ALS Project MinE

Searching for the genes that cause ALS (motor neurone disease)

https://www.projectmine.com/
**Project MinE**

- Collects DNA scans from 19 countries
- Each country has different Grid certificate procedure
  - Some countries don't (Australia)
  - Huge threshold
- Medical data transfers need encryption
  - dCache GridFTP does not support data channel encryption (yet)
  - `globus-url-copy -dcpriv` to dCache appears to encrypt data while in fact it doesn't!

https://github.com/globus/globus-toolkit/issues/121
Requirements for uploading data

- Simple authentication
  - No X509

- Easy client installation
  - No root CA certs, fetch-crl

- Encrypted data transfers
  - No dCache GridFTP
WebDAV

- Authentications
  - X509
  - Username/password
- Can use port 443, bypassing firewall misery
- Redirects (to HTTP)
  - On: load balancing, but unencrypted
  - Off: TLS data encryption
- webdav.grid.surfsara.nl DNS round robin
Clients

- web browsers (read only)
- wget (read only)
- curl
- Cyberduck
- Rclone (no x509 auth)
- FTS (third party file transfers)
- gfal* CLI and Python lib
- WebDAV Nav+ app for iPhone
- ... many more
<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Last Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>illumina_upload</td>
<td></td>
<td>Fri Dec 15 12:53:40 CET 2017</td>
</tr>
<tr>
<td>DiskOnly</td>
<td></td>
<td>Mon Oct 16 11:22:00 CEST 2017</td>
</tr>
<tr>
<td>TapeOnly</td>
<td></td>
<td>Fri Jun 23 12:01:25 CEST 2017</td>
</tr>
<tr>
<td>upload</td>
<td></td>
<td>Thu Mar 01 22:05:19 CET 2018</td>
</tr>
<tr>
<td>Tape</td>
<td></td>
<td>Mon Feb 27 15:24:35 CET 2017</td>
</tr>
<tr>
<td>Disk</td>
<td></td>
<td>Mon Feb 27 15:23:43 CET 2017</td>
</tr>
<tr>
<td>README.txt</td>
<td>1651</td>
<td>Mon Jan 15 15:01:33 CET 2018</td>
</tr>
</tbody>
</table>
It works!

- Installing rclone, configuring it, uploading test files: all in 7 minutes
- 6 TB uploaded from McGill university, Canada (cross Atlantic over public internet)

But wait...
Challenges

- Certificates & DNS round robin
- Certificate chain
- Cipher hardening
- Abandon 1 project -> 1 account mapping
- View locality
- View checksums
- Stage files through webdav?
Certificate & DNS round robin

- `webdav.grid.surfsara.nl` is DNS round robin to 64 hosts
  - Simple load balancing
  - Why?
    - dCache WebDAV redirects to **HTTP**, not **HTTPS**!
      - So we use non-redirecting doors.
      - No load balancing there.
- Host `guppy1.grid.surfsara.nl` != DNS name `webdav.grid.surfsara.nl`
- Each host cert has `webdav.grid.surfsara.nl` in subjectAltNames
  - DNS name always matches certificate
Certificate chain

- Installing CA root certs & fetch-crl difficult for users
- Our host certs chain:
  - DigiCert Assured ID Root CA
  - Terena eScience SSL CA 3
  - webdav.grid.surfsara.nl
- Terena is not in browsers & distros.
- But DigiCert is!
- We provide host cert + intermediate cert.
- All clients trust our webdav!
- How set up? See next slide...
Build certificate chain

```bash
echo "Composing chain file /etc/grid-security/chain.pem..."
cd /etc/grid-security
issuer_dn=$(openssl x509 -in hostcert.pem -noout -issuer | sed -e 's/issuer= //')
issuer_infofile=$(grep -l "subjectdn = .$issuer_dn" certificates/*.info)
issuer_pem=$(sed -e 's/\..info$/\..pem/' <<< "$issuer_infofile")
cat $issuer_pem hostcert.pem > chain.pem
```

dCache config

```bash
webdav.authn.hostcert.cert=/etc/grid-security/chain.pem
```
Cipher hardening

- java.security
- dcache.conf
- layout file
java.security

- Java version 8
- Disable 3DES (= DESede in Java)

[root@door1 ~]# grep -A 1 '^jdk.tls.disabledAlgorithms' /usr/lib/jvm/jre/lib/security/java.security
jdk.tls.disabledAlgorithms=SSLv3, DES, DESede, RC4, MD5withRSA, DH keySize < 768, EC keySize < 224
dcache.conf

dcache.authn.ciphers

- DISABLE_EC
  - Remove this to have Perfect Forward Secrecy, but test it first!
- DISABLE_RC4
  - RC4 unsafe, so you want this.
layout file

[webdav2880-$\{\text{host.name}\}$Domain]
[webdav2880-$\{\text{host.name}\}$Domain/webdav]
webdav.cell.name=webdav2880-$\{\text{host.name}\}$

# Disable redirects because they send client to HTTP, not HTTPS!
webdav.redirect.on-read=false
webdav.redirect.on-write=false

# Username/password auth

webdav.authn.basic=true
webdav.authn.protocol=https
webdav.net.port=2880

# Also interesting:
webdav.authn.accept-client-cert = true
Abandon 1 project -> 1 account mapping

- Most projects have FQAN to UID mapping: /vo/group/Role=*/Capability=*/ -> one single username
- WebDAV & username/password auth
  - each user must have his own username!
- Project MinE needed that anyway
  - Any user can be in a unique combination of multiple groups
  - Each group provides access to one country's data
    - Needed ACLs for permission inheritance
  - 18 countries -> 18 groups
    - NFS has a limit of 16 groups
Locality & checksums

With CURL, you can get both the locality and the checksum of a file through WebDAV.

Examples:
http://doc.grid.surfsara.nl/en/latest/Pages/Advanced/storage_clients/webdav.html#querying-file-properties

Thanks Paul!
Pre-staging with WebDAV

Theoretically possible with a dirty trick:
Use `curl --range` to read only 1 byte.

Alternatives:

- srm-bring-online, gfal
Security testing
Testing with nmap

onno$ ~/nmap/bin/nmap --script ssl-enum-ciphers -p 2880 -P0 webdav.grid.surfsara.nl
...

<table>
<thead>
<tr>
<th>PORT</th>
<th>STATE</th>
<th>SERVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2880/tcp</td>
<td>open</td>
<td>https</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ssl-enum-ciphers:</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLSv1.0:</td>
</tr>
<tr>
<td>ciphers:</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A</td>
</tr>
<tr>
<td>compressors:</td>
</tr>
<tr>
<td>NULL</td>
</tr>
<tr>
<td>cipher preference: server</td>
</tr>
<tr>
<td>TLSv1.1:</td>
</tr>
<tr>
<td>ciphers:</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A</td>
</tr>
</tbody>
</table>

....
Testing with Wireshark

- `yum install wireshark wireshark-gnome`
- If you don't use port 443, tell Wireshark it's an SSL connection (Analysis -> Decode as); you'll get full TLS analysis.
- In my rclone test, I found that `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA` was used. That's good: it provides Forward Secrecy. Still trying to improve it though.
- Search for "client hello" to see which ciphers the client supports.
Testing with Greenbone/OpenVAS

- http://www.openvas.org/
- Score 2.6 (Low), good
Testing with Qualys SSLtest

- Grade B
  - Because unable to enforce Forward Secrecy
    - Java 8 thingy
RCauth - proxies without certificates
Project MinE

- 19 countries, 19 procedures to get certificate
- Uploading/downloading => WebDAV
- Processing => ?
RCauth

• Provides a grid proxy based on username & password instead of grid certificate
• AARC (Authentication and Authorisation for Research and Collaboration) project
• https://rcauth.eu/
• Operated by Nikhef, our neighbours at Amsterdam Science Park & Tier 1 partners

So, how does it work?
22:57 mine-ui.grid.surfsara.nl:/home/onno
onno$ startGridSessionRCauth lsgrid:/lsgrid/Project_MinE
Starting firefox to bring you to portal https://rcdemo.nikhef.nl/projectmine/?role=. This may take a few seconds.

Please enter the authentication hash that you retrieved from https://rcdemo.nikhef.nl/projectmine/. 
ProjectMinE one-time-password certificate service

Request VOMS Role (optional):

start
Geef je gebruikersnaam en wachtwoord

Voor deze dienst is authenticatie vereist. Geef je gebruikersnaam en wachtwoord in onderstaand formulier.

Gebruikersnaam
onno

Wachtwoord

Inloggen
Toestemming voor het vrijgeven van persoonsgegevens

U gaat inloggen bij een dienst RCAuth.eu WAYF. Tijdens het loginproces stuurt de identity provider zgn. attributen met daarin informatie over uw identiteit voor deze dienst. Bent u het daarmee eens?

☑ Bewaar toestemming

[ja, ik ga akkoord] [Nee, ik weiger]

Informatie die naar RCAuth.eu WAYF zal worden gestuurd

urn:oid:2.5.4.3
Onno Zweers
RCauth.eu Online CA consent page

The Master Portal below is requesting access to your personal information and to act on your behalf.

If you approve, please accept, otherwise, cancel.

Details on which attributes are released, why, to whom, and how they are processed can be found in the RCauth Pilot ICA G1 CA privacy policy.
For further information on the CA see the RCauth.eu homepage.

☑️ Remember

[button] Yes, continue  [button] No, cancel
Dear onno_31029@surfsara.nl,

Please start startGridSessionRCauth on the mine-ui and enter the following hash:

6e5d337c6e1e922ebe3a1a740f55a556d39302cb4543985b044964775990e0b4

NOTE:

- This hash will expire in **10 minutes** (at 21:10:56 UTC)
- You can use this link only **once**

[return to client](#)
22:57 mine-ui.grid.surfsara.nl:/home/onno
onno$ startGridSessionRCauth lsgrid:/lsgrid/Project_MinE
Starting firefox to bring you to portal https://rcdemo.nikhef.nl/projectmine/?role=.
This may take a few seconds.
Please enter the authentication hash that you retrieved from https://rcdemo.nikhef.nl/projectmine/. 6e5d337c6e1e922ebe3a1a740f55a556d39302cb4543985b044964775990e0b4
22:57 mine-ui.grid.surfsara.nl:/home/onno
onno$ startGridSessionRCauth lsgrid:/lsgrid/Project_MinE
Starting firefox to bring you to portal https://rcdemo.nikhef.nl/projectmine/?role=.
This may take a few seconds.

Please enter the authentication hash that you retrieved from https://rcdemo.nikhef.nl/projectmine/. 6e5d337c6e1e922ebe3a1a740f55a556d39302cb4543985b044964775990e0b4

Two VOMS proxies have been created:
- One valid for 7 days, uploaded to the MyProxy server px.grid.sara.nl.
- One valid for 24 hours, downloaded to /tmp/x509up_u31029.
Your delegation ID is: onno

23:01 mine-ui.grid.surfsara.nl:/home/onno
onno$
onno@mine-ui:~ ssh -X -C onno@mine-ui.grid.surfsara.nl -- 106x29

23:01 mine-ui.grid.surfsara.nl:/home/onno
onno$ voms-proxy-info -all
subject : /DC=eu/DC=rcauth/DC=rcauth-clients/O=surfsara.nl/CN=Onno Zweers Cx9goNTnglkpBisF/CN=1807010170/CN=1218129715/CN=2607047521
issuer : /DC=eu/DC=rcauth/DC=rcauth-clients/O=surfsara.nl/CN=Onno Zweers Cx9goNTnglkpBisF/CN=1807010170/CN=1218129715
identity : /DC=eu/DC=rcauth/DC=rcauth-clients/O=surfsara.nl/CN=Onno Zweers Cx9goNTnglkpBisF
name : RFC3820 compliant impersonation proxy
strength : 1024
path : /tmp/x509up_u31029
timeleft : 23:58:34
key usage : Digital Signature, Key Encipherment, Data Encipherment

=== VOMS lsgrid extension information ===

VO lsgrid
subject : /DC=eu/DC=rcauth/DC=rcauth-clients/O=surfsara.nl/CN=Onno Zweers Cx9goNTnglkpBisF
issuer : /O=dutchgrid/O=hosts/OU=sara.nl/CN=voms.grid.sara.nl
attribute : /lsgrid/Project_MINe/Role=NO/Capability=NULL
attribute : /lsgrid/Role=NULL/Capability=NULL
timeleft : 163:58:33
uri : voms.grid.sara.nl:30018

23:02 mine-ui.grid.surfsara.nl:/home/onno
onno$ rpm -qa | grep -i rcauth
ca_RAuth-Pilot-ICA-G1-1.91-1.noarch

23:07 mine-ui.grid.surfsara.nl:/home/onno
onno$
More info:
Mischa Salle, msalle@nikhef.nl
David Groep, davidg@nikhef.nl
Questions?