

Electronic Payments

Cyber Security Lab

Spring 2006

In the beginning there was SET

- Secure Electronic Transactions (SET)
 - Sponsored by VISA
 - Going to save the world in the late 90's
 - Requires mutual authentication via certificates
 - Certificates required an infrastructure upgrade for buyers and sellers
- Background reading
 - “Credits and Debits on the Internet”, M. A. Sirbu, 1997,
<http://ieeexplore.ieee.org/iel3/6/12295/00570823.pdf?tp=&arnumber=570823&isnumber=12295>
 - Why SET failed
<http://www.versaggi.net/ecommerce/articles/set.htm>

E-Cash and Micropayments

- Also a big buzz in the late 90's
 - Make it easy to pay small amounts (10's of cents) for web access, songs, stock quotes, etc.
- Many companies started proposing alternate electronic cash
 - CyberCash, DigiCash, Flecks
 - SmartCards and electronic wallets
 - They all failed
- Many interesting problems posed by electronic cash
 - Transferring the e-cash safely and efficiently without involving a central authority
 - Minting money
 - Many papers written
- Folks in general lost interest in micropayments
 - Required a lot of people to buy into a new financial infrastructure
 - Went with an advertising or a subscription model

Reality Ended Up More Evolutionary

- Not optimally secure, but more convenient
 - No certificate hierarchies required
 - No full scale infrastructure upgrade
- Online shopping
 - Credit/debit card
- Person to person (p2p)
 - Third party intermediaries like PayPal or e-Gold
- Automated Clearing House (ACH)
 - Direct Deposit expanded
- Electronic Bill Presentation and Payment (EBPP) – Paying bills online
 - Via biller's site
 - Via bank's site
 - Via 3rd party site, like check free

Online Credit Card

- Credit cards numbers can be cribbed in physical situations
 - E.g. by disgruntled waiter or cashier
- Some credit card fraud rate is higher online
 - Merchants with higher fraud rates pay higher credit card rates to cover the difference.
 - Merchents are motivated to detect fraudulent situations.
- Consumer is only liable for relatively small fixed amount in the effect of a fraudulent charge
 - Many are sanguine about using credit cards online in today's world of weak authentication
 - The benefits outweigh the risks

Card Authentications

- PIN
 - Combined with account info and cryptography
 - Compared against stored PIN offset
- Card Verification Code (CVV)
 - Cryptographic check of the account number
 - Only displayed on the physical card
 - Card verification key pair
- <http://www.amarshall.com/crypt101.html>
 - Somewhat random google hit, but seems like reasonable description of credit card crypto

PayPal

- An intermediary for the traditional financial system
- Follows a Western Union Model
 - Sender must be registered to send money
 - Receiver can register later
 - Uses email ID as the identity
- Bills and notices of payment are exchanged through email
- Uses SSL when communicating with the PayPal site
- Password protecting account

Paypal accounts

- Bringing money into the system
 - Register a bank account (see ACH)
 - Makes two random small payments
 - Must report the size of the payments before the account is activated
 - Weak authentication
 - Attempts to bar folks who only know account info but don't have actual access to the account
 - Register a credit card
 - Cannot accept a credit card payment with the freebie account.
 - Credit card transactions have overheads that the receiver must pay

PayPal Edge

- Relatively low fraud rate.
- Igor anomaly detection system
 - Freezes accounts with anomalous behavior
 - Over eager for a while and pissed off a lot of customers
- Credit card companies did not have as good of an anomaly detection system and/or did not turn off folks without calling up first
 - C2IT, CitiBank's competitor went belly up
- Articles
 - A very positive article
<http://www.technologyreview.com/articles/01/12/schwartz1201.asp>
 - A critical review
http://www.wilsonweb.com/wct5/paypal_assess.htm

PayPal Problems

- Phishing attacks
 - Emails contain links which are easy to redirect
 - Due to current spam volumes, valid notices of bills/payments can easily get caught in spam filters
- Not a bank. Not the same regulations
- Fraud against your account
 - Any protections?
- Money laundering scams
- Unsavory sellers
 - Low effort to be an e-bay seller

E-Gold

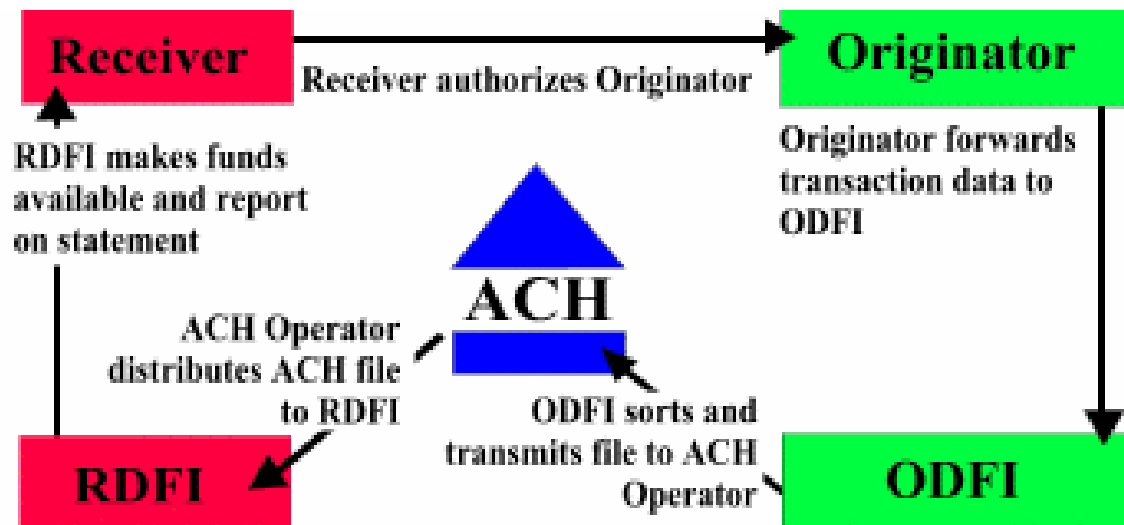
- Digital commerce backed by gold
 - <http://www.e-gold.com>
- According to wikipedia, about \$6 million of e-gold spends per day
- Makes money by fees
 - Approximately 1% per year storage fees
 - Sliding fees per transaction

E-Gold Issues

- Non-reversible transactions
 - Hard currency like banks
 - Unlike paypal
- In 2005 got hit by key loggers
 - Attackers completely cleared out compromised accounts
- Now have mouse entry keyboard for passphrase entry

Automated Clearing House (ACH)

- Originally designed for direct deposit
- Now used many other cases
 - Recurring bill payment
 - Moving money between bank and brokerage accounts
- http://www.nacha.org/About/what_is_ach_.htm



ACH Providers

- Electronic Payments Network
 - Serves part of the ACH network
 - The only private Sector ACH operator
 - <http://www.epaynetwork.com/index.php>
- FedACH 80% market share 100% gov't market share
 - <http://www.frbervices.org/index.html>
- Presumably there is communication between ACH Providers
 - When originating and receiving financial institutions subscribe to different providers

ACH Communication

- Dialup
 - Low volume or backwards compatible
- Dedicated lines, e.g., frame relay
 - “Private” network. Hopefully more secure
- VPN over the internet
 - IPSec or SSL
 - Only as good as your configuration
 - Seems like a good and juicy target

Vendor interface to ACH

- Banks/brokers allow customers to move funds between accounts using ACH
 - Need bank routing numbers and account numbers
 - Some verification that you authorize the exchanges
 - Maybe a signed physical form initially
 - After that, rely on your password

Electronic Bill Presentation and Payment (EBPP)

- Federal Reserve Article that outlines some of the legal issues
 - <http://www.chicagofed.org/publications/publicpolicystudies/emergingpayments/pdf/eps-2001-4.pdf>
 - Existing regulations are bound to state law.
 - The Internet blurs geographic constraints
 - *Electronic Funds Transfer Act (EFTA)* provides consumer protection against faulty transfers
- Examples
 - Checkfree
 - Your bank
 - Your power, phone, credit card company, etc.

EBPP's

- Bills are electronically forwarded to EBPP server or user gets paper copy
 - User gives account and password information to authorize bill forward
 - Presumably SSL encrypted
- User uses web site to indicate who to pay
 - EBPP server uses ACH to electronically move money from user's account to payee
 - Or sends a paper check if payee does not accept ACH
- Use SSL and passwords to access EBPP site
 - With all the identity proof problems that come along with it.

Identity Theft

- Generally a human issue
 - Not clear improved security protocols would help much
- Stolen backup tapes
 - Bank of America, - Feb 2005 – 1,200,000 government employee IDs
- Information sold to improper agents
 - ChoicePoint – Feb 2005 – 145,000 ID's
 - <http://www.washingtonpost.com/wp-dyn/articles/A30897-2005Feb16.html>
- Compromised passwords ?
 - Lexis/Nexis – March/April 2005 – 32,000 then 280,000 IDs
 - <http://www.msnbc.msn.com/id/7475594/>
- Sundry breaches this year
<http://www.privacyrights.org/ar/ChronDataBreaches.htm>

Conclusions

- Currently limping by with weak authentication
 - Lots of passwords or somewhat easily learned account #'s.
- As long as fraud rate is low enough, things will not change
 - Buyers risk is bound
 - Merchant bears the lose due to fraud
- Stronger authentication, i.e. certificate hierarchies will probably come along eventually
 - Even strong authentication does not solve all the problems