

# eCommerce

Presented by:  
Michael R. Fatica

# Fundamental Components of eCommerce

- A Web site
- Shopping cart
- A check out form
- A secure certificate
- Products or services available to purchase
- Shipping options
- A gateway to dispatch transactions to the financial network
- Customer service mechanisms

# Common Internet Transaction Scenarios


- Purchasing an item or items with shipping
  - Amazon.com
- Making a one-time, non-material purchase
  - Plane ticket
- Initiating a recurring transaction
  - Gym membership

# Security Practices

- Occurrences of identity theft are increasing dramatically
- Do not experiment with eCommerce
- Understand what you are doing
- Customer data should only be stored when absolutely necessary and only as long as it is needed
- Outsource services to those who spend night and day ensuring their systems are secure

# The Payment Gateway

- Defined:
  - Transmits transaction information from a Web server through the complex financial network.
- Data is typically submitted via a POST operation in a format specific to the gateway's API
- Takes 3-10 seconds depending on the gateway
- Interpret the response (request/response)
- Authorization with optional delayed capture



# The Checkout Process

## *The Authorize.net API*

- Forming the URL to POST
- Request returns the response
- [www.authorize.net/support/AIM\\_guide.pdf](http://www.authorize.net/support/AIM_guide.pdf)

# PHP Sample

- See [www.fatica.net](http://www.fatica.net) or the email list for a link to the sample code. Also available on Authorize.net

# The Web site

- An interactive way of choosing products or services to purchase
- Popular eCommerce “solutions”
  - OSCommerce
  - Mals eCommerce
  - PayPal
- Vulnerabilities
  - Cart hacking, price changes, storing customer profiles

# HTTPS, Certificates and CAs

- Required when you want to encrypt transmissions between the browser and your Web server
- An SSL Certificate has a public and private key used in encrypting transmissions between the client and server
- A certificate is issued and signed by a Certification Authority (E.g. Verisign, TrustE, Thawte)
- Browsers know of a few CAs, but you could become your own.
- Certs are signed using a CSR, generated by your Web server
- HTTPS is required in the *transmission* of customer data and is not required for your entire site, but it is recommended.

# Merchant Accounts

- Required to post credit card transactions to you or your business directly
- Must be Internet-enabled merchant accounts (retail ma's may not support req'd financial networks)
- Setup costs
- High-risk merchants (low volume, bad credit)
- Pass-through services (e.g. CCBill) use their merchant account and charge you more.

# Shipping

- UPS, FEDEX, USPS and ...offer freight cost calculation APIs.
- Nearly all accessed via Web services

# Implementation scenarios

- Cheapest shopping cart

- Mals eCommerce

- Hosted form
    - Hosted customer information
    - Optionally Integrates with PayPal
    - Supports manual credit card processing

# Enterprise Recurring Charge

- Single form for registration for monthly email
  - Option to purchase an entire year
  - Form transmits essential information plus custom fields (Comments1 & 2)
  - Deductions are made monthly
  - Credit cards expire