RFID Privacy: What's in Your Pocket?

Kevin Fu

kevinfu@cs.umass.edu

Assistant Professor
Department of Computer Science
University of Massachusetts Amherst, USA

www.rfid-cusp.org

The Sixth Conference on Computers, Freedom, and Privacy

CFP96@MIT

March 27-30, 1996
Massachusetts Institute of Technology
Cambridge, Massachusetts

CLIPPER 2.1

SpyWare

(NIST 64-bit Software Key Escrow Encryption standard

Features

- Mandatory key escrow (MKE)
- Government certified escrow agents
- Compatability with national wiretap plan
- NON-interoperable with all current crypto systems
- Limited key length and no Triple-DES

EPIC Review

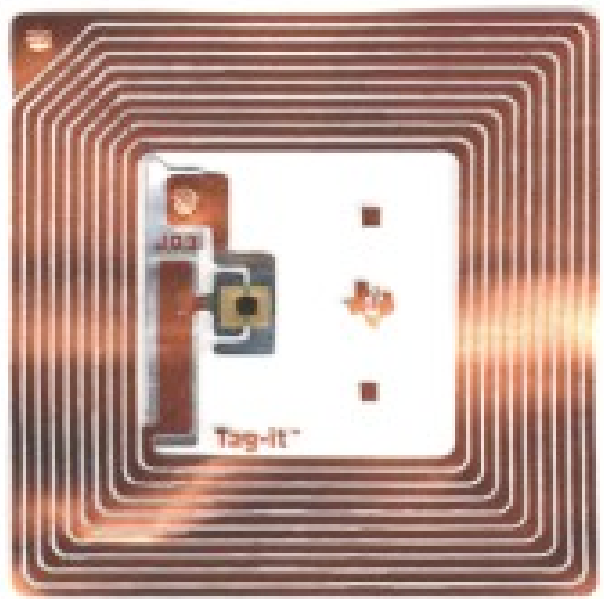
"Clipper 2.1 is the software implementation of the popular Clipper chip. With all the great features of the original, NIST picks up where the NSA left off. Some undocumented features."

From the (classified) Users Manual:
"Prohibits cryptography that is not capable of real-time decryption by law enforcement"

Electronic Privacy Information Center
Washington, DC
http://www.epic.org/

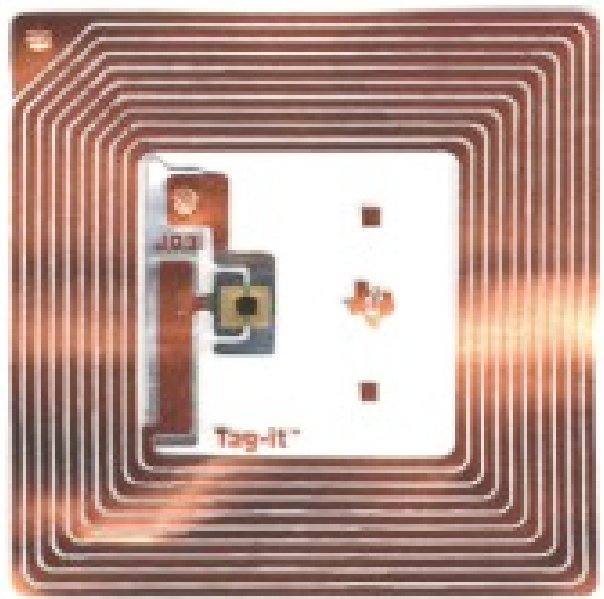
ters,

RFID tags in a nutshell



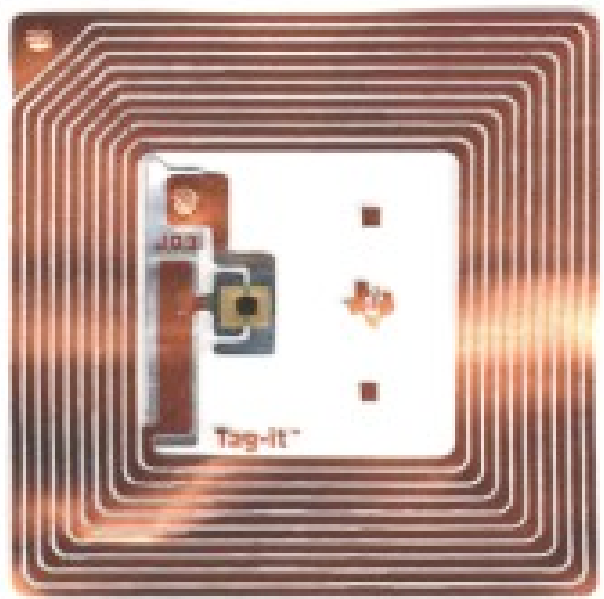
RFID tags in a nutshell

- Originally simple bar code replacement



RFID tags in a nutshell

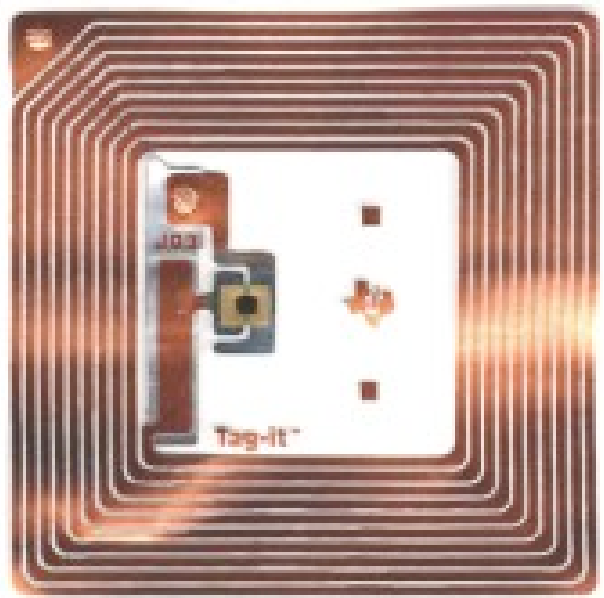
- Originally simple bar code replacement
- Now are mini, low-power computers



RFID tags in a nutshell

- Originally simple bar code replacement
- Now are mini, low-power computers

Identify a class
of product

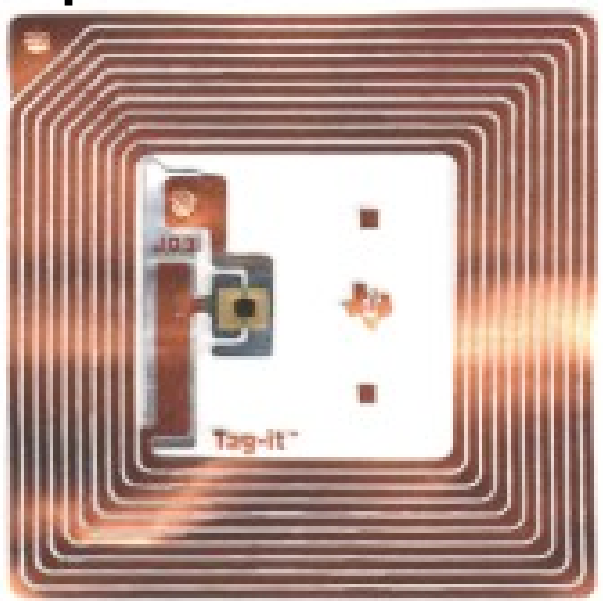


RFID tags in a nutshell

- Originally simple bar code replacement
- Now are mini, low-power computers

Identify a class of product

Identify a particular item



RFID tags in a nutshell

- Originally simple bar code replacement
- Now are mini, low-power computers
- Applications

RFID tags in a nutshell

- Originally simple bar code replacement
- Now are mini, low-power computers
- Applications
  - E-commerce

RFID tags in a nutshell

- Originally simple bar code replacement
- Now are mini, low-power computers
- Applications
  - E-commerce
  - Public transportation

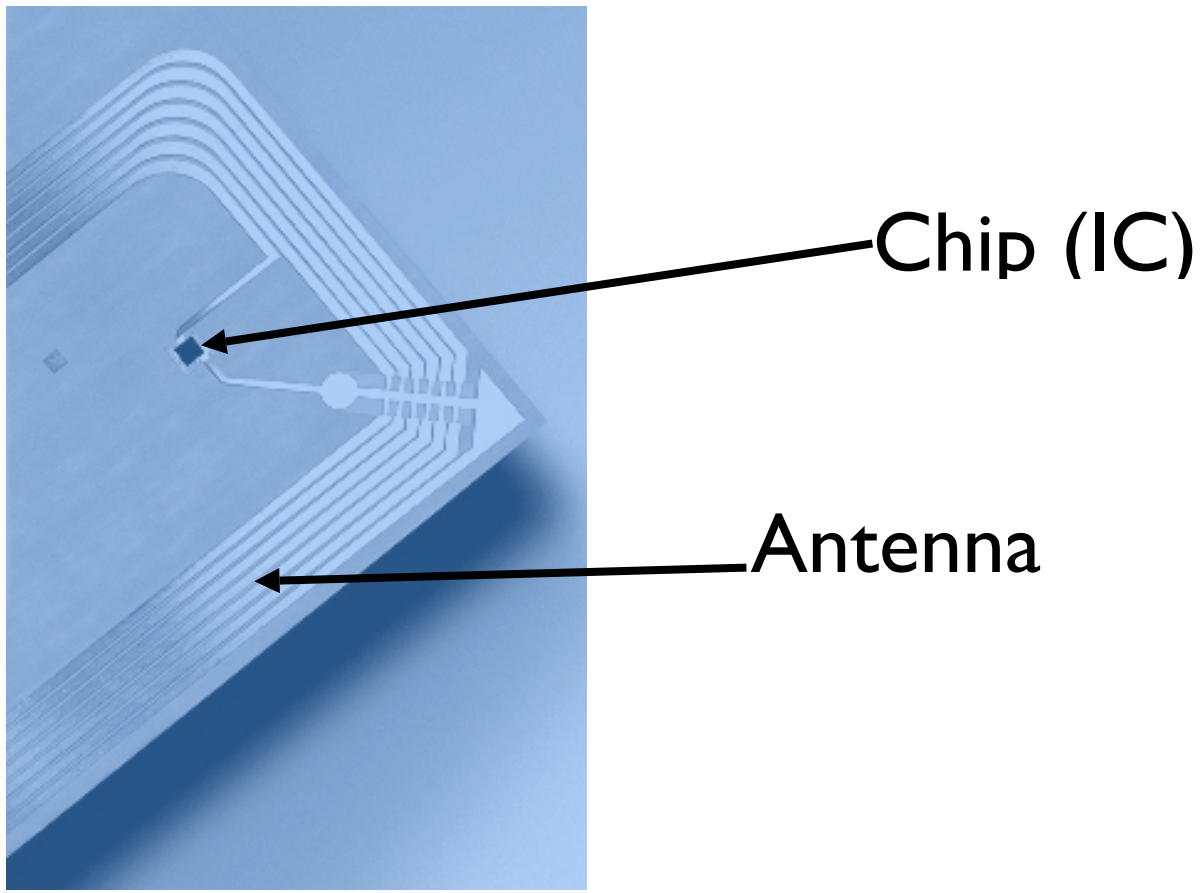
RFID tags in a nutshell

- Originally simple bar code replacement
- Now are mini, low-power computers
- Applications
  - E-commerce
  - Public transportation
  - Pharmaceutical anti-counterfeiting

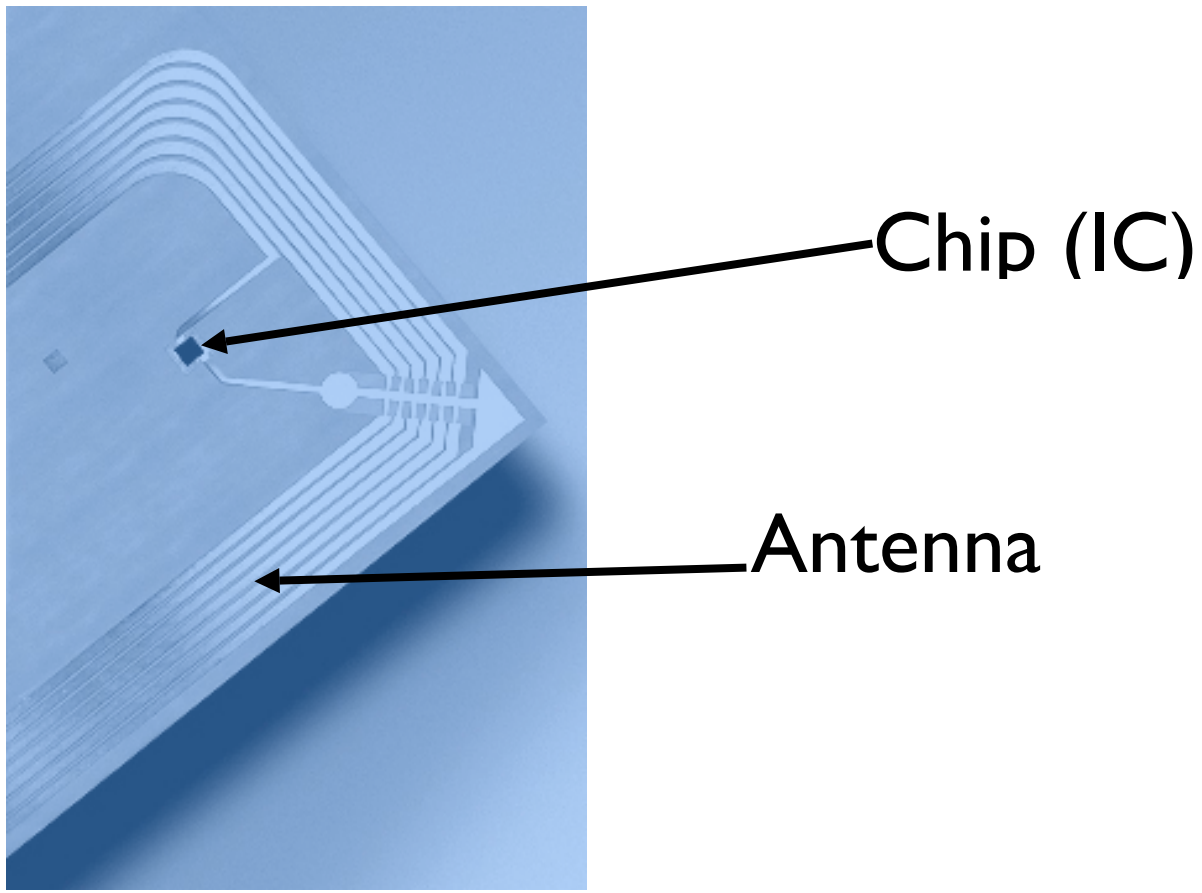
RFID tags in a nutshell

- Originally simple bar code replacement
- Now are mini, low-power computers
- Applications
  - E-commerce
  - Public transportation
  - Pharmaceutical anti-counterfeiting
  - Medical applications

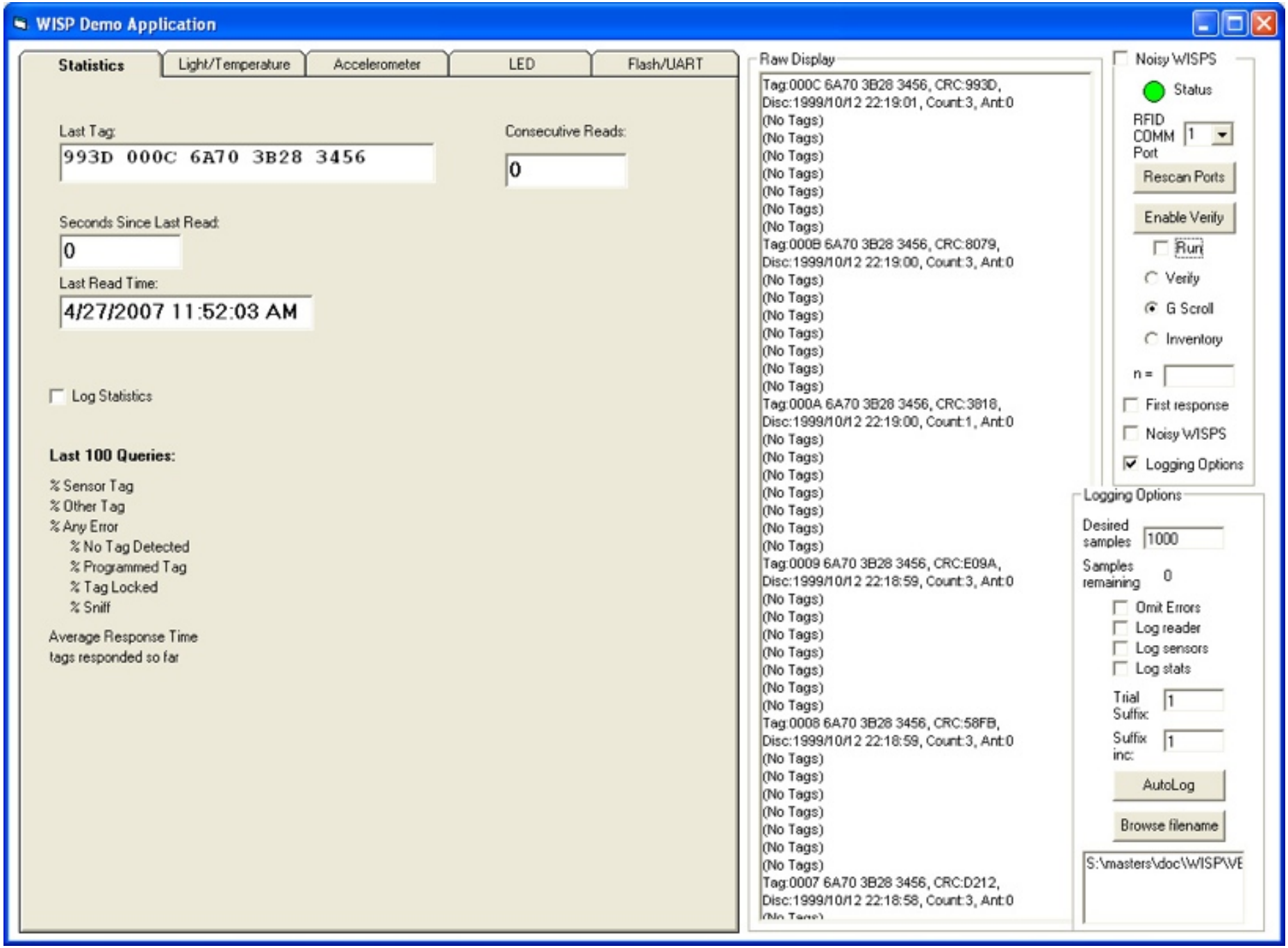
What's a Radio-Frequency Identification (RFID) tag?



What's a Radio-Frequency Identification (RFID) tag?



EPC "supply chain" tags


WISP Demo Application
Statistics
Light/Temperature
Accelerometer
LED
Flash/UART
Last Tag:
993D 000C 6A70 3B28 3456
Consecutive Reads:
0
Seconds Since Last Read:
0
Last Read Time:
4/27/2007 11:52:03 AM
Log Statistics
Last 100 Queries:
% Sensor Tag
% Other Tag
% Any Error
% No Tag Detected
% Programmed Tag
% Tag Locked
% Sniff
Average Response Time
tags responded so far
Raw Display
Tag:000C 6A70 3B28 3456, CRC:993D,
Disc:1999/10/12 22:19:01, Count:3, Ant:0
(No Tags)
Tag:000B 6A70 3B28 3456, CRC:8079,
Disc:1999/10/12 22:19:00, Count:3, Ant:0
Tag:000A 6A70 3B28 3456, CRC:3818,
Disc:1999/10/12 22:19:00, Count:1, Ant:0
Tag:0009 6A70 3B28 3456, CRC:E09A,
Disc:1999/10/12 22:18:59, Count:3, Ant:0
Tag:0008 6A70 3B28 3456, CRC:58FB,
Disc:1999/10/12 22:18:59, Count:3, Ant:0
Tag:0007 6A70 3B28 3456, CRC:D212,
Disc:1999/10/12 22:18:58, Count:3, Ant:0
Noisy WISPS
Status
RFID COMM Port
1
Rescan Ports
Enable Verify
Run
Verify
G Scroll
Inventory
n =
First response
Noisy WISPS
Logging Options
Logging Options
Desired samples
1000
Samples remaining
0
Omit Errors
Log reader
Log sensors
Log stats
Trial Suffix
1
Suffix inc:
1
AutoLog
Browse filename
S:\masters\doc\WISP\VE

Capabilities of basic RFID tags

Capabilities of basic RFID tags

- Often no tethered power

Capabilities of basic RFID tags

- Often no tethered power
- Limited memory

Capabilities of basic RFID tags

- Often no tethered power
- Limited memory
- Limited computational power

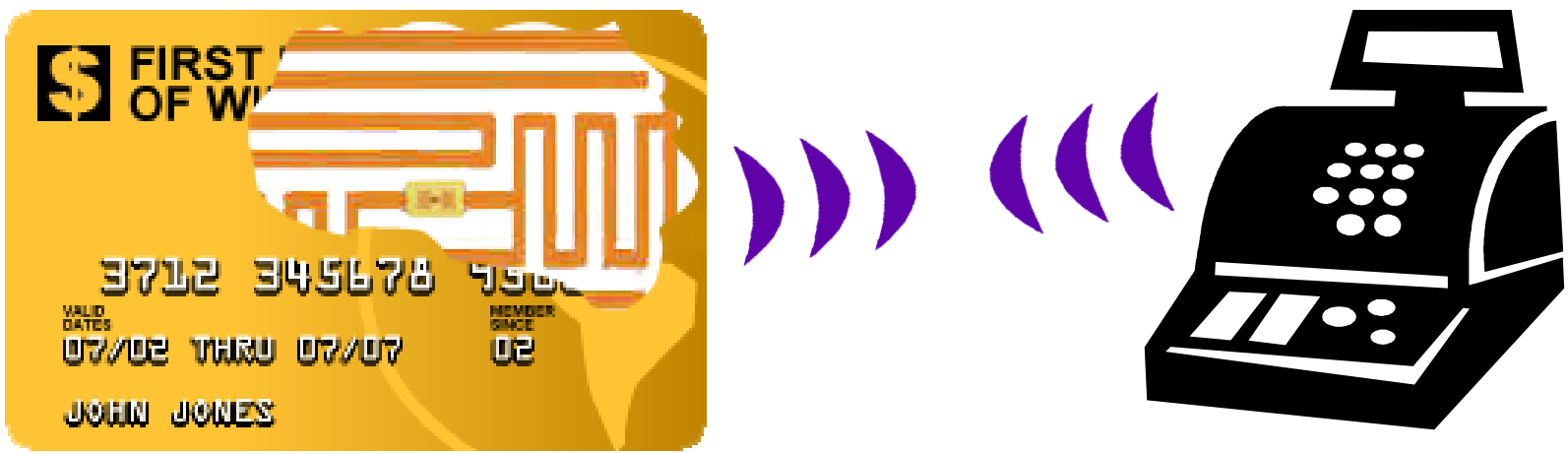
Capabilities of basic RFID tags

- Often no tethered power
- Limited memory
- Limited computational power
- Debatable read ranges

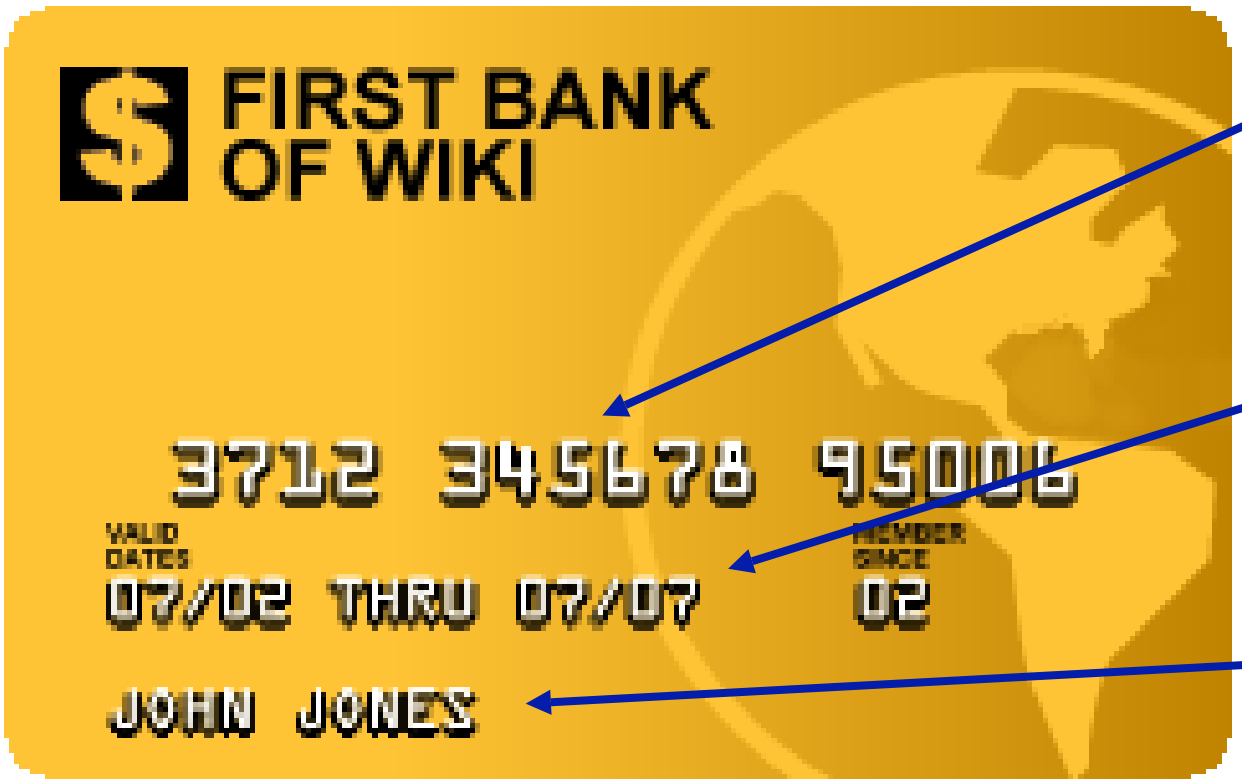
Case Study:
RFID Credit Cards

What are RFID Credit Cards?

- **"No-swipe"** credit card
- "fastest acceptance of new payment technology in the history of the industry." [VISA; As reported in the Boston Globe, August 14th 2006]



What do RFID CCs Reveal?



- Credit card number
- Expiration date
- Cardholder name


MASTERCARD COMMERCIAL
abc NEWS

How to disable an RFID CC

How to improve privacy

- Consumers need
  - ✓ Justified confidence
    - Not just "security theater" marketing
- Technology must be **open** to public scrutiny
  - RFID CCs use **proprietary** methods
  - ✓ Secure Web sites use a **public** methods

Summary of RFID CCs

- More convenient? (maybe)
- Good fraud control? (maybe)
- Consumer Privacy? (not yet)