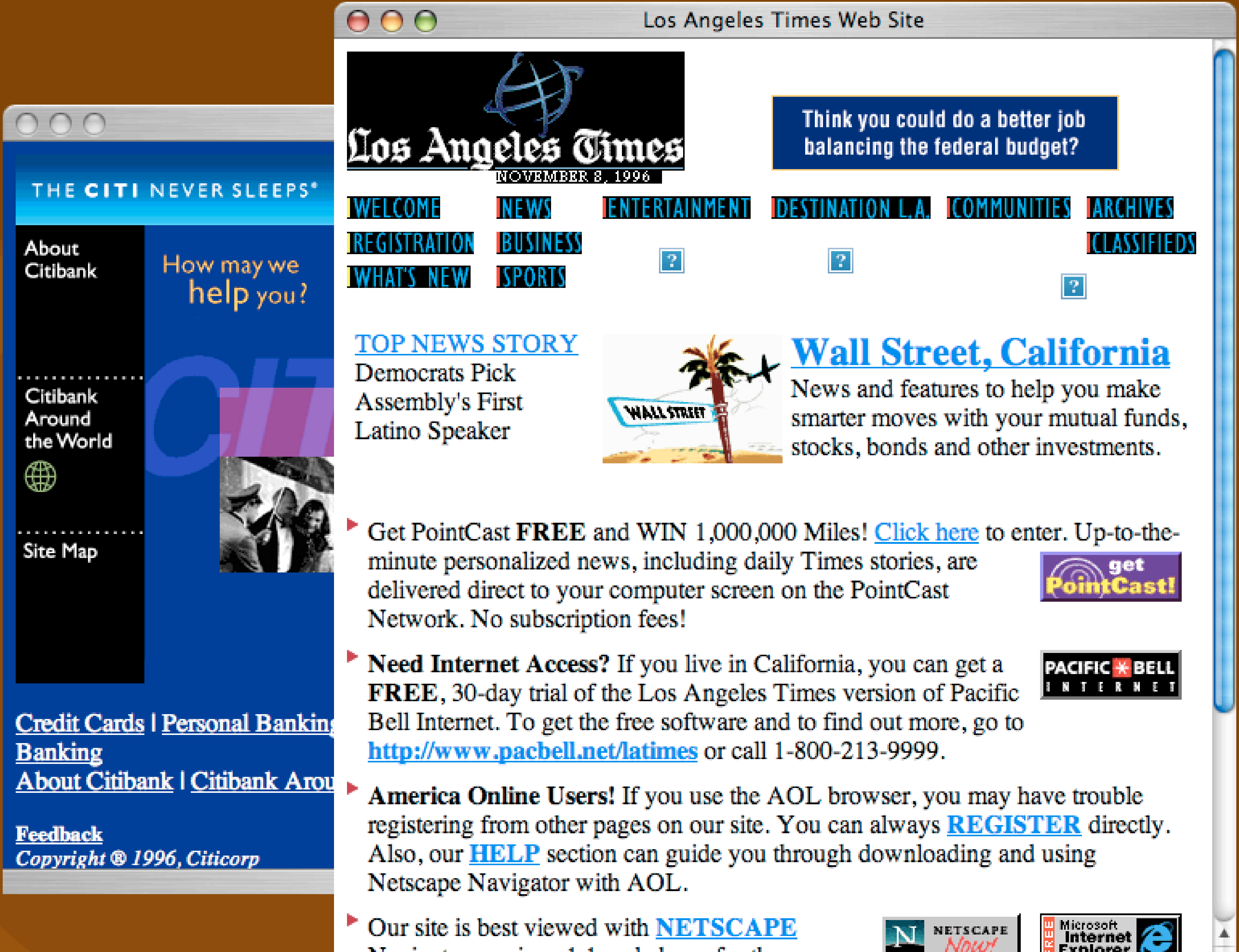
A Unified Security Model for Web Applications

Richard S. Cox, Steven D. Gribble,
Henry M. Levy



THE CITI NEVER SLEEPS®

About Citibank

How may we help you?

Citibank Around the World

Site Map

Credit Cards | Personal Banking

Banking

About Citibank | Citibank Arou

Feedback

Copyright © 1996, Citicorp

Los Angeles Times

NOVEMBER 8, 1996

Think you could do a better job balancing the federal budget?

TOP NEWS STORY
Democrats Pick Assembly's First Latino Speaker

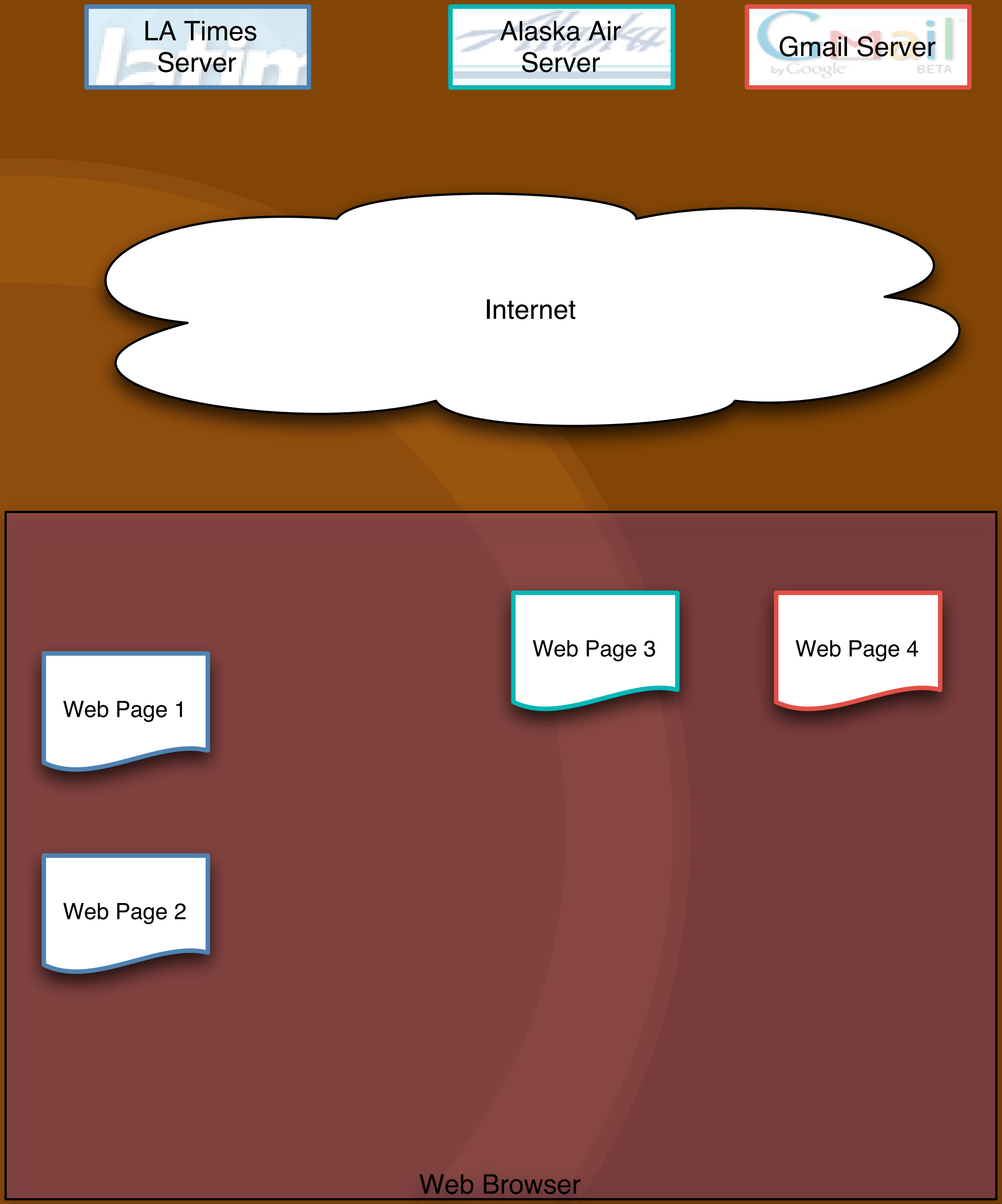
Wall Street, California
News and features to help you make smarter moves with your mutual funds, stocks, bonds and other investments.

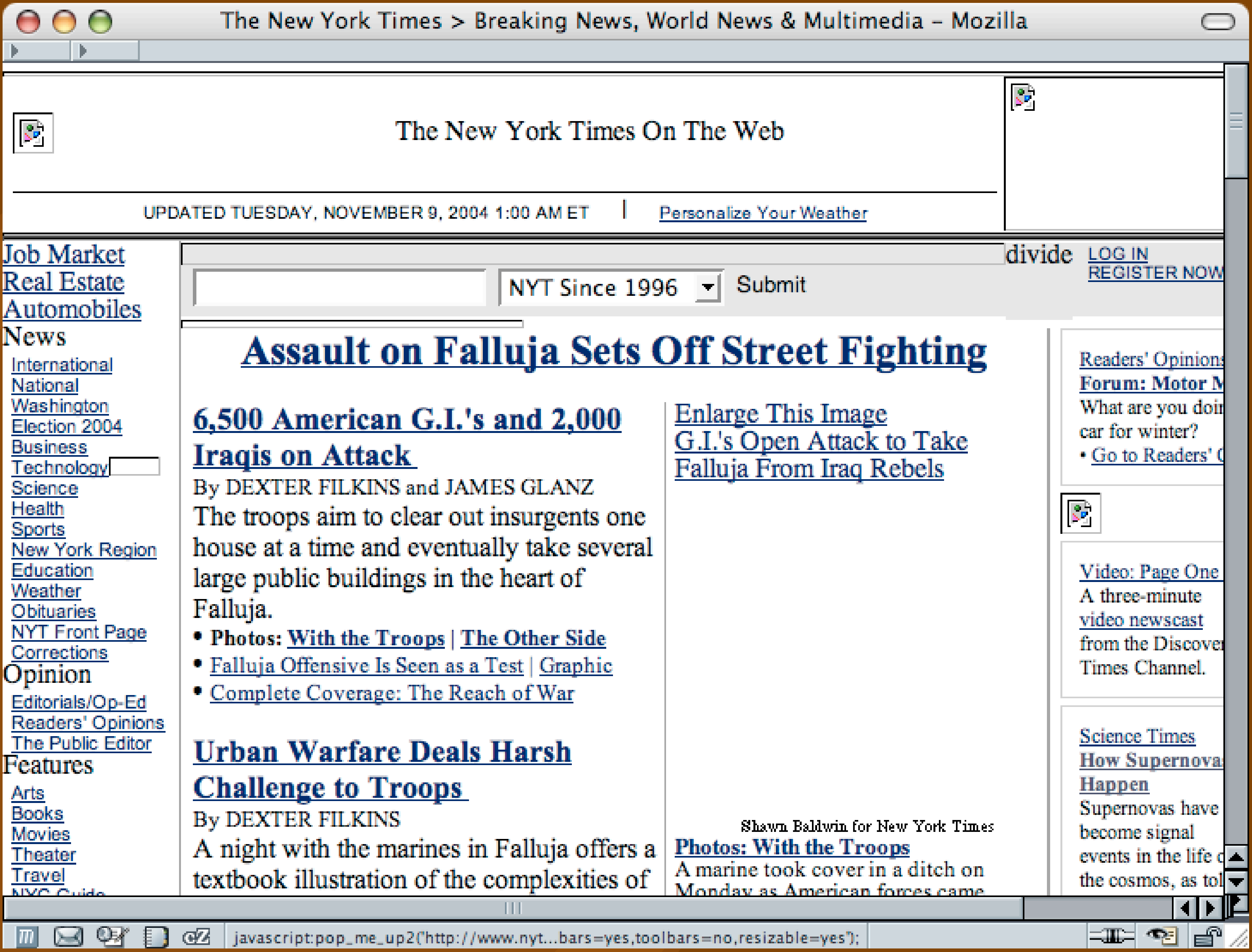
- Get PointCast **FREE** and WIN 1,000,000 Miles! Click here to enter. Up-to-the-minute personalized news, including daily Times stories, are delivered direct to your computer screen on the PointCast Network. No subscription fees!

- **Need Internet Access?** If you live in California, you can get a **FREE**, 30-day trial of the Los Angeles Times version of Pacific Bell Internet. To get the free software and to find out more, go to http://www.pacbell.net/latimes or call 1-800-213-9999.

- **America Online Users!** If you use the AOL browser, you may have trouble registering from other pages on our site. You can always REGISTER directly. Also, our HELP section can guide you through downloading and using Netscape Navigator with AOL.

- Our site is best viewed with NETSCAPE


LA Times Server
Alaska Air Server
Gmail Server
Internet
Web Page 3
Web Page 4
Web Page 1
Web Page 2
Web Browser



The New York Times > Breaking News, World News & Multimedia - Mozilla

The New York Times On The Web

UPDATED TUESDAY, NOVEMBER 9, 2004 1:00 AM ET | Personalize Your Weather

Job Market
Real Estate
Automobiles
News
International
National
Washington
Election 2004
Business
Technology
Science
Health
Sports
New York Region
Education
Weather
Obituaries
NYT Front Page
Corrections
Opinion
Editorials/Op-Ed
Readers' Opinions
The Public Editor
Features
Arts
Books
Movies
Theater
Travel
NYC Guide

NYT Since 1996 ▾ Submit

divide LOG IN
REGISTER NOW

Assault on Falluja Sets Off Street Fighting

6,500 American G.I.'s and 2,000 Iraqis on Attack

By DEXTER FILKINS and JAMES GLANZ

The troops aim to clear out insurgents one house at a time and eventually take several large public buildings in the heart of Falluja.

- **Photos: With the Troops** | **The Other Side**
- Falluja Offensive Is Seen as a Test | Graphic
- Complete Coverage: The Reach of War

Urban Warfare Deals Harsh Challenge to Troops

By DEXTER FILKINS

A night with the marines in Falluja offers a textbook illustration of the complexities of

Enlarge This Image
G.I.'s Open Attack to Take Falluja From Iraq Rebels

Shawn Baldwin for New York Times

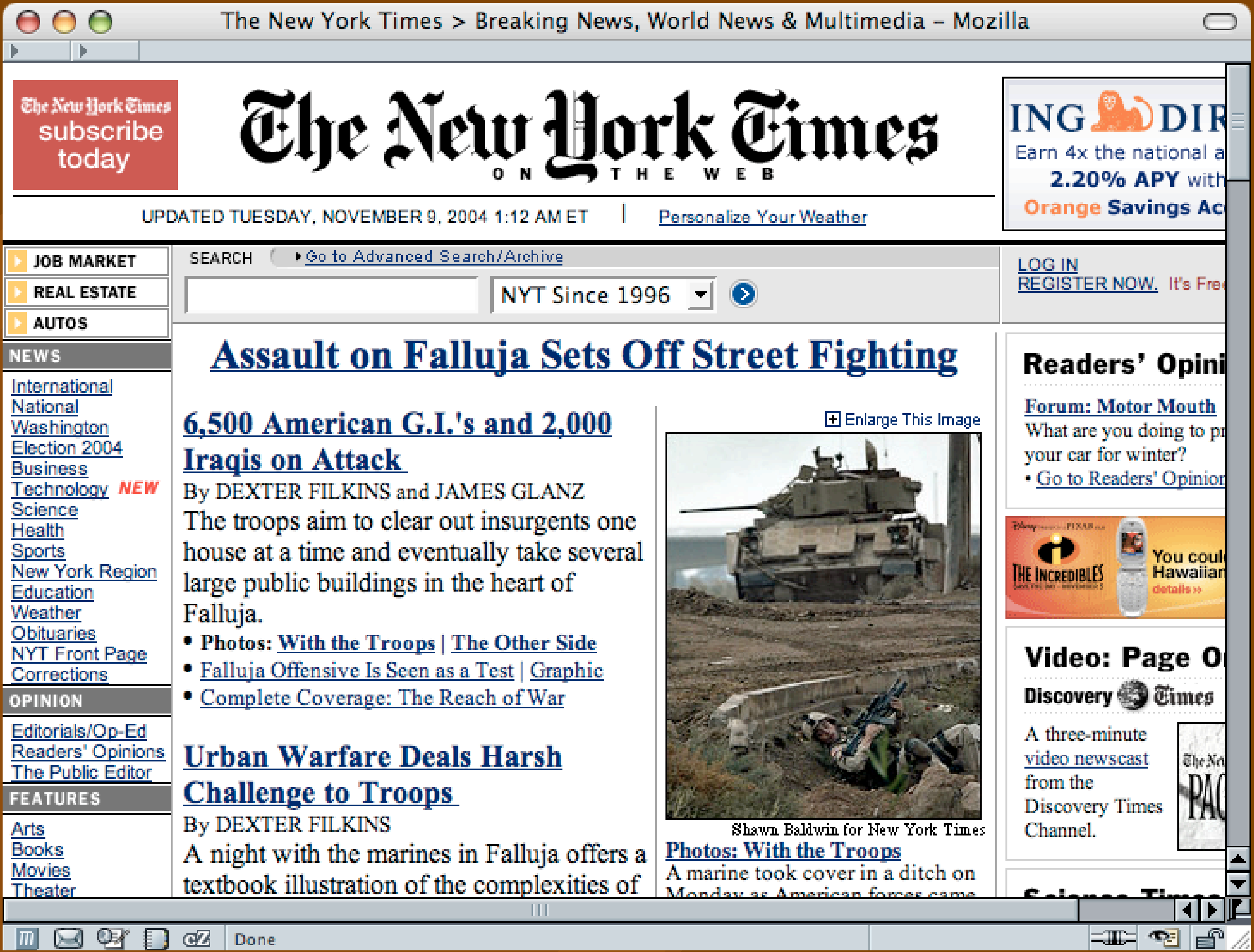
Photos: With the Troops
A marine took cover in a ditch on Monday as American forces came

Readers' Opinions
Forum: Motor M
What are you doir car for winter?
• Go to Readers' (

Video: Page One
A three-minute video newscast from the Discover Times Channel.

Science Times
How Supernovas Happen
Supernovas have become signal events in the life of the cosmos, as tol

javascript:pop_me_up2('http://www.nyt...bars=yes,toolbars=no,resizable=yes');



The New York Times > Breaking News, World News & Multimedia – Mozilla

The New York Times ON THE WEB

UPDATED TUESDAY, NOVEMBER 9, 2004 1:12 AM ET | Personalize Your Weather

JOB MARKET
REAL ESTATE
AUTOS

NEWS
- International
- National
- Washington
- Election 2004
- Business
- Technology NEW
- Science
- Health
- Sports
- New York Region
- Education
- Weather
- Obituaries
- NYT Front Page
- Corrections

OPINION
- Editorials/Op-Ed
- Readers' Opinions
- The Public Editor

FEATURES
- Arts
- Books
- Movies
- Theater

SEARCH · Go to Advanced Search/Archive

NYT Since 1996

LOG IN
REGISTER NOW. It's Free

Assault on Falluja Sets Off Street Fighting

6,500 American G.I.'s and 2,000 Iraqis on Attack

By DEXTER FILKINS and JAMES GLANZ

The troops aim to clear out insurgents one house at a time and eventually take several large public buildings in the heart of Falluja.

- **Photos:** With the Troops | The Other Side
- Falluja Offensive Is Seen as a Test | Graphic
- Complete Coverage: The Reach of War

Urban Warfare Deals Harsh Challenge to Troops

By DEXTER FILKINS

A night with the marines in Falluja offers a textbook illustration of the complexities of

Enlarge This Image

Shawn Baldwin for New York Times

Photos: With the Troops

A marine took cover in a ditch on Monday as American forces came

Readers' Opini

Forum: Motor Mouth

What are you doing to pr your car for winter?

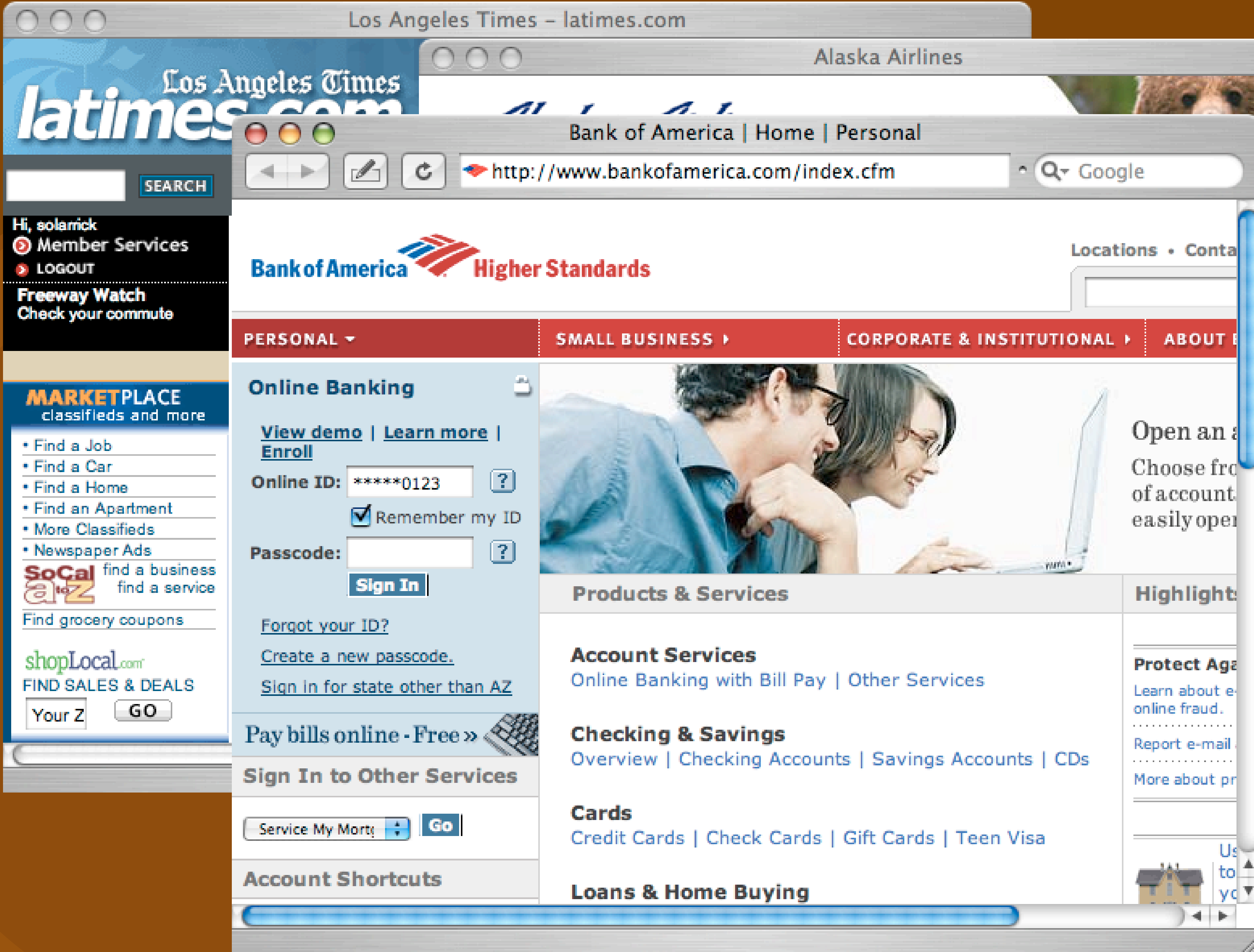
• Go to Readers' Opinion

Video: Page O

Discovery Times

A three-minute video newscast from the Discovery Times Channel.

Done



Los Angeles Times – latimes.com

Los Angeles Times latimes.com

SEARCH

Hi, solamick

Member Services

LOGOUT

Freeway Watch
Check your commute

MARKETPLACE
classifieds and more

- Find a Job
- Find a Car
- Find a Home
- Find an Apartment
- More Classifieds
- Newspaper Ads

SoCal a to Z find a business find a service

Find grocery coupons

shopLocal.com
FIND SALES & DEALS

Your Z GO

Alaska Airlines

Bank of America | Home | Personal

http://www.bankofamerica.com/index.cfm

Google

Bank of America Higher Standards

Locations • Conta

PERSONAL ▾ | SMALL BUSINESS ▸ | CORPORATE & INSTITUTIONAL ▸ | ABOUT

Online Banking

View demo | Learn more | Enroll

Online ID: *****0123 ?

☑ Remember my ID

Passcode: ?

Sign In

Forgot your ID?

Create a new passcode.

Sign in for state other than AZ

Pay bills online - Free »

Sign In to Other Services

Service My Mortg Go

Account Shortcuts

Open an a
Choose fro
of account
easily oper

Products & Services

Account Services
Online Banking with Bill Pay | Other Services

Checking & Savings
Overview | Checking Accounts | Savings Accounts | CDs

Cards
Credit Cards | Check Cards | Gift Cards | Teen Visa

Loans & Home Buying

Highlight

Protect Aga
Learn about e
online fraud.

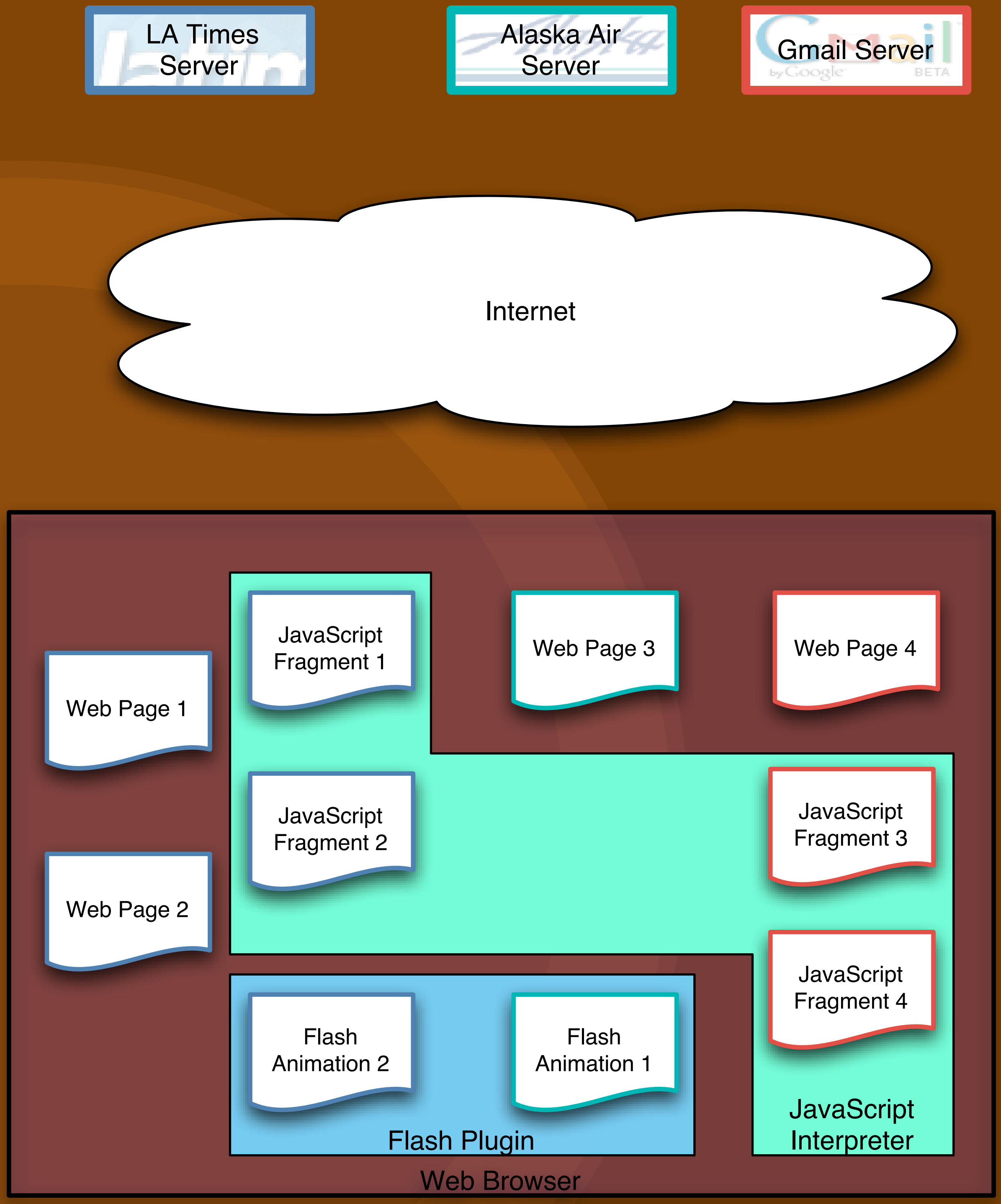
Report e-mail

More about pr

Us
to
yo

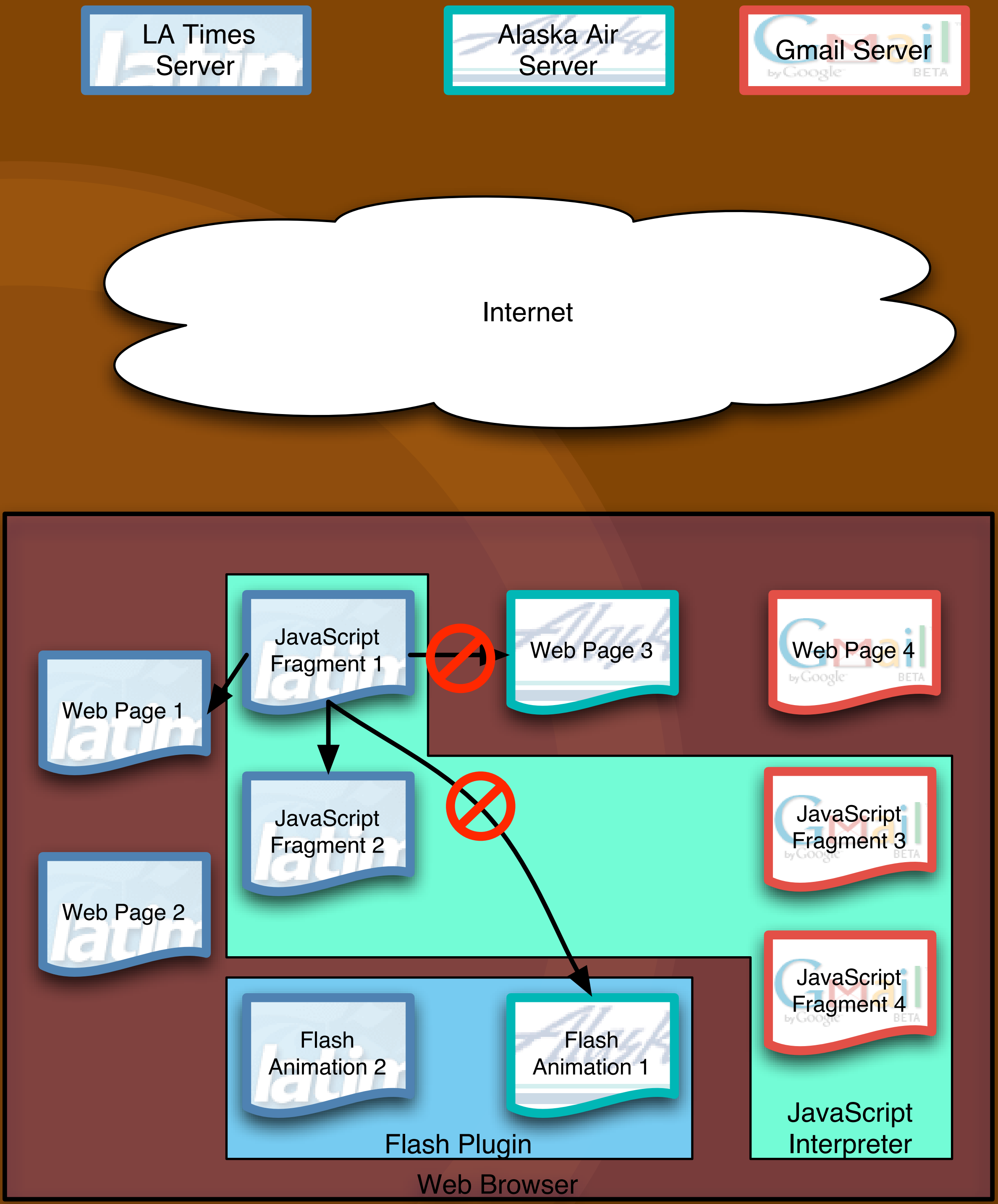
latimes.com

- 90+ HTTP connections
- 40+ pieces of code
  - JavaScript, VisualBasic, Flash
  - From 5 different servers
- 11 images from external sites
- 3 forms


LA Times Server
Alaska Air Server
Gmail Server
Internet
Web Page 1
Web Page 2
JavaScript Fragment 1
JavaScript Fragment 2
Web Page 3
Web Page 4
JavaScript Fragment 3
JavaScript Fragment 4
Flash Animation 2
Flash Animation 1
Flash Plugin
JavaScript Interpreter
Web Browser

Same Origin Policy

- Each object labeled with domain that sent it
- Allow access if domains are equal
- Used by JavaScript, Flash, ActiveX


LA Times Server
Alaska Air Server
Gmail Server
Internet
JavaScript Fragment 1
Web Page 3
Web Page 4
Web Page 1
JavaScript Fragment 2
JavaScript Fragment 3
Web Page 2
JavaScript Fragment 4
Flash Animation 2
Flash Animation 1
Flash Plugin
JavaScript Interpreter
Web Browser

Browser = OS

- Provides
  - Abstractions/APIs
  - Resource Allocation
  - Isolation
- Sites do not directly interact with host OS (mostly)

Outline

- Web Evolution
- Problem 1: Implementation Bugs
- Problem 2: User Interface
- Applications, not Documents
- Conclusions

Implementation Bugs

Threat Model

- Attacker can send any content to browser (e.g. in email)
- Browser has bugs
- Attacker cannot modify base browser

Attacker Goals

- Compromise host OS
- Steal data from external sites
  - User-input, displayed content, cookies, cache, etc.
- Spoof

Attacker Goals

- Modify external sites
  - Insert advertising (AdWare)
  - Just to mislead user

Vulnerabilities

- Of 55 Mozilla security bugs:
- Code Injection: 14
  - Buffer overflows: 10
- Sharing Policy/Mechanism: 36
- User Interface: 3
- Other: 2

User Interface

Controlling Apps

- Users cannot manage the web sites
  - Closing a window != Quit
  - Can't delete only one app
- No accounting
  - Who is playing that MIDI?

End-to-End Security

- Last link is from screen to user
- Need to secure that link too
- Users do not reason well about security today

SSL is per-document

- How do I know if hfs.washington.edu is affiliated with www.onlinecardoffice.com?
- SSL only tells me that each of them is who they claim to be

Apps, not Docs

Why?

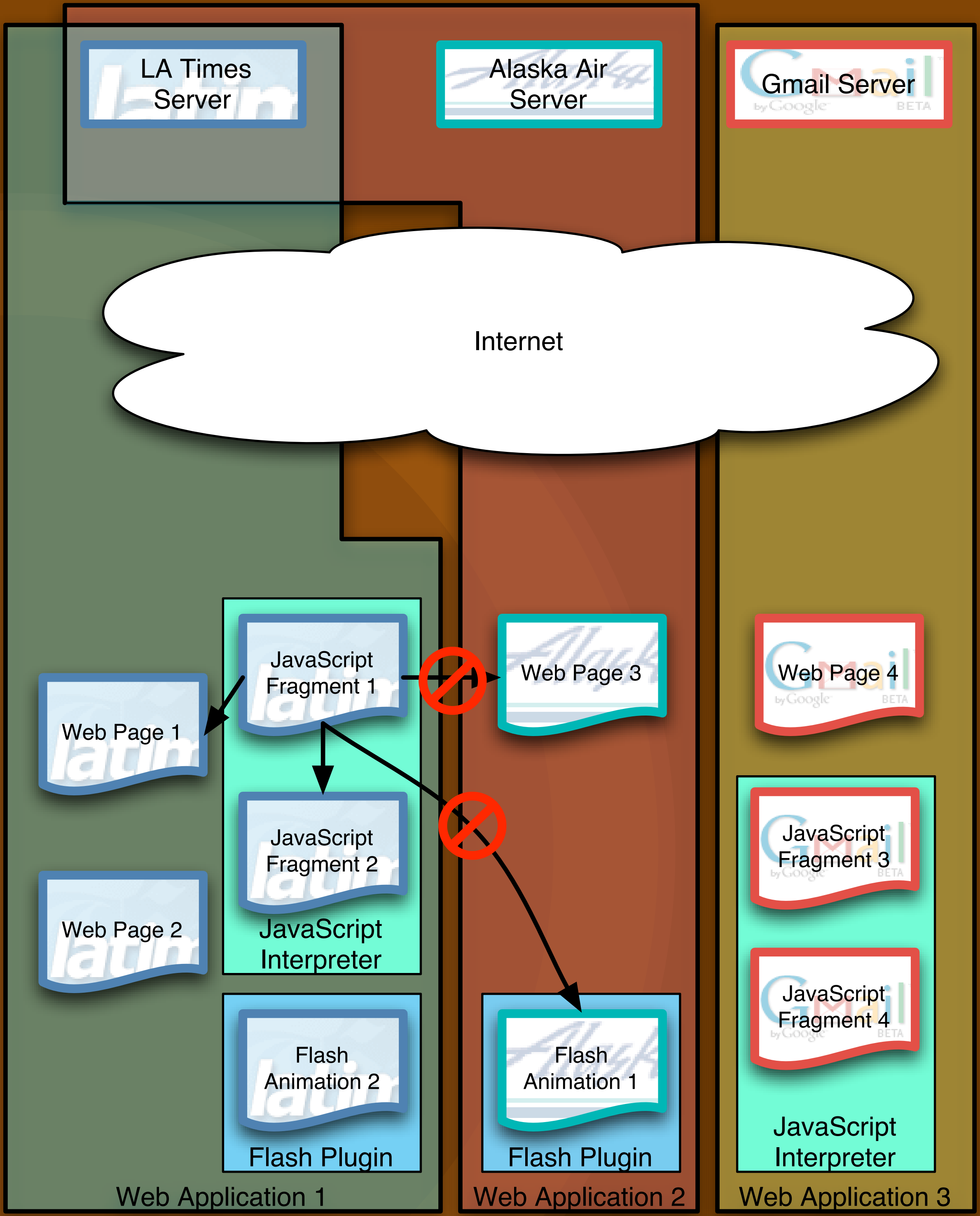
- Treat web sites as applications, not collections of documents
- Inter-document interfaces are complex
- Inter-application interfaces are very narrow

What is a Web App?

- Collection of
  - Servers speaking HTTP(S)
  - HTML, image, movie, sound documents
  - JavaScript, Flash, Java, ActiveX client-side code
  - Client-side state (cookies)

What is a Web App?

- All cooperating to implement a single service


LA Times Server
Alaska Air Server
Gmail Server
Internet
JavaScript Fragment 1
Web Page 1
Web Page 3
Web Page 4
JavaScript Fragment 2
JavaScript Interpreter
Web Page 2
JavaScript Fragment 3
JavaScript Fragment 4
JavaScript Interpreter
Flash Animation 2
Flash Plugin
Flash Animation 1
Flash Plugin
Web Application 1
Web Application 2
Web Application 3

Application Interface

- Draw in window
- File access (rare)
- Print
- Play sound
- Make network connections
  - What to do about SSL?

App Manifests

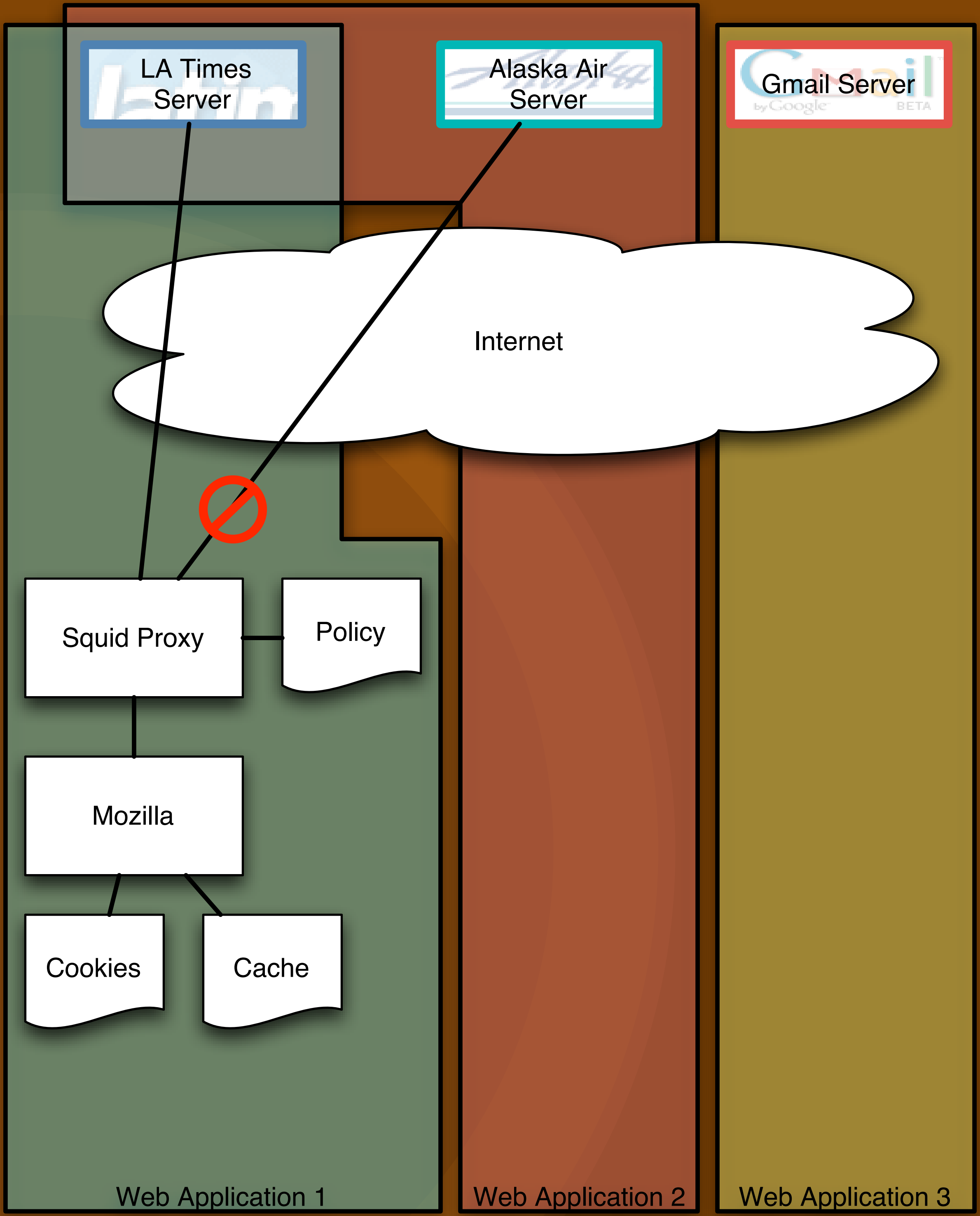
- Problem: What goes in each box?
- Web applications defined by a manifest file
- One* manifest per application
- Provided by server

App Manifests

- Defines the content that is part of application
  - By hostname, certificate, hash
- Defines network resources app expected to use
- Digitally signed

Current Prototype

- Use a full Mozilla per app
  - Private cookies, cache, prefs, bookmarks
- Squid proxy enforces policy
- Isolated in UNIX processes

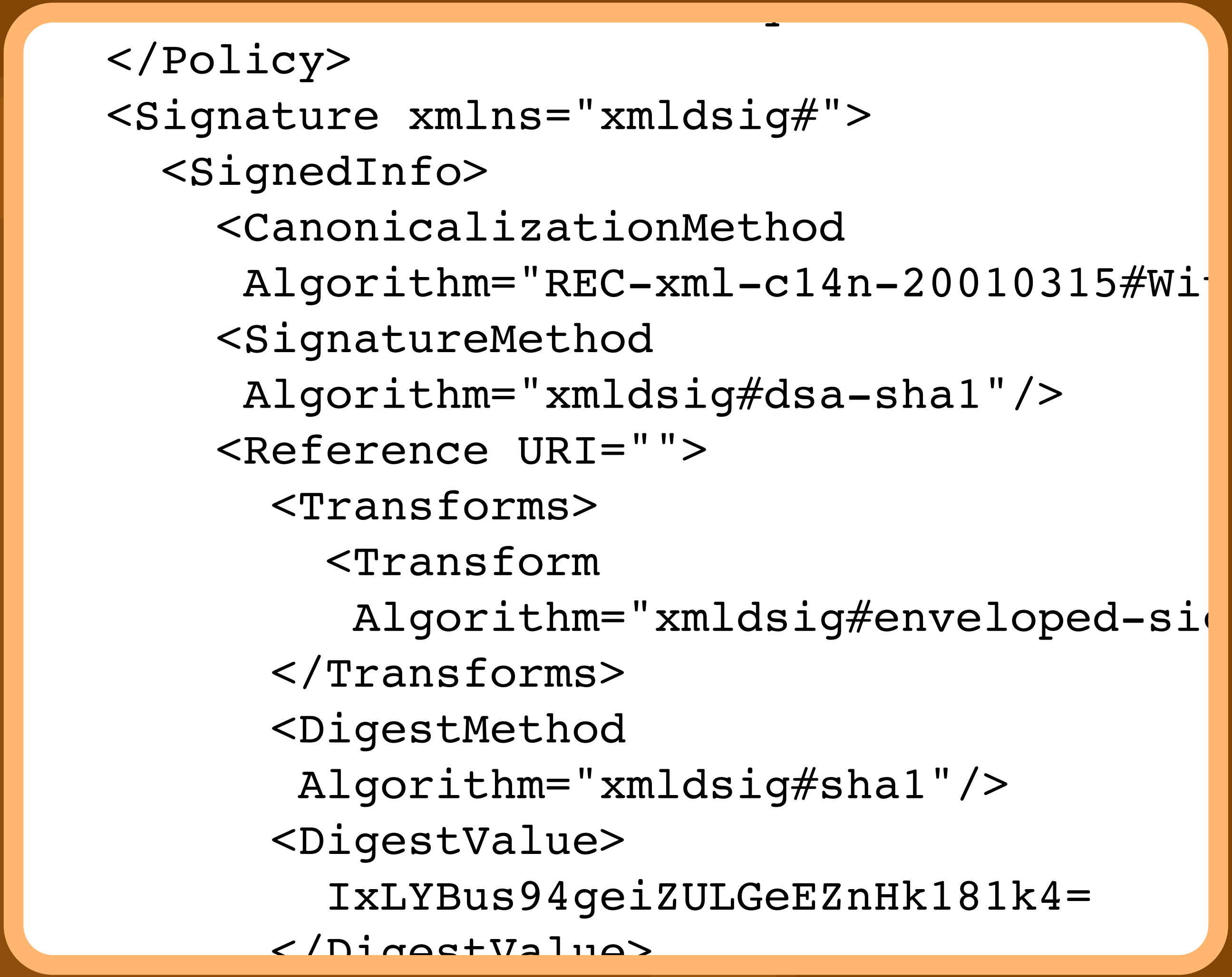

LA Times Server
Alaska Air Server
Gmail Server
Internet
Squid Proxy
Policy
Mozilla
Cookies
Cache
Web Application 1
Web Application 2
Web Application 3

Example Manifest

```
<?xml version="1.0"?>
<tahoma-application>
  <name>urn:orkut.com:applications:orkut</r
  <start-url>http://www.orkut.com/</start-u
  <browser-configuration/>
  <Policy ...>
    ...
    <Rule RuleId="connect:443:0" Effect="Pe
      <Target>
        ...
        <Actions>
          <Action>
            <ActionMatch
          MatchId="function:string-equal">
              <ActionAttributeDesignator
               DataType="string"
         AttributeId="action:action-id"/>
```

```
<Rule RuleId="connect:443:0" Effect="P
  <Target>
    ...
    <Actions>
      <Action>
        <ActionMatch
     MatchId="function:string-equal">
          <ActionAttributeDesignator
           DataType="string"
    AttributeId="action:action-id"/>
          <AttributeValue
           DataType="string">
              CONNECT
          </AttributeValue>
        </ActionMatch>
      </Action>
    </Actions>
```

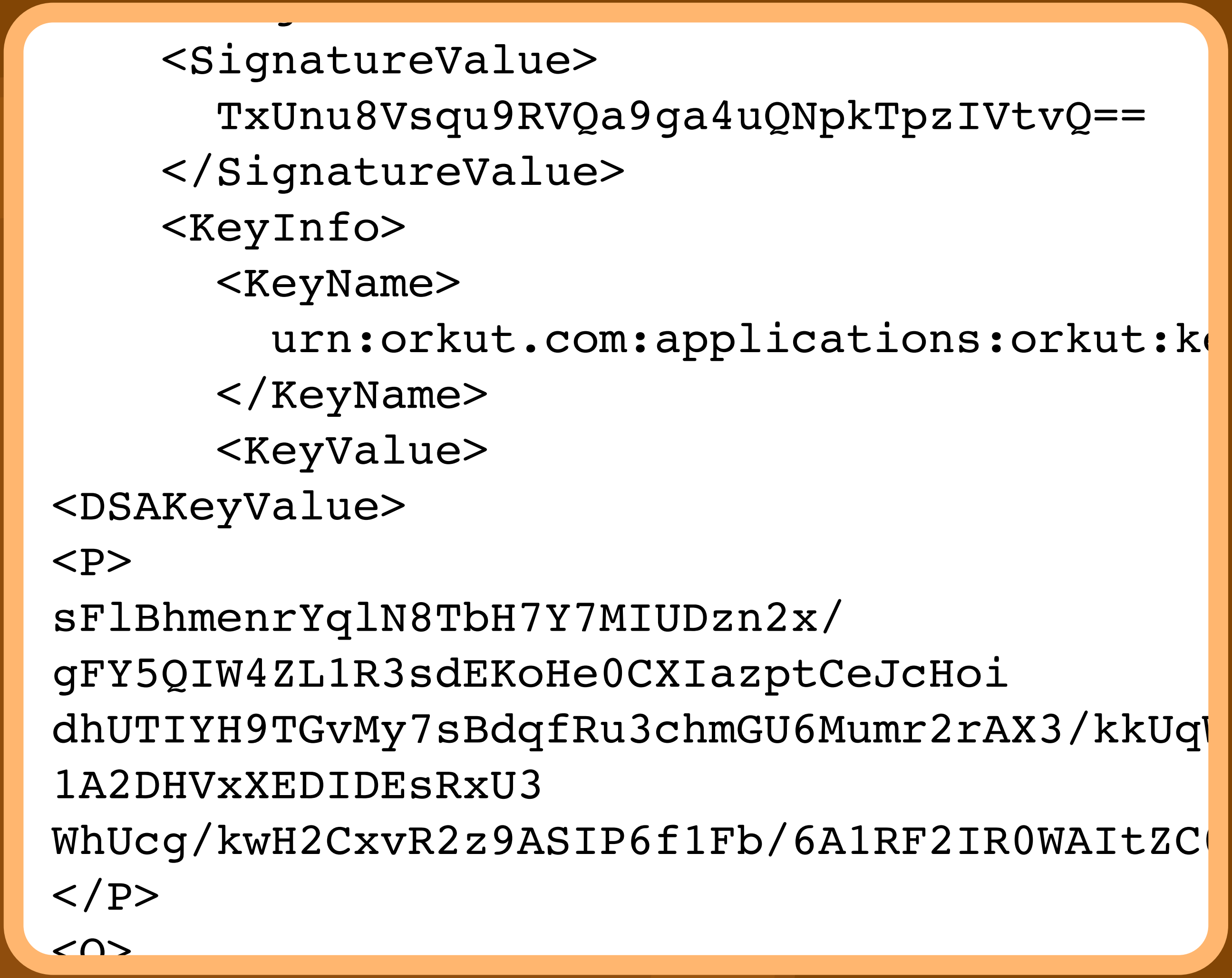
Example Manifest



```
</Policy>
<Signature xmlns="xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod
     Algorithm="REC-xml-c14n-20010315#Wi
    <SignatureMethod
     Algorithm="xmldsig#dsa-sha1"/>
    <Reference URI="">
      <Transforms>
        <Transform
         Algorithm="xmldsig#enveloped-si
      </Transforms>
      <DigestMethod
       Algorithm="xmldsig#sha1"/>
      <DigestValue>
        IxLYBus94geiZULGeEZnHk181k4=
      </DigestValue>
```

Example Manifest

Example Manifest



```
    <SignatureValue>
      TxUnu8Vsqu9RVQa9ga4uQNpkTpzIVtvQ==
    </SignatureValue>
    <KeyInfo>
      <KeyName>
        urn:orkut.com:applications:orkut:k
      </KeyName>
      <KeyValue>
<DSAKeyValue>
<P>
sFlBhmenrYqlN8TbH7Y7MIUDzn2x/
gFY5QIW4ZL1R3sdEKoHe0CXIazptCeJcHoi
dhUTIYH9TGvMy7sBdqfRu3chmGU6Mumr2rAX3/kkUq
1A2DHVxXEDIDEsRxU3
WhUcg/kwH2CxvR2z9ASIP6f1Fb/6A1RF2IR0WAItZC
</P>
<Q>
```

Managing Web Apps

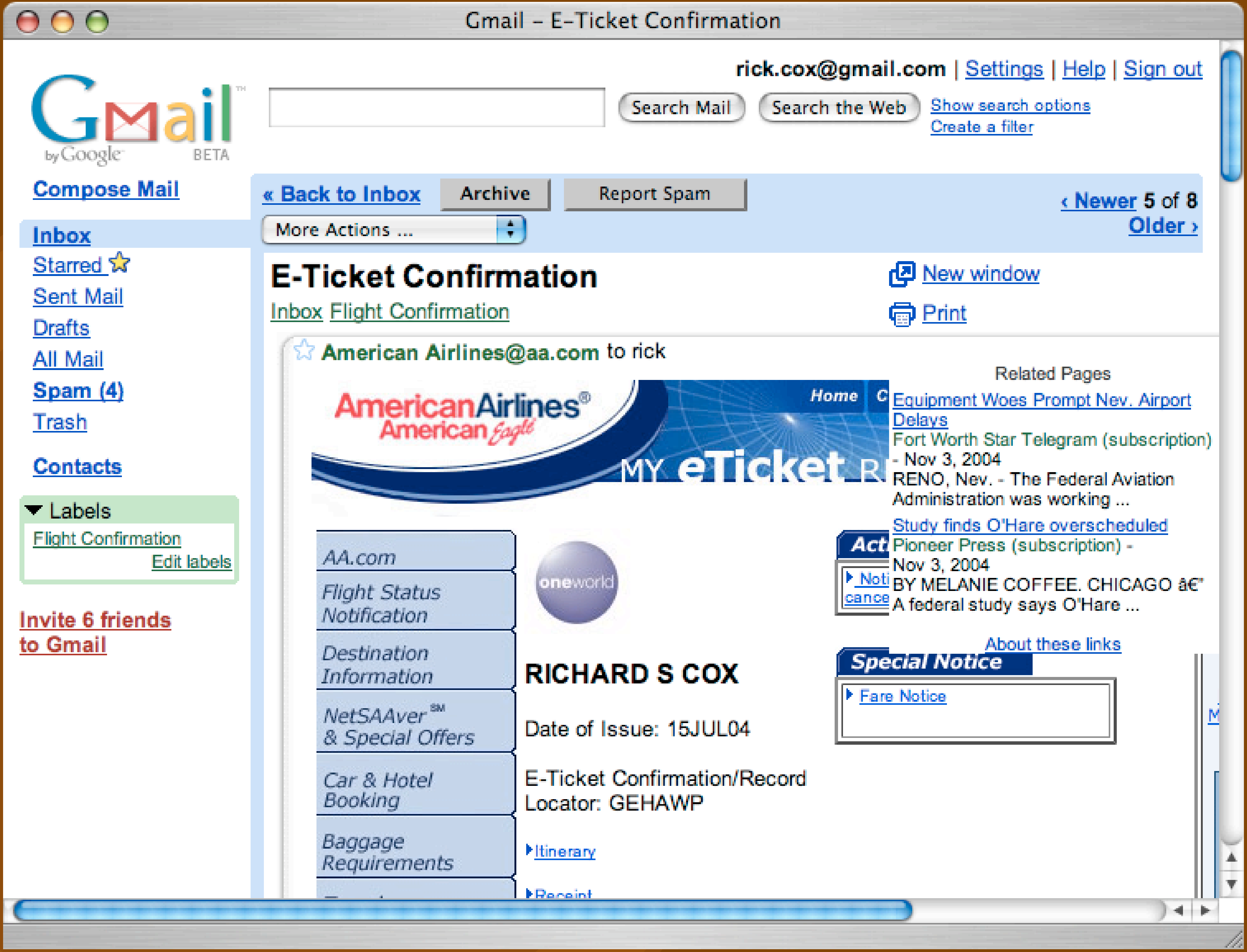
- Install: Download manifest, verify identity
- Run: Create new environment, load first piece of content
- Quit: Reclaim all memory of running app
- Uninstall: Delete manifest, cookies, etc.

Potential Fixes

- Bugs that would still be:
- Code Injection: 0/14
  - Buffer overflows: 0/10
- Sharing Policy/Mechanism: 3/36
- User Interface: 2/3
- Other: 2/2

Delivery Independent

- Manifests can authenticate content not delivered over HTTP(S)
  - Emails
  - By hash, signature, or other
- Can grant that content same access as rest of app



E-Ticket Confirmation

Inbox Flight Confirmation

American Airlines@aa.com to rick

RICHARD S COX

Date of Issue: 15JUL04

E-Ticket Confirmation/Record Locator: GEHAWP

Itinerary

Receipt

Related Pages

Equipment Woes Prompt Nev. Airport Delays
Fort Worth Star Telegram (subscription) - Nov 3, 2004
RENO, Nev. - The Federal Aviation Administration was working ...

Study finds O'Hare overscheduled
Pioneer Press (subscription) - Nov 3, 2004
BY MELANIE COFFEE. CHICAGO â€" A federal study says O'Hare ...

About these links

Conduit Apps

- Use our delivery independence
- Gmail delivers
  - Email
  - Manifest
- Manifest either included in email or new, temporary manifest

Conclusions

- Browsers do not implement the world users expect
- Isolation of web applications, not particular content-types, is the solution