SPMS Security Issues

JACoW Team Meeting 2011 – SINAP

Ivan Andrian <ivan.andrian@elettra.trieste.it>

Current security flaws

- SPMS is Oracle-based, installed in the Regional Support Centres
- The Upload/Download scripts are Perl-based, and run on a different server (the conference FileServer)
- The scripts do NOT have access to the DB for security reasons
  - Different institutes/teams/policies
  - Shared Oracle servers / conference server

URL spoofing

- By knowing the syntax of a Download URL it is possible to download whatever other Paper you want
- By building a well done HTML form, it is also possible to inject files onto the conference fileserver
  - Limited to the “papers” directory (O.S. is safe!)
  - All versions are kept and logs taken

Possible methods of security enhancement

- Connection to the DB (impossible for security reasons)
- Shared password (needs to be passed via HTTP – insecure)
- Web Server “source” (SPMS) control (Apache, IIS, …) – custom and non standard
- HTTP_REFERER – medium quality measure (browser based)
- Hashed passwords

HTTP_REFERER check

- When clicking on a URL on a web page (or posting a FORM) usually brings the “source” URL to the target
- The web browser controls this behaviour
  - Depends on the client’s browser
  - Custom-hacked browsers can modify this value
  - Spoofable, even if difficult for the average user
  - Proxies and firewalls can modify this value
- http://www.w3.org/Security/faq/wwwsf2.html

HTTP_REFERER tests

- Upload/Download Scripts modified during IPAC2011
- Now it is possible to configure a number of URLs as valid referrers in the configuration file
- A global password can override this behaviour (for direct downloads in batch – Volker's JPSP)
- Unfortunately... doesn't work!

IPAC2011 “production” tests

- SPMS @ CERN RSP
  - Oracle infrastructure (web/application server)
- File server @ ESS Bilbao
  - Ubuntu Linux 10.04 LTS

Debugging: CERN → ESS

```
JACoW file upload (Perl) - DEBUG

OPTIONS:
{
          'timeout' => 600,
          'debug' => 1,
          'referer_pwd_override' => 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX',
          'referer' => 0,
        }
REFERER ==

Server filesystem type: Unix.
Client platform detected: Linux

FILENAME PARTS (NAME,DIR,EXT):
   FRYCA01.txt
   ./

uploaded_file_info {
     'Content-Type' => 'text/plain',
     'Content-Disposition' => 'form-data; name="file_name"; filename="FRYCA01.txt"'
}
```

Debugging: Elettra → ESS

JACoW file upload (Perl) – DEBUG

```
OPTIONS:
{
          'timeout' => 600,
          'debug' => 1,
          'referer_pwd_override' => 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX',
          'referer' => 0,
        }
REFERER == http://localhost/~ivan/IPAC2011/file_upload.html

Server filesystem type: Unix.
Client platform detected: Linux

FILENAME PARTS (NAME,DIR,EXT):
FRYCA01.txt
./

uploaded_file_info {
     'Content-Type' => 'text/plain',
     'Content-Disposition' => 'form-data; name="file_name"; filename="FRYCA01.txt"'
}
```

Debugging: CERN → Elettra

JACoW file upload (Perl) – DEBUG

```
OPTIONS:
{
          'timeout' => 600,
          'debug' => 1,
          'referer_pwd_override' => 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX',
          'referer' => 0,
        }
REFERER ==

Server filesystem type: Unix.
Client platform detected: Linux

FILENAME PARTS (NAME,DIR,EXT):
FRYCA01.txt
./

uploaded_file_info {
     'Content-Type' => 'text/plain',
     'Content-Disposition' => 'form-data; name="file_name"; filename="FRYCA01.txt"'
}
```

Another solution

- Preshared key in SPMS & Scripts
- The SPMS could send (in clear) a HASH of the password **and** the paper code
- The Scripts could check the HASH against the known preshared key
- A different HASH for each paper ID – not usable for cross-paper ID spoofing

What’s needed for this method

- Agree on a hash algorithm (MD5? SHA1? …)
- Modify the SPMS code to pass this hash
    - easy (Matt)
- Modify the Scripts to use/check this hash
    - easy (Ivan)
- Use it!
    - easy (*)

Conclusions

- We can improve security
- Modifying the upload/download scripts isn't enough
- With small changes to SPMS and UDS we can strengthen the SPMS