SSL Transitioning

Grid and Web Services Working Group
May 2017
IVOA Interop Shanghai

Discussion Items

- US Government website transitioning from HTTP -> HTTPS
  - HEASARC
  - IPAC
- Aladin Lite experience with SSL support
- TOPCAT SAMP SSL support

HEASARC HTTPS Transition

Tom McGlynn

Background

- US Federal OMB mandate that all US government web site use HTTPS
- Implemented at HEASARC in March/April 2017.
- All HTTP addresses redirected to equivalent HTTPS address using Apache to return Permanently Moved (301).
- HTTPS was available as option on HEASARC previously
- New certificates used for all HEASARC and associated web sites

Changes needed

- Interactive use
  - Browsers generally followed redirection automatically so that interactive users did not see issues (usually!).
- External dynamic links
  - Published links to HEASARC services needed to be updated in services like VO registry. For some sites (e.g., *SkyView*) this could not be done early since HTTPS was enabled only a few weeks before it was mandatory.
- External static links
  - Links in external software which directly addressed our sites is beyond our ability to control. Can only publish information about the upcoming change and hope that service can handle redirects.
- Internal static links
  - These are hard to find since even when running in a test environment they may use absolute addresses that point to the operational environment and thus work until the operational environment is closed to HTTP. We found a number of internal static links where we used web services at the HEASARC that only came to light after we made the transition and things stopped working.
- Internal redirects
  - There are a fair number of places where internal redirects were used to point to HEASARC services (e.g., the HEASARC's published cone searches use an internal redirect). These often redirected to HTTP which where then redirected back to HTTPS. Even when this worked it was inefficient.

Problems seen

Two problems were seen with Java clients:

1. Java will not redirect http -> https automatically so that Java based clients generally would not follow the redirects and failed.
   - Possible to write Java code defensively to handle this but that does not seem to be the general practice
   - In absence of above, Java programs must use the HTTPS addresses, cannot rely on redirects.
2. Java requires that it be able to resolve the certificate authority. Since many new systems were being added to HTTPS the HEASARC decided to use a new and more flexible certificate authority but this was only recognized by recent versions of Java.
   - System was able to eventually use older certificates for main HEASARC site but not generally (e.g., SkyView)
   - Only Java versions released since late 2016 worked with new certificates.
3. Significant drop in HEASARC VO usage during transition. Still not recovered.

WGET also showed some incompatibility with new certificates but could be used with appropriate arguments. Scripts using WGET needed updating. No problems seen with CURL.

One major HEASARC interface (CFITSIO) has no support for HTTPS. Needed to redirect CFITSIO access to HEASARC archvve to use FTP (but this is not particularly VO related).

Understanding the various HTTP Redirect Status Codes

From RFC 7538

	Permanent	Temporary
Allows changing the request method from POST to GET	301	302
Does not allow changing the request method from POST to GET	308	307

From RFC 2616

"The 301 redirect is considered a best practice for upgrading users from HTTP to HTTPS"