AdJail: Practical Enforcement of Confidentiality and Integrity Policies on Web Advertisements

Mike Ter Louw  Karthik T. Ganesh  V.N. Venkatakrishnan

Systems and Internet Security Lab

Department of Computer Science
UNIVERSITY OF ILLINOIS AT CHICAGO
COLLEGE OF ENGINEERING
Banner ad
Simple rectangular area

WIRED on iPad
Reimagined. Redesigned. Remarkable. !!!! DOWNLOAD NOW !!
Get the entire June issue, including 41 exclusive interactive extras—video, slideshows, music and more.

Digital security essentials

's not so private

to investigate the feature of many Web aren't all that private information can be the mode. The paper is it the USENIX security

UIC
UMore: Why Yahoo Just Killed Its AdSense Clone

Here’s a memo Yahoo just sent to publishers. In it, Yahoo suggests its customers might consider Chitika if they need an ad network.

Dear Publisher,

Yahoo! continuously evaluates and prioritizes our products and services, in alignment with business goals and our continued commitment to deliver the best consumer and advertiser experiences. After conducting an extensive review of the Yahoo! Publisher Network beta program, we have decided to close the program effective April 30, 2010. We expect to deliver

**See Also:**

Does Google Stand A Chance In China? No.
Inline text ad
Ad pops up on mouseover
Example of webmail application with ads
Will demonstrate goals using webmail example

Webmail application

1. Banner ("skyscraper") ad
2. Inline text ad
Example of webmail application with ads
Will demonstrate goals using webmail example

Webmail user interface

1. Banner ("skyscraper") ad
2. Inline text ad
Example of webmail application with ads
Will demonstrate goals using webmail example

Message list and headers

1. Banner ("skyscraper") ad
2. Inline text ad
Example of webmail application with ads
Will demonstrate goals using webmail example

Message body

1. Banner (“skyscraper”) ad
2. Inline text ad
Example of webmail application with ads
Will demonstrate goals using webmail example

Advertisements

1. Banner ("skyscraper") ad
2. Inline text ad
How basic banner ads work
1. Webmail site embeds ad network's script
How basic banner ads work

1. Webmail site embeds ad network's script
2. Ad script reads message for context
How basic banner ads work

1. Webmail site embeds ad network's script
2. Ad script reads message for context
3. Ad script writes ad content
Fake anti-virus attack on New York Times

Fake anti-virus attack on New York Times

Ad on Facebook.com misuses confidential data

Image from: http://www.culturesmithconsulting.com/2009/07/change-your-facebook-settings-or-else
Ad on Facebook.com misuses confidential data

Image from: http://www.culturesmithconsulting.com/2009/07/change-your-facebook-settings-or-else
Outline

Overview of goals

Approach

Evaluation

Conclusion
Goal 1: Enforce confidentiality and integrity policies on ad scripts (control rogue ads)
Goal 1: Enforce confidentiality and integrity policies on ad scripts (control rogue ads)

Allow reading message text for context
Goal 1: Enforce confidentiality and integrity policies on ad scripts (control rogue ads)

Webmail User Interface
- Message List
- Message Headers
- Message Body

Allow reading message text for context

Allow writing ad

Ad Script

Ad
Goal 1: Enforce confidentiality and integrity policies on ad scripts (control rogue ads)

Allow reading message text for context

Allow writing ad

Webmail User Interface
Message List
Message Headers
Message Body
Ad Script
Ad
Goal 1: Enforce confidentiality and integrity policies on ad scripts (control rogue ads)

Deny writing over trusted interface

Allow writing ad

Allow reading message text for context
Goal 1: Enforce confidentiality and integrity policies on ad scripts (control rogue ads)

Deny writing over trusted interface

- Webmail User Interface
- Message List
- Message Headers
- Message Body
- Ad Script
- Ad

Allow reading message text for context

Deny reading confidential data

Allow writing ad

X

X
Goal 2: Consistent user experience (don’t break ads)

- Many ads are interactive: respond dynamically to user events
Goal 3: Allow advertiser’s contextual targeting scripts (support expected ad behavior)

Image from: http://www.oddee.com/item_87332.aspx
Goal 4: Transparency in ad billing (mechanism transparent to ad network)

- Ads consist of external resource files, such as:
  - Images, iframes, Flash objects, scripts, etc.

- Ads are billed based on:
  1. Impressions – how many times an ad is shown to a user
  2. Clicks – how many times an ad is clicked by a user

- Click and impression rates are based on number of requests for resource files detected by server

- Thus, important to avoid altering clicks and impressions!
Goal 5: Work on current versions of mainstream web browsers (security effective now)

- Ads rely on high visibility to achieve success
- Therefore, it’s important to support all mainstream browsers:
  1. Firefox
  2. Google Chrome
  3. Internet Explorer
  4. Opera
  5. Safari
- Creating new browser features takes a long time to reach end users
Five major goals

1. Enforce confidentiality and integrity policies on ad scripts
   - Publisher should have control over rogue ads

2. Consistent user experience
   - Don’t break existing ads

3. Allow advertiser’s contextual targeting scripts
   - Permit benign / expected script operations

4. Transparency in ad billing
   - Security mechanism transparent to ad networks

5. Work on current versions of mainstream web browsers
   - Don’t require creating new web standards or browser features
Five major goals

1. Enforce confidentiality and integrity policies on ad scripts
   - Publisher should have control over rogue ads

2. Consistent user experience
   - Don’t break existing ads

3. Allow advertiser’s contextual targeting scripts
   - Permit benign / expected script operations

4. Transparency in ad billing
   - Security mechanism transparent to ad networks

5. Work on current versions of mainstream web browsers
   - Don’t require creating new web standards or browser features
Five major goals

1. Enforce confidentiality and integrity policies on ad scripts
   - Publisher should have control over rogue ads

2. Consistent user experience
   - Don’t break existing ads

3. Allow advertiser’s contextual targeting scripts
   - Permit benign / expected script operations

4. Transparency in ad billing
   - Security mechanism transparent to ad networks

5. Work on current versions of mainstream web browsers
   - Don’t require creating new web standards or browser features
Five major goals

1. Enforce confidentiality and integrity policies on ad scripts
   - Publisher should have control over rogue ads

2. Consistent user experience
   - Don’t break existing ads

3. Allow advertiser’s contextual targeting scripts
   - Permit benign / expected script operations

4. Transparency in ad billing
   - Security mechanism transparent to ad networks

5. Work on current versions of mainstream web browsers
   - Don’t require creating new web standards or browser features
Five major goals

1. Enforce confidentiality and integrity policies on ad scripts
   - Publisher should have control over rogue ads

2. Consistent user experience
   - Don’t break existing ads

3. Allow advertiser’s contextual targeting scripts
   - Permit benign / expected script operations

4. Transparency in ad billing
   - Security mechanism transparent to ad networks

5. Work on current versions of mainstream web browsers
   - Don’t require creating new web standards or browser features
Outline

Overview of goals

Approach
- Ad security enforcement
- Consistent user experience
- Contextual targeting support
- Ad billing transparency
- Existing browser support

Evaluation

Conclusion
Preventing ad script access to sensitive data

“Shadow” page created, contains no sensitive data

Offline Changes

Webmail User Interface
- Message List
- Message Headers
- Message Body
- Ad Script

Real page

No Sensitive Data!

Shadow page
Preventing ad script access to sensitive data
Use of different domains invokes browser same-origin policy

Offline Changes

Webmail User Interface
- Message List
- Message Headers
- Message Body

Ad Script

Real page

No Sensitive Data!

Shadow page
Preventing ad script access to sensitive data
Ad script moved to shadow page

Offline Changes

Real page

Webmail User Interface
Message List
Message Headers
Message Body
Ad Script

Shadow page

No Sensitive Data!
Ad Script
Move
Preventing ad script access to sensitive data
Ad script no longer on same page as sensitive data

Offline Changes

Real page

Webmail User Interface
Message List
Message Headers
Message Body

No Sensitive Data!

Ad Script

Shadow page
Preventing ad script access to sensitive data

Access blocked by browser SOP enforcement

Offline Changes

Real page

Webmail User Interface
Message List
Message Headers
Message Body

Shadow page

No Sensitive Data!

Ad Script
Preventing ad script access to sensitive data
Access blocked by browser SOP enforcement

Goal 1 Accomplished

Webmail User Interface
- Message List
- Message Headers
- Message Body

Real page
No Sensitive Data!
Ad Script

Shadow page
Rendering ad using shadow page

Offline Changes

Real page

Webmail User Interface
Message List
Message Headers
Message Body

Shadow page

No Sensitive Data!

Ad Script
Rendering ad using shadow page
AdJail scripts added to both pages
Rendering ad using shadow page
Real and shadow pages render in a browser

Rendering Process

Real page
Webmail User Interface
Message List
Message Headers
Message Body
AdJail Script B

Shadow page
No Sensitive Data!
AdJail Script A
Ad Script
Rendering ad using shadow page
Communication link established between AdJail scripts

Rendering Process

Real page
Webmail User Interface
Message List
Message Headers
Message Body
AdJail Script B

Shadow page
No Sensitive Data!
AdJail Script A
Ad Script
Rendering ad using shadow page
AdJail scripts communicate via `postMessage()` API
Rendering ad using shadow page
Ad script writes ad content

Rendering Process

Real page

Webmail User Interface
Message List
Message Headers
Message Body
AdJail Script B

Shadow page
No Sensitive Data!
Ad
AdJail Script A
Ad Script
Rendering ad using shadow page
AdJail reads ad and sends to real page

Rendering Process

Webmail User Interface
- Message List
- Message Headers
- Message Body

AdJail Script B

Real page

No Sensitive Data!

AdJail Script A
Ad Script

Shadow page
Rendering ad using shadow page
AdJail creates mirrored ad on real page (subject to policy)
Rendering ad using shadow page
Only static content (defined in whitelist – no scripts!) is rendered

Rendering Process

Static content only!

Real page

Webmail User Interface
Message List
Message Headers
Message Body
AdJail Script B

Shadow page
No Sensitive Data!
Ad
Ad
Ad Script
AdJail Script A

Rendering Process
Outline

Overview of goals

Approach
- Ad security enforcement
- Consistent user experience
- Contextual targeting support
- Ad billing transparency
- Existing browser support

Evaluation

Conclusion
Preserve interactive user experience
Event listeners registered on real page ad

Event Forwarding

Webmail User Interface
- Message List
- Message Headers
- Message Body
Ad
AdJail Script B
Real page

No Sensitive Data!
Ad
AdJail Script A
Ad Script
Shadow page
Preserve interactive user experience
When event is triggered, AdJail is notified

Event Forwarding

Webmail User Interface
Message List
Message Headers
Message Body
Ad
AdJail Script B
Real page

No Sensitive Data!
Ad
Ad
AdJail Script A
Ad Script
Shadow page
Preserve interactive user experience
AdJail sends event to shadow page, and dispatches event to shadow page ad

Event Forwarding

Webmail User Interface
- Message List
- Message Headers
- Message Body
- AdJail Script B

Real page

No Sensitive Data!

Shadow page
- AdJail Script A
- Ad Script
Preserve interactive user experience
Event listener triggered on shadow page

Event Forwarding

Real page
Shadow page

Webmail User Interface
Message List
Message Headers
Message Body
Ad
AdJail Script B

No Sensitive Data!
Ad
AdJail Script A
Ad Script
Preserve interactive user experience
Event listener triggered on shadow page

Goal 2 Accomplished

Webmail User Interface
- Message List
- Message Headers
- Message Body
- Ad
- AdJail Script B

Real page

No Sensitive Data!
- Ad
- AdJail Script A
- Ad Script

Shadow page
Outline

Overview of goals

Approach
- Ad security enforcement
- Consistent user experience
- Contextual targeting support
- Ad billing transparency
- Existing browser support

Evaluation

Conclusion
Support for contextual targeting
Shadow page lacks contextual data for targeted ads

Rendering Process

Real page

Webmail User Interface
Message List
Message Headers
Message Body
AdJail Script B

Shadow page

No Sensitive Data!
AdJail Script A
Ad Script
Support for contextual targeting
AdJail extracts readable data

Rendering Process

Webmail User Interface
- Message List
- Message Headers
- Message Body

AdJail Script B

Real page

No Sensitive Data!

AdJail Script A

Ad Script

Shadow page
Support for contextual targeting
Readable data is sent to shadow page via postMessage() and reconstructed
Support for contextual targeting
Shadow page now has context for targeted ads

Rendering Process

Real page
- Webmail User Interface
  - Message List
  - Message Headers
  - Message Body
  - AdJail Script B

Shadow page
- No Sensitive Data!
  - Message Body
  - AdJail Script A
  - Ad Script
Support for contextual targeting
Ad script reads copy of message text to select relevant ad

Rendering Process

Real page
Webmail User Interface
Message List
Message Headers
Message Body
AdJail Script B

Shadow page
No Sensitive Data!
Message Body
AdJail Script A
Ad Script
Support for contextual targeting
Ad script creates relevant ad

Rendering Process

Real page
Webmail User Interface
Message List
Message Headers
Message Body
AdJail Script B

Shadow page
No Sensitive Data!
Message Body
AdJail Script A
Ad Script
Ad

UIC
Support for contextual targeting
Ad script creates relevant ad

Goal 3 Accomplished

Real page

Shadow page

Webmail User Interface
Message List
Message Headers
Message Body
AdJail Script B
No Sensitive Data!
Message Body
AdJail Script A
Ad Script
Ad
Overview of goals

Approach
- Ad security enforcement
- Consistent user experience
- Contextual targeting support
- Ad billing transparency
- Existing browser support

Evaluation

Conclusion
Two copies of ad created:

1. One on real page
2. One on shadow page

Must ensure external resource files are only fetched once by browser

- Can’t rely on cache — it can be disabled, blocked, etc.

Use Document Object Model interposition to prevent images, etc. from loading on shadow page

1. Prevent setting src (and similar) attributes
Conserving impression counts

Original Page

Real Page

Shadow Page

Ad script (<script>)

Image (<img>)

Iframe (<iframe>)

Ad script (<script>)

Image (<img>)

Iframe (<iframe>)
Conserving impression counts

Goal 4 Accomplished

Original Page

Real Page + Shadow Page

Ad script (<script>)
Image (<img>)
Iframe (<iframe>)
Ad script (<script>)
Image (<img>)
Iframe (<iframe>)

UIC
Overview of goals

Approach
- Ad security enforcement
- Consistent user experience
- Contextual targeting support
- Ad billing transparency
- Existing browser support

Evaluation

Conclusion
Browser compatibility challenges

Goal 5

- DOM API interposition was biggest challenge
- Needed to support content mirroring, event forwarding, and conserving impressions
- DOM Mutation events insufficient and not universally supported
- Synthesized mutation events using:
  1. Augment DOM prototype objects
  2. DOM object wrappers

Goal 5 Accomplished
Browser compatibility challenges

Goal 5

- DOM API interposition was biggest challenge
- Needed to support content mirroring, event forwarding, and conserving impressions
- DOM Mutation events insufficient and not universally supported
- Synthesized mutation events using:
  1. Augment DOM prototype objects
  2. DOM object wrappers
- Goal 5 Accomplished
Outline

Overview of goals

Approach

Evaluation
  Security
  Compatibility
  Performance

Conclusion
Goals of evaluation

1. Test security claims
2. Assess compatibility with existing ads and ad networks
3. Measure performance latencies
Evaluating Ad Networks

Test 6 popular ad networks (each serve a variety of ads):

<table>
<thead>
<tr>
<th>Ad Network</th>
<th>Type of ad</th>
<th>U.S. Market Reach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yahoo! Network</td>
<td>banner</td>
<td>86.6%</td>
</tr>
<tr>
<td>Google AdSense</td>
<td>banner</td>
<td>85.3%</td>
</tr>
<tr>
<td>Microsoft Media</td>
<td>banner</td>
<td>72.4%</td>
</tr>
<tr>
<td>AdBrite</td>
<td>inline text</td>
<td>47.2%</td>
</tr>
<tr>
<td>Federated Media</td>
<td>inline text</td>
<td>\textit{unk.}</td>
</tr>
<tr>
<td>Clicksor</td>
<td>inline text</td>
<td>\textit{unk.}</td>
</tr>
</tbody>
</table>
Outline

Overview of goals

Approach

Evaluation
  Security
  Compatibility
  Performance

Conclusion
Security evaluation

- Integrated AdJail with Roundcube webmail application
- Mounted attacks to test confidentiality and integrity policy enforcement
- Evaluated policy implications for other known threats
  - Clickjacking
  - UI Spoofing
  - Oversized ad
Outline

Overview of goals

Approach

Evaluation
  Security
  Compatibility
  Performance

Conclusion
Compatibility and transparency evaluation

- Manually tested ads to verify correct functionality
- Determined most restrictive policy for each ad network
- Routed through proxy to verify clicks and impressions conserved
- Some minor compatibility issues can be found in the paper
Outline

Overview of goals

Approach

Evaluation
  Security
  Compatibility
  Performance

Conclusion
Ad display latency

(b) Ad display latency (ms)

Original
AdJail

AdBrite
Clicksor
Federated
Google
Microsoft
Yahoo!
Ad render time

(a) Ad render time (ms)

- AdBrite
- Clicksor
- Federated
- Google
- Microsoft
- Yahoo!

- Original
- AdJail
Outline

Overview of goals

Approach

Evaluation

Conclusion
Conclusion

- Developed enforcement mechanism supporting confidentiality and integrity policies over third-party ads
- Supports interactive ads
- Supports ad targeting algorithms
- Preserves number of ad impressions
- Uses only common browser features
Thanks for your attention!

Questions?
### Supported policies

<table>
<thead>
<tr>
<th>Permission</th>
<th>Values (defaults in red)</th>
</tr>
</thead>
<tbody>
<tr>
<td>read-access</td>
<td>none, subtree</td>
</tr>
<tr>
<td>write-access</td>
<td>none, append, subtree</td>
</tr>
<tr>
<td>enable-images</td>
<td>allow, deny</td>
</tr>
<tr>
<td>enable-iframe</td>
<td>allow, deny</td>
</tr>
<tr>
<td>enable-flash</td>
<td>allow, deny</td>
</tr>
</tbody>
</table>
| max-height, max-width | none, 0, n% (0 ≤ n ≤ 100),  
|                    | n cm, n em, n ex, n in, n mm,  
|                    | n pc, n pt, n px (n ≥ 0)    |
| overflow           | allow, deny               |
| link-target        | blank, top, any           |