Real Time e-Commerce Broker System

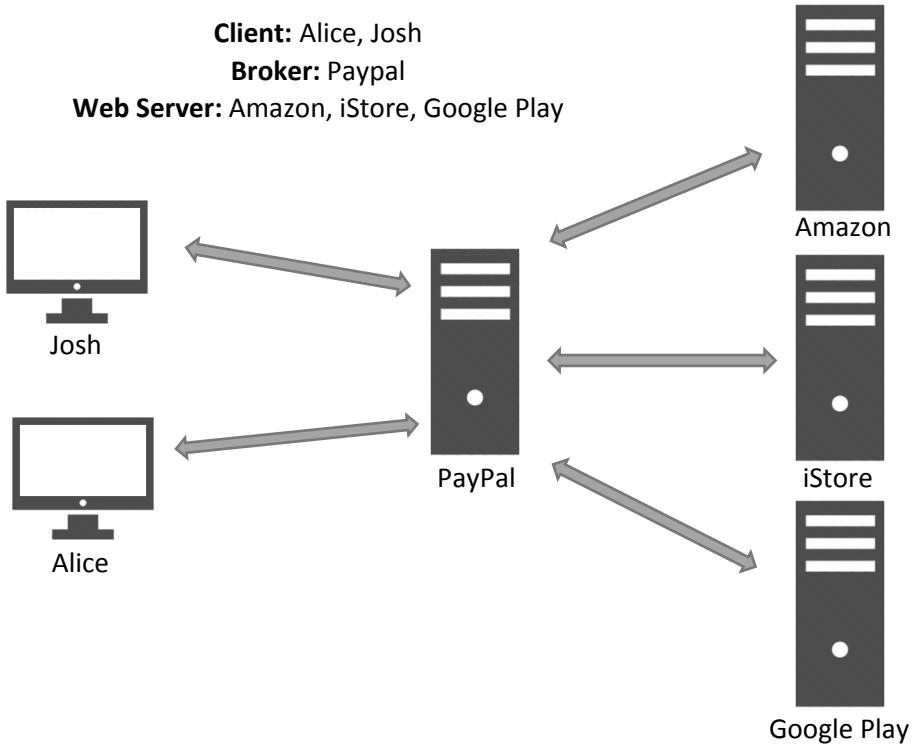
CS6349 Network Security

Class Project / Fall 2018

omer@utdallas.edu

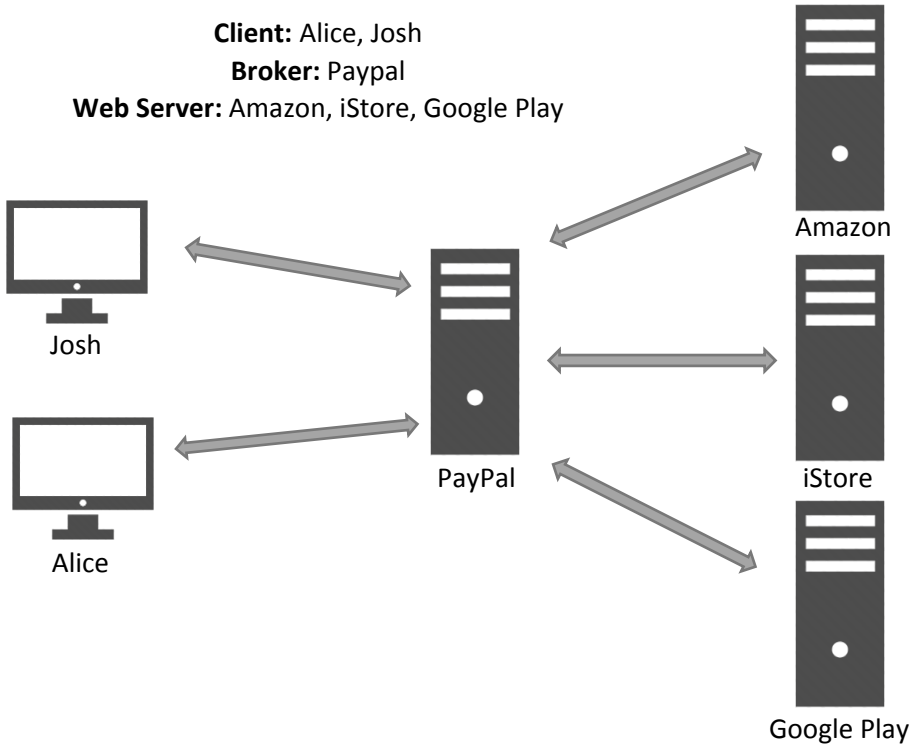
Project Description

- Anonymous online purchase system through a broker.
- Components:
  - Client
    - e.g. Alice, Josh
  - Broker
    - e.g. PayPal
  - e-Commerce Website
    - Referred as “Seller” in short in this presentation.
    - e.g. Amazon, iStore, Google Play



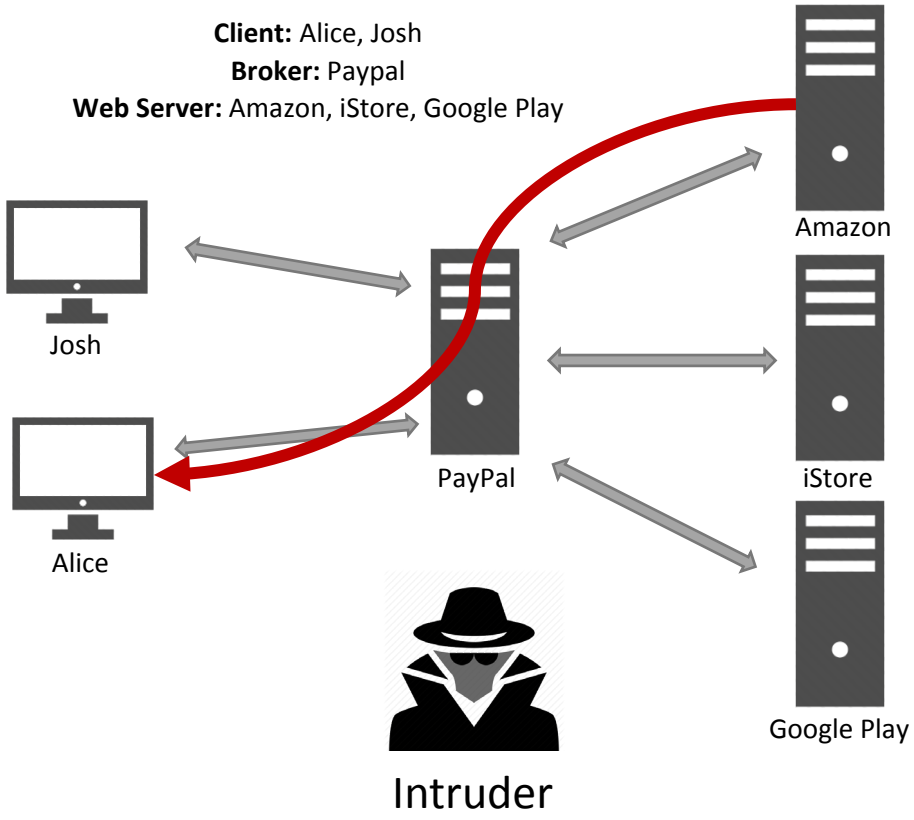
Goal I: Authentication

- Clients authenticate brokers and sellers.
- Brokers authenticate clients and sellers.
- Sellers authenticate *only* brokers.
- You can assume exchanged keys are verified by an imaginary CA for the sake of simplicity.



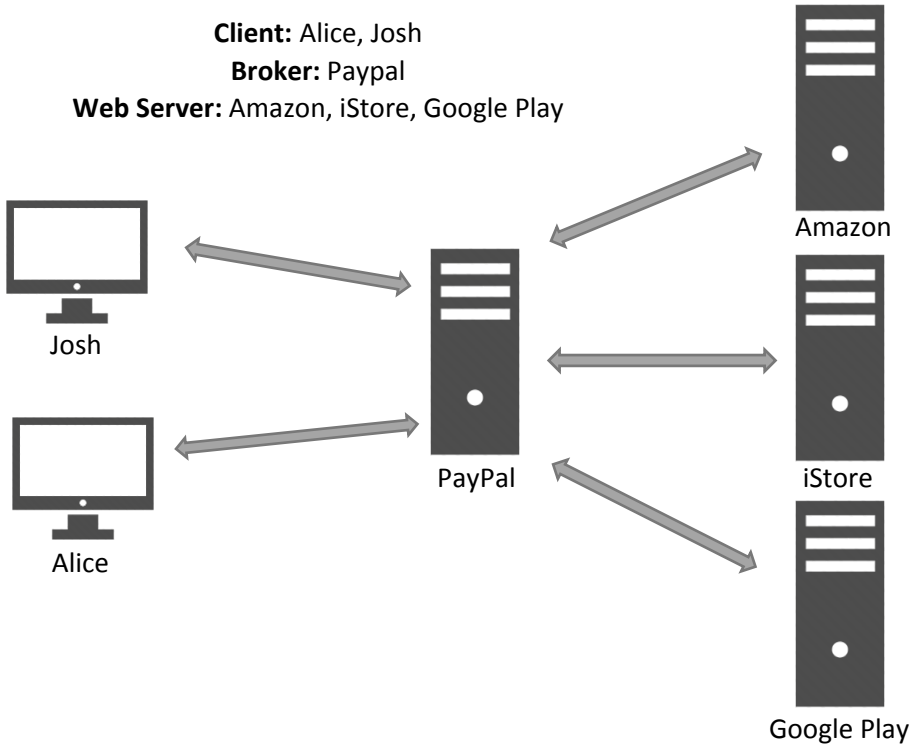
Goal II: Message Integrity

- Integrity of messages going through an insecure network should be ensured.
  - e.g. Alice should be able to tell if a message coming from Amazon is modified by PayPal or Intruder.



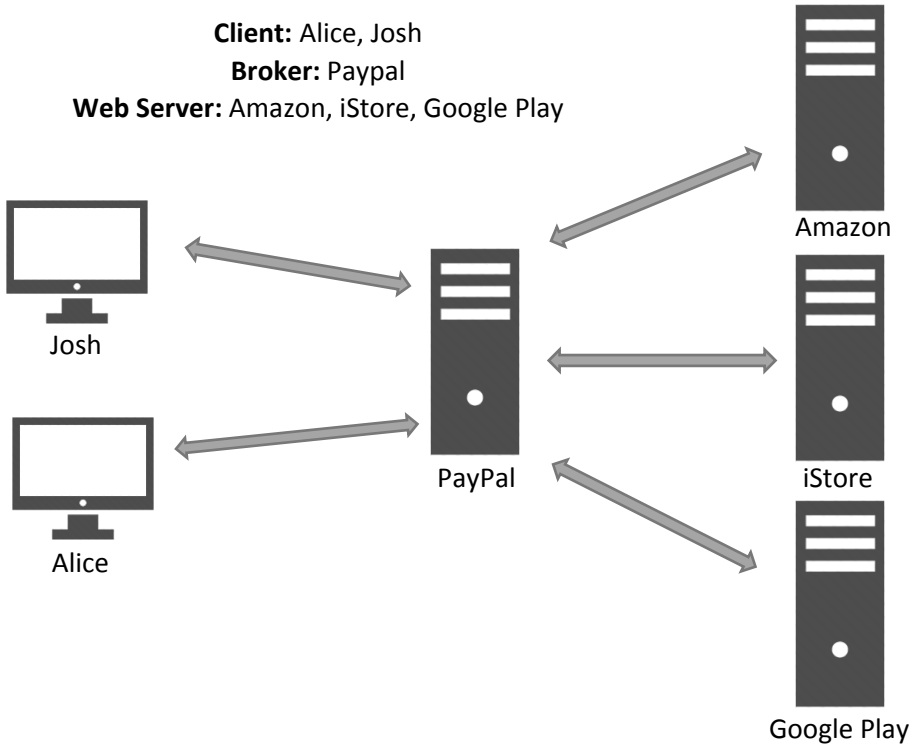
Goal III: Privacy/Confidentiality

- All communication should be encrypted.
  - Between client and broker.
  - Between broker and seller.
  - Between client and seller.



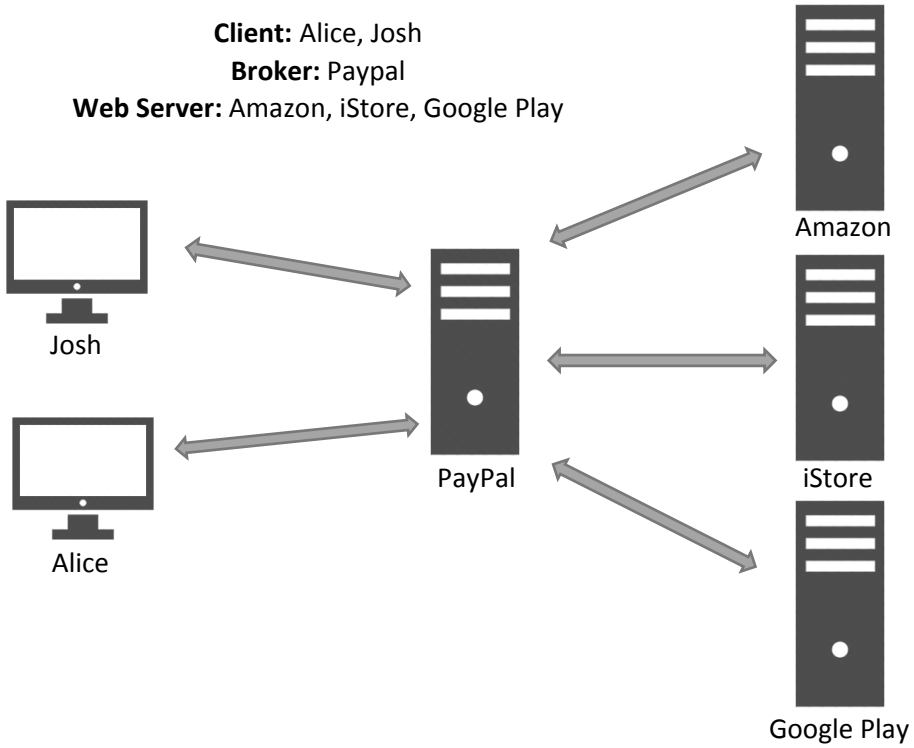
Goal IV: Anonymity

- Seller shouldn't know identity of buyer.
  - i.e. Seller can know only the identity of broker.
- i.e. Broker shouldn't know what client browses or buys.
  - i.e. Broker can know identities of both client and seller, the transaction date and amount, but *not* what is bought.

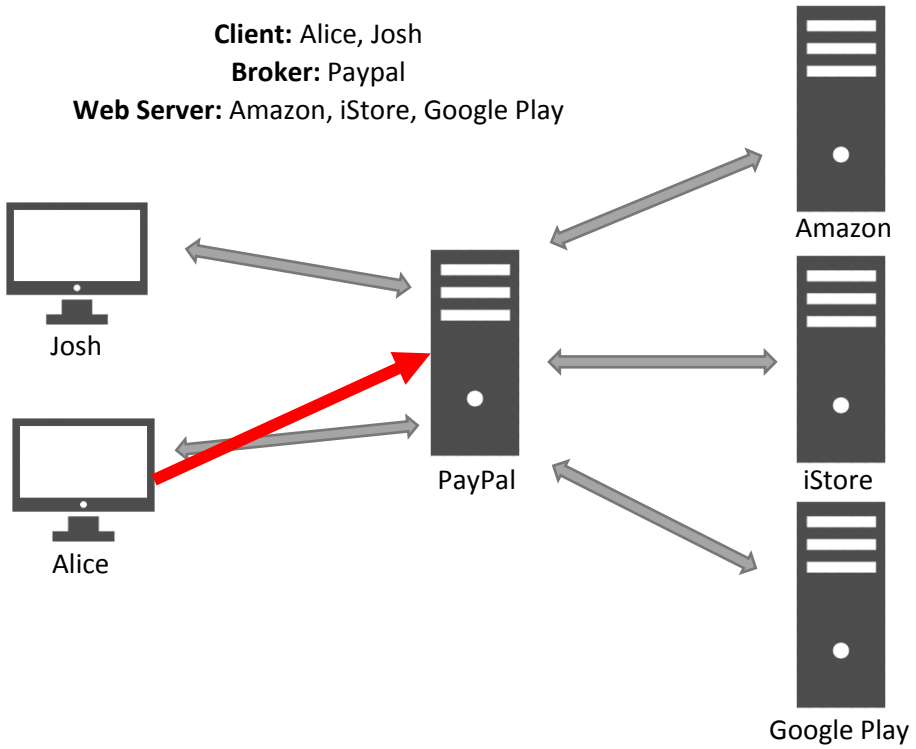


Goal V: Non-repudiation

- Broker can prove that it's the client who authorized payment for an order.

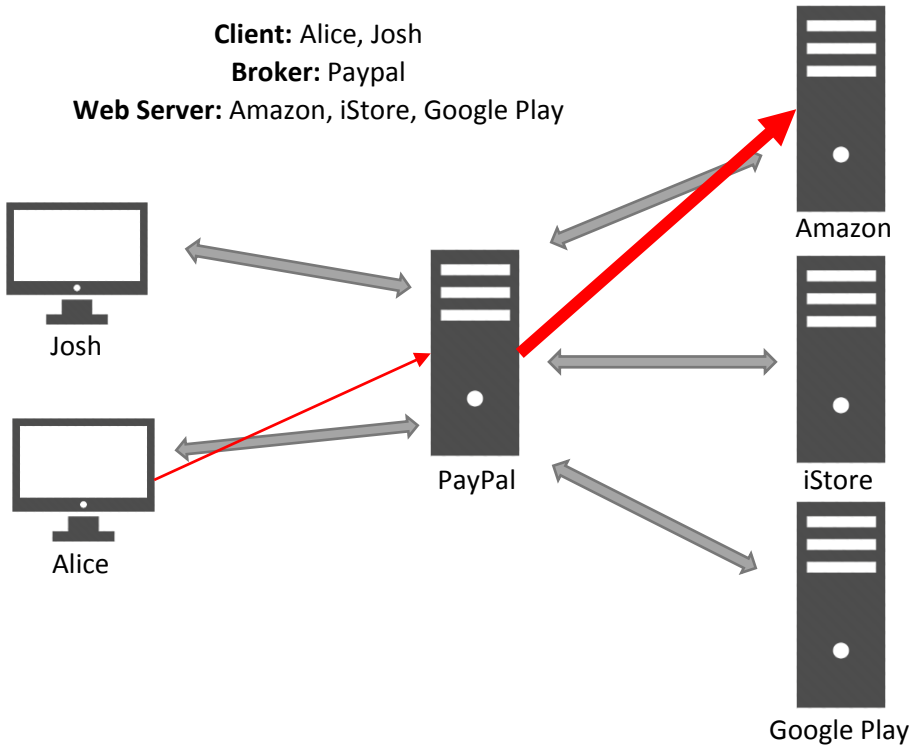


Example



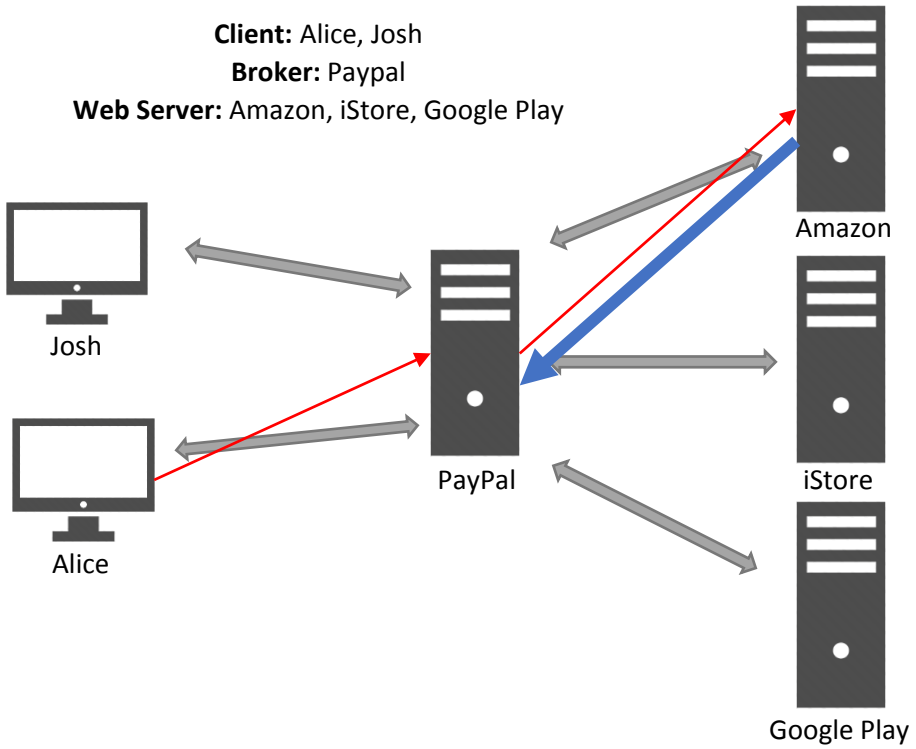
(1) Alice will initiate the process by informing PayPal that she wants to browse Amazon website.

Example (cont'd)



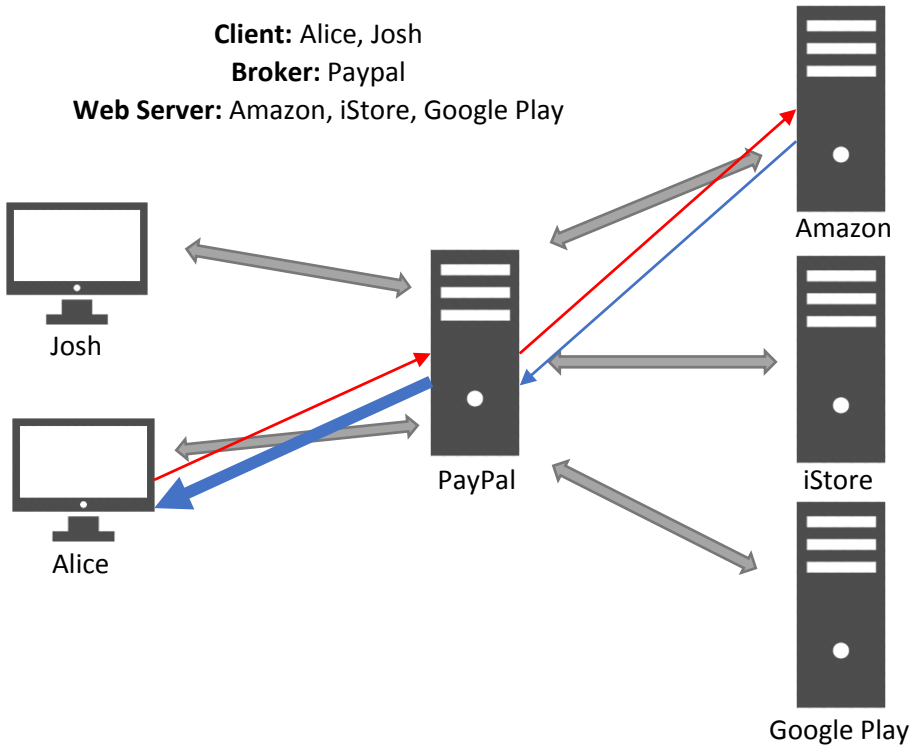
(2) PayPal will create a connection with Amazon.

Example (cont'd)



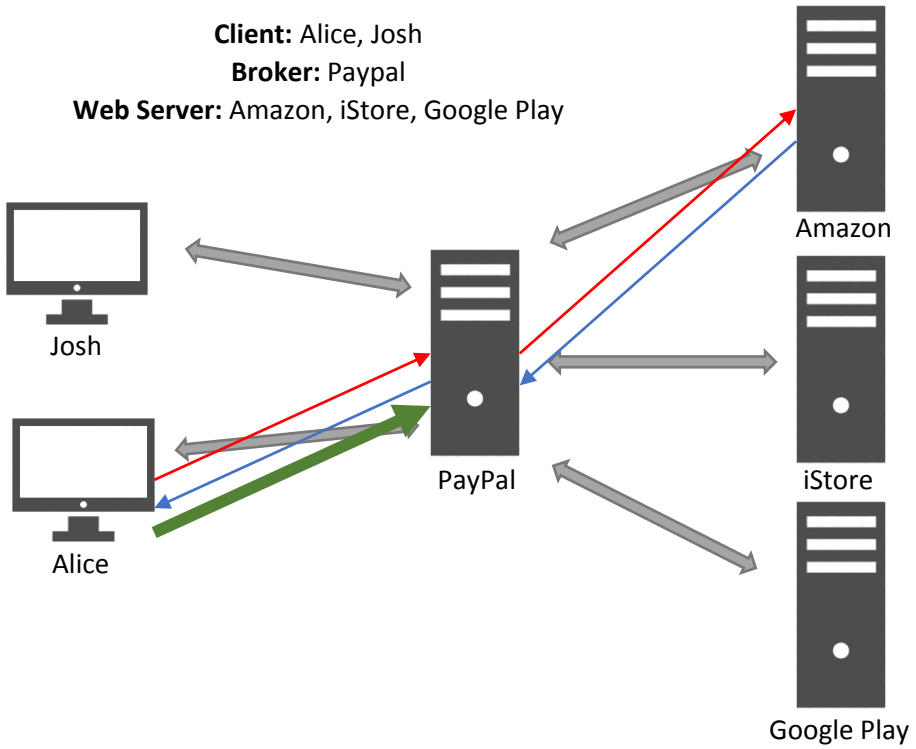
(3) Alice and Amazon will communicate with each other through PayPal in such a way that PayPal cannot decrypt any information.

Example (cont'd)



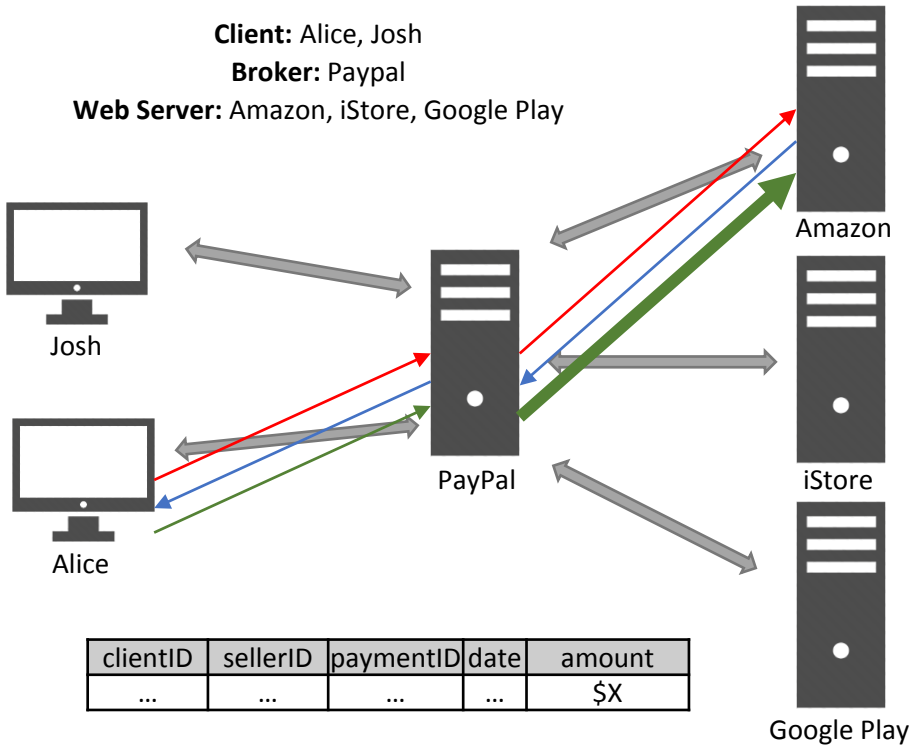
(4) Amazon will send the product catalog file to Alice.

Example (cont'd)



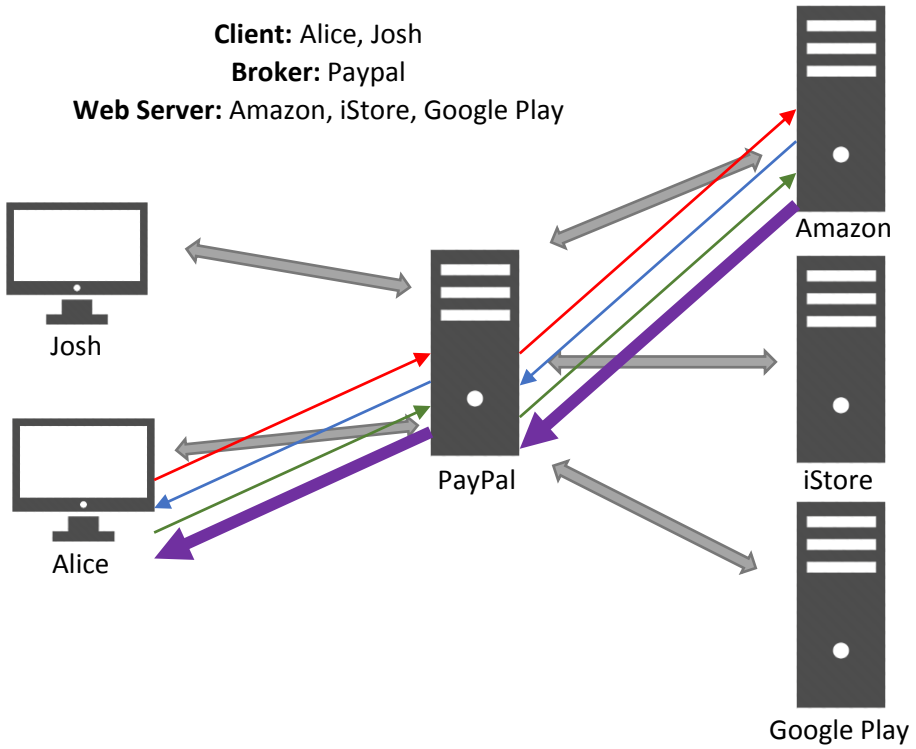
(5) Alice will choose the product and will tell PayPal to pay $X to Amazon.

Example (cont'd)



(6) PayPal will store the payment order from Alice to its database and will pay Amazon.

Example (cont'd)



(7) Amazon will send the product to Alice over the tunnel through PayPal.

Other Requirements

- Group project (3 people)
- C/C++/Java/Python
- Using cryptography library is okay.
- Using ready-to-use secure socket protocols and functionalities such as SSL/TLS is not okay. Write your own protocol using cryptographic primitives.
  - This is a requirement for this class project. Not a real-life advice though.
- Using other libraries such as http libraries (except https features), serialization libraries (json, protobuf etc.) is okay.

Submission

- Plan-of-Action Due: October 21
  - Details of implementation as you understand it and team work
  - 10% of grade
- Full Submission Due: December 1
  - You have to show the working of at least 1 client, one broker and two sellers.
  - README: Instructions to compile/use and other details
- Demo Time: TBA

Thank you

Questions???