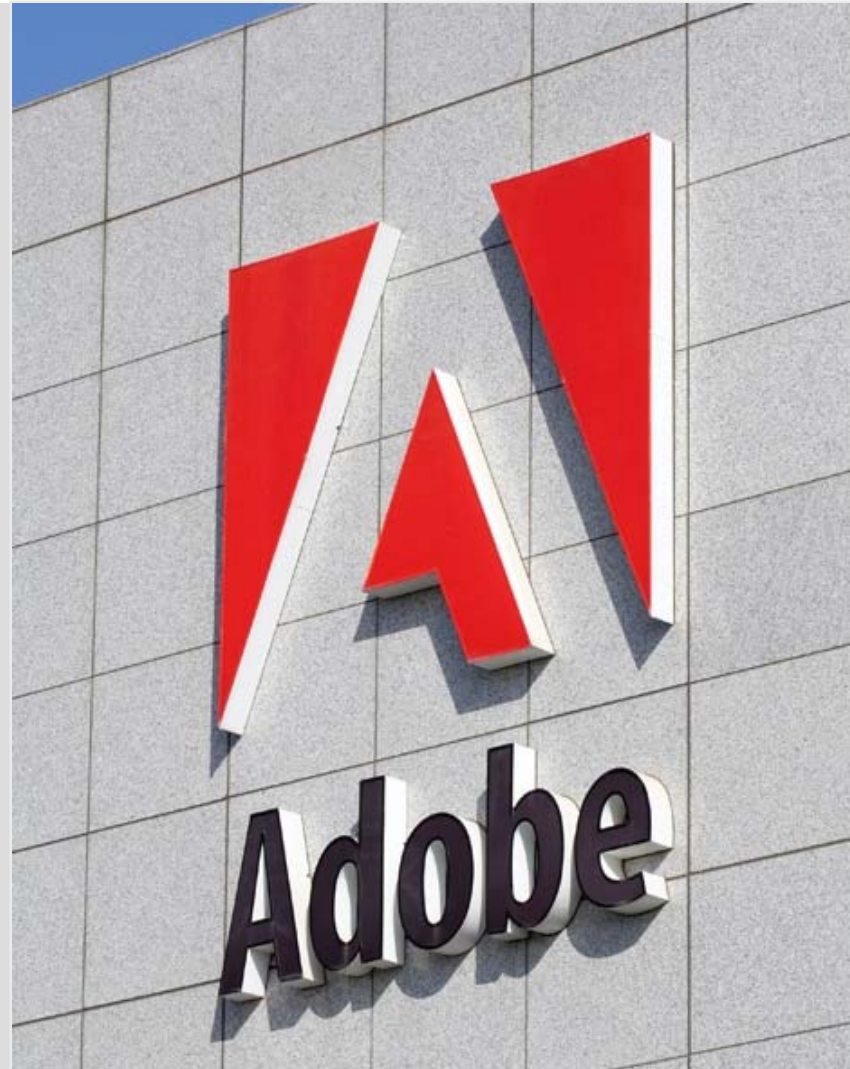


Flash Player Security *and Cross-domain Policy Files*

Trevor McCauley

Quality Engineer

Adobe Systems Inc.



Flash Player 9 April 2008 Security Update

(Flash Player 9,0,124,0)

Changes

- **javascript:** pseudo-protocol restricted in networking APIs
- **allowScriptAccess** defaults to “sameDomain” for all content
- **Custom headers** sent cross-domain require permission from a cross-domain policy file
- **Socket connections** require socket-based policy files to verify the connection

javascript:

- Now only works in getURL/navigateToURL

```
navigateToURL(new URLRequest("javascript: foo();"));
```

allowScriptAccess:

- Did default to “always” for content SWF7 and below
- SWF8 and above was changed to “sameDomain”
- Now all SWFs default to “sameDomain”

```
<param name="allowScriptAccess"  
value="sameDomain" />
```

Custom Headers:

- When sent cross-domain, requires cross-domain policy file to allow

```
<allow-http-request-headers-from  
    domain="example.com"  
    headers="Custom-Header"/>
```

Sockets:

- Require socket-based cross-domain policy files
 - Applies to all socket connections, even same-domain
 - HTTP cross-domain policy files no longer authenticate socket connections
 - A socket server may need to be updated to facilitate this

Resources

- *Understanding Flash Player 9 April 2008 Security Update compatibility*
http://www.adobe.com/devnet/flashplayer/articles/flash_player9_security_update.html

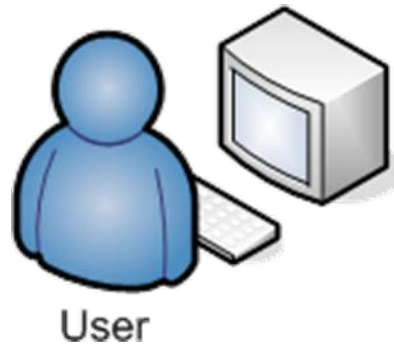
Cross-domain Policy Files

Cross-domain Policy Files:

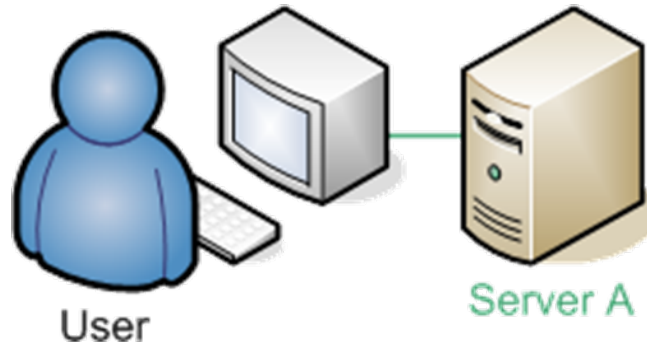
- Are XML
- Define policies for transferring data across domains
- Are used by Adobe Flash Player

```
<?xml version="1.0"?>
<cross-domain-policy>
  <allow-access-from domain="*.macromedia.com" />
  <allow-access-from domain="*.adobe.com" />
</cross-domain-policy>
```

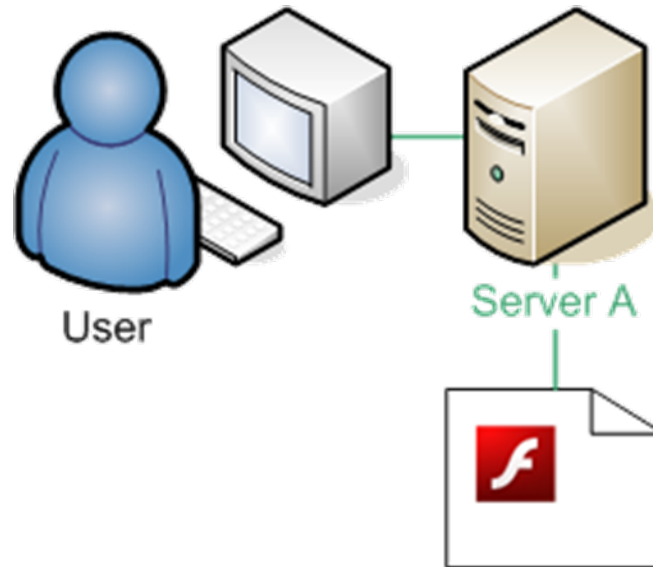
Process



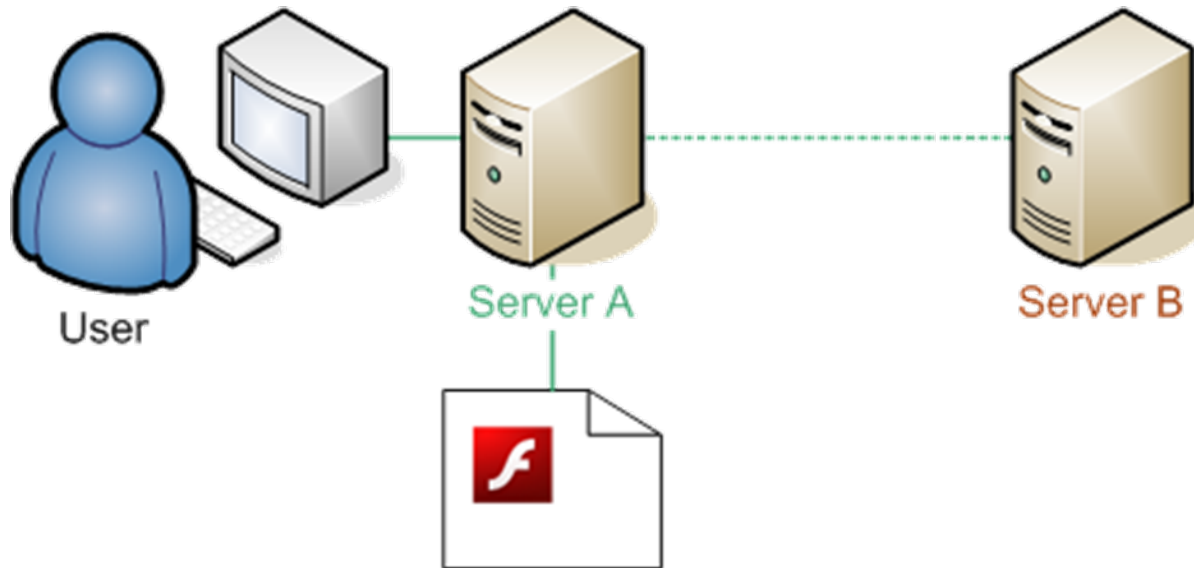
Process



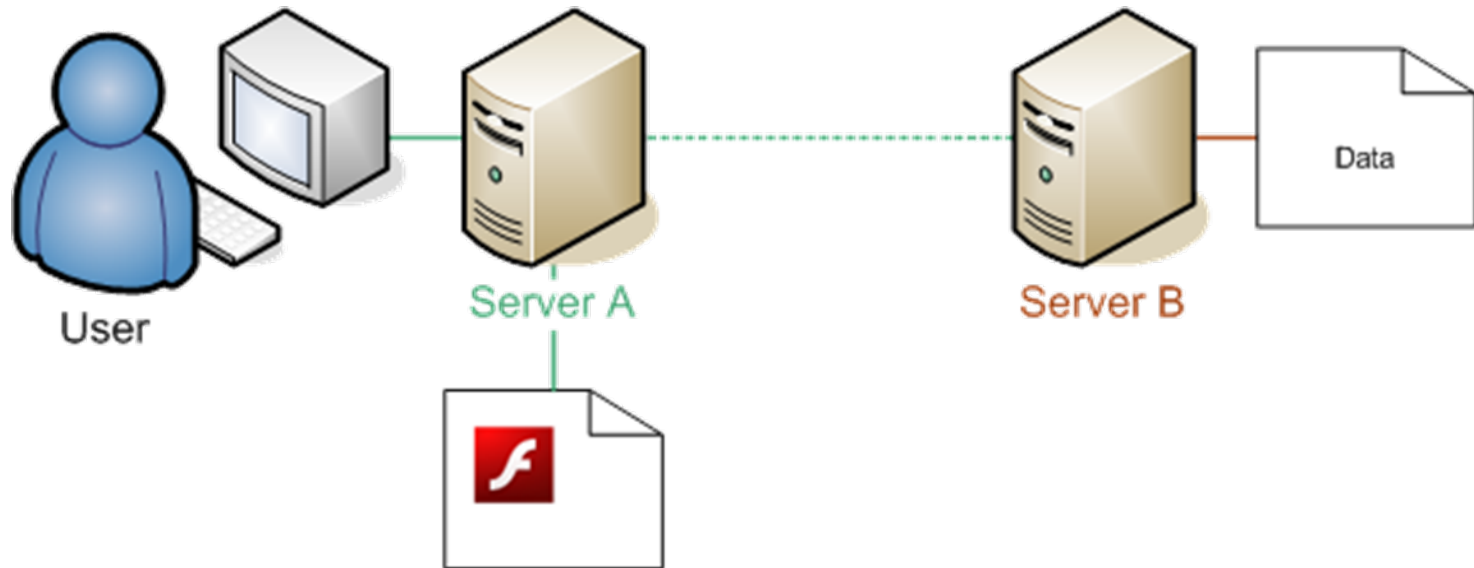
Process



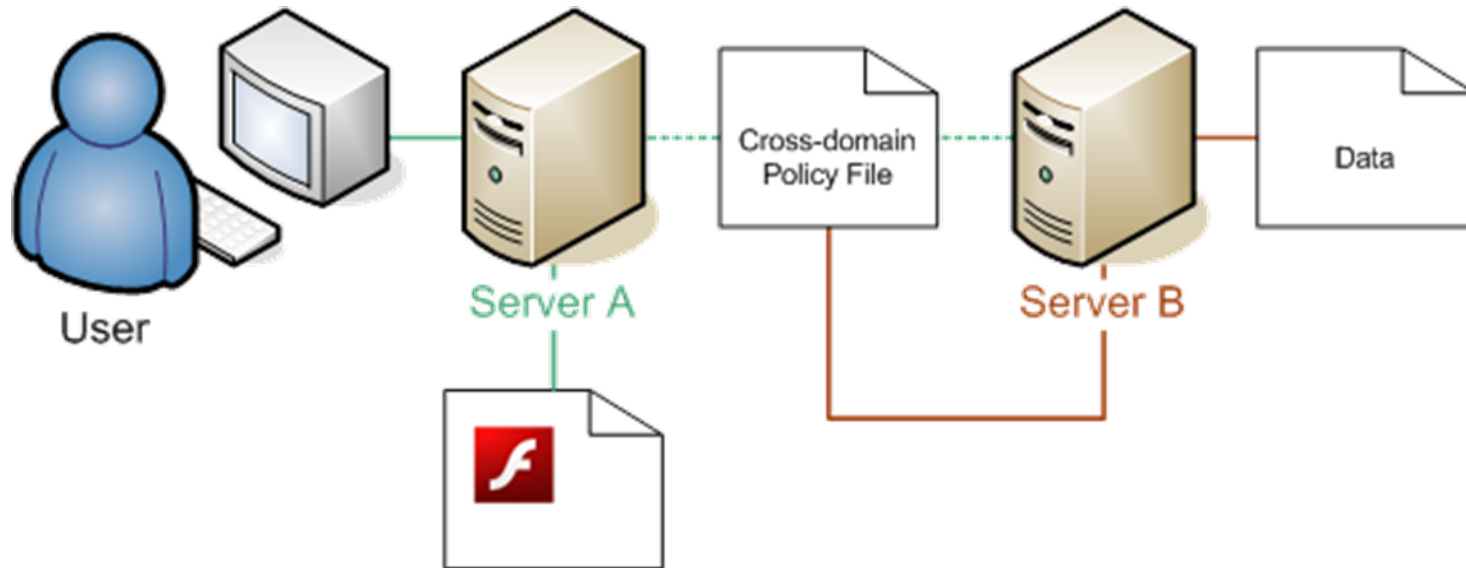
Process



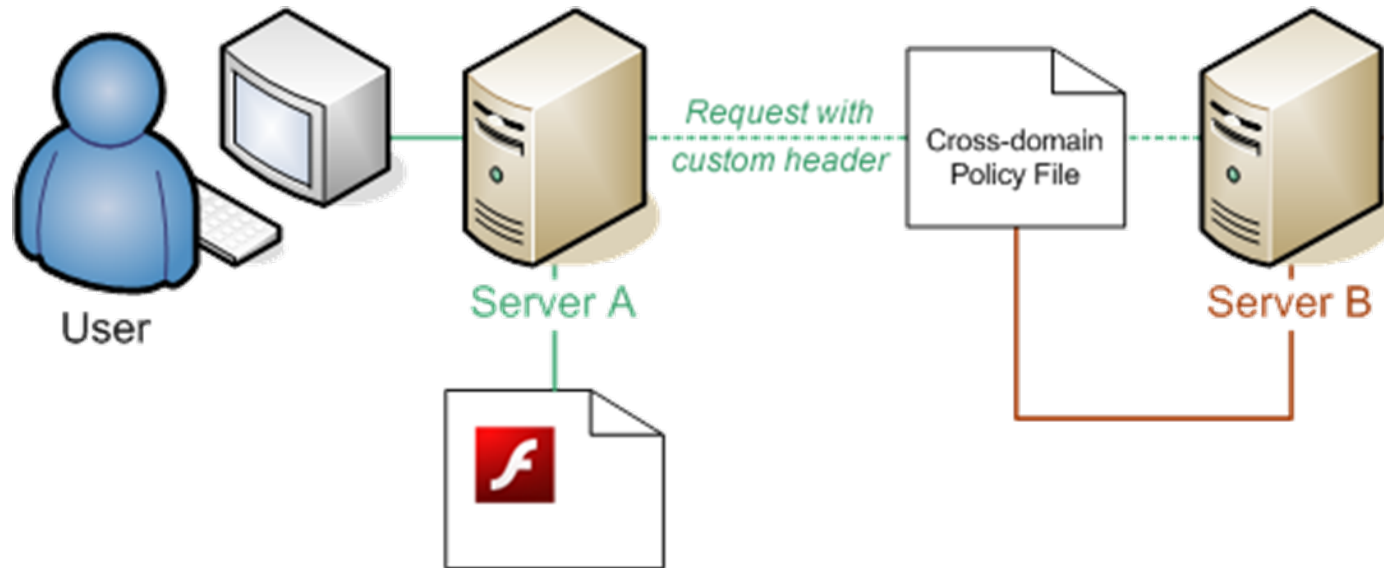
Process



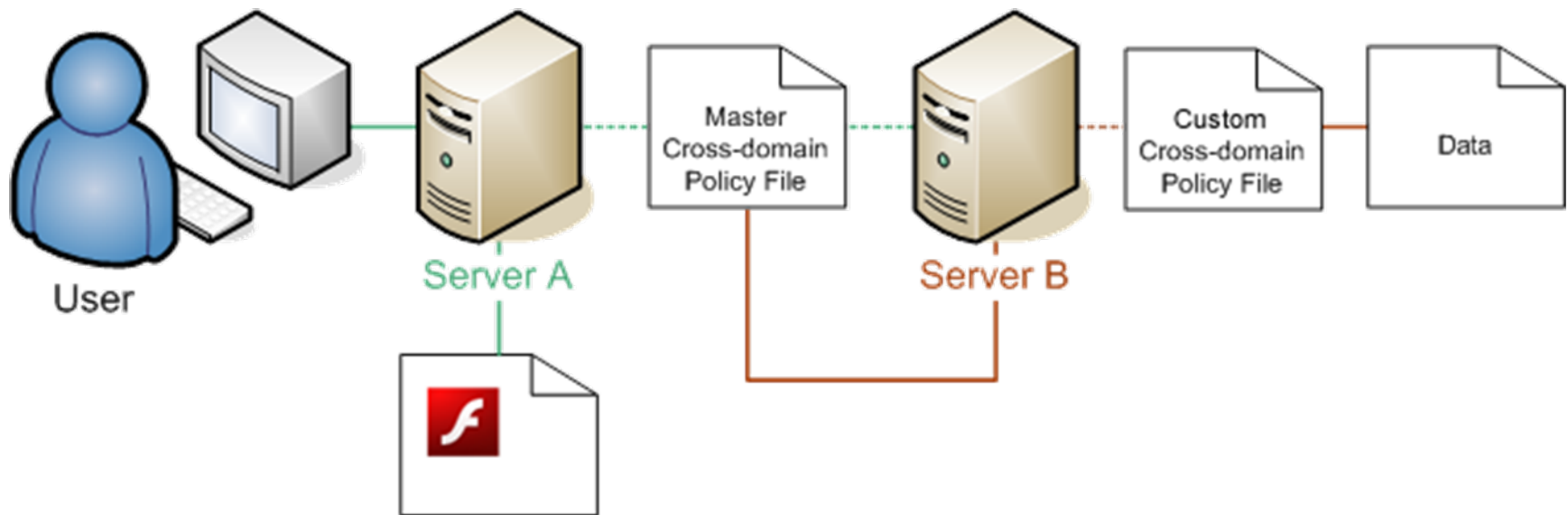
Process



Process



Process



Master Policy Files:

- Have the filename `crossdomain.xml`
- Are saved in the root of a domain e.g.
<http://www.example.com/crossdomain.xml>
- Can define meta-policies

Meta-policies:

- Are “policies for policy files”
 - Determine if a policy file is valid
- Can be defined:
 - In master policy files
`<site-control ... />`
 - Through the server header
`X-Permitted-Cross-Domain-Policies`
- Introduced in Flash Player 9,0,115,0

Policy files do NOT:

- Fully protect your online data
 - A client (Flash Player) must respect a cross-domain policy file
 - Other people/applications can easily access your data if it's public

Resources

- *Policy file changes in Flash Player 9*

http://www.adobe.com/devnet/flashplayer/articles/flashplayer9_security_03.html

- *Cross-domain Policy File Specification*

http://www.adobe.com/devnet/articles/crossdomain_policy_file_spec.html

Better by Adobe.™