6.915 Computer and Network Security **Fall Term, 1995**

Lecture 17 : November 7, 1995

Lecturer: Ron Rivest *Scribe: Jason Thomas*

1 Electronic Money

The primary means of making monetary transactions on the Internet today is by sending credit card information or establishing an account with a vendor ahead of time. This method works fine for large purchases, but since the processing cost of credit card transactions is upwards of \$.25, this method is not feasible for micro-payments. The schemes we cover today can all handle small payments. They differ in the amount of security they offer, whether they are on-line or off-line, the computational complexity, and in who generates the money.

Each scheme suffers from the chicken and the egg problem. Does the merchant deliver the goods first before the customer pays, or vice-a-versa? For large, well known merchants, one could see the customer paying ahead of time. But on fly-by-night Internet shops, this is not appropriate.

1.1 First Virtual

–

Informations about First Virtual can be found at `http://www.fv.com`.

The First Virtual System is unique in two aspects. First, it is in use today. According to their web site, 22 merchants now accept this money and more are coming. Customers can sign up by giving their credit-card information to First Virtual via email or telnet sessions.

Secondly, it uses no cryptographic techniques. The payment protocol is an account based system in which identification information travels in the clear. Confirmation of purchases is done through a separate channel of email. In this protocol, consumers get the goods before transmitting their approval and can cheat customers. The designers of this system say they will close the account of customers who engage in this activity too often.

1. Customer and Merchant establish accounts with the sole broker. Each get account identifications.
2. Customer->Merchant :: Request
3. Merchant->Customer :: Price
4. Customer->Merchant :: Customer OK
5. Merchant->Customer :: Requested Material
6. Customer->Merchant :: Customer ID
7. Merchant->Broker :: Customer ID, Merchant ID, Cost
8. Broker->Customer :: Email verification
9. Customer->Broker :: Email confirmation

1.2 Millicent

The Millicent system was devised by Mark Manasse. More info at the following URL: `http://www.research.digital.com/SRC/personal/Mark_Manasse/uncommon/ucom.html`

Millicent is an on-line electronic payment scheme that uses merchant specific scrips, whose validity is based on hash functions. In this scheme, a customer purchases a quantity of scrip from their broker. Now when they wish to purchase goods from a vendor, they give broker scrip to their broker, who in exchange, will give them vendor scrip, and change in broker scrip. Now the customer can pay for the item in vendor scrip. At any time, customers can get cash back by returning scrip to their broker (who forwards it to the appropriate vendor). Vendors get paid when the broker credits their account after asking for vendor scrip. Only the creator of the scrip can verify its validity.

Identification = (VendorID, Value, Serial Number, Expiration Date) Scrip = (Identification, MAC(Identification, Key_Vender))

1. Customer and Merchant establish accounts with the sole broker. The vendors are given identification numbers.
2. Broker->Customer :: ScripBroker, debit customer account
3. Customer->Merchant :: Request for Goods

4. Merchant->Customer :: Price
5. Customer->Broker :: ScripBroker
6. Merchant->Broker :: ScripMerchant, credit merchant account
7. Broker->Customer :: ScripMerchant, Change in ScripBroker
8. Customer->Merchant :: ScripBroker, receives goods

1.3 Payword

This is a new system devised by Ron Rivest and Adi Shamir. This is an off-line scheme of electronic money that is based on certificates and s-keys, and where the customer generates the money. When a customer makes an account with a broker, they receive a commitment and their private key. Afterwards, the customer is the party that makes new money. This comes in the form of generating commitments.

To make a purchase, a customer first makes a new commitment, and keeps the chain of s-keys, W0 - WN. Next, he forwards his certificate and commitment to the vendor. To make a purchase, he now sends the {Wl, l}. The vendor now verify that the customer indeed knows the s-key chain, and can send deliver the goods. At the end of the day, the merchant forwards this material to the broker, who again verifies the transaction, credits the merchants account and debits the customers account.

Certificate = [Name, Internet Delivery Address, Account Identification, Expiration Date, Customer Public Key]priv_key_signing_authority

Commitment = [Certificate, Date, VendorName, W0, Value_of_each_W]priv_key_client

1. Customer->Merchant :: Cert, Commitment
2. Customer->Merchant :: Wn, N
3. Merchant->Broker :: Commitment, Cert, Wl, L

1.4 Micromint

This will be covered in the next lecture.