Data Security Risks:
RFID Lab Research

Kevin Fu

kevinfu@cs.umass.edu

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

www.rfid-cusp.org

Computer Science UMASS

RFID Consortium for Security and Privacy

RFID tags in a nutshell

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

Identify a class of product

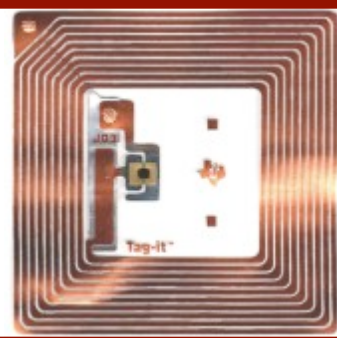
Identify a particular item

RFID tags in a nutshell

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

Wide variety of RFID tech

- Low-frequency tags
  - Car immobilizer, human implants
- High-frequency tags
  - Credit card, passport, subway pass



- Ultra-high-frequency tags
  - Supply chain, EZPass toll

Japan Public Transportation

Current Balance

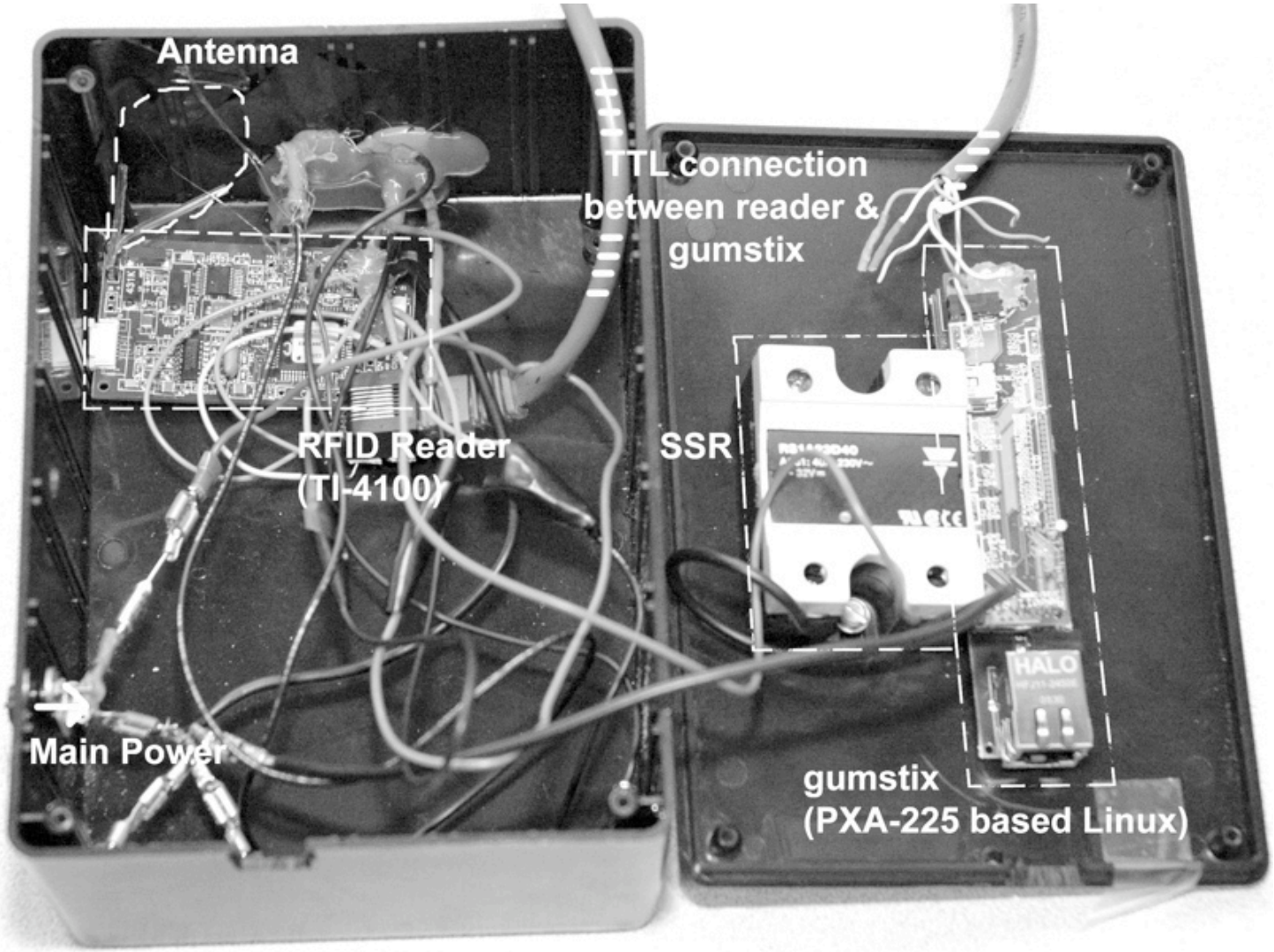
Entrance and exit date and station

Details of merchandise purchase

Beginning Balance

RFID Applications from the Lab

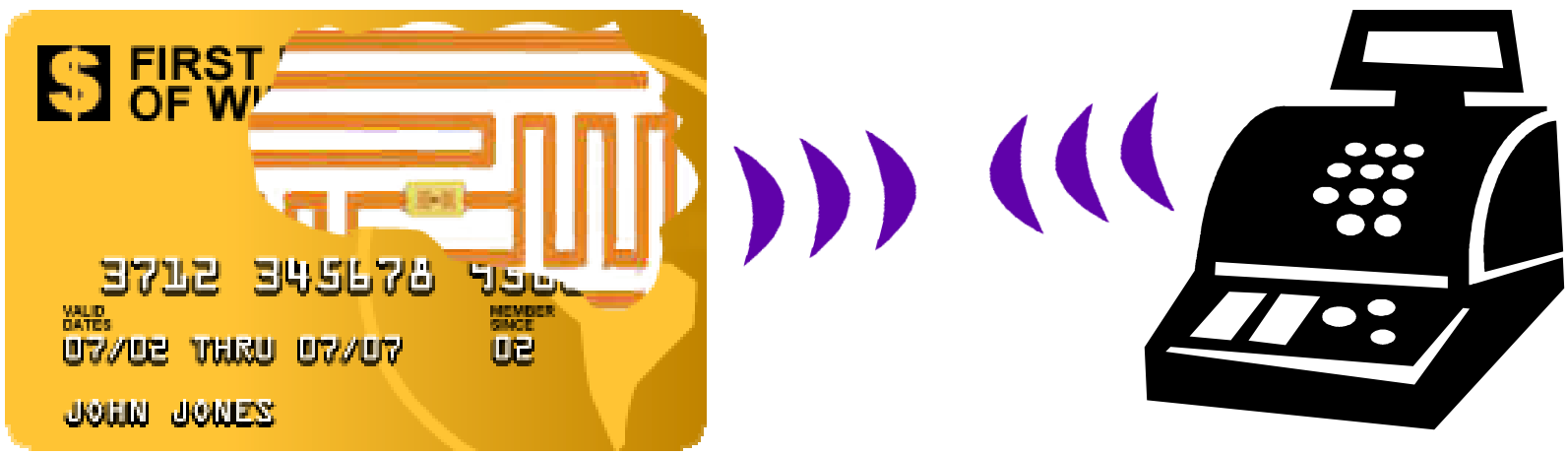
espress pay


Antenna
TTL connection
between reader &
gumstix
RFID Reader
(TI-4100)
SSR
Main Power
gumstix
(PXA-225 based Linux)

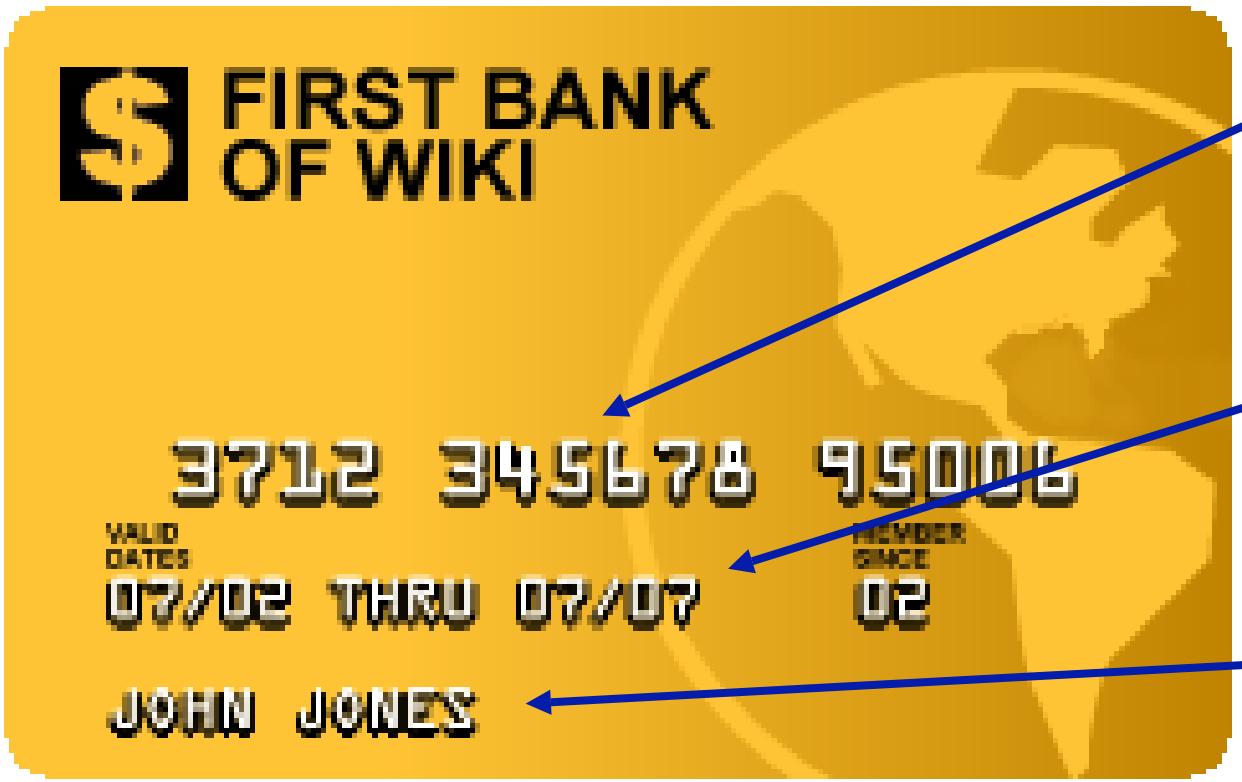
Case Study:
RFID Credit Cards

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

The New York Times

Researchers See Privacy Pitfalls in No-Swipe Credit Cards

By JOHN SCHWARTZ
Published: October 23, 2006

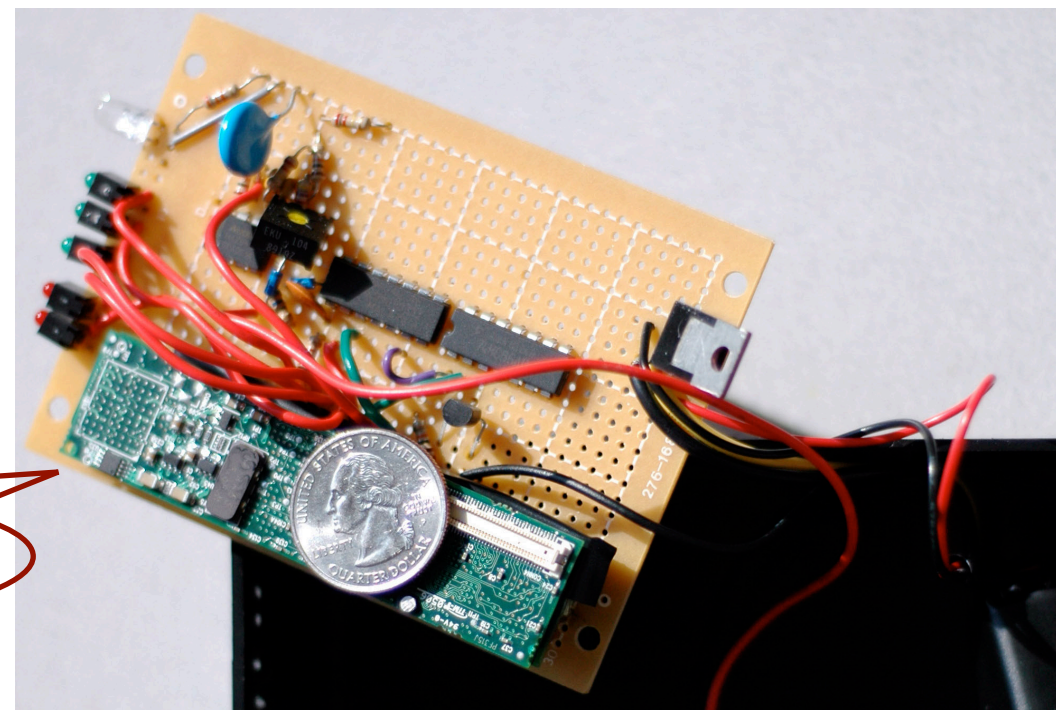

MASTERCARD COMMERCIAL
abc NEWS

Replay: Credit Card Cloning

- Some cards send same data for diffrent transactions
- Our device replays the radio conversation

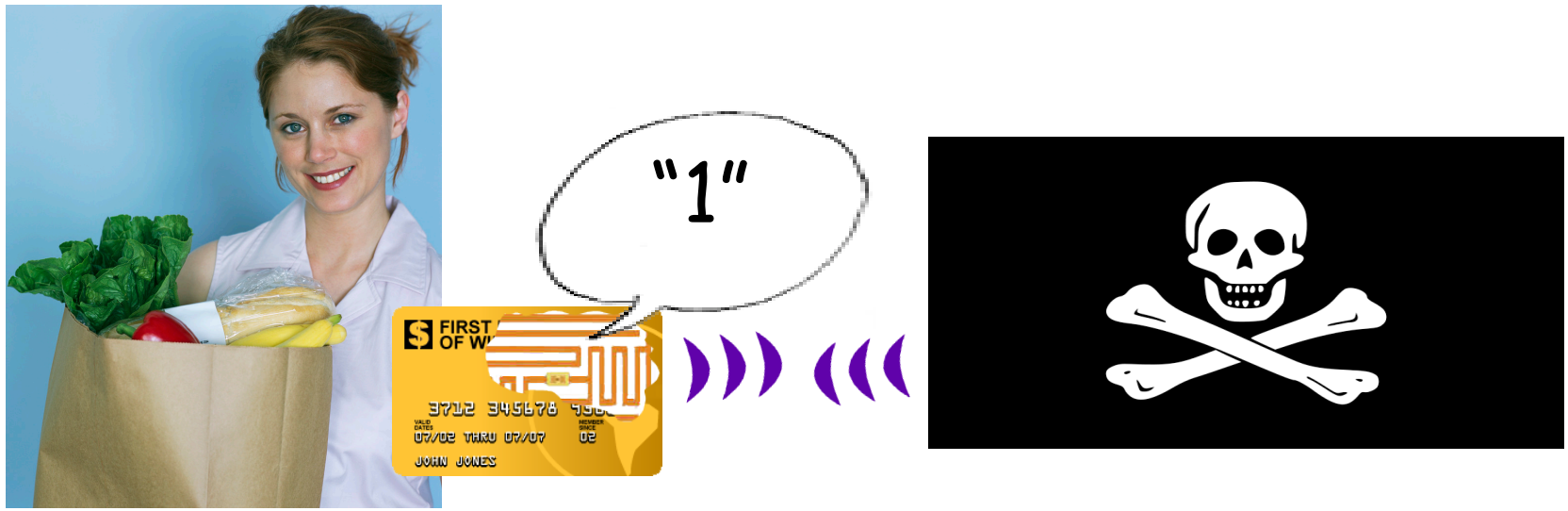
I'm Kevin's Card.
I'm Kevin's Card.
I'm Kevin's Card.

I'm Kevin's Card.



Replay: Transaction Counters

- A transaction counter can deter simple replays

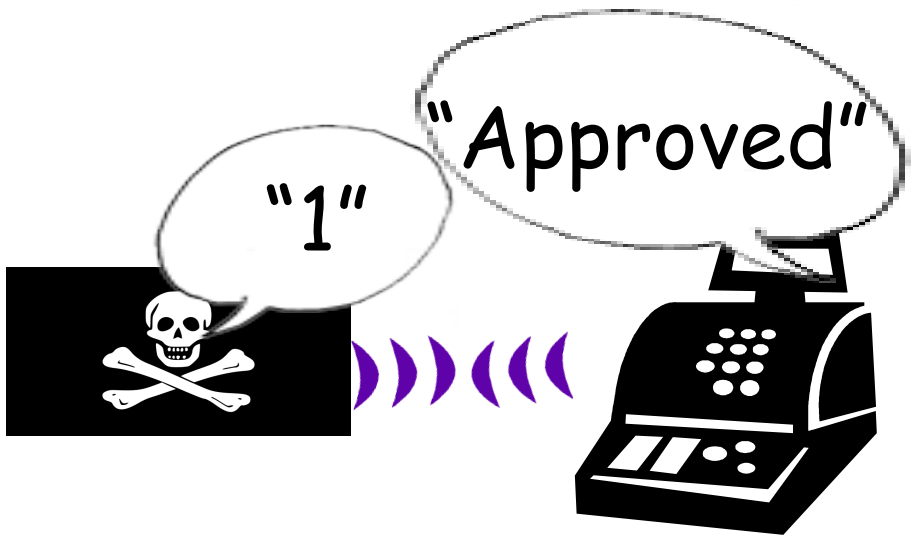


Replay: Transaction Counters

- Under some circumstances counter prevents replay

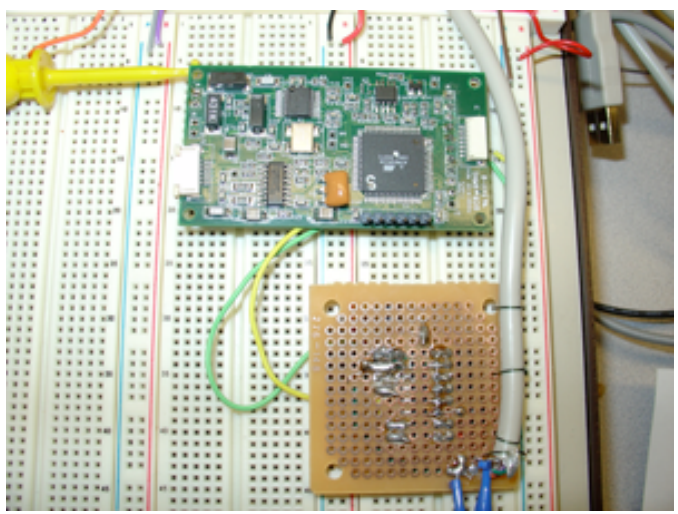
Replay: Transaction Counters

- But the counter is not foolproof



Cross contamination of other payment media

- New credit card in sealed envelope
- Scanned with programmable reader
- Retrieved address from phone book
- Bought electronics online



Countermeasures

- Radio shielding
  - Caution: Does not protect during use

- Recent cards omit cardholder name
  - Caution: Could lower the bar on other attacks

Countermeasures

- Better use of cryptography
  - Not only prevent fraud
  - But also protect privacy
- Smarter devices (e.g., NFC)
  - Easier for user to give consent
  - Capable of much more!

How to improve privacy

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

Beware: Academics create insecure RFID too

- Protocol authenticates a tag
- Tag supposed to be hard to clone
- Seems secure in theory:
  40 trillion attempts to crack (centuries)
- But not really:
  3 attempts in practice (seconds)

["Lightweight Authentication Protocols for Low-Cost RFID Tags" by I. Vajda and L. Buttyan. In UBICOMP, 2003.]

Conclusions: RFID Security Research

- RFID is neither good nor bad
  - But should be used properly and responsibly
- RFID credit cards
  - Personal information disclosed
- Future RFID security and privacy
  - Better security is coming, but check the fine print

RFID

Consortium for Security and Privacy

rfid-cusp.org

UNIVERSITY OF MASSACHUSETTS AMHERST 1863

Johns Hopkins University Information Security Institute

NSF

RSA

The Security Division of EMC

UMass RFID Research Center

Yanlei Diao
RFID data management

http://rfid.cs.umass.edu/

UMass Center for Advanced RFID Research

5 faculty + 9 students

Prashant Shenoy
RFID software systems

Kevin Fu
RFID security & privacy

Wayne Burleson
Secure RFID Hardware

Mark Corner
RFID locationing and mobile readers

Computer Science UMASS

rfid-cusp.org

RFID Consortium for Security and Privacy