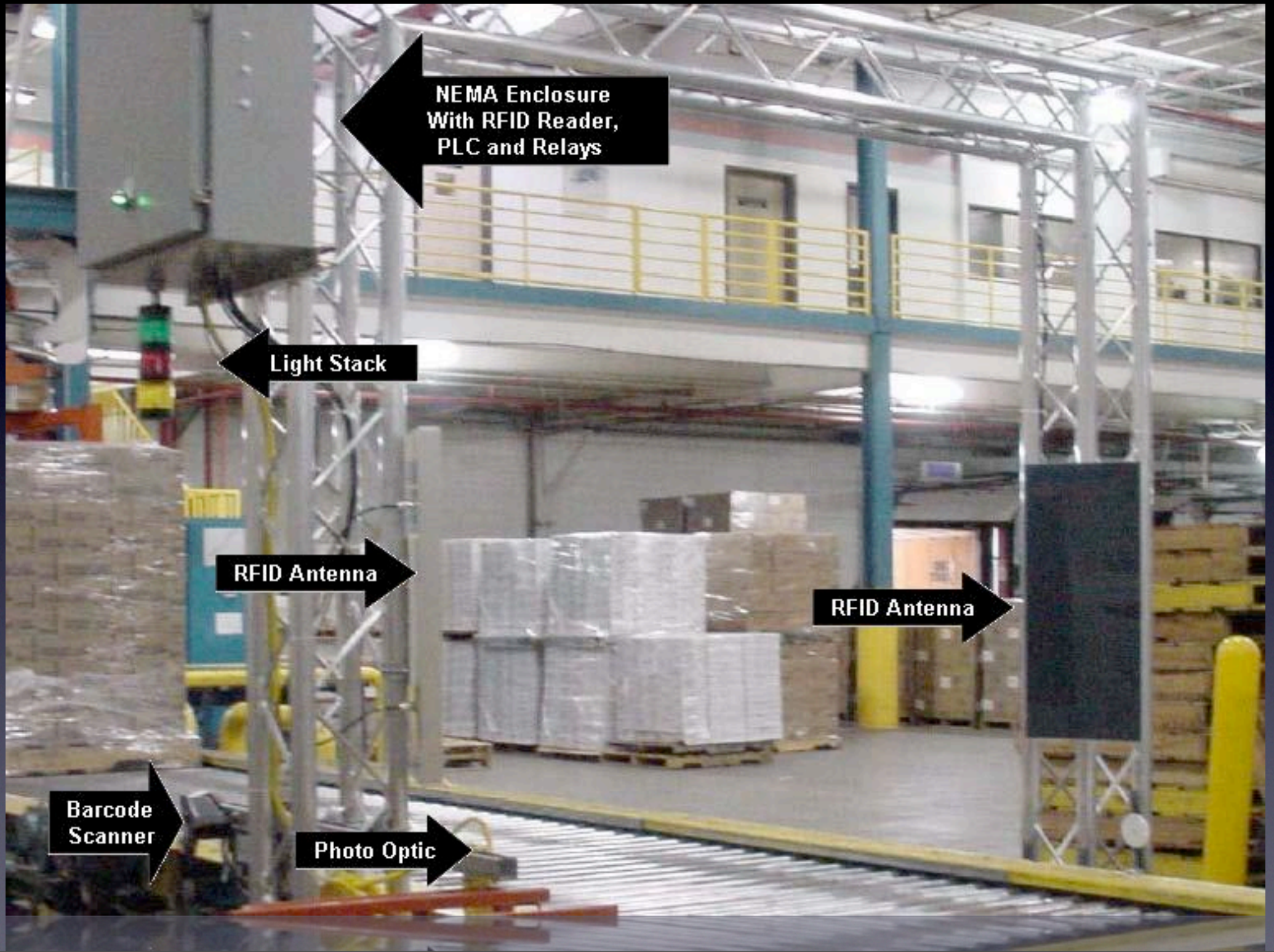
| Class | Name | Memory | Power Source | Features |
|---|---|---|---|---|
| A | EAS | None | Passive | Article Surveillance |
| B | Read-only EPC | Read-Only | Passive | Identification Only |
| C | EPC | Read/Write | Passive | Data Logging |
| D | Sensor Tags | Read/Write | Semi-passive | Environmental Sensors |
| E | Motes | Read/Write | Active | Ad Hoc Networking |

# Standards and Patents

- EPC (UHF)
- ISO 11784, 11785,18000-, 14223, 10536, 14443, 15693 (LF, HF, UHF, Microwave)
- ONS (not widely used)
- Over 1800 RFID related patents
- Over 5600 patents are backlogged

# Challenges

- Technical:
  1. environmental noise
  2. interference
  3. human elements
- Economic
- Security and Privacy


NEMA Enclosure
With RFID Reader,
PLC and Relays
Light Stack
RFID Antenna
RFID Antenna
Barcode
Scanner
Photo Optic

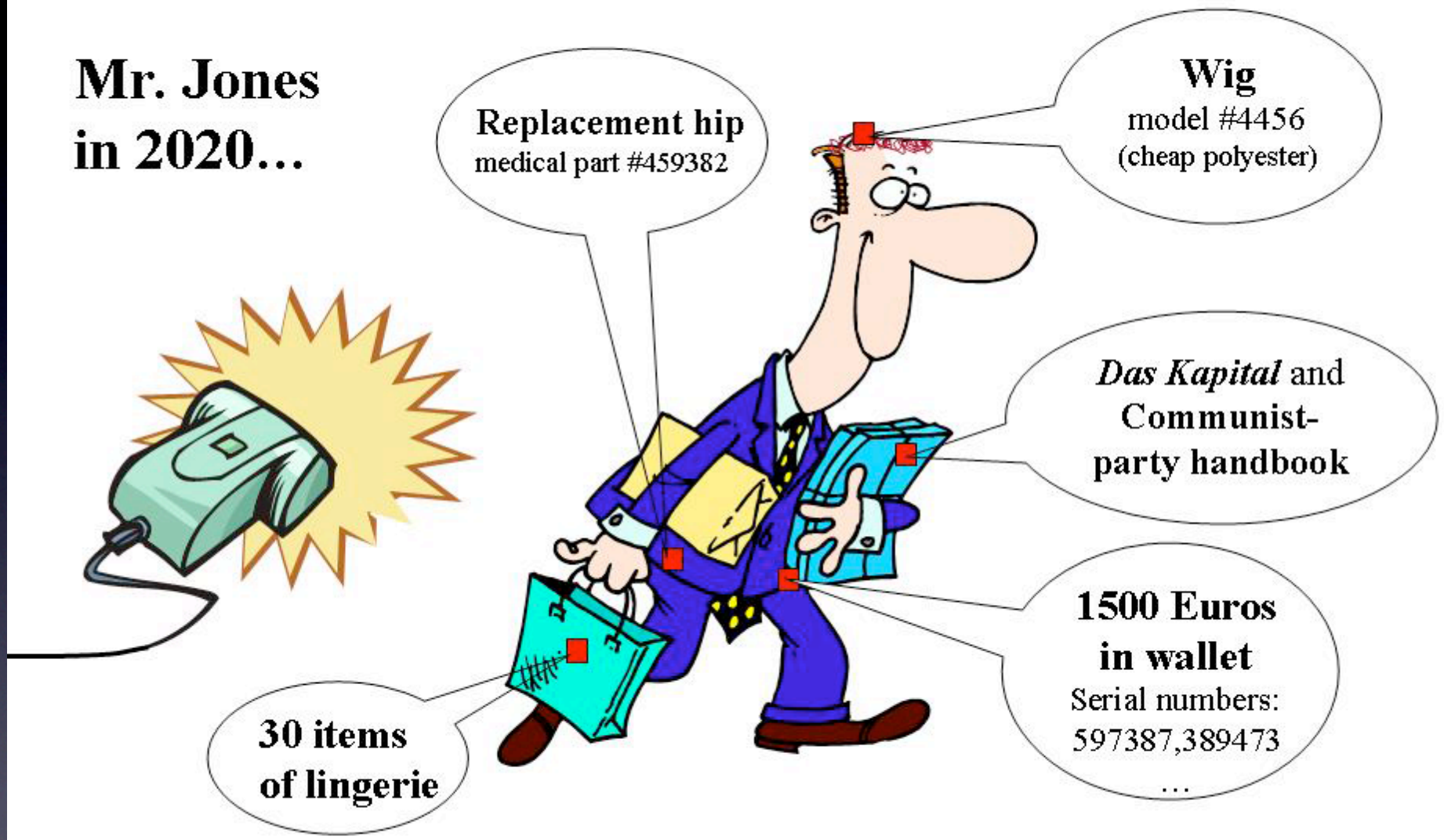
# Challenges

- Technical:
  1. environmental noise
  2. interference
  3. human elements
- Economic
- Security and Privacy

# Part II: Privacy and Security

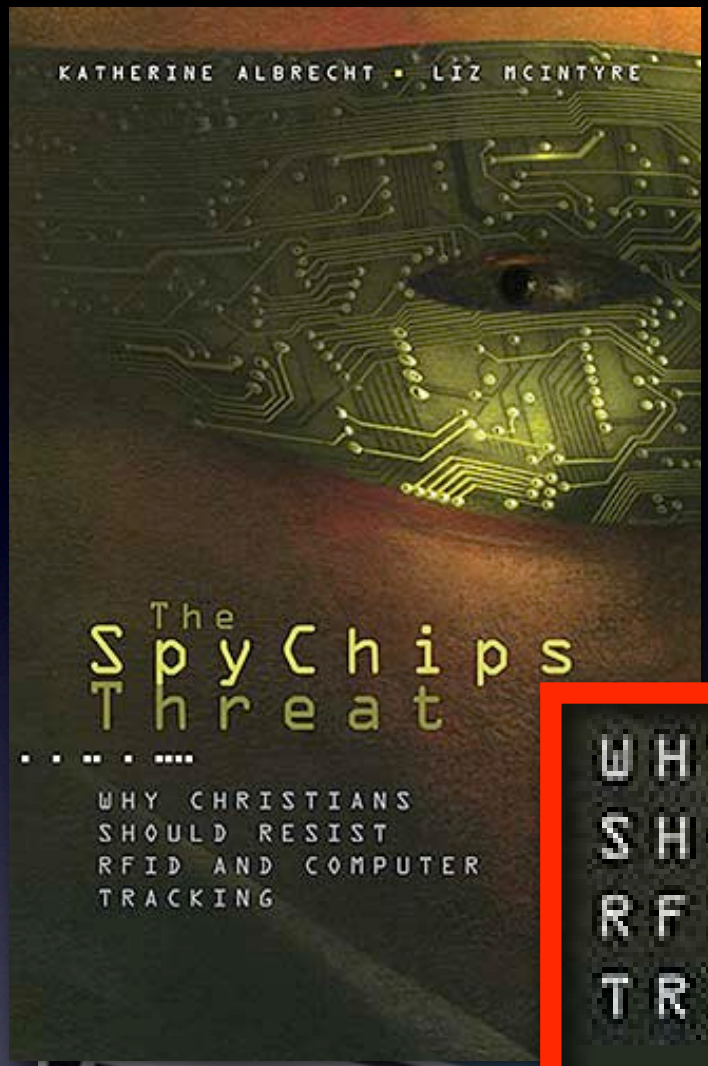
- Main focus on low-cost RFID (EPC):
  1. Present most challenges
  2. Will be most pervasive

# Mr. Jones in 2020…

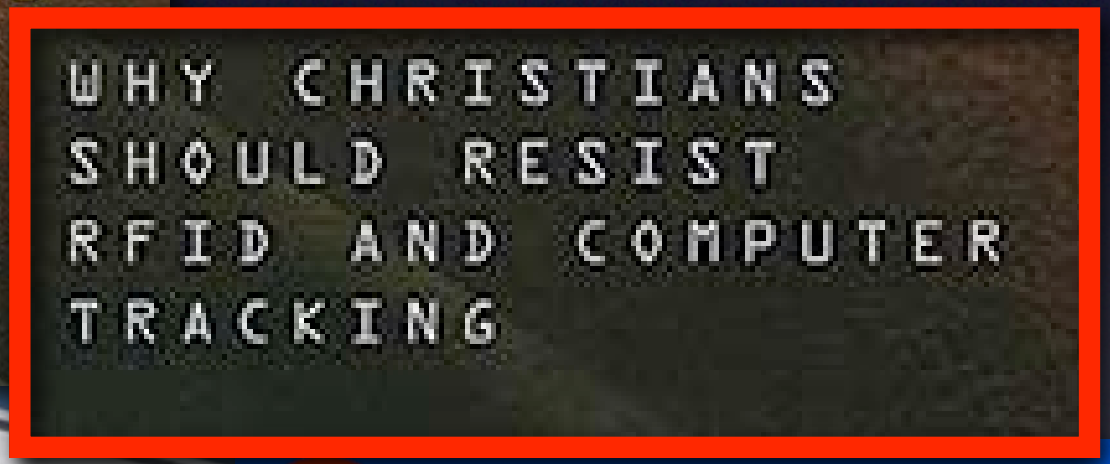


# Privacy Concerns

- *Tracking* and *inventorying:*
  1. Tags respond without alerting owner/bearer
  2. Clandestine tracking is a plausible threat
  3. Unique identifiers - can determine what objects a person is carrying
- As of today, still of limited concern:
  1. RFID infrastructure is scarce and fragmentary
  2. Tagging of individual items is still years away
  3. But might become serious threat in the future




- ...Big Brother's spychip?
- ...terrorist targeting device?
- ...work of the anti-Christ?




RFID NINETEEN EIGHTY-FOUR


Notags.co.uk

RFID Kills.com

# “Mark of the Beast”

*“And he causeth all, both small and great, rich and poor, free and bond, to receive a mark in their right hand, or in their foreheads. And that no man might buy or sell, save he that had the mark, or the name of the beast, or the number of the beast. Here is the wisdom. Let him that hath understanding count the number of the beast for it is a human number. His number is - 666.” - Revelation 13:16-18*

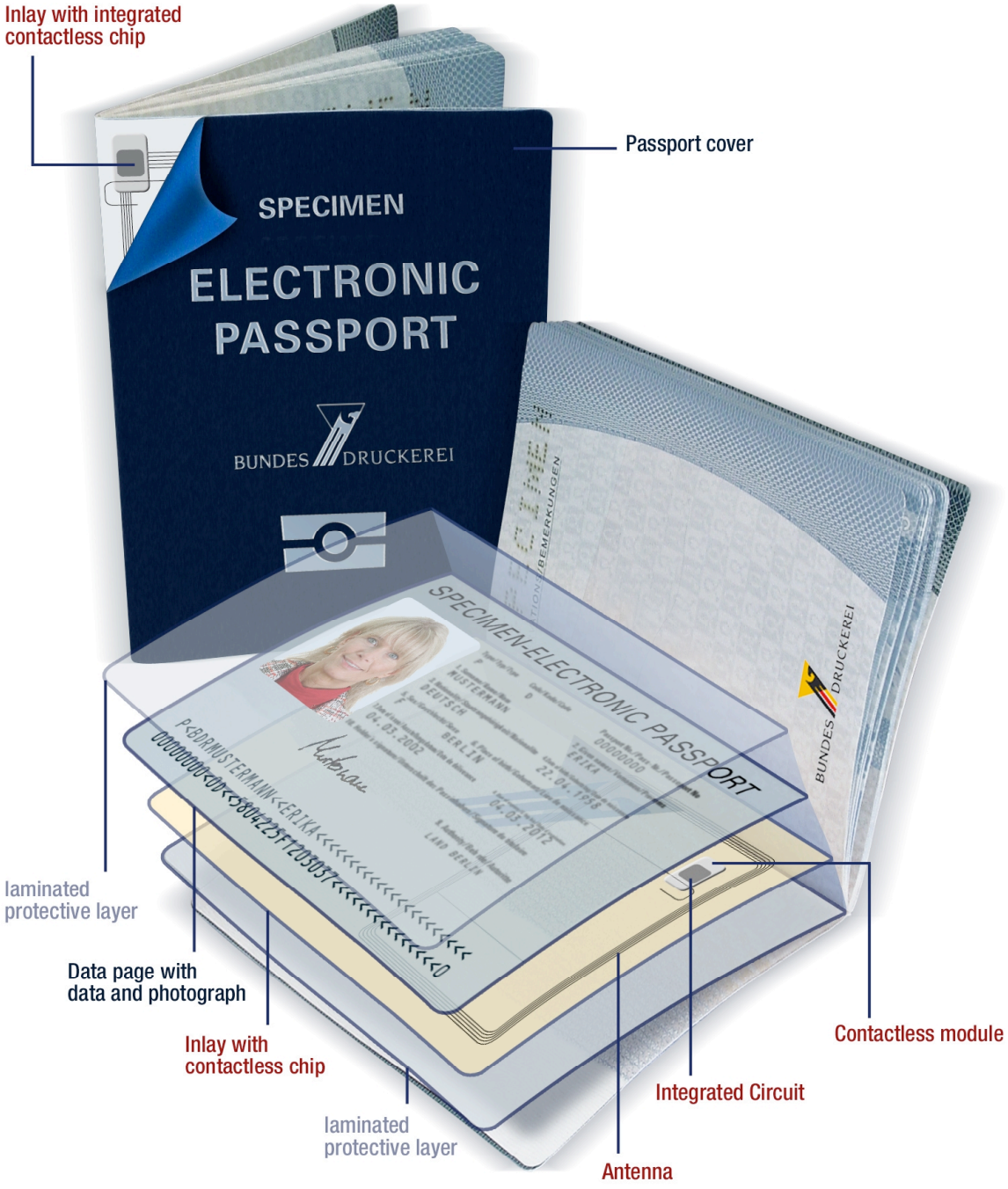
The argument:

- RFID will replace currencies/credit cards and serve as identification.
- Since tags are used as identification, they should be implanted.
- The ideal location for the implant is the forehead or the hand.

A similar argument has been made against bar-codes...

# Current Areas of Concern

- Toll payment transponders
- Euro bank-notes
- Libraries
- Supermarket cards
- Passports (US)

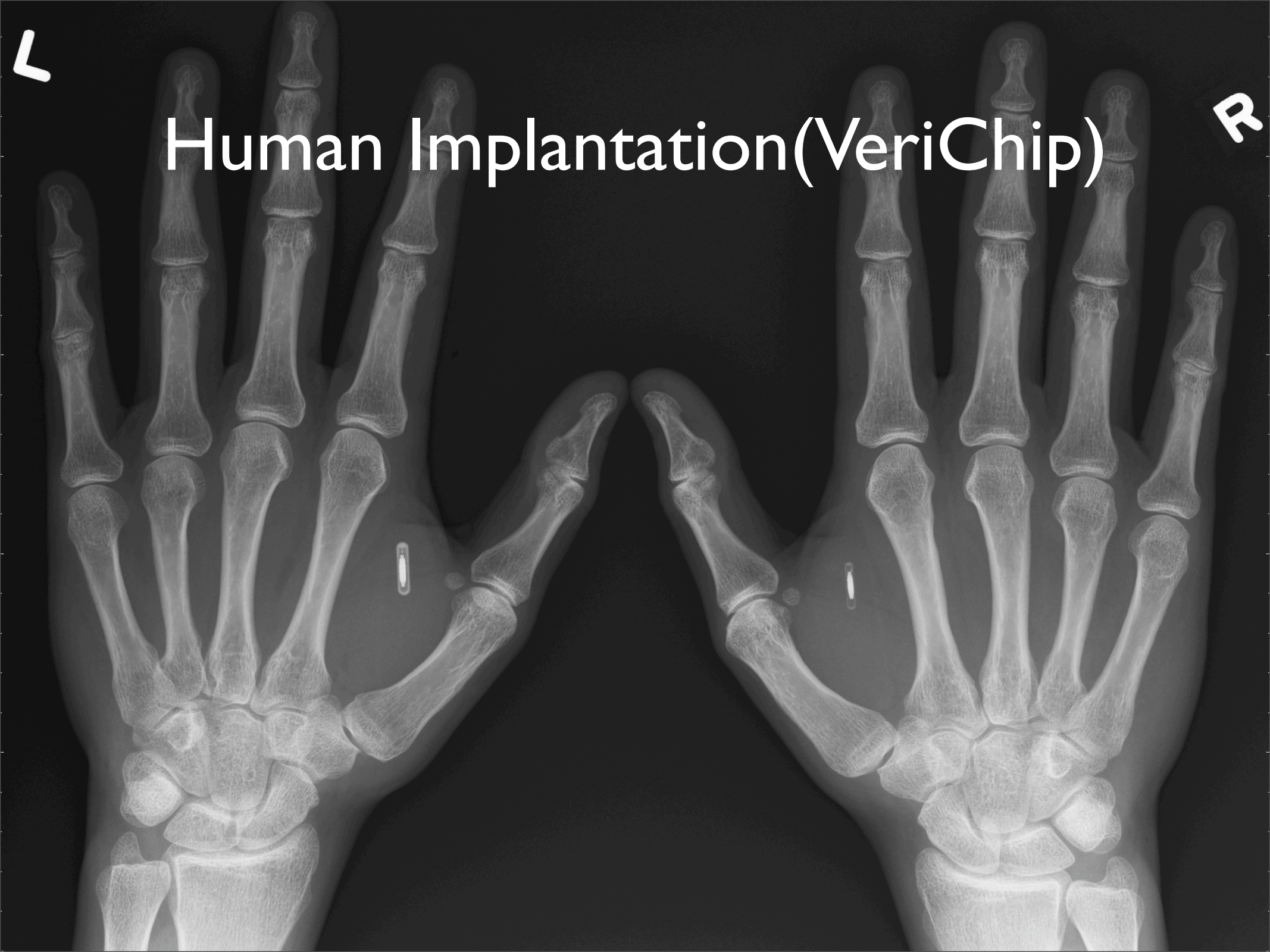



Source-Bundesdruckerei GmbH

▶ The contactless chip can be integrated into either the cover page or the data page.

# RFID Passports?

- What biometrics are stored on passports?
- Why? Who is authorized to read it?
- How can the data be abused?
- Revocation? What if I lose my passport?
- Why wireless? Why not contact?




# Human Implantation(VeriChip)

# Human Implantation(VeriChip)

# Human Implantation(VeriChip)

# Human Implantation(VeriChip)

# What About Cell Phones?

# What About Cell Phones?

- Require special equipment for reading
- Cell phones have computing power
- Bluetooth, WiFi - concerns similar to RFID

# Security Concerns

- Privacy is not the only concern
- Also relevant:
  1. Military intelligence
  2. Corporate espionage
- RFID authentication:
  1. protect against misbehaving (cloned) tag
  2. FDA called for using RFID in pharmaceutical industry
  3. Cloning is hard to prevent on EPC tags...

# Attacks on RFID

- Some possible attacks:
  1. Sniffing/eavesdropping
  2. Tracking
  3. Spoofing/cloning
  4. Replay
  5. Denial of service
- Big question: do the attacks scale up?

ExxonMobil SpeedPass

Skimming Equipment

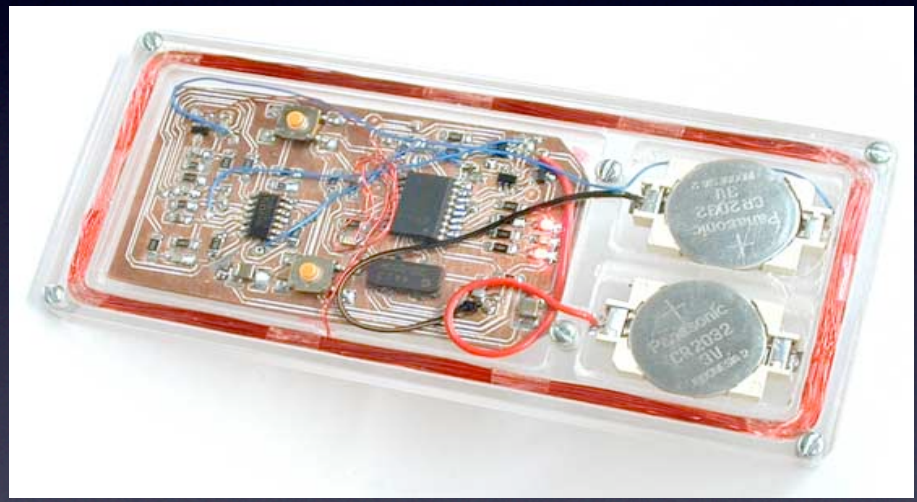
Cracking the TI DST

Buying gas with a clone

Images courtesy of rfidanalysis.org

# Proximity Card Attack


MIT RFID Proximity Card



A proximity card emulator

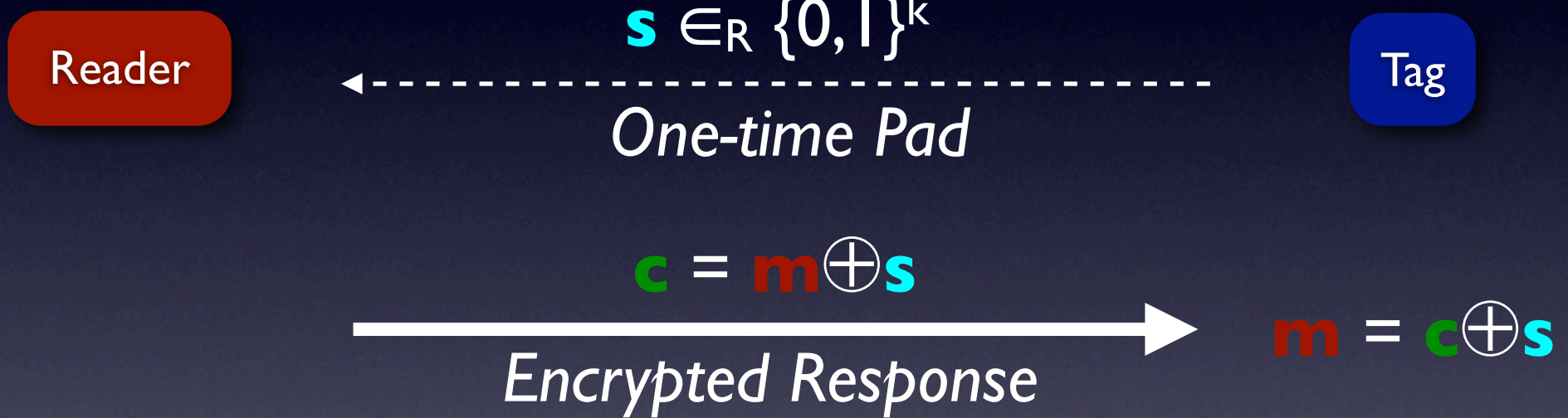
# Modeling the Adversary

- What does it mean to violate security/ privacy?
  1. Doesn't require to define what is privacy...
  2. May be application dependent
- Power of the adversary:
  1. Access to the system - reader/tag
  2. Not always in range - only occasionally

# Reading Ranges

- Nominal reading range.
- Rogue scanning range.
- Tag-to-Reader eavesdropping range.
- Reader-to-Tag eavesdropping range.
- Detection range.

# A Simple Countermeasure




- Backwards one-time pad
- Used in EPCGlobal Class-1, Gen-2

# Other Countermeasures

- RFID blocker (human body...)
- Destroy at checkout (or “kill”)
- Restrict access to ONS
- “re-labeling”
- Cryptography

# Blocker Tags

- Juels, Rivest & Szydlo (2003)
- Device for enhancing personal privacy
- Injects itself in anti-collision protocol to restrict access to tags a person carries
- An idea is to put blocker tags in bags
- Not a commercial product

# Privacy Bits

- Juels and Brainard
- Tag responses contain an access control policy: "It's okay/not okay to read me"
- Readers may choose to obey policy
- Corrupt readers risk being caught

# Destroy at Checkout

- EPC enables to “kill” tag
- Removable RFID price tag works well
- Only addresses individual privacy issues
- Does not allow end-user applications
- “sleep” instead of “kill?”

SIMPill

# Back-End Access Control

- Object Naming Service (ONS) -- look up ID numbers and returns product codes
- Why not restrict access to ONS?
- Still allows tracking of predictable tags
- Centralized lookups are too slow
- Could change tag IDs. How to manage?

# Cryptography

- Use secure authentication protocols
- Problems:
  1. Hard to find source of randomness
  2. Very low computing capabilities
  3. Moore's law in conflict w/ large scale economics

# Cryptography Costs

- Standard DES and AES take 4-20K gates
- SHA-1 hash function takes ~20K gates
- Most tags couldn't even hold an RSA key
- Some hope: Low-cost AES, ECC, NTRU, low-cost authentication (more later)

# Hash-Based Schemes

- Several ideas rely on one-way functions
- Access Control (aka Hash Locks):
  Reader locks tag with $H(x)$, unlocks with $x$
- Private Identification:
  Tag sends $(r, H(ID,r))$, reader hashes its IDs
- How do we build cheap one-way functions?

# Low Cost Protocols

- Juels and Weis (05) propose several authentication protocols
- Extremely hardware efficient
- Based on protocols for human identification (Hopper-Blum).
- Rely on hardness of learning parity w/ noise

# Conclusion

- Over-hype.
- Lots of privacy issues
- We barely scratched the surface:
  1. Talked only about tags and readers
  2. What about infrastructure?
- Large scale is a dominant factor:
  1. Key/PIN management
  2. ONS management