Bringing End-to-End Cryptography to Web Mashups

Paul Knickerbocker
pknicker@cs.uoregon.edu
NetSec Lab - University of Oregon

Advisors: Jun Li (lijun@cs.uoregon.edu), Du Li (lidu008@gmail.com)

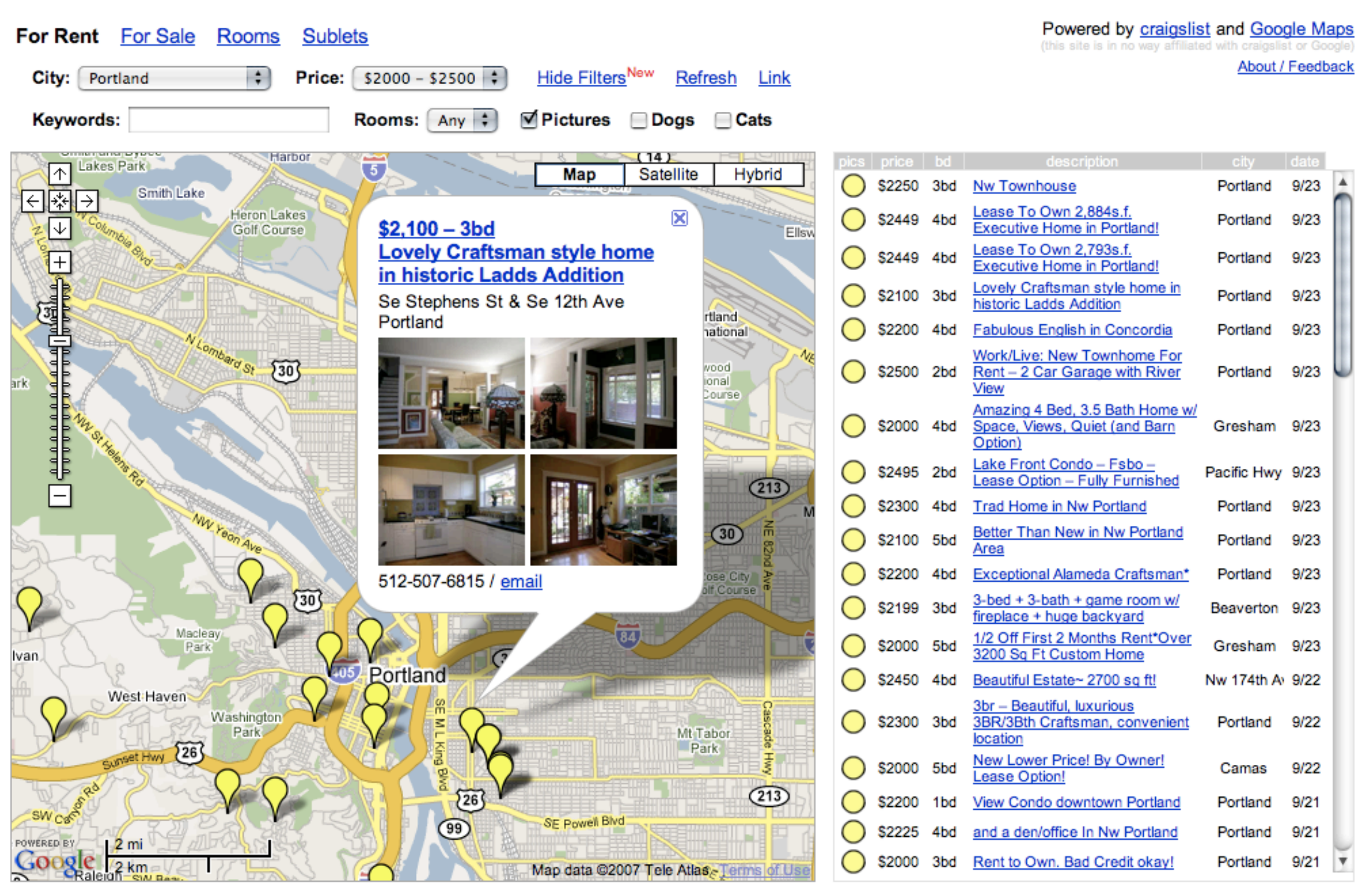
Web Mashups: Data Integration Artwork

Web Mashups are third-party web applications that integrate data collected from several other data sources in novel ways.

Mashups not only pull from different data sources but also collect different types of data. RSS feeds, multimedia, HTML and services like E-Mail can all be presented through a single web page.

Web Mashups have become one of the textbook examples of what is often called "Web 2.0". Mashups are the result of collaboration and extensibility, these are the cornerstones of Web 2.0 design.

Google Maps is a very popular choice for Mashup sites due Google's flexablie API. *HousingMaps.com* uses Google Maps to create a map of housing rentals in an area by using the postings from Craigslist. Other Mashups using Google Maps pull from diverse sources such as census data, weather reports, public transit timetables, public restroom locations and election results.

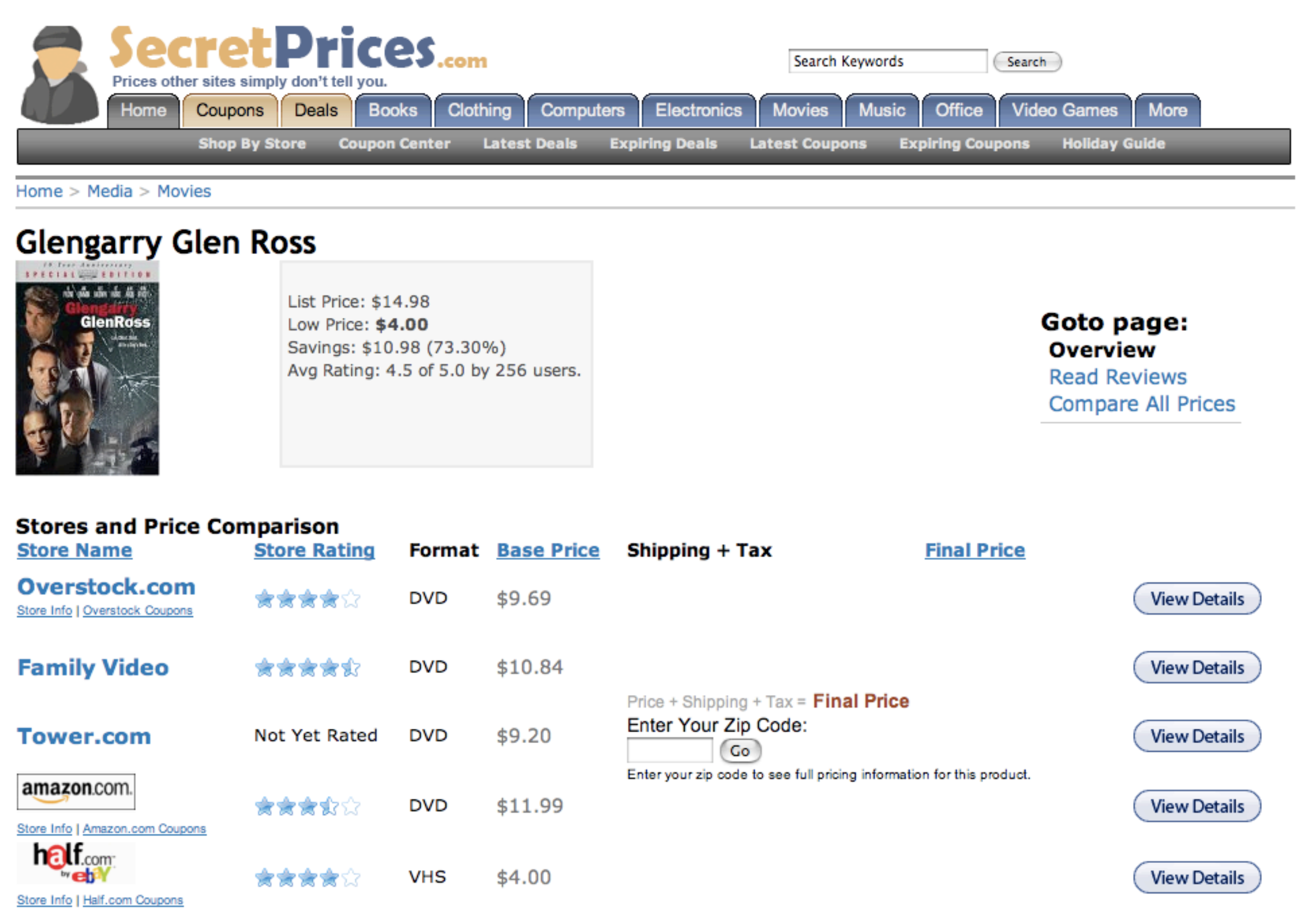

For Rent For Sale Rooms Sublets
City: Portland Price: $2000 - $2500 Hide Filters New Refresh Link
Keywords: Rooms: Any ☑ Pictures ☐ Dogs ☐ Cats
Powered by craigslist and Google Maps
(this site is in no way affiliated with craigslist or Google)
About / Feedback

$2,100 – 3bd
Lovely Craftsman style home in historic Ladds Addition
Se Stephens St & Se 12th Ave
Portland
512-507-6815 / email

pics	price	bd	description	city	date
○	$2250	3bd	Nw Townhouse	Portland	9/23
○	$2449	4bd	Lease To Own 2,884s.f. Executive Home in Portland!	Portland	9/23
○	$2449	4bd	Lease To Own 2,793s.f. Executive Home in Portland!	Portland	9/23
○	$2100	3bd	Lovely Craftsman style home in historic Ladds Addition	Portland	9/23
○	$2200	4bd	Fabulous English in Concordia	Portland	9/23
○	$2500	2bd	Work/Live: New Townhome For Rent – 2 Car Garage with River View	Portland	9/23
○	$2000	4bd	Amazing 4 Bed, 3.5 Bath Home w/ Space, Views, Quiet (and Barn Option)	Gresham	9/23
○	$2495	2bd	Lake Front Condo – Fsbo – Lease Option – Fully Furnished	Pacific Hwy	9/23
○	$2300	4bd	Trad Home in Nw Portland	Portland	9/23
○	$2100	5bd	Better Than New in Nw Portland Area	Portland	9/23
○	$2200	4bd	Exceptional Alameda Craftsman*	Portland	9/23
○	$2199	3bd	3-bed + 3-bath + game room w/ fireplace + huge backyard	Beaverton	9/23
○	$2000	5bd	1/2 Off First 2 Months Rent*Over 3200 Sq Ft Custom Home	Gresham	9/23
○	$2450	4bd	Beautiful Estate~ 2700 sq ft!	Nw 174th A	9/22
○	$2300	3bd	3br – Beautiful, luxurious 3BR/3Bth Craftsman, convenient location	Portland	9/22
○	$2000	5bd	New Lower Price! By Owner! Lease Option!	Camas	9/22
○	$2200	1bd	View Condo downtown Portland	Portland	9/21
○	$2225	4bd	and a den/office In Nw Portland	Portland	9/21
○	$2000	3bd	Rent to Own. Bad Credit okay!	Portland	9/21

Retrieved from http://www.HousingMaps.com on 24 Sep 2007. Results of a search for housing w/ pictures in Portland, OR within a $2000-$2500 per month price range

Online shopping has also fueled the growth of Mashups which compare prices through various venders to find consumers the best deal. *SecretPrices.com* integrates product data from Shopping.com and Amazon.com to compare prices and vender ratings.


SecretPrices.com
Prices other sites simply don't tell you.
Home > Media > Movies

Glengarry Glen Ross

List Price: $14.98
Low Price: **$4.00**
Savings: $10.98 (73.30%)
Avg Rating: 4.5 of 5.0 by 256 users.

Goto page:
Overview
Read Reviews
Compare All Prices

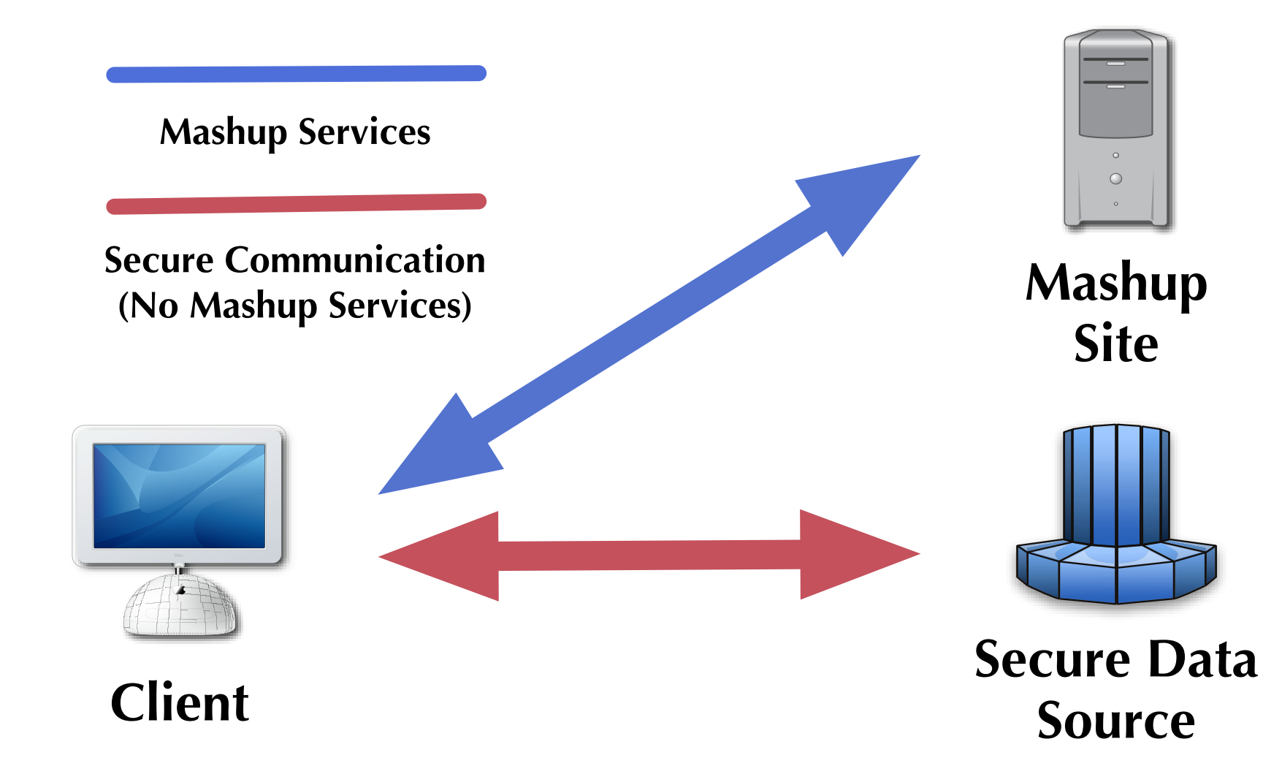
Stores and Price Comparison

Store Name	Store Rating	Format	Base Price	Shipping + Tax	Final Price	
Overstock.com	★★★★☆	DVD	$9.69			View Details
Family Video	★★★★½	DVD	$10.84			View Details
Tower.com	Not Yet Rated	DVD	$9.20	Price + Shipping + Tax = Final Price Enter Your Zip Code: Go Enter your zip code to see full pricing information for this product.		View Details
amazon.com	★★★½☆	DVD	$11.99			View Details
half.com by ebay	★★★★☆	VHS	$4.00			View Details

Retrieved from http://www.SecretPrices.com on 24 Sep 2007. Results of a product search for the movie Glengarry Glen *Ross*

Problems for End-to-End Cryptography

As useful as Mashups are, they pose serious problems for traditional cryptography protocols. But without a system that allows Mashups to have a role in secure communications their overall usefulness is limited.



! Negotiating a secure communication through a Mashup (e.g. for analyzing investment data) is a direct violation of the principle of **End-to-End cryptography**. *But any secure communication that does not include the Mashup will have none of its benefits.*

! In cryptographic terms, Mashups are a identical to **Man-in-the-middle attackers**. *In order to use Mashups to process secure data efficiently we have to develop a protocol that allows for third parties with varying levels of trust.*

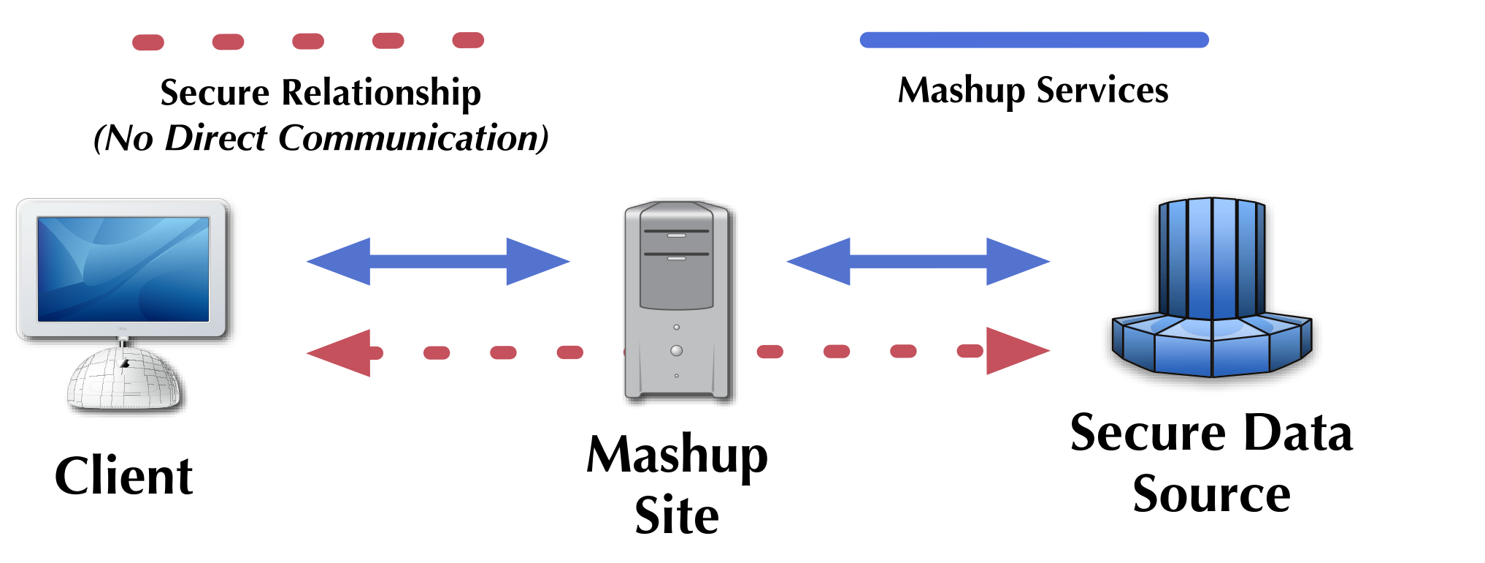
A Layered Approach

In order to integrate Mashups into secure communication without compromising sensitive information we have combined the ideas of **One-Time Use Tickets** and **Layered Cryptography**. The tickets provide the security while the layering allows us to have data flow through several different Mashups.

By allowing Mashups to participate in every step of the secure communication we can benefit from the Mashup's data processing and integration services. At the same time we can still maintain complete control over all data disclosure.

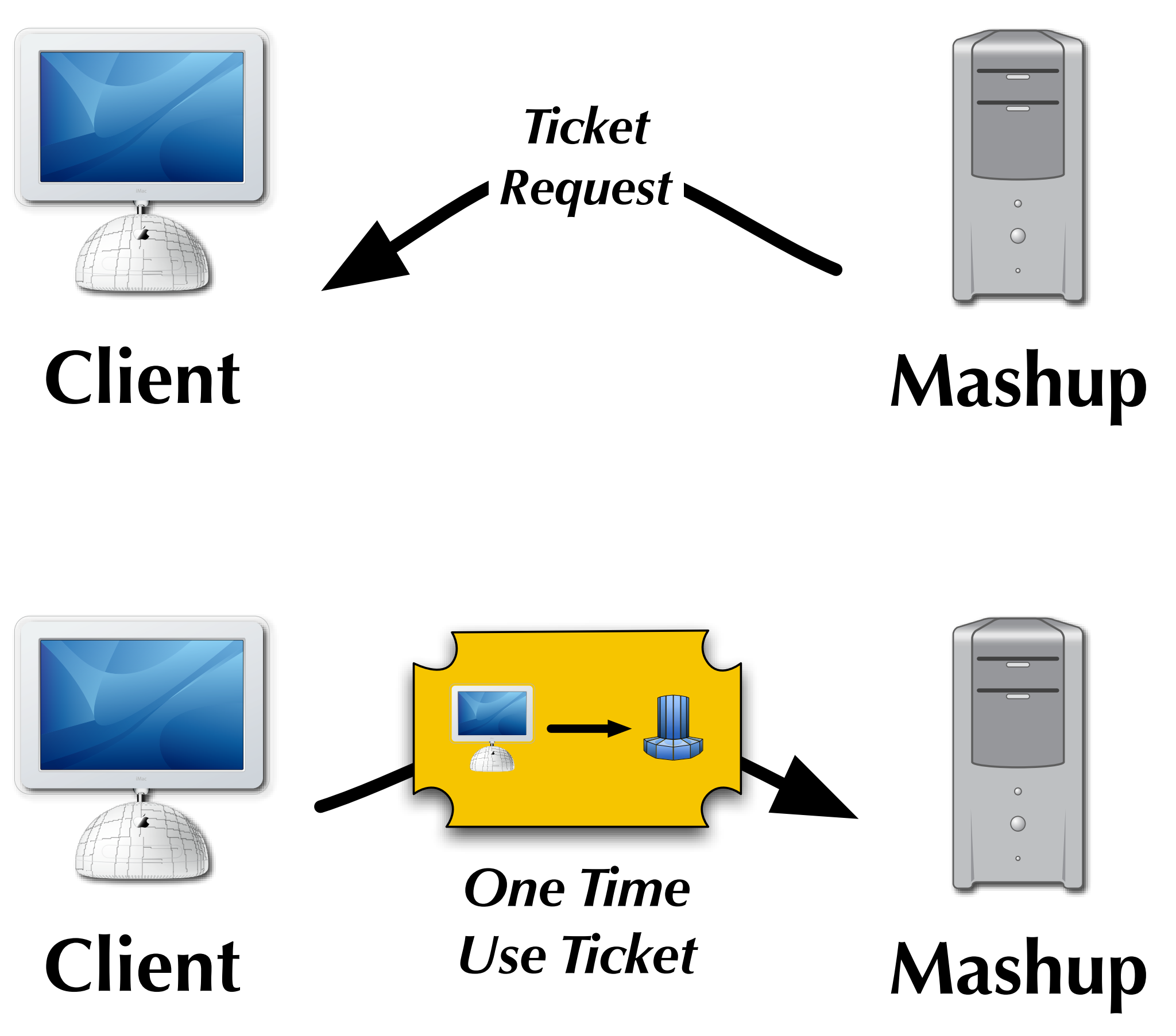
Our layered approach allows us to:

- have numerous Mashups provide services during secure data retrieval
- request data securely through numerous Mashups without unauthorized disclosure
- provide for secure transfer between every machine participating in the communication.



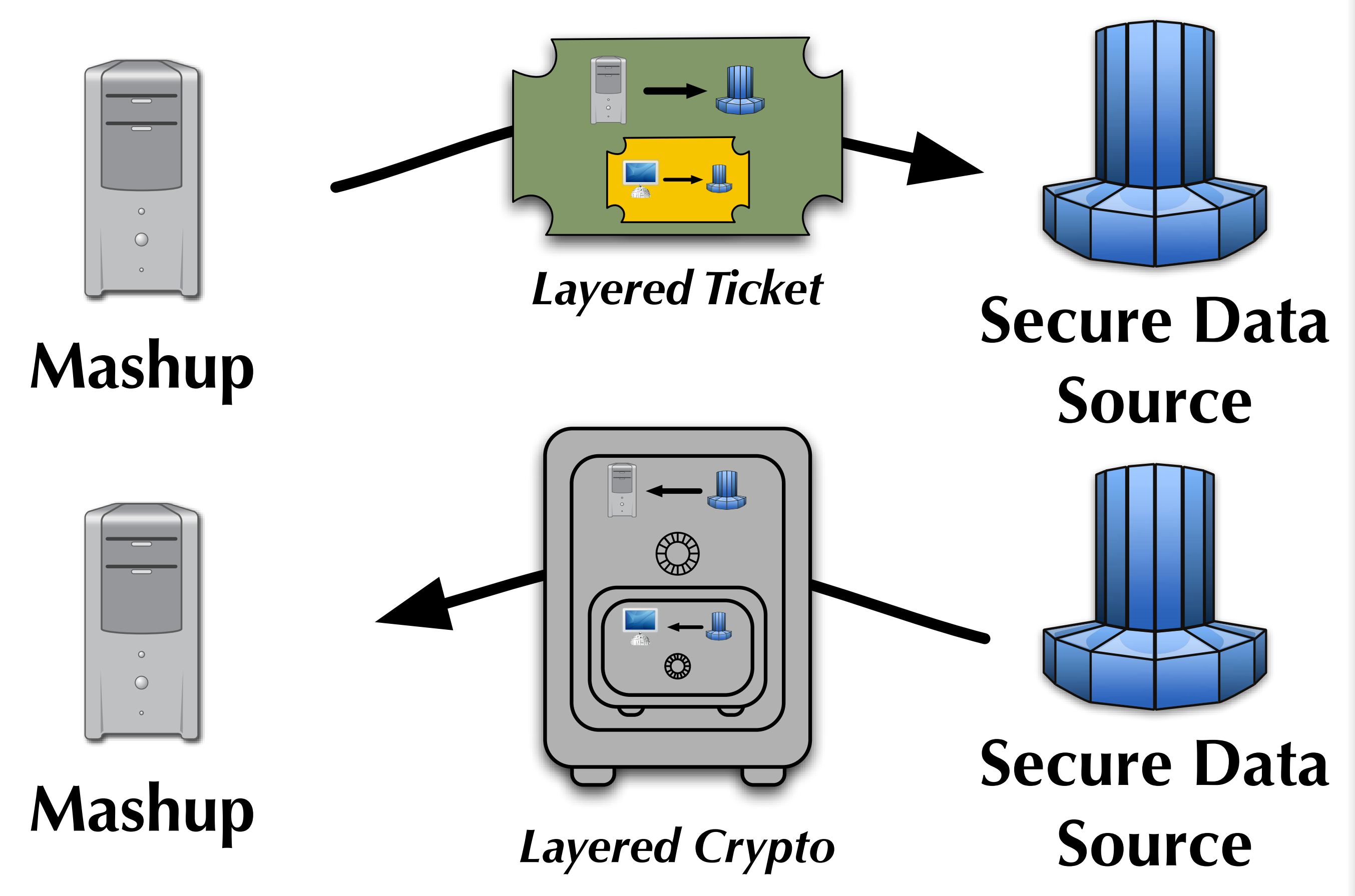
Step #1 - Mashup Requests Ticket

- Mashup server requests the client release of information from a site that requires the client's authentication. The data requested is separated into two groups:
  1. Data that the Mashup needs to process ***before*** returning the web page.
  2. Data that can be processed by the user's browser ***after*** returning the web page.
- Client creates a signed ticket for the Secure Server that the Mashup can use to obtain the authorized information. The ticket contains:
  1. The client's authentication data, this reliably confirms the ticket and its contents are from the user and cannot be used again.
  2. Identification of the Mashup server which is to receive the information.
  3. The type of information which will be released to the Mashup Server.
  4. The type of information which is only to be released back to the Client.



Step #2 - Mashup Retrieves Secure Data

- The Mashup wraps the Client's ticket in its own ticket and sends it to the Secure Server. The Mashup's ticket contains:
  1. Authentication data which verifies the Mashup sending the request is the same one authorized by the Client.
  2. Details on how to securely transmit the returned data.
- The Secure Server unwraps both the Mashup and Client Ticket and verifies the identity of both parties.
- The Secure Server retrieves the User's requested data and atomizes it according to a published schema so that the mashup can properly process the data when it is returned. The atomized data is then grouped by who the data will be disclosed to, Mashup or Client.
- Data intended for the client alone is encrypted with the client's encryption key.
- The entire response with the Mashup's authorized data and user's encrypted data is secured using the Mashup's key and send back to the Mashup for processing.

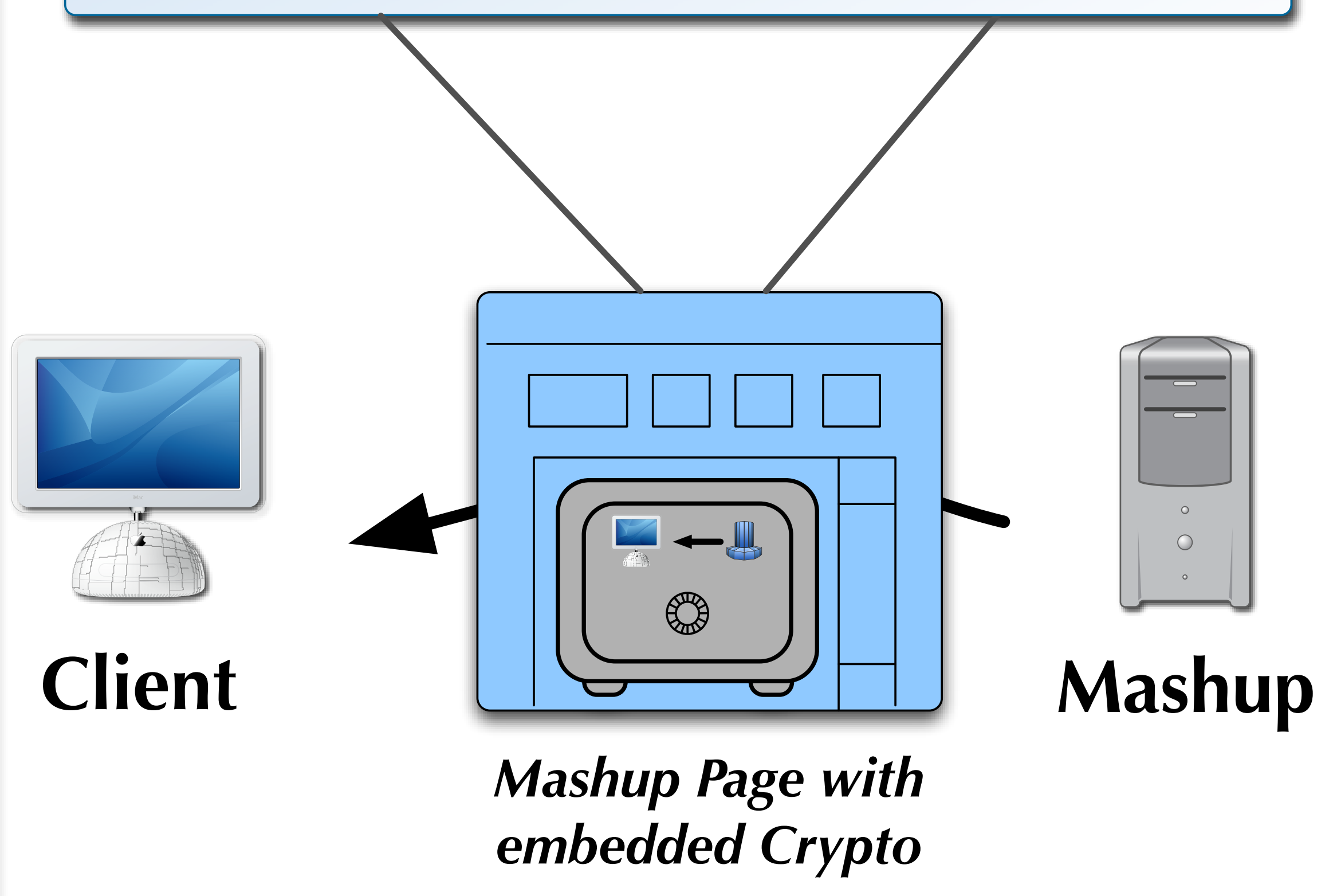


Step #3 - Mashup Returns the Webpage

- The Mashup decrypts the message from the Secure Server and processes the information that has been released to it. The encrypted data viewable only by the Client is embedded into the Mashup page along with the scripts needed to process it.
- The user renders the page and in the process decrypts the private data, processes it with the scripts provided by the mashup, and integrates it into the displayed page.

Sample Mashup HTML

```
<html>
    ...
    Code from Mashup processing of secure data from Secure Server
    ...
    <Encrypted Data>
        Encrypted Data from Secure Server readable only by Client
    </Encrypted Data>
    <Script>
        Code for processing Decrypted Data
    </script>
    ...
</html>
```


Client
Mashup
Mashup Page with embedded Crypto