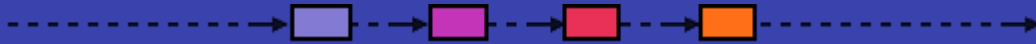# JCP.org update

January 2011

History

- Two years ago we decided to add collaborative software (bulletin boards, wikis, etc.) to our existing business logic.
- We chose the PHP-based *Bitweaver* open-source *Content Management System* as our platform.
  - This is widely used, and apparently feature-rich.
- We integrated Bitweaver into our existing site (single sign-on, linked aliases to bulletin-boards, etc.)
- We never really succeeded in unlocking all that it seemed to offer.
  - We were increasingly short of staff (Max Lanfranconi used to do a significant amount of technical work.)
  - Bitweaver proved less stable and solid than we had expected.

Requirements

- Even before the attack it was clear that we weren't able to provide all of these features reliably and flexibly.

- We've been thinking about outsourcing the collaborative features of the site.

- Spec-leads want (and our transparency initiatives require):
  - Flexible email aliases with browsable archives.
  - File-sharing and document management.
  - Issue tracking.
  - Public discussion mechanisms (forums and/or Wikis.)

The attack
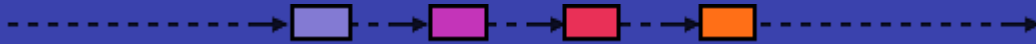
- In May 2010 a PHP-based "Web Shell" backdoor was installed on the jcp.org webserver system.
  - Permits shell command-line access to the system, file upload and download, etc.
- In December 2010, presumably via this backdoor, Bitweaver files were hacked to modify the footer that is displayed on Wiki (and other?) pages.
  - The hacked footer contains a pointer to a multi-level marketing site.
    - An attempt to boost their Google page-ranking?
- We have no evidence of further tampering, but it's possible that jcp.org logins and passwords have been compromised.

Our response

- The Web Shell has been removed.
- PHP (and therefore Bitweaver) execution has been disabled.
- EC passwords have been changed.
- The system will be re-installed (without PHP and Bitweaver) after this f2f meeting.
- Password encryption will be added.
- All users will be informed of the problem and required to reset their passwords.
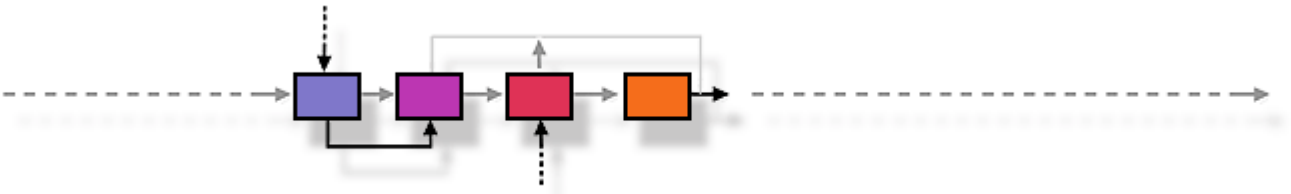
Next steps

- We are investigating alternative ways to provide collaborative features.
  - A *JCP Community* at java.net is an obvious choice.
    - java.net provides forums, wikis, issue tracking, file sharing, and other collaborative features.
  - Need to ensure that the transition to Project Kenai infrastructure will not destabilize the site.
  - Need to provide transition support for those using jcp.org.
- We are also doing our own mailing-list management, maintaing antivirus and anti-spam software, and some system administration (including backups.)
  - We want to get out of this business!
- Oracle IT and/or java.net should be able support us, freeing us to concentrate on core business logic.

Thank You!

http://jcp.org