A Unified Security Model for Web Applications

Richard S. Cox, Steven D. Gribble, Henry M. Levy
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](http://) 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](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](http://) directly. Also, our [HELP](http://) section can guide you through downloading and using Netscape Navigator with AOL.

- Our site is best viewed with [NETSCAPE](http://) Navigator versions 1.1 and above for the Macintosh, or 2.0 and above for Windows. Other browsers may not display all elements properly.
40 pieces of JavaScript
4 from external sites
1 VisualBasic script
1 Flash object
11 images from external sites
3 forms
Vulnerabilities

- Cross-domain access
- Buffer overruns
- Spoofs/Phishing attacks
What is a Web App?

- Collection of
  - Servers speaking HTTP(S)
  - HTML, image, movie, sound documents
  - JavaScript, Flash, Java, ActiveX client-side code
- Cooperating to implement a single service
App Manifests

Problem: What goes in each box?

Web applications defined by a manifest file

One manifest file 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
Conclusions

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