Payment Systems for E-Commerce

Shengyu Jin

4/27/2005

Reference Papers

1. **“Research on electronic payment model”,2004**

2. **“An analysis and comparison of different types of electronic payment systems” 2001**

3. ***“The Verification of an Industrial Payment Protocol: The SET Purchase Phase” 2002***

4. **“SET and SSL: electronic payments on the Internet” IEEE 1998**

5. ***“Automatic Generation of Reliable E-Commerce Payment Process”* 2000**

complete reference is present in the term paper

Contents

I. Introduction [ref1][ref2]

- Payment is critical element in E-commerce

- Difference types of E-payment Systems

- Credit Card Payment
- Electronic Cash
- Smart card
- E-mail Payment
- Other Payment systems: E-check, mobile…

Credit Card-based System

- Most of the online transactions in B2C E-commerce handled with Credit Cards
- Security concerns due to the macro- payment and sensitive information (e.g. credit card number)
- Dimensions of E-Commerce Security
  - Authentication
  - Data Integrity
  - Confidentiality
  - Non repudiation
  - Privacy

Use of Cryptography

- Without encryption: First Credit card system

- SSL/TLS:
  - ? Provide data integrity and confidentiality while transmitted
  - ? does not protect user's data stored at the merchant's site
  - ? does not protect merchant from fraud

- SET: ? payment protocol to solve these problems developed by Visa, MasterCard and other companies to provide confidentiality of payment and order information

Electronic Cash

Also called e-money, digital cash and cybercash

- Traditional electronic cash (on-line)
  - Purchase e-cash from the issuer bank
  - Money deducted against the prepaid account
  - Accessible to people who don't have credit card
  - Concerns on use in crime, and double spending

- Smart card-based Electronic cash (off-line)
  - Micro payment market: vending machines, parking meters and ticket machine
  - Hard to use online without smart card reader

E-mail Payment

- Wide used in P2P system and small business (e.g. eBay auction)
- Paypal became a global leader in online payment solution
- E-mail only used for notification between payer and payee
- Funds(e-cash, credit card payment) still transferred the way banks settle inter-bank transaction

II. SET Overview [ref 3]

- Entities of SET protocol

  Cardholder (digital wallet); Merchant (POS software); Payment Gateway

- Three sub protocols in SET protocol

- **Pre-registration**

  cardholder, merchant and payment gateway required to register with a Certificate Authority

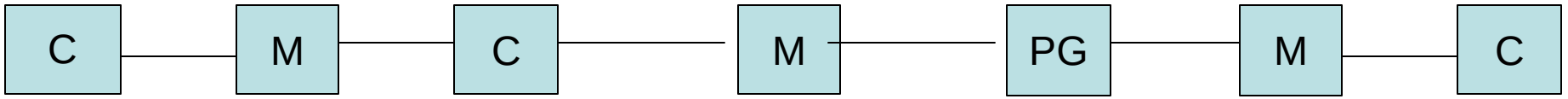
- **Purchase phase**

  allows cardholder to purchase from merchant, merchant can verify the buyer from the payment gateway

- **Payment Capture**

  used by merchant for actual funds transfer

- SET only invoked in Purchase phase
- SSL used in Pre registration and Payment Capture



Message flow in SET purchase phase:

1. Purchase Initialization Request (C? M)
2. Purchase Initialization Response (M? C)
3. Purchase Request (C? M)
4. Authorization Request (M? PG)
5. Authorization Response (PG? M)
6. Purchase Response (M? C)

III. A verification of SET purchase phase [ref 3]

- Complicated verification due to
  1. the multiple nested encryptions
  2. duplicated message
  3. many alternative protocol path: signed and unsigned
- Successfully verify the confidentiality based on many assumptions
- Impossible to prove the cardholder and the Payment Gateway agree on the latter's identity

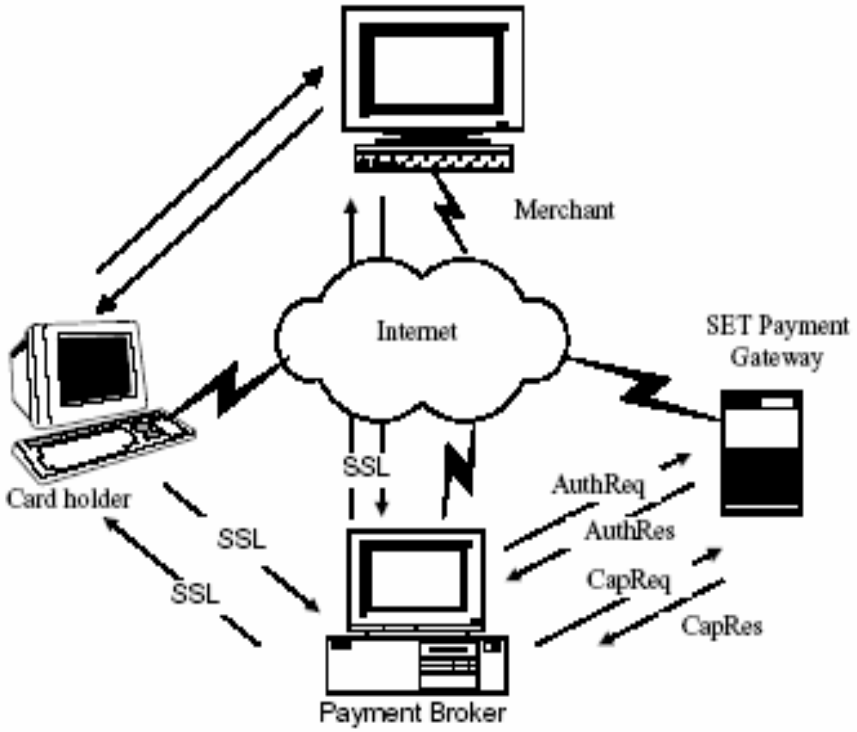
A possible scenario

- A bad payment gateway colludes with a bad merchant to deceive an honest PG.
- This will not happen in the real world
- Cardholders do not trust all the Payment Gateways
- Cardholder’s E-wallet software will abort the transaction if the Payment gateway is not certified by his/her credit card company

IV. Comparison of SSL and SET [ref 4]

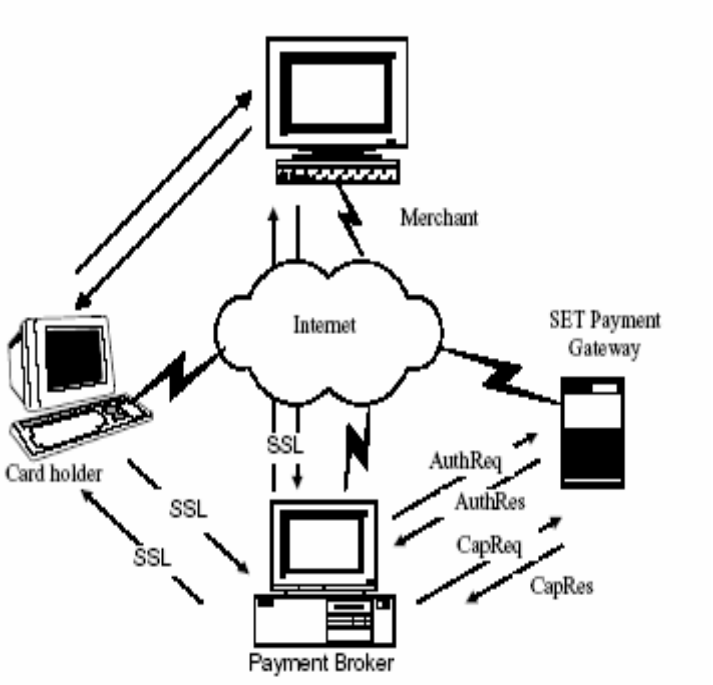
	SSL	SET
Protocol Type	Secure communication protocol (end to end)	Secure payment protocol (multi-party)
Entities	Buyer-to-seller	C, M, PG
Authentication	Only merchant authentication	Mutual authentication
Privacy	No privacy from merchant	Good: by using dual signature
Ease of Use	good: convenience	Consumer credit card certification required
Mobility	Good: can be used on any machine	Fair: restricted on computer installed SET certification
Efficiency	Good:	Fair: due to the complex cryptography
Popularity	Very adopted	Not very adopted

V. A hybrid SSL/SET architecture [ref 4]



- Adding a new entity called “Payment broker” between the Payment Gateway and other entities.
- Cardholders send credit card info to broker using SSL
- Broker initiates the SET transaction with PG on behalf of the cardholder

Interface of the broker and the merchant



- Broker hosts the merchant

"The Payment broker can act on behalf of the cardholder and play the role of the merchant to initiate the SET transaction with the SET payment gateway"[ref4]

- Broker and merchant servers are distinct

merchant pass the purchase info to the broker, broker initiates the SET on the user's behalf

In both cases, cardholder's info Stored in the Broker's sever, merchant can not see it

Pros and Cons of the architecture

- ✓ SET operation is completely transparent to the end-user
- ✓ Certification burden is on the broker

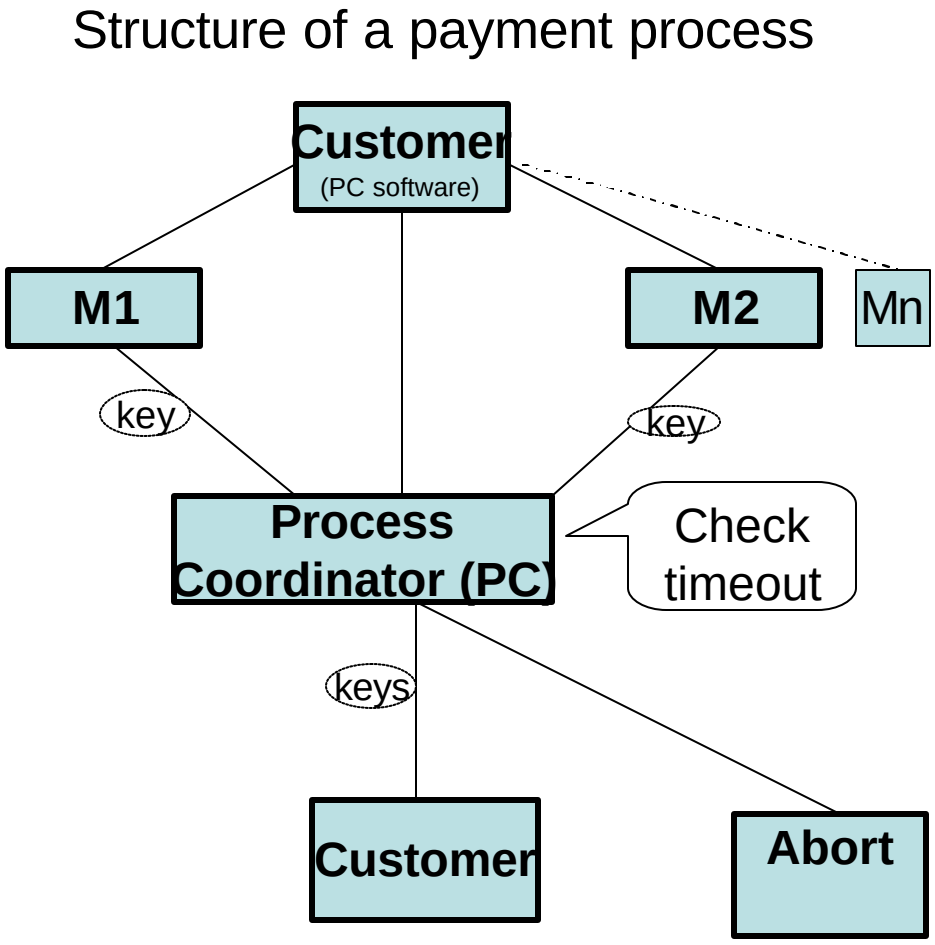
  (a user sign-up required by the broker)

- ➢ The paper fails to present the drawbacks
- ➢ Payment broker store a large numbers of credit card details which, if compromised, could lead to large-scale fraud.

VI. Distributed E-payment [ref 5]

- “Enable customer purchase goods originating from different merchants within one single E-Commerce transaction”[ref5]
- Using the notion of transactional process
- Payment Coordinator control the execution of the payment process
- Payment coordinator has to be located in a trustworthy and reliable site such as certificate authority or clearing house

Structure of a payment process



- **Customers send credit card info to the PC**
- **PC verifies the credit card and requests all the merchants to send the keys used to decrypt the original encrypted goods to the PC**
- **PC performs timeout check after received all the keys**

Structure of a payment process

- If timeout check satisfied, PC determines the success of the process, and sends all the keys to the consumer and confirmation to the merchants
- If failed, an abort of the process is issued by the PC, failure notifications are sent to all participants
- Timeout check provides the atomicity (all or nothing) of the distributed payments
- No merchants will hold a reservation for an unlimited time.