Securing Web Content

Joakim Koskela, Nicholas Weaver,
Andrei Gurtov and Mark Allman
ReArch'09
Rome, December 1st 2009
How do we protect the user without dwarfing the web experience?

• Nature of the web has changed
• Simple hyperlinked documents -> complex collages
  – Mashups, cross-site delegation, Flash, JavaScript..
• Single producer -> collection of providers
• Security model outdated
Securing content

• Add accountability to individual content components
• Handled according to the preferences and experiences of the user
  – Opportunistic Personas
  – History with an actor, the *trackrecord*
Securing the page structure

• Sign the page with the site's key
  – Integrity (as in SSL)

• Sets the general attitude
  – Browser caches, pre-filled input fields
  – Detect phishing attempts
Content components

• Add signature to HTML content blocks
  – <div>s
  – Signature and key as attributes

• Different strategies
  – Sign tag contents as-is
  – Decorate the tag interiors
    • Fill child elements with data from a signed block
Decoration example

- `op_*` attributes identifies the div

```html
<div id="sdiv5" class="entry"
    op_data="header=Hi&message=Testing+123"
    op_signature="OyjONQTCAR6Mv/sBjRaF.."
    op_key="LS0tLS1CRUdJTiBQVUJMSUMgS0..">
    <div>Posted 11:43:51</div>
    <div id="sdiv5_header"></div>
    <div id="sdiv5_message"></div>
</div>
```
Decoration example

- `op_*` attributes identifies the div
- `<div>`'s id is prefixed to the id of child elements

```html
<div id="sdiv5" class="entry"
    op_data="header=Hi&message=Testing+123"
    op_signature="OyjONQTGAR6Mv/sBjRaF.."
    op_key="LS0tLS1CRUdJTiBQVUJMSUMgS0..">"/>
  <div>Posted 11:43:51</div>
  <div id="sdiv5_header"></div>
  <div id="sdiv5_message"></div>
</div>
```
Decoration example

- `op_*` attributes identifies the div
- `<div>`'s `id` is prefixed to the id of child elements
- `op_key` and `op_signature` contain author's key & signature

```html
div id="sdiv5" class="entry"
    op_data="header=Hi&message=Testing+123"
    op_signature="OyjONQTCAR6Mv/sBjRaF.."
    op_key="LS0tLS1CRUdJTiBQVUJMSUMgS0.."
posted 11:43:51
  <div id="sdiv5_header"></div>
  <div id="sdiv5_message"></div>
</div>
```
Decoration example

- `op_*` attributes identifies the div
- `<div>`'s id is prefixed to the id of child elements
- `op_key` and `op_signature` contain author's key & signature
- `op_data` is the signed key-value data

```html
<div id="sdiv5" class="entry"
     op_data="header=Hi&message=Testing+123"
     op_signature="OyjONQTCAR6Mv/sBjRaF.."
     op_key="LS0tLS1CRUdJTiBQVUJMSUMgS0..">
  <div>Posted 11:43:51</div>
  <div id="sdiv5_header"></div>
  <div id="sdiv5_message"></div>
</div>
```
Decoration example

- `op_*` attributes identifies the div
- `<div>`'s id is prefixed to the id of child elements
- `op_key` and `op_signature` contain author's key & signature
- `op_data` is the signed key-value data
- Data is inserted into child elements, matching value keys with element ids

```html
<div id="sdiv5" class="entry"
    op_data="header=Hi&message=Testing+123"
    op_signature="OyjONQTCAR6Mv/sBjRaF.."
    op_key="LS0tLS1CRUdJTiBQVUJMSUMgS0..">
    <div>Posted 11:43:51</div>
    <div id="sdiv5_header">Hi</div>
    <div id="sdiv5_message">Testing 123</div>
</div>
```
External content

- External content can be included by signature in tag attributes
  - `<img>  <link>  <video> etc.`
Partnerships

- **Partners** delivering dynamic content
  - Advertisers, CDNs, search bars
- A method for indicating partnerships
  - Trust is not transitive
  - An indication to expect *something*
- Include partner key in tag attributes
Trust and security policies

• Framework: the opportunistic personas
  – Track record, Peer review, Web-of-Trust, Trust Databases

• Knowledge of actors
  – What do we know about someone?
  – How do we know that?
  – How well?

• Policies
  – Accept, ignore, sanitize, sandbox
Prototype

- FireFox plugin, persona (key-) daemon and server library
- Experimented with a subset
  - Page signatures
  - `<div>` tag signatures and decoration
  - External content
  - Signing content submissions (POSTs)
- Server-side required only a user-space library
- Persona daemon provided the track record
  - Recorded keys from web, e-mail, P2P IM and VoIP
  - Provided statements about actors
    - “You trust this person, knowing him well (through browsing and e-mails)”
- Simple security policies
Conclusions

• The way the web is composed today provides plenty of opportunities for malicious activity

• Our model points out the content that sites will not vouch for
Thank you for your attention!

joakim.koskela@hiit.fi
http://www.hiit.fi/netwr
http://www.icsi.berkeley.edu
Four parts

• Securing the page structure
• Content components
• External content
• Partnerships
...010010100111101001001110010101001111...