A Unified Security Model for Web Applications

Richard S. Cox, Steven D. Gribble, Henry M. Levy
DEMOCRATS PICK ASSEMBLY'S FIRST LATINO SPEAKER

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 Navigator version 1.1 and above, or the Microsoft Internet Explorer version 2.0 and above.
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

Shawn Baldwin for New York Times

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

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

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

<?xml version="1.0"?>
<tahoma-application>
  <name>urn:orkut.com:applications:orkut</name>
  <start-url>http://www.orkut.com/</start-url>
  <browser-configuration/>
  <Policy ...>
    ...
    <Rule RuleId="connect:443:0" Effect="Permit">
      <Target>
        ...
      </Target>
      <Actions>
        <Action>
          <ActionMatch
            MatchId="function:string-equal">
            <ActionAttributeDesignator
              DataType="string"
              AttributeId="action:action-id"/>
            <AttributeValue
              DataType="string">CONNECT</AttributeValue>
          </ActionMatch>
        </Action>
      </Actions>
      <Condition FunctionId="function:and">
        <Apply FunctionId="function:regexp-string-match">
          <AttributeValue
            DataType="string">.orkut.com$</AttributeValue>
        </Apply>
        <Apply FunctionId="urn:iced-mocha.org:tahoma:xacml:function:uri-part-host">
          <Apply FunctionId="function:anyURI-one-and-only">
            <ResourceAttributeDesignator
              DataType="anyURI"
              AttributeId="resource:resource-id"/>
          </Apply>
        </Apply>
        <Apply FunctionId="function:integer-equal">
          <AttributeValue
            DataType="integer">443</AttributeValue>
        </Apply>
        <Apply FunctionId="urn:iced-mocha.org:tahoma:xacml:function:uri-part-port">
          <Apply FunctionId="function:anyURI-one-and-only">
            <ResourceAttributeDesignator
              DataType="anyURI"
              AttributeId="resource:resource-id"/>
          </Apply>
        </Apply>
      </Condition>
    </Rule>
    <Rule RuleId="urn:orkut.com:applications:orkut:rule:http:any:0" Effect="Permit">
      <Condition FunctionId="function:and">
        <Apply FunctionId="function:regexp-string-match">
          <AttributeValue
            DataType="string">.orkut.com$</AttributeValue>
        </Apply>
        <Apply FunctionId="urn:iced-mocha.org:tahoma:xacml:function:uri-part-host">
          <Apply FunctionId="function:anyURI-one-and-only">
            <ResourceAttributeDesignator
              DataType="anyURI"
              AttributeId="resource:resource-id"/>
          </Apply>
        </Apply>
        <Apply FunctionId="function:integer-equal">
          <AttributeValue
            DataType="integer">80</AttributeValue>
        </Apply>
        <Apply FunctionId="urn:iced-mocha.org:tahoma:xacml:function:uri-part-port">
          <Apply FunctionId="function:anyURI-one-and-only">
            <ResourceAttributeDesignator
              DataType="anyURI"
              AttributeId="resource:resource-id"/>
          </Apply>
        </Apply>
      </Condition>
    </Rule>
    <Rule RuleId="rule:denyother" Effect="Deny"/>
  </Policy>
  <Signature xmlns="xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod
        Algorithm="REC-xml-c14n-20010315#WithComments"/>
      <SignatureMethod
        Algorithm="xmldsig#dsa-sha1"/>
      <Reference URI="">
        <Transforms>
          <Transform
            Algorithm="xmldsig#enveloped-signature"/>
        </Transforms>
        <DigestMethod
          Algorithm="xmldsig#sha1"/>
        <DigestValue>IxLYBus94geiZULGeEZnHk181k4=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>TxUnu8Vsqu9RVQa9ga4uQNpkTpzIVtvQ==</SignatureValue>
    <KeyInfo>
      <KeyName>
        urn:orkut.com:applications:orkut:key
      </KeyName>
      <KeyValue>
        <DSAKeyValue>
          <P>
            sFlBhmenrYqlN8TbH7Y7MIUDzn2x/gFY5QIW4ZL1R3sdEKoHe0CXIazptCeJcHoi
dhUTIYH9TGvMy7sBdqfRu3chmGU6Mumr2rAX3/kkUqWH2/1A2DHVxXEDIDEsRxU3
WhUcg/kwH2CxvR2z9ASIP6f1Fb/6A1RF2IR0WAItZC0=
          </P>
          <Q>
            nATcF2fjt2xcLy/cZNE3+b1ZUYE=
          </Q>
          <G>
            c7LWmqYis3lQMAbaY8E289/lTiDKF0NsYmvqg7Oe6e99HAijrmuU4/
Wenm1i6xMM
Z3UOJXLqMvG49sWRDC82QAtU3hvKnRrYpB0TLkfJPZWrBaSk+a6LJWkUmQhMIWN8
iBQdYmrhWzCIz/sltUcjeTFXm3vdRKnPkN8qjPhq1+4=
          </G>
          <Y>
            inkWJ5Xtkt9srIEneWVWShnRUico96U5INxkEx6x4H/qXQ9Hvf4tnnEfk0PXEgkO
X5SZ2XB5yDcEkHtupMJhSz5S0HobIF0u9FA4X/PKiGCJCLl8pi8KjTkiN+TWr6u0
HhT3n7uDIaga7KvBjIKVogTGiMYosX/06/PjvsyntMA=
          </Y>
        </DSAKeyValue>
      </KeyValue>
    </KeyInfo>
  </Signature>
</tahoma-application>
Example Manifest

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

<s:Signature xmlns="xmldsig#">
  <s:SignedInfo>
    <s:CanonicalizationMethod Algorithm="REC-xml-c14n-20010315#WithComments"/>
    <s:SignatureMethod Algorithm="xmldsig#dsa-sha1"/>
    <s:Reference URI="">
      <s:Transforms>
        <s:Transform Algorithm="xmldsig#enveloped-signature"/>
      </s:Transforms>
      <s:DigestMethod Algorithm="xmldsig#sha1"/>
      <s:DigestValue>
        IxLYBus94geiZULGeEZnHk181k4=
      </s:DigestValue>
    </s:Reference>
  </s:SignedInfo>
  <s:SignatureValue>
    TxUnu8Vsqu9RVQa9ga4uQNpkTpzIVtvQ==
  </s:SignatureValue>
  <s:KeyInfo>
    <s:KeyName>
      urn:orkut.com:applications:orkut:ke
    </s:KeyName>
    <s:KeyValue>
      <s:DSAKeyValue>
        <s:P>
          sFlBhmenrYqlN8TbH7Y7MIUDzn2x/
          gFY5QIW4ZL1r3sdEKOHe0CXIazptCeJcHoi
dhUTiyh9TGVMy7sBdqfRu3chmGU6Mumr2rAX3/kkUq
1A2DHVxXEDIDEsRxB3
WhUcg/kwH2CxVR2z9ASIP6f1Fb/6A1RF2IR0WAItZC
</s:P>
        </s:DSAKeyValue>
      </s:KeyValue>
    </s:KeyInfo>
  </s:Signature>
</s:Signature>

(Tahoma Application)

(name) = urn:orkut.com:applications:orkut
(start-url) = http://www.orkut.com/
(browser-configuration) =

Policy

(Rule RuleId="connect:443:0" Effect="Permit")
  <Target>
  
  </Target>
  <Condition FunctionId="function:and">
    <Apply FunctionId="function:regexp-string-match">
      <AttributeValue DataType="string">
        .orkut.com$
      </AttributeValue>
      <Apply FunctionId="urn:iced-mocha.org:tahoma:xacml:function:uri-part-host">
        <Apply FunctionId="function:anyURI-one-and-only">
          <ResourceAttributeDesignator DataType="anyURI" AttributeId="resource:resource-id"/>
        </Apply>
      </Apply>
      <Apply FunctionId="function:integer-equal">
        <AttributeValue DataType="integer">
          443
        </AttributeValue>
        <Apply FunctionId="urn:iced-mocha.org:tahoma:xacml:function:uri-part-port">
          <Apply FunctionId="function:anyURI-one-and-only">
            <ResourceAttributeDesignator DataType="anyURI" AttributeId="resource:resource-id"/>
          </Apply>
        </Apply>
      </Apply>
    </Apply>
    <Apply FunctionId="function:and">
      <Apply FunctionId="function:regexp-string-match">
        <AttributeValue DataType="string">
          .orkut.com$
        </AttributeValue>
        <Apply FunctionId="urn:iced-mocha.org:tahoma:xacml:function:uri-part-host">
          <Apply FunctionId="function:anyURI-one-and-only">
            <ResourceAttributeDesignator DataType="anyURI" AttributeId="resource:resource-id"/>
          </Apply>
        </Apply>
      </Apply>
      <Apply FunctionId="function:integer-equal">
        <AttributeValue DataType="integer">
          80
        </AttributeValue>
        <Apply FunctionId="urn:iced-mocha.org:tahoma:xacml:function:uri-part-port">
          <Apply FunctionId="function:anyURI-one-and-only">
            <ResourceAttributeDesignator DataType="anyURI" AttributeId="resource:resource-id"/>
          </Apply>
        </Apply>
      </Apply>
    </Apply>
  </Condition>
  <Rule RuleId="urn:orkut.com:applications:orkut:rule:http:any:0" Effect="Permit">
    <Condition FunctionId="function:and">
      <Apply FunctionId="function:regexp-string-match">
        <AttributeValue DataType="string">
          .orkut.com$
        </AttributeValue>
        <Apply FunctionId="urn:iced-mocha.org:tahoma:xacml:function:uri-part-host">
          <Apply FunctionId="function:anyURI-one-and-only">
            <ResourceAttributeDesignator DataType="anyURI" AttributeId="resource:resource-id"/>
          </Apply>
        </Apply>
      </Apply>
      <Apply FunctionId="function:integer-equal">
        <AttributeValue DataType="integer">
          80
        </AttributeValue>
        <Apply FunctionId="urn:iced-mocha.org:tahoma:xacml:function:uri-part-port">
          <Apply FunctionId="function:anyURI-one-and-only">
            <ResourceAttributeDesignator DataType="anyURI" AttributeId="resource:resource-id"/>
          </Apply>
        </Apply>
      </Apply>
    </Condition>
  </Rule>
  <Rule RuleId="rule:denyother" Effect="Deny"/>
</Policy>
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
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

American Airlines

RICHARD S COX

Date of Issue: 15JUL04

E-Ticket Confirmation/Record Locator: GEHAWP

AA.com
Flight Status Notification
Destination Information
NetSAAver & Special Offers
Car & Hotel Booking
Baggage Requirements

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

About these links

Fare Notice
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