USING THE INTERNET TO REDUCE SOFTWARE PIRACY
on Anonymous Receipts, Anonymous ID Cards, and Anonymous Vouchers

Ralf C. Hauser

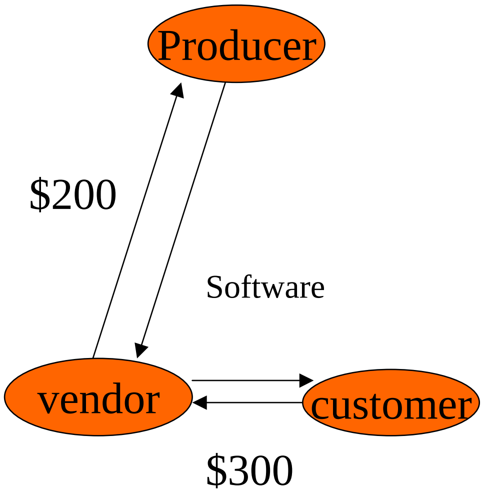
April 4, 1995

Reviewer : Xiao Wang

Introduction

- ⌘New Software Vending Method
- ⌘Anonymous ID Cards
- ⌘Anonymous Receipts
- ⌘Fully Network situation

Background



Producer

$200

Software

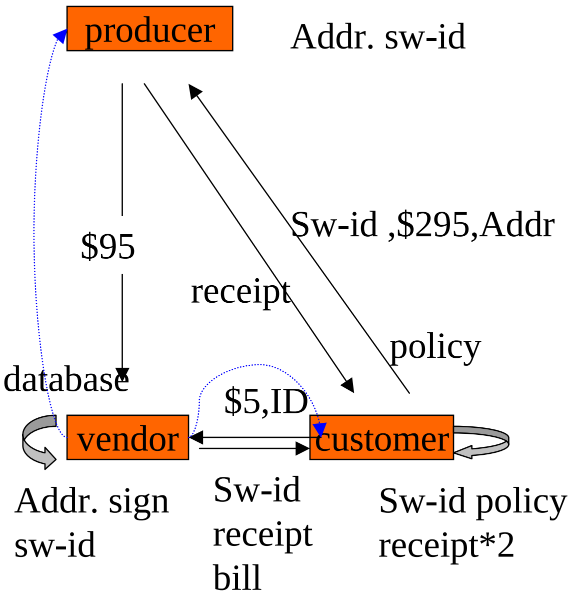
vendor

customer

$300

- Physical software copy is valuable
- Dishonest customer can cheat producer by copying illegally
- Vendor can cheat user and producer by selling bootleg software copy

New Software Vending Method



producer

Addr. sw-id

$95

receipt

Sw-id ,$295,Addr

policy

database

$5,ID

vendor

customer

Addr. sign
sw-id

Sw-id
receipt
bill

Sw-id policy
receipt*2

- Show ID to Vendor
- Get less valuable software copy
- Get bill with unique SW-ID
- Use policy file to verify vendor and producer
- Pay producer
- Vendor gets profit from producer
- erase client from debt list by SW-ID

- Vendor may remind consumer
- Vendor ask profit from producer with consumer’s receipt

Evaluation

Stop piracy

Physical copy is not valuable , paid sw-id is valuable

•Stop bootleg copy from vendor

•Stop dishonest customer

Intrude privacy

•Show customer’s ID to vendor

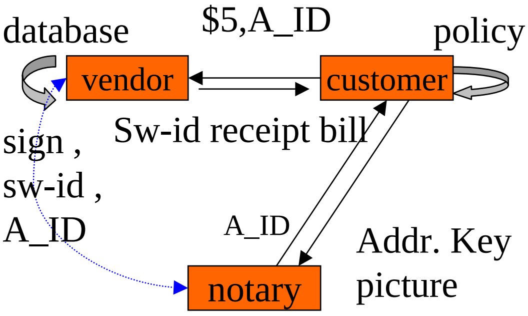
•Give producer customer’s address for receipt

How to protect privacy ?

Anonymous ID Cards

The notary registers the consumer's address and signs asymmetric public key without adding any address and name information. And include secure hash value of a digital passport picture of the consumer .

Sn(PseudonymA , E_{Atemp} , MD5(A.img))

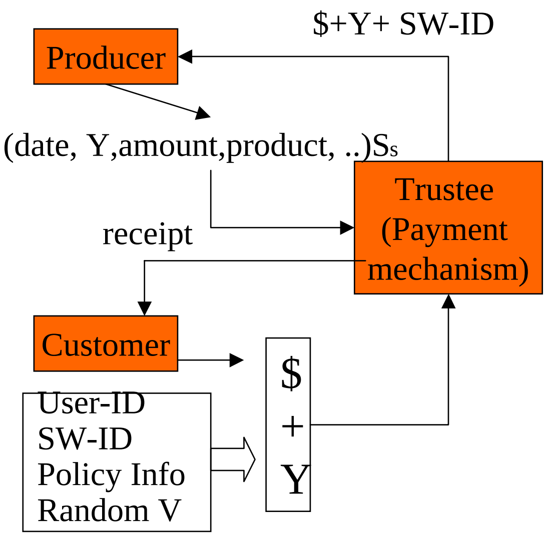


- hands a diskette containing this notary statement and the passport picture
- cashier's PC displays the picture to verify the holder of this digital ID

- vendor sends a reminder to the notary
- notary can reveal the identity of the consumer during dispute

What is the use of the public key ?

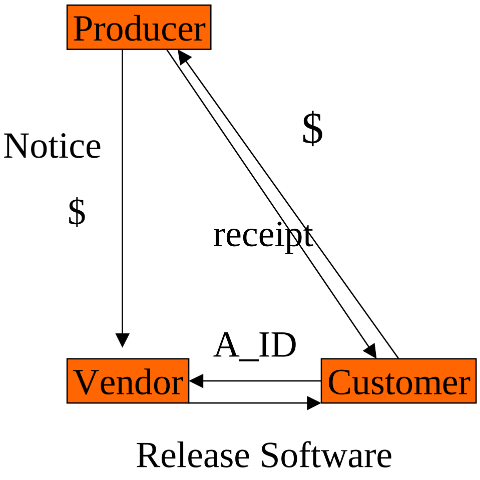
Anonymous Receipts



- ⌘ Create Y (hash of the receipt information by a secured one-way function)
- ⌘ Trustee pay out funds , forward Y SW-ID
- ⌘ Create Ss(signature key of producer) return to trustee as receipt
- ⌘ Trustee forward receipt to customer and remove customer information after customer getting receipt .

What is the use of the Random value ?

Fully Network



- ⌘ use public key to secure the delivery of the software
- ⌘ Replace Trustee with payment mechanisms .
- ⌘ Release software after getting paid to producer

Conclusion

- This paper shows a new vending method which can reduce software piracy .
- It also gives solution to keep privacy and can provide identity at the same time -- using one way cryptography .

Questions

- Judging from this paper , do you think the author use the hash value of the photo MD5(A.img) as the Anonymous ID number ? If not , it can be the ID number or not ?