6.857 Computer and Network Security	Fall Term, 1997
Lecture 23 : November 25, 1997	
Lecturer: Ron Rivest	*Scribe: Lynn Qu*

1 Electronic Cash

- Desiderata
- Checks
- Payword
- Lottery Ticket
- Double Spending (partial discussion)

People have used different items as currency for a long time: shells, tobacco leaves, and such. Now if you want to pay someone electronically, say over the web or something...

1.1 Desiderata

- cannot be forged
- no double spending
- anonymity, for payer AND payee
- divisibility, i.e. 10 = 2 * 5
- clear value (face value)
- designated spender – controlled access to "wallet"
- ease of use
- transferable between users
- "backup" electronic cash (but not applicable with real money)

- traceability (for law enforcement)
- work with different banks
- small transaction fees
- efficient computationally
- no adverse social effects
- make specific payments as authorized
- smooth transition to new scheme – backward compatible
- universal
- durable
- scalable
- non-repudiation

There are two forms of e-cash:

- account-based (with a bank)
- token-based (posession of bits)

1.2 Electronic Checks

- certificate from bank saying P_{KAlice} is an account in good standing as of...
- "To:" field corresponds to an account number of the recipient
- merchant needs to verify that the bank is valid: additional certificate of bank from the Federal Reserve
- serial number – to prevent replay
- background interaction between acquiring bank and issuing bank

As the world gets networked together, electronic monetary transfer will become more important. But at the same time, it is costly – banks are involved each time

1.3 Payword

You want to write one check for each site you visit, and pay vendor the i^{th} penny to spend (assumming each site costs a penny)

1. start off with X_0, and give it in check.
2. compute all values of X for the sites you'll be visiting

$$X_i = \text{hash}(X_{i+1})$$

3. give vendor X_i, vendor checks that it hashes to X_{i-1}

When done, vendor takes the chain of X's and send to bank with the check. Bank does all the hashes to verify; it essentially processes a check for every site visted.

1.4 Lottery Ticket as Micropayment/Probablistic Checks

- a $10.00 check is valid with probability of 1/1000, so it is really worth $.01
- so vendor either deposits a $10.00 check (with chance of 1 in 1000), or does nothing
- now the bank processes the same amount of money but with much fewer transactions

Maybe we can use a random number generator based on the MASS Lottery...

1. vendor gives secure commitment h(w)
2. user writes check, "worth $10 if w is such that it has these least significant bits..."
3. vendor can check immediately

So now we have each check X_i and vendor commitment h(w_i) make up an independent trial to see whether the check is worth $10. This would not work well for the vendor if he tends to have bad luck.

1.5 Double Spending

- double spending is a real concern
- prevention is needed, perhaps with special-purpose hardware which disallows duplication of bits or does not honor second deposits
- also dectection is important to identify who double-spent

Simple "token-based" digital coin

- coin has a message signed by bank, "I am worth 10 cents and my serial number is 11235"
- bank must keep track of all the serial number on its "minted coins" with a database
- modification: bank blindly signs the message/coin, but needs a different key for each denomination, i.e. a "dime-key"
- with the modification, bank cannot identify coin as belonging to the user when it comes back