Vulnerabilities in First-Generation RFID-enabled Credit Cards

Thomas S. Heydt-Benjamin[1], Daniel V. Bailey[2], Kevin Fu[1], Ari Juels[2], and Thomas O'Hare[3]

[1]University of Massachusetts Amherst
Department of Computer Science

[2]*RSA Laboratories*

RSA
The Security Division of EMC

[3]*Innealta, Inc.*

What are RFID Credit Cards?

- Small mobile computing devices
- Transmit credit card information to reader over RF
- Passive 13.56MHz RFID transponder (ISO 14443-B)
  - Read range unknown, suspected to be around 10cm to 30cm
- “fastest acceptance of new payment technology in the history of the industry.”

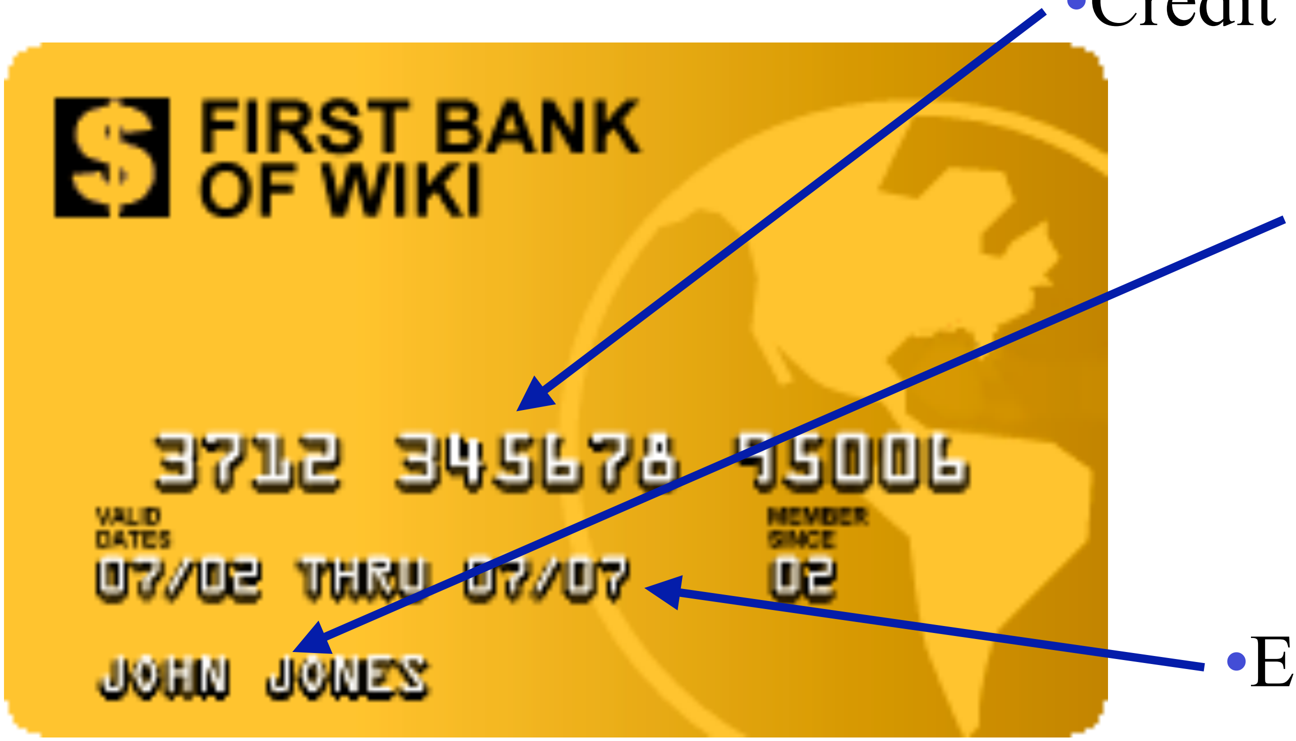
[VISA; As reported in the Boston Globe, August 14th 2006]

An RFID Credit Card Purchase

- User “Alice” authorizes purchase by simply bringing card into proximity with reader
- Some kinds of fraud can be detected or prevented by the back-end charge processing network
- Charge processing networks are complex and heterogeneous
- In this work we primarily consider the security of the RF portion of the transaction

FIRST OF W
3712 345678 9
07/02 THRU 07/07
JOHN JONES
COMPLEX!

Some of the data revealed over RF



- Credit card number
- Cardholder name
- Expiration date

- Exceptions:
  - One type of card uses separate numbers for front of card and RF interface.
  - We have recently observed cards that withhold the Cardholder name

Talk Outline

- Background
  - What vulnerabilities exist?
- Selected Experiments
  - How can the vulnerabilities be demonstrated?
- Countermeasures
  - How can the vulnerabilities be mitigated?

What Vulnerabilities Exist?

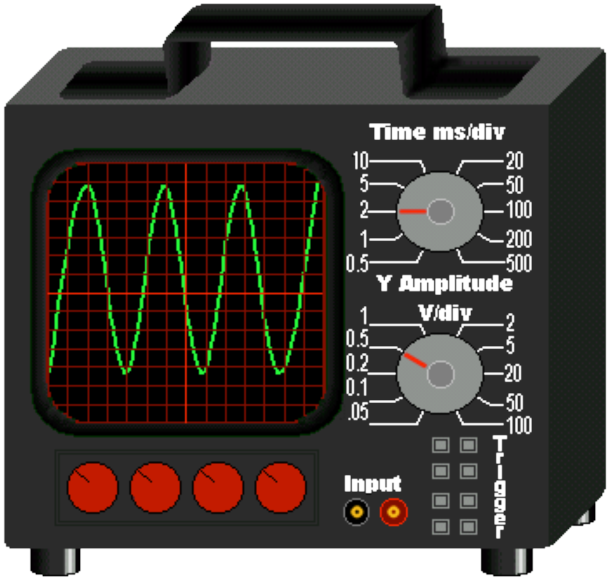
- Personally Identifying Data (PID) Disclosure
  - Credit card or other user specific data disclosed
  - Financial fraud is not the only reason to protect PID
    - Consumer confidence
    - Legal concerns
- Cross-Contamination
  - Data from RF transmission used in a different context
  - For example; a web purchase

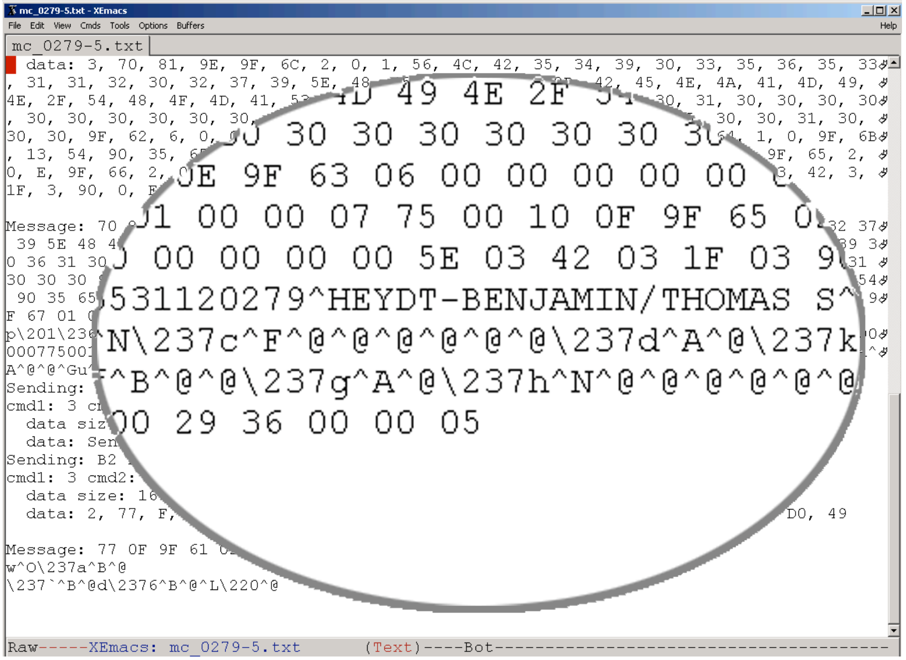
What Vulnerabilities Exist?

- Replay
  - Data obtained over RF are played back by adversary
- Relay
  - Queries from reader relayed by adversary to credit card without Alice's knowledge or consent
- Many other RFID privacy vulnerabilities
  - For example: [JMW05]

Eavesdropping

- Equipment: Antenna, Oscilloscope, Laptop
- Demonstrates:
  - Data disclosed in the clear before any challenge-response
  - No authentication of reader



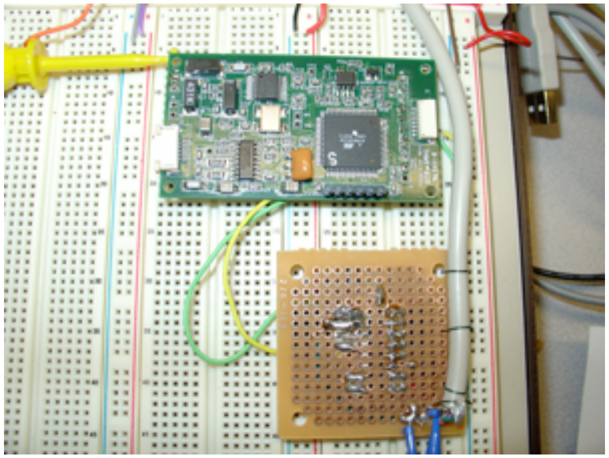

mc_0279-5.txt - XEmacs
File Edit View Cmds Tools Options Buffers Help
mc_0279-5.txt
Raw-----XEmacs: mc_0279-5.txt (Text)----Bot------------------------------------

```
 data: 3, 70, 81, 9E, 9F, 6C, 2, 0, 1, 56, 4C, 42, 35, 34, 39, 30, 33, 35, 36, 35, 33
, 31, 31, 32, 30, 32, 37, 39, 5E, 48                42, 45, 4E, 4A, 41, 4D, 49,
4E, 2F, 54, 48, 4F, 4D, 41,                          30, 31, 30, 30, 30, 30
, 30, 30, 30, 30, 30, 30,                             30, 30, 31, 30,
30, 30, 9F, 62, 6, 0,                                  1, 0, 9F, 6B
, 13, 54, 90, 35,                                        9F, 65, 2,
0, E, 9F, 66, 2,                                         3, 42, 3,
1F, 3, 90, 0, F

Message: 70                                                   32 37
 39 5E 48 4                                                   39 3
0 36 31 30                                                    31
30 30 30                                                      54
 90 35 65                                                     9
F 67 01 0
p\201\236                                                     0
000775001                                                     ^
A^@^@^Gu
Sending:
cmd1: 3 c
  data siz
  data: Sen
Sending: B2
cmd1: 3 cmd2:
  data size: 16
  data: 2, 77, F,                                            D0, 49

Message: 77 0F 9F 61 0
w^O\237a^B^@
\237`^B^@d\2376^B^@^L\220^@
```

```
4D 49 4E 2F 54
00 30 30 30 30 30 30 30
0E 9F 63 06 00 00 00 00 00 0
01 00 00 07 75 00 10 0F 9F 65 0
0 00 00 00 00 5E 03 42 03 1F 03 9
531120279^HEYDT-BENJAMIN/THOMAS S^
^N\237c^F^@^@^@^@^@^@\237d^A^@\237k
F^B^@^@\237g^A^@\237h^N^@^@^@^@^@^@
00 29 36 00 00 05
```

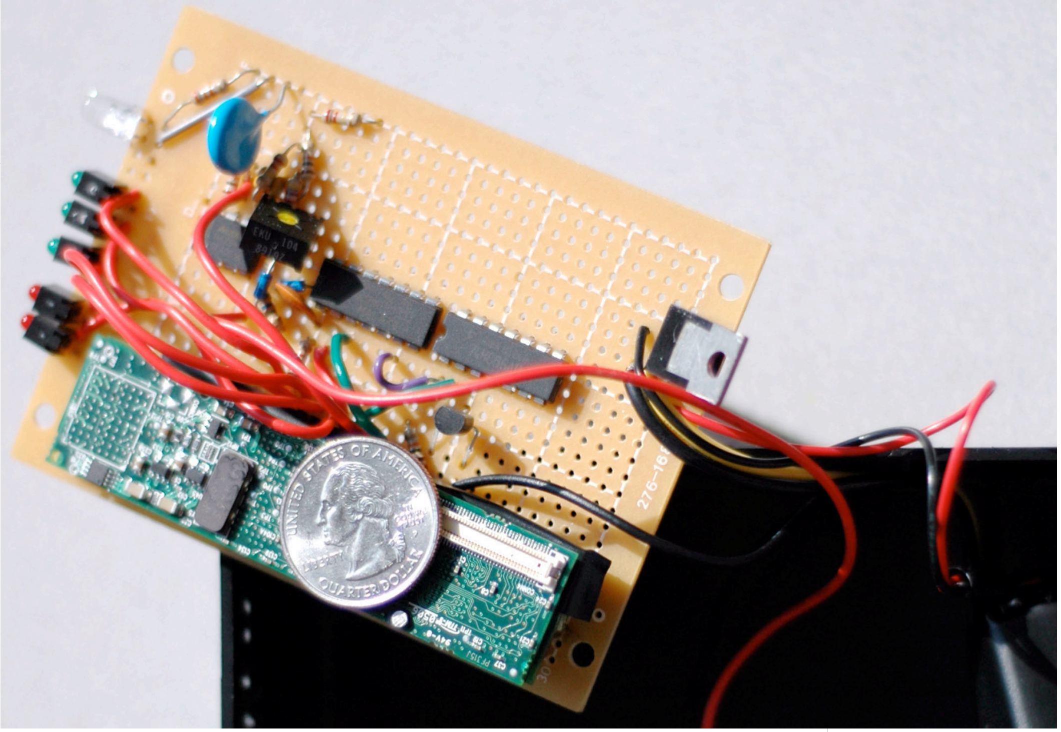
Cross-Contamination

- Are PID disclosed sufficient for financial fraud?
  - Maybe…
  - CVC absent from RF data, card face, mag-stripe
  - Collection of CVC varies with merchant and transaction type
- In some cases, yes: We successfully performed a purchase
  - New credit card in sealed envelope
  - Scanned card with programmable RFID reader kit
  - "Alice's" address retrieved from phone book



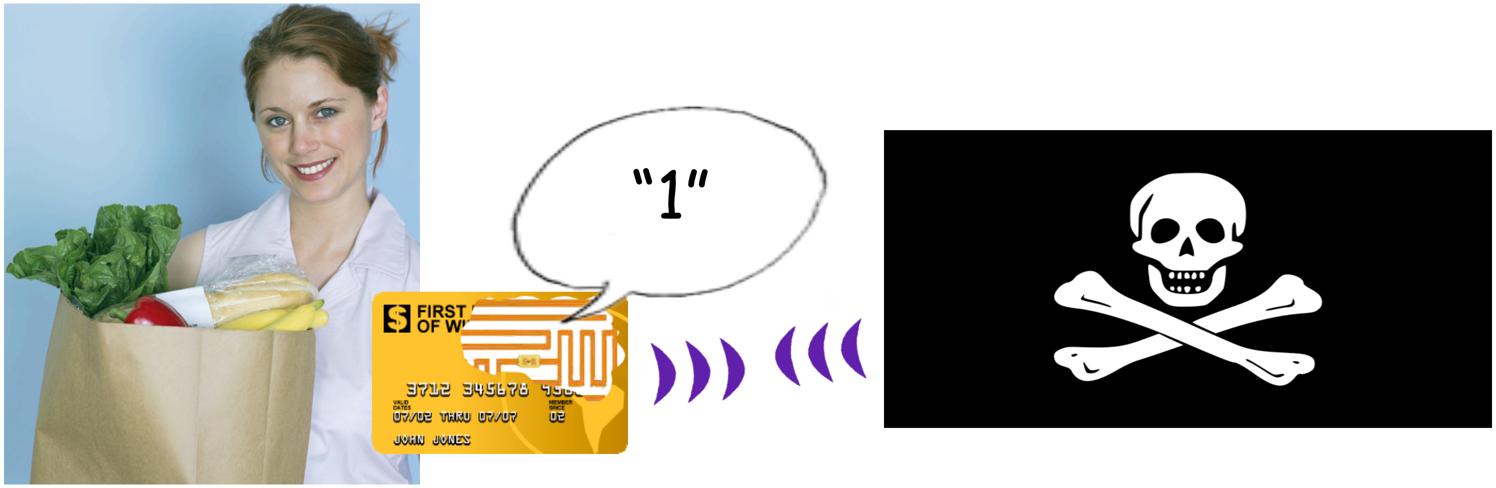
Replay: Credit Card Cloning

- Some cards: data sent to commercial reader is always the same with successive transactions
- We built a device that can replay these data
- Commercial readers accept the replay



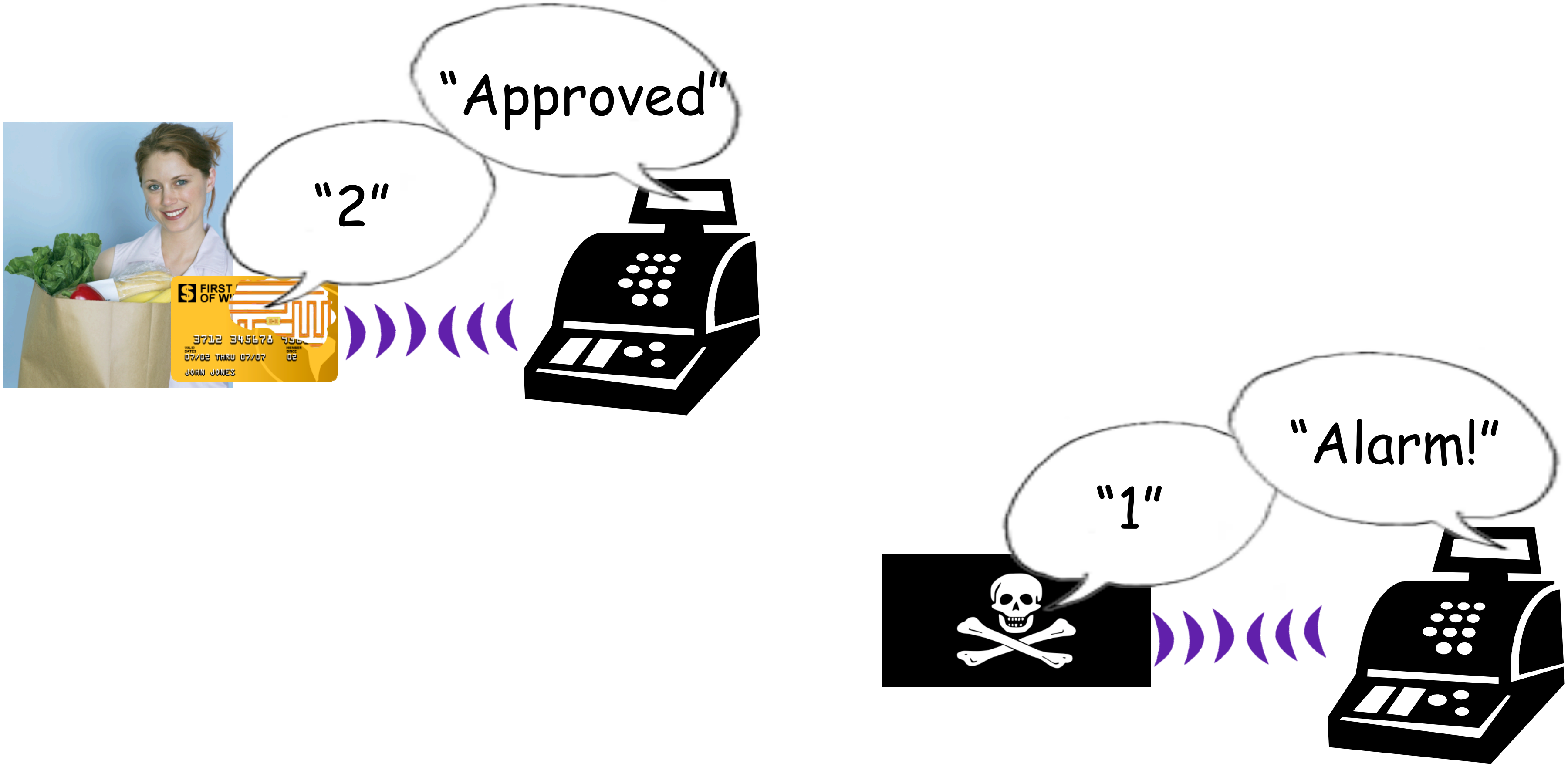
Replay and Transaction Counters

- Some Cards: counter increases with each RF transaction
- Unfortunately counters create a race condition



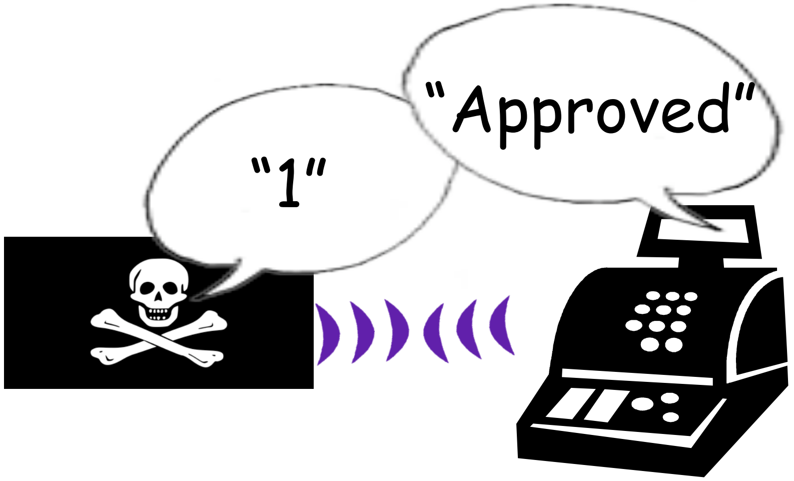
Replay and Transaction Counters

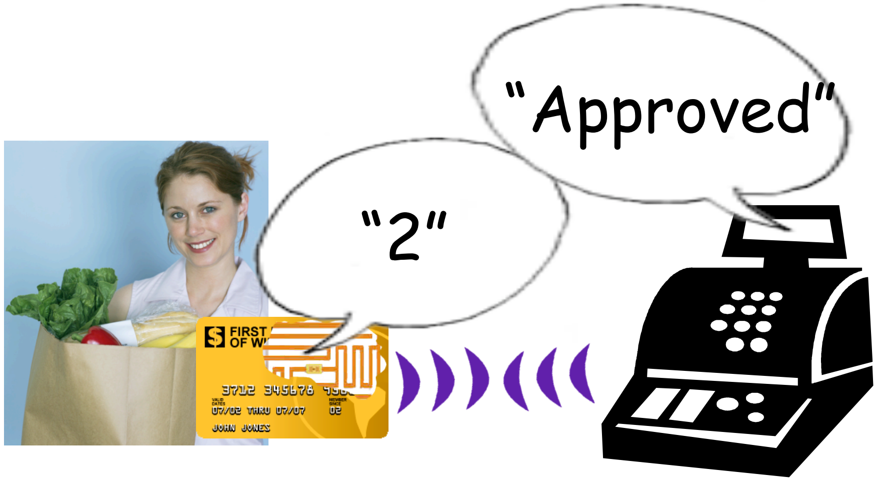
- Under some circumstances counter prevents replay



Replay and Transaction Counters

- Some times the counter will not prevent replay



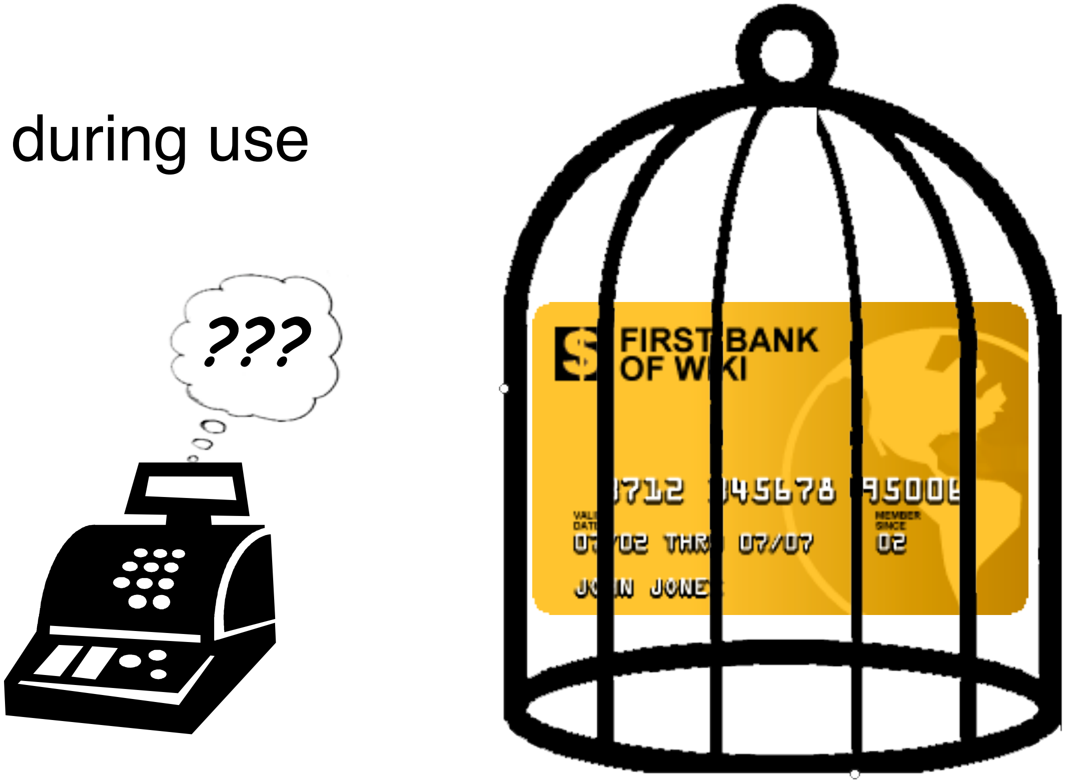


Replay and Challenge-Response

- Some cards use a challenge-response protocol
  - Details of algorithm unknown
  - Can protect against replay if back-end network is configured correctly
  - Challenge-response not used for protecting PID

Countermeasures

- Faraday cage
  - Doesn’t protect during use



- Recent cards omit cardholder name
  - Caution: This lowers the bar on other attacks

Countermeasures

- Better use of cryptography
  - Some current cards may use cryptography
  - All we have seen transmit credit card data in the clear
- Smarter devices [Chaum 85]
  - Easier to assure user consent
  - More resources for cryptographic protocols

The big problem: Paradigm shift

- Most of the vulnerabilities for RFID credit cards are similar to those for the EMV cards in previous talk
- The same attacks are, however, much easier in the wireless paradigm
- PID disclosure in particular must be thought of quite differently

Conclusion

- Current RFID credit cards are vulnerable to PID disclosure, cross-contamination, relay, and to some extent replay
- End to end communication between card and back-end mitigates some but not all vulnerabilities
- Financial companies must not only think about fraud, but also about other consumer rights and concerns
- Mechanisms for fixing most of these vulnerabilities already exist