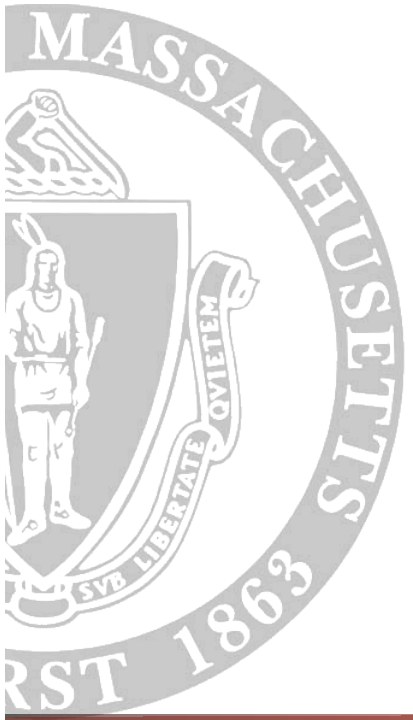
RFID Security & Privacy:
What's in Your Pocket?



Dr. Kevin Fu, PhD
Department of Computer Science
University of Massachusetts Amherst

http://www.cs.umass.edu/~kevinfu/

2008 Payments Conference, June 6, 2008
Federal Reserve Bank of Chicago

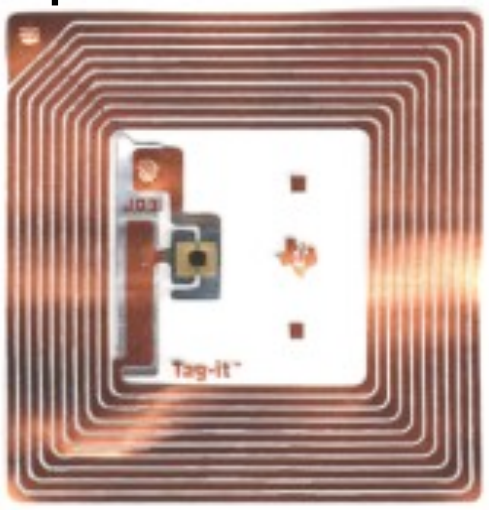
No-swipe credit cards

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



What's special about security?

Correctness is easy.

Security is hard.

Case Study: RFID Credit Cards

What are RFID-enabled 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]

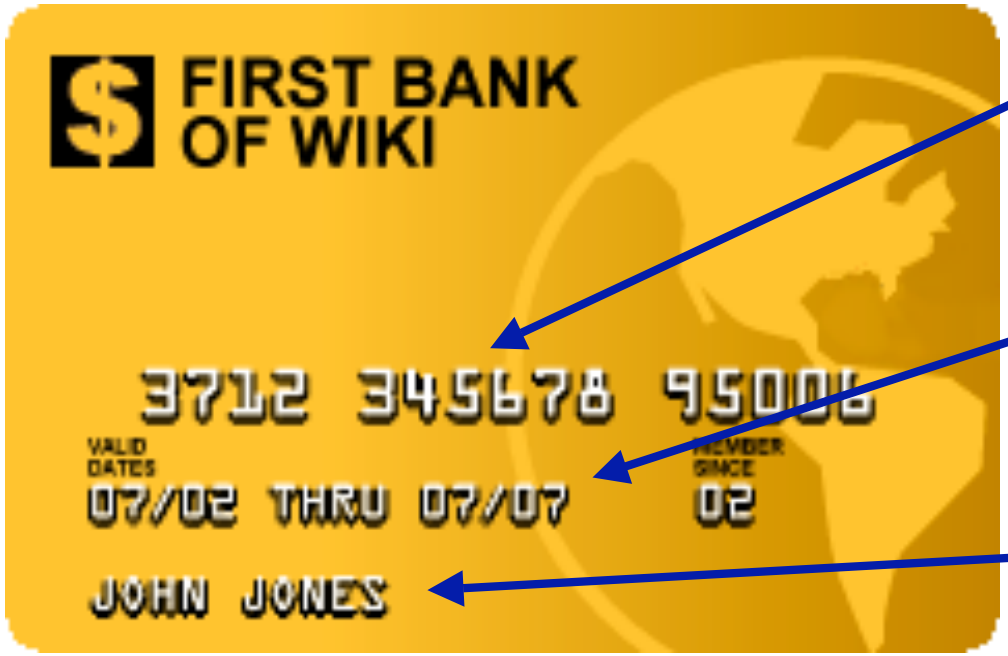
The New York Times

Researchers See Privacy Pitfalls in No-Swipe Credit Cards

By JOHN SCHWARTZ
Published: October 23, 2006

E-MAIL

What do RFID CCs Reveal?



Credit card number

Expiration date

Cardholder name

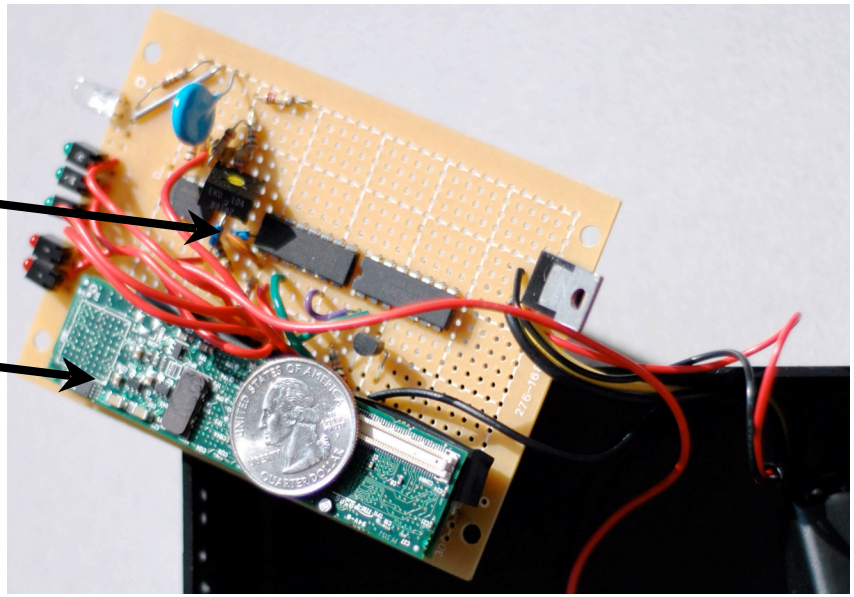
- Newer cards are beginning to withhold the cardholder name


sports drink: $2
abc NEWS

Replay: Credit Card Cloning

Radio modulation

Gumstix w/ Linux



How to Disable an RFID-enabled CC

Next: NFC Phones and Security?

NFC Usage Concept

- Touch tag with your mobile phone
  - Phone reads tag ⇨ performs action

Next: NFC Phones and Security?

RFID WORLD

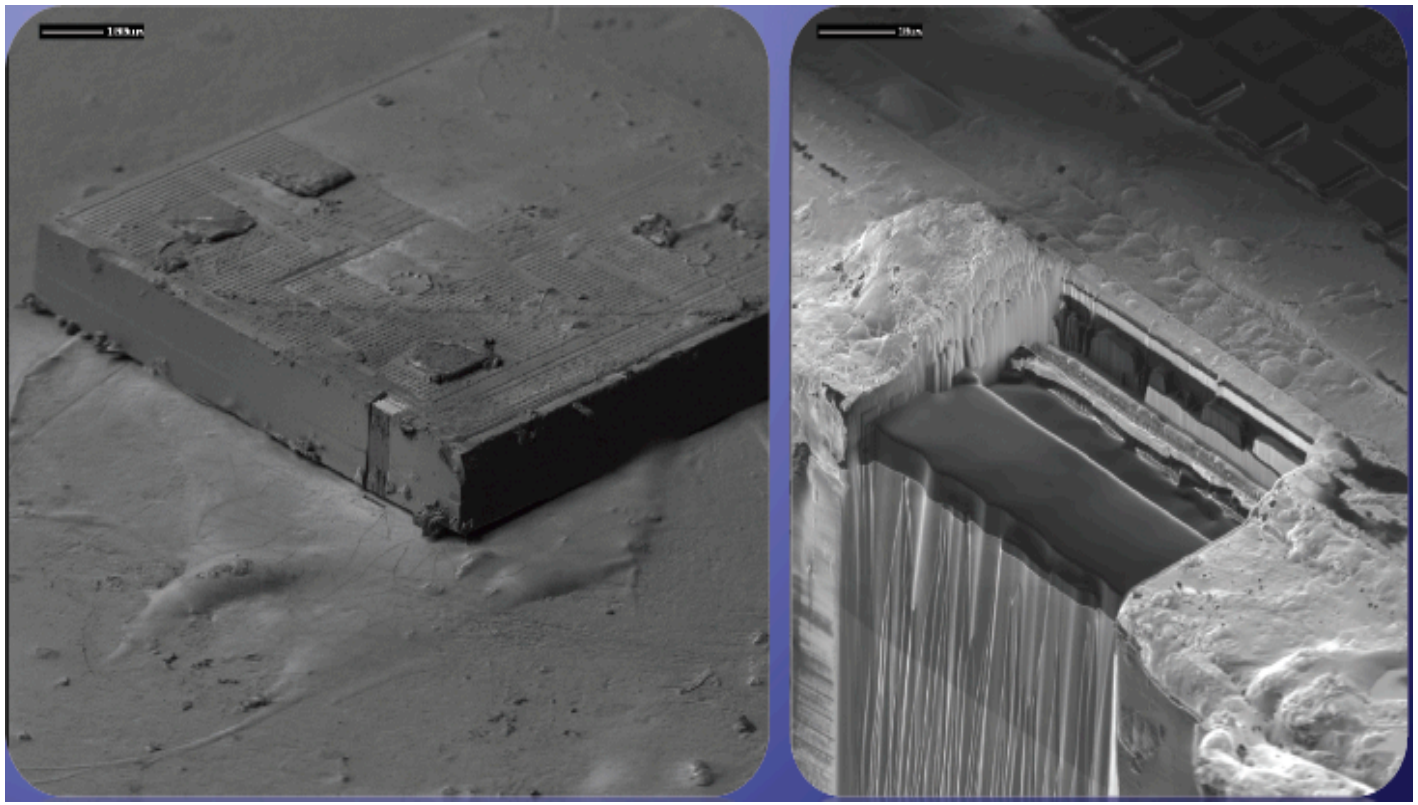
April 2008

NFC Phones: Next Hacker Target

By Karsten Nohl, doctorial candidate at the University of Virginia

"The **lack of mandatory security** for NFC-RFID communication reflects the general immaturity of RFID technology, which still progresses toward lower prices rather than better protection."

Next: NFC Phones and Security?



Credit: Karsten Nohl

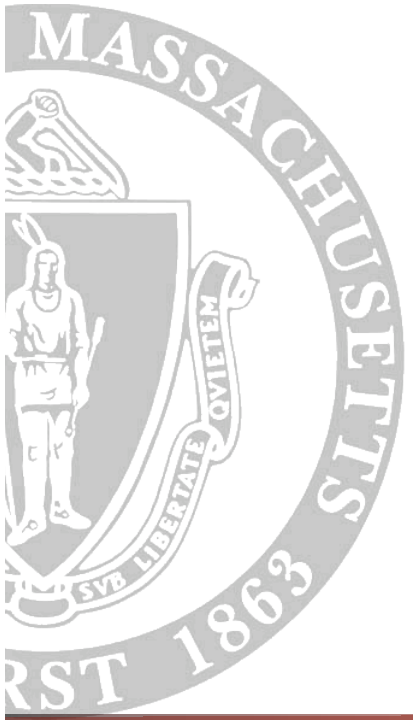
Next? Chip and Pin

http://www.cl.cam.ac.uk/research/security/banking/ped/

Summary: How to Improve Privacy

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

RFID Security & Privacy:
What's in Your Pocket?



Dr. Kevin Fu, PhD
Department of Computer Science
University of Massachusetts Amherst

http://www.cs.umass.edu/~kevinfu/

2008 Payments Conference, June 6, 2008
Federal Reserve Bank of Chicago

RFID Consortium for Security & Privacy

RFID

Consortium for Security and Privacy

rfid-cusp.org

The Security Division of EMC

Acknowledgments

Dan Bailey, Wayne Burleson, Thomas S. Heydt Benjamin, Hee-Jin Chae, Benessa Defend, Daniel Holcomb, Ari Juels, Tom O'Hare, Joshua Smith, Dan Yeager