Online Electronic Payment Systems

Introduction to Computer Security

Week 15

JINAN UNIVERSITY

Electronic Online Payment

Electronic Online Payment

Online Payment (Security) Requirements

- Convenient to use and widely accepted
- Hard to fake and cheat
  - Authentication
  - Non-repudiation
- Confidentiality
- Anonymity

Online Payment (Security) Requirements

- Convenient to use and widely accepted
- Hard to fake and cheat
  - Authentication
  - Non-repudiation
- Confidentiality
- Anonymity
- Usually cannot have all

A Few Payment Systems

To compare them regarding convenience, security (to present fraud) and anonymity

- Commodities, Cash

A Few Payment Systems

To compare them regarding convenience, security (to present fraud) and anonymity

- Commodities, Cash (inconvenient for online payment)

A Few Payment Systems

To compare them regarding convenience, security (to present fraud) and anonymity

- Commodities, Cash (inconvenient for online payment)
- Credit card

A Few Payment Systems

To compare them regarding convenience, security (to present fraud) and anonymity

- Commodities, Cash (inconvenient for online payment)
- Credit card (Book entry system, bad anonymity & confidentiality)

A Few Payment Systems

To compare them regarding convenience, security (to present fraud) and anonymity

- Commodities, Cash (inconvenient for online payment)
- Credit card (Book entry system, bad anonymity & confidentiality)
- Cheque and bank transfer

A Few Payment Systems

To compare them regarding convenience, security (to present fraud) and anonymity

- Commodities, Cash (inconvenient for online payment)
- Credit card (Book entry system, bad anonymity & confidentiality)
- Cheque and bank transfer (Book entry system, need trusted middle party to deliver payment, not instantaneous)

A Few Payment Systems

To compare them regarding convenience, security (to present fraud) and anonymity

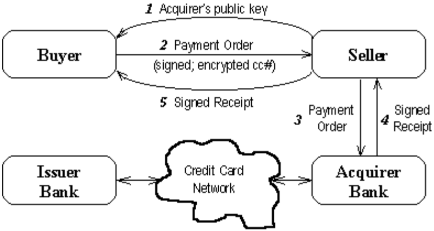
- Commodities, Cash (inconvenient for online payment)
- Credit card (Book entry system, bad anonymity & confidentiality)
- Cheque and bank transfer (Book entry system, need trusted middle party to deliver payment, not instantaneous)
- Protocol combinations
  - Credit card over SSL
  - Paypal, Alipay, wechat, Apple pay ...

A Few Payment Systems

To compare them regarding convenience, security (to present fraud) and anonymity

- Commodities, Cash (inconvenient for online payment)
- Credit card (Book entry system, bad anonymity & confidentiality)
- Cheque and bank transfer (Book entry system, need trusted middle party to deliver payment, not instantaneous)
- Protocol combinations
  - Credit card over SSL
  - Paypal, Alipay, wechat, Apple pay ...
  - e-cheque, Netcash, Virtual credit cards
  - Digicash
  - Crypto-currencies based on Blockchain (e.g., Bitcoin)

Credit Card Online Payment



- Authentication is online
- Settlement is usually offline (batch processed at the end of the day)
- SSL can be used between the customer and the merchant, and between the merchant and the bank

Credit Card Online Payment—Common Risks

- Merchant website stores customer's credit card number to expedite future transactions
- Merchant websites frequently hacked and CC numbers stolen
- The bank learns that you made a transaction with merchant X for amount Y
- Merchant may charge a larger amount than agreed by client

Credit Card Online Payment

- Consumer cannot detect fraud until the statement arrives
  (Internet access has reduced the window somewhat)
- Merchant pays royalty for each credit card network
- Merchant carries the risk of fraud in card
- Consumer liability is limited (in many countries)
- Originally far more merchant fraud than consumer fraud
  Internet has shifted the balance towards the consumer side
- Reduced fraud with PIN/sms authentication/Smart card
- Convenient, but no privacy/confidentiality to consumers

Paypal and other Third Party payment schemes

- Founded in Dec 1998, now completely owned by eBay
- A typical Third Party payment with eBay as its killer application (same as Alipay + Taobao)
- User account authentication (credit card and regular bank account)
- User's account linked to his/her Paypal account, and Paypal acts as an escrow agent
- When a payment is by a credit card, the transaction is over SSL
- Used mostly in the US, with similar products in other countries

Electronic Payment Systems

- Does not inflate money supply (unlike Paypal & Alipay)
- Sometimes implemented with heavy weight cryptographic protocols
- Improved security and privacy for users
- However not as widely used today (due to different reasons)

Virtual PIN, 1994

- Started by a company called First Virtual Holding
- Customer enrolls by providing credit card information to First Virtual by phone
- First Virtual verifies customer credit card information, and issue virtue PIN to customer
- To online purchase
  1. Customer gives the merchant his virtual PIN
  2. The merchant sends the virtual PIN and the amount of transaction to First Virtual
  3. First Virtual sends an e-mail to the customer to confirm the purchase
  4. The customer can answer: Yes, No, or Fraud
- Virtual PIN protects custmer's anonymity/privacy
- e-mail confirmation protects against fraud

Proposals to improve security of Credit Card Payments

- iKP protocols (IBM)
- SEPP (Mastercard/IBM)
- STT (VISA/Microsoft)
- SET (consortium, Mastercard, VISA, Netscape, IBM, Microsoft)
  - combined ideas from iKP, SEPP, STT
  - first version 1997
  - provides a secure communication channel among all parties involved in a transaction
  - provides trust by the use of X.509v3 digital certificates

Secure Electronic Transaction (SET)

- Parties to the Payment
  - Customer C
  - Merchant M
  - Payment Gateway P — a proxy for Merchant's bank & Customer's bank
- Objective
  - Customer C wishes to obtain goods/service from merchant M
  - Merchant M wishes to receive payment from gateway P
  - Payment gateway P charges payment to customers account

Customer Requirements

- Proof of Transaction Authorization by Payment Gateway

  The customer must have a proof that the payment gateway authorized the transaction
- Receipt from Merchant

  The customer must have a proof that the merchant who has made the offer has received payment and promised to deliver the goods/service
- Confidentiality

  The customer's account information (including credit card number) should not be known to the merchant

Non-repudiation Requirements

For Merchants

- Proof of Transaction authorized by Payment Gateway
- Proof of transaction authorized by customer

For Payment Gateway

- Proof of Transaction authorized by merchant
- Proof of transaction authorized by customer

Secure Electronic Transaction (SET) Protocol

over 400 pages of specification:

1. Cardholder Registration — cardholder registers signature key and a PIN-like secret with Certificate Authority
2. Merchant Registration —- merchant registers signature and encryption keys
3. Purchase request — cardholder places order with merchant
4. Payment Authorization — merchant verifies cardholder details with payment gateway, which authorizes transaction
5. Payment capture — transfer of funds to merchant

Secure Electronic Transaction (SET) Protocol

1. Customer searches for products and negotiate for price ...
2. Customer initiates payment phase
   $C \longrightarrow M$: initiate
3. Merchant provides a transaction identifying number TID, signed with Merchant's private key
   $M \longrightarrow C : \{\mathrm{TID}\}_{K_M^{-1}}$
4. Customer sends Merchant the agreed price, plus encrypted information for forwarding to Payment Gateway:
   $C \longrightarrow M$:
   $\{\mathrm{TID}\}_{K_C^{-1}}$,
   $\{\mathrm{TID}, Price_M\}_{K_M}$,
   $\{\{\mathrm{TID}, Price_C, CCNumber, PIN\}_{K_P}\}_{K_C^{-1}}$

Secure Electronic Transaction (SET) Protocol

1. Customer searches for products and negotiate for price ...
2. Customer initiates payment phase
   $C \longrightarrow M$: initiate
3. Merchant provides a transaction identifying number TID, signed with Merchant's private key
   $M \longrightarrow C : \{\mathrm{TID}\}_{K_M^{-1}}$
4. Customer sends Merchant the agreed price, plus encrypted information for forwarding to Payment Gateway:
   $C \longrightarrow M$:
   $\{\mathrm{TID}\}_{K_C^{-1}}$,
   $\{\mathrm{TID}, Price_M\}_{K_M}$,
   $\{\{\mathrm{TID}, Price_C, CCNumber, PIN\}_{K_P}\}_{K_C^{-1}}$

- The message sent to the Payment Gateway is first encrypted with P's public key and then signed with C's private key
- CCNumber and PIN not revealed to the merchant

Secure Electronic Transaction (SET) Protocol

- Merchant forwards the encrypted message to Payment Gateway
  $M \longrightarrow P$:
  $\{\{\mathrm{TID}, Price_C, CCNumber, PIN\}_{K_P}\}_{K_C^{-1}}$,
  $\{\mathrm{TID}\}_{K_M^{-1}}$,
  $\{\mathrm{TID}, Price_M, MAC\}_{K_P}$

where

1. K_P is Payment Gateway's public key
2. $Price_M$ is the price merchant asks to be charged to client account
3. MAC is merchant account number for deposit

P verifies PIN, checks if $Price_M = Price_C$.

Secure Electronic Transaction (SET) Protocol

- In the end, Payment Gateway confirms transaction result
  $P \longrightarrow M : \{\mathrm{TID}, \mathit{Result}\}_{K_P^{-1}}$
- The result is also forwarded to the customer
  $P \longrightarrow C : \{\mathrm{TID}, \mathit{Result}\}_{K_P^{-1}}$

Summary on SET

1. Both merchant and customer get a receipt/confirm from Payment Gateway
2. The transaction proceeds only on agreed price, which is supposed to be fair
3. Confidentiality: customer's CC number and PIN are protected by encryption
4. Non-repudiation: requests sent to Payment Gateway are signed by involved parties
5. Anonymity: your bank still learns that you made a transaction with merchant X for amount Y, and can build up a profile of you
6. Similar problems for other third party payments: Paypal, Alipay, wechat pay . . .
7. In the real world, paying in *cash* prevents this problem — Digital cash attempts to reproduce this privacy property in the digital world

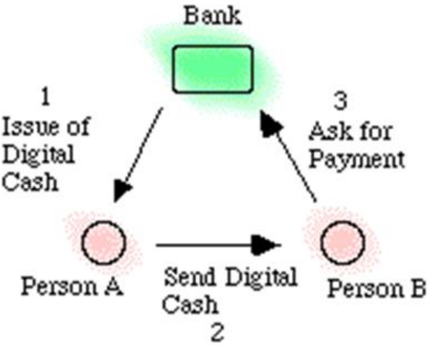
Real Life Cash vs Digicash

- Both backed by bank
- Paper cash contains: serial number, value, paper median that is hard to forge
- Digicash: serial number, value, digitally signed by the bank

General Structure of digital cash protocols

- customer withdraws money from her account, receives digital cash
- customer transfers digital cash to merchant in exchange for goods
- merchant deposits digital cash in his account

General Structure of digital cash protocols



Two types of digital cash protocols

- **Online:** merchant verifies digital cash with bank at time of transaction
- **Offline:** merchant verifies digital cash with bank some time after the transaction (e.g., deposits all cash at the end of the day)

Risks to be avoided

- Forgery of digital cash
  — use authenticity mechanism to check that coin has been issued by bank it purports to come from
- Double spending
  — bank maintains record of serial numbers of coins once used
  - Oneline protocols: check against multiple spending at time of transaction
  - Offline protocols: use mechanism to detect cheater identity in case of multiple spending

How to verify authenticity of a coin

- Get the bank to sign a message
  "This is a coin of value \$1 with number 121000004554X issued by bank B"
- Problem: bank can then link the coin's serial number to the customer it was issued to

Blind Signature

- Customer puts paper with coin number and value + carbon paper in a sealed envelop
- Bank signs the envelope (pressing hard), returns to customer
- Customer opens envelope and gets a carbon copy of banks signature
- A few public key encryption algorithm (such as RSA) supports blind signature

Blind Digital Signature Based on RSA

- Let Bob (the banker)'s public key is (e, n) and private key is (d, n)
- Remember $n = p \times q$ where p and q are very large prime numbers, and $e \cdot d \equiv q \ mode \ (p-1)(q-1)$
- To get Bob's blind signature
  1. Alice generates a random number k relatively prime to n,
  2. Alice computes $k^e \cdot M$, on which Bob signs
- The signed message is $(k^e \cdot M)^d \ mod \ n$ which is $k \cdot M^d \ mod \ n$
- The first part can be cancelled with $k^{-1} \ mod \ n$ by Alice

A Potential Problem with Blind Signing

How to prevent Alice (the customer) putting a piece of paper with message M for a one-million-dollar note and claim it to be \$1?

A Potential Problem with Blind Signing

How to prevent Alice (the customer) putting a piece of paper with message M for a one-million-dollar note and claim it to be $1?

Blind signing may also be deployed to breach confidentiality

A Potential Problem with Blind Signing

How to prevent Alice (the customer) putting a piece of paper with message M for a one-million-dollar note and claim it to be \$1?

Blind signing may also be deployed to breach confidentiality

- solution one: Bank uses different keys for different coin values

A Potential Problem with Blind Signing

How to prevent Alice (the customer) putting a piece of paper with message M for a one-million-dollar note and claim it to be \$1?

Blind signing may also be deployed to breach confidentiality

- solution one: Bank uses different keys for different coin values
- solution two: Customer sends 100 identical sealed envelops, bank randomly chooses 99 of them and asks customer to open (e.g., to reveal k in the RSA blind signature scheme), and signs the remaining envelope

An Online Digital Cash Protocol

Withdrawal

- Alice creates a coin of value X, and blinds it
- Alice sends the blinded coin to the bank
- Bank signs the blinded coin and debits Alice's account to value X
- Bank sends the signed coin back to Alice
- Alice unblinds the coin
- Alice may give the coin to anyone to spend

An Online Digital Cash Protocol

Payment and Deposit

- Alice (or her friend) pays Bob the coin in exchanges for goods/services
- Bob contacts Bank and sends the coin
- Bank verifies signature on the coin
- Bank checks its database and verfies the coin has not already been spent
- Bank enters coin in spent-coin database
- Bank credits Bob's account and informs Bob
- Bob delivers goods/services

How to Make an Offline Digital Cash Protocol

- Basic idea: to include identifying information hidden in the coin, that is usually invisible
- If someone double spends the coin, his/her identity will be revealed
- This can be implemented by trusted tamper resistant hardware that is used for process transaction/payment
- The withdrawal and deposit parts are identical to online protocols

Basic Idea in Double Spending prevention

- Transaction are recorded by the tamper resistant devices with partial information of the spender and receiver for each coin (identified by its serial number)
- If the same coin being spent twice by the same spender, two pieces of information can be combined to reveal the double spender

Basic Idea in Double Spending prevention

- Transaction are recorded by the tamper resistant devices with partial information of the spender and receiver for each coin (identified by its serial number)
- If the same coin being spent twice by the same spender, two pieces of information can be combined to reveal the double spender
- If ever caught, the double spender will be blacklisted

Basic Idea in Double Spending prevention

- Transaction are recorded by the tamper resistant devices with partial information of the spender and receiver for each coin (identified by its serial number)
- If the same coin being spent twice by the same spender, two pieces of information can be combined to reveal the double spender
- If ever caught, the double spender will be blacklisted
- Secret sharing/splitting protocols are used to encode partial information
- Commitment schemes can be used to set up user's (split) identity

Secret splitting

- Give a secret message to Alice and Bob, in the way that
  1. Them individually cannot tell anything about the secret,
  2. If they get together then they can reconstruct the secret
- If we split the secret string M into two parts, M_1 and M_2, such that $M = M_1 \cdot M_2$ (concatenation)
  This is not very satisfactory because Alice and Bob each has some information of the message.

Secret splitting

- Give a secret message to Alice and Bob, in the way that
  1. Them individually cannot tell anything about the secret,
  2. If they get together then they can reconstruct the secret
- If we split the secret string M into two parts, M_1 and M_2, such that $M = M_1 \cdot M_2$ (concatenation)
  This is not very satisfactory because Alice and Bob each has some information of the message.
- Generate a random number r, give r to Alice, and $m\ XOR\ r$ to Bob.
- Alternatively, a few Zero Knowledge Proof protocols can be applied in double spending prevention

Commitment Schemes

- Alice and Bob wanted to flip a fair coin, if the result is odd, Alice wins, if even, Bob wins.

Commitment Schemes

- Alice and Bob wanted to flip a fair coin, if the result is odd, Alice wins, if even, Bob wins.
  - Alice (randomly) chooses a bit b_A, and Bob (randomly) chooses a bit b_B, and the result is $b_A \otimes b_B$
  - Who is to announce his/her choice first?

Commitment Schemes

- Alice and Bob wanted to flip a fair coin, if the result is odd, Alice wins, if even, Bob wins.
  - Alice (randomly) chooses a bit b_A, and Bob (randomly) chooses a bit b_B, and the result is $b_A \otimes b_B$
  - Who is to announce his/her choice first?
  - Alternatively, Alice writes down a single bit wrapped in an envelop and seal it, then Bob announces his bit

Commitment Schemes

- Alice and Bob wanted to flip a fair coin, if the result is odd, Alice wins, if even, Bob wins.
  - Alice (randomly) chooses a bit b_A, and Bob (randomly) chooses a bit b_B, and the result is $b_A \otimes b_B$
  - Who is to announce his/her choice first?
  - Alternatively, Alice writes down a single bit wrapped in an envelop and seal it, then Bob announces his bit
- The wrapped bit is a commitment
- A commitment can be a string longer than a single bit
- The purpose is to commit now and reveal later

Commitment Schemes

- Bit commitment using symmetric cryptography
  - Bob generates a random-bit string, R,
    $B \rightarrow A : R$
  - Alice creates a message consisting of the bit she wishes to commit to, b, and a random key k,
    $A \rightarrow B : E_k(R, b)$.
  - When it comes time for Alice to reveal b,
    $A \rightarrow B : k$.

Commitment Schemes

- Bit commitment using symmetric cryptography
  - Bob generates a random-bit string, R,
    $B \to A : R$
  - Alice creates a message consisting of the bit she wishes to commit to, b, and a random key k,
    $A \to B : E_k(R, b)$.
  - When it comes time for Alice to reveal b,
    $A \to B : k$.
- Bit commitment using cryptographic hash
  - Alice generates two random-bit strings, R_1 and R_2,
  - $A \to B : hash(R_1, R_2, b), R_1$
  - When it comes time for Alice to reveal b,
    $A \to B : R_1, R_2, b$

The Off-line Digicash Protocol Against Double Spending

- Alice prepares n anonymous digital coins for the bank to sign, each copy of the coin contains
  - the amount value
  - a unique serial number of the
  - n pairs of id bit strings $(I_{1L}, I_{1R}), \ldots (I_{nL}, I_{nR})$, such that for each pair, given both (I_{iL} and I_{iR}), we get the identity of Alice.
- The bank checks $n - 1$ copies, including the amount and the commitments, if satisfied, signs the last copy

The Off-line Digicash Protocol Against Double Spending

- Alice prepares n anonymous digital coins for the bank to sign, each copy of the coin contains
  - the amount value
  - a unique serial number of the
  - n pairs of id bit strings $(I_{1L}, I_{1R}), \ldots (I_{nL}, I_{nR})$, such that for each pair, given both (I_{iL} and I_{iR}), we get the identity of Alice.
- The bank checks $n - 1$ copies, including the amount and the commitments, if satisfied, signs the last copy
- When Alice uses the digital coin to pay Bob who is a merchant, Bob provides Alice a random string of n bits, and ask Alice to (partially) open the commitments. E.g, if the string is $0110\ldots$, then Alice reveals $I_{1L} I_{2R} I_{3R} I_{4L} \ldots$.
- If Alice tries to spend the same coin again to Clare, she will be asked to reveal her commitments again.
- When the spent coins are used to deposit by both Bob and Clare, the bank has $1 - \frac{1}{2^n}$ chance to reveal Alice's identity.

The company

- The technology is invented and patented by David Chaum in late 1980s
- Chaum started a company Digicash in 1990
- Digicash went into bankruptcy in 1998, acquired by ePay
- ePay was later acquired by Infospace, patents sold to First Data
- The algorithms used in Digicash are considered fundamental in development of digital money

The company

- The technology is invented and patented by David Chaum in late 1980s
- Chaum started a company Digicash in 1990
- Digicash went into bankruptcy in 1998, acquired by ePay
- ePay was later acquired by Infospace, patents sold to First Data
- The algorithms used in Digicash are considered fundamental in development of digital money
- Even less popular today when the new generation of Blockchain based crypto-currencies become dominant

Summary

- Cash — good anonymity
- Credit card + SSL — still the most widely used
- Protocols based on third party authority — Paypal, wechat pay, Alipay . . .
- Online electronic protocols — more privacy, but less widely used than credit cards and third party authority payments
- Digicash — good anonymity, but considered complex
- Bitcoin — relatively good anonymity (pseudonymity), a decentralized system, slow transaction and low throughput