CERIAS

the center for education and research in information assurance and security

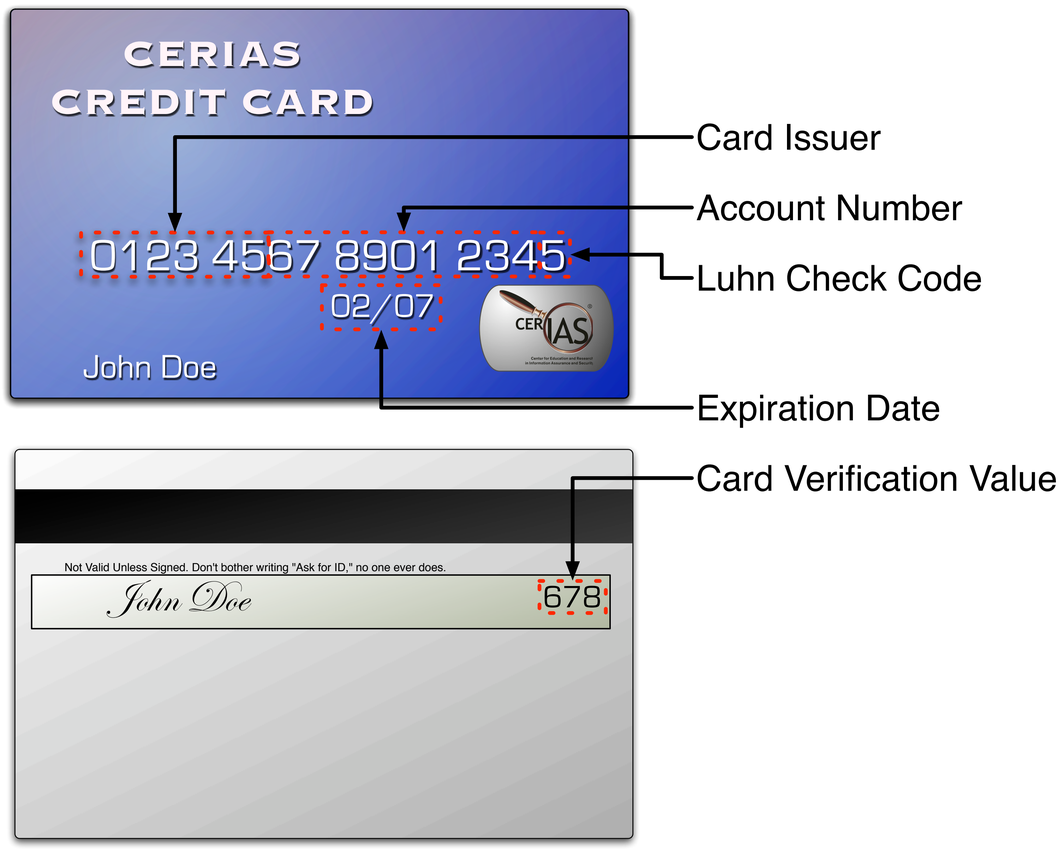
Dynamic Virtual Credit Card Numbers

Ian Molloy, Jiangtao Li, and Ninghui Li

What's the problem?

Credit Card Numbers get Stolen

- Laptop with credit card info for 80,000 DOJ workers stolen
  March 31, 2005
- Hotels.com Credit-Card Numbers Stolen
  June 2, 2006
- Amazon Unit Loses Credit Card Data to Hackers
  March 6, 2001
- 40 Million Credit Card Numbers Hacked
  June 18, 2005



Why do we send our *actual* account number?

Previous Work

- Microsoft Patent 5883810 Transaction-proxy Numbers
  - Implemented by Orbiscom for Discover, CitiBank, MBNA, and PayPal
  - Requires Card Issuer to generate new account number

Can we do this *offline*?

Dynamic Virtual Credit Card Numbers

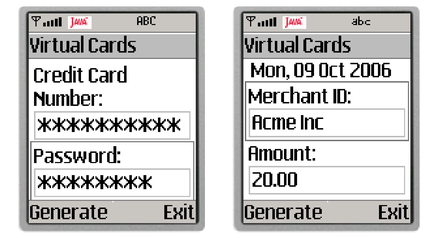
- Calculate Keyed MAC of transaction
- Use MAC in place of account number
- Card Issuer can verify the MAC
- Binds the merchant, date and amount to the account number
- Stolen card numbers loose their value
- Don't need to trust the merchant

Miscellaneous

- We can create multi-use numbers
- Unaffected by collisions in the account space
- Can handle collisions from AVS

Implementation

- Java 2 MicroEdition MIDlet 2.0
- Runs on everyone's favorite ubiquitous computing device: mobile phones



Transaction Parameters

- Expiration Date
- Merchant
- Amount
- Billing Address

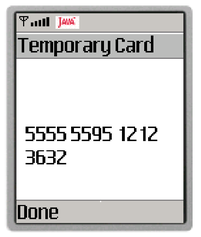
Shared Secrets

- Account Number
- Password

Account & CVV

$$k = \text{SHA1}(\texttt{Account}||\texttt{Password})$$

$$V = \text{HMAC}_k(\texttt{Transaction})$$



Security

- Complete
  - Can always generate an account number
- Sound
  - Can always identify the correct account
- Secure Against Forgery
  - No VCC numbers can be forged
- Secure Against Account Recovery
  - No adversary can gain the *actual* account number

For further details, see our paper in the *Eleventh International Conference on Financial Cryptography and Data Security 2007*

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center