Security Activities and Plans

Scope of the Security Activities

- Security software and services *development, maintenance and support*
- Vulnerability and Risk Assessment (“RAT”)
- Incident handling

Security Software Components

- Access control to services
  - ‘AuthZ callout’ to attribute-based (‘VOMS’) access
  - extend coverage to all Globus services
- Configuration of security services
  - AdHoc VOMS Management integration
  - system configuration
- Interoperability
  - authz-interop.org XACML profile
  - SAML2XACML2 to site-central services
    (in EGI: largely Argus, elsewhere: GUMS/SAZ)

What did already happen up to now?

- Extension of VOMS-awareness beyond the Gatekeeper (#95, #151,#152)
  - gsissh needed patching – patch (with Brian Bockelmann, Nebraska) now going into mainstream *allows gsissh and other to use one-off authZ via the call-out mechanism to LCMAPS*
  - extension of interfaces for GK & gsissh in LCMAPS *allows passing of cert chain to Argus (EMI) for EGI whilst preserving access to other callouts+*
  - some of these patches were quite low-level, so had to be 'internally contributed' to LCMAPS as-is so not explicit in IGE or UMD release

+ such as tracking GIDs, the JobRepository, local account maps, process tree isolation; which the Argus-only GT call-out cannot do

What did already happen up to now?

- Packaging and distribution compliance
  - re-factoring of much of the site-access-control code to make it build-compliant with EPEL &c
  - in the IGE updates/ repo
  - packages previews at software.nikhef.nl
  - *IGE actually the only project* doing *the packaging compliance as promised ...*
  - few odd bits left that violate fedora guidelines: Argus PEP-C client (java/maven issue), gSOAP dependence in SAML2XACML2 (work with Joe Bester to solve this one)

What did already happen up to now?

- SAML2XAML2 interop
  - our joint effort (OSG/Provilege, Globus, EGEE) on authz-interop.org profile going forward to OGF
  - needs evolution to make it accepted global standard
- AdHoc VOMS agent
  - available now in testing/ repo

Software Vulnerability Group (SVG)

- https://wiki.egi.eu/wiki/SVG
- assess vulnerabilities in *deployed* software
- taking into account *operational environment*
- for all of the UMD and related software

Risk Assessment Team (RAT)

- experts from operations and multiple M/Ws
- defined assessment and disclosure process
- very few Globus vulnerabilities as of yet

Certification and operational issues

- Validation of security components
  - aim is to *validate in real-life 'EGI'* environment
  - so nothing on the Nikhef test bed (ve.nikhef.nl) is re-compiled from source, only packages are used *building from source should not be our aim, since that does not demonstrate usability for operations*
  - packages work for GridFTP
    gatekeeper: thread mixing problem, gsiSSH: needs BB's patch
  - GT5.2 however is completely new game,
    and needs everything re-tested ...

Items related Globus Online

- dCache endpoint SARA (EGI/PRACE) added
  - interop testing for GridFTP with VOMS
  - useful as dCache now attempts
    to evolve the GridFTP protocol (delegation-less)
- As IGE GO instance becomes more production
  - beware of operational trust issues – and be wary of user-provided CAs in the trust fabric ...
  - consider also PRACE/EGI security policies??
- *SCG: not too middleware-oriented for now*

Upcoming issues and plans

Requests and Issues

- Old-style proxy support (RT#96)
  - fails in 5.0.{x,y} for some x and y: pushing upstream
- Correlation of grid(VOMS) identity and subsequent non-grid job accounting (RT#162)
  - assigned to GridSAFE for now
- Accounting derived from LCMAPS logs (#159)
  - the NGS did some local specific config
  - use case described already part of default setup, and will get there for gsissh with code already there

Requests and Issues

- Log level modifications (EGI RT#1983)
  - logs are used for accounting by many projects
  - Honouring single change requests is dangerous – it may break parsers in different accounting systems
- Accounting support from VOMS (by DW/NGS)
  - instead of writing out log files, we have a module (and some supporting tools) for directly pushing job credential information into a database:
    the lcmaps-job-repository plugin
  - Not currently in use, needs integration in rest of IGE

Other open issues we may have to consider

- Is GridWay fully VOMS-aware yet ...
  - use of VOMS attributes in matching to infosys
  - vomsified renewal for long running jobs (e.g. by interfacing to MyProxy, and there’s a renewal-daemon already in the UMD)
- APEL accounting interface for EGI
  - encryption of quasi-UR records (but NOT UR-WG!)
  - either use file-system based messaging system by APEL folks, or talk directly to APEL SSM broker
  - former case: write compliant UR lists
    latter case: send compliant encrypted messages

Other open issues we may have to consider

- gsissh support in next release
  - besides NGS use also in LCG VOBOX
- delegation-less 3rd party GridFTP transfers?
  - EGI wants to rely on plain SSL instead of ‘httpg’
  - remove delegation where not needed
  - data management taking lead –
    the GSM WG has this on their agenda
  - track developments ongoing in dCache who appear interested in evolving the protocol
- limits for proxy life time (through SCG/TCB)
  - for initial long-term MyProxy proxy and for leaves

Other open issues we may have to consider

- Semi-automatic configuration of security components
  - no intent to duplicate ‘yaim’, but now it’s too complex
  - debconf is a nice example of what might be
  - slightly better than RH system-config-* or *-tui model
  - how do other components solve this?

Upcoming formal requests for functionality

- Coming soon in the EGI TCB near you: functional authentication requirements
  - IGTF ‘Wish List’
  - IGE Globus complies with most of them already and has at least no plans to break things
  - and for other elements, external patches to Globus are already available but just need integration

- List will come through TCB
  - *or I can tell you all details now if you want ...*

IGTF Wish List things for Globus

- proxy cert length to 1024 by default
- does everything work with SHA-2 family
- RPDNC Namespaces support (or evolution)
- certificatePolicies OID checks & decisions
  - this will enable multi-LoA support
- beware of NSS – and avoid it where you can
  - EL6 is moving there, and it breaks the drop-in trust anchor store model and RFC3820 proxy support
  - system libraries (like CURL) are suddenly useless
- support OCSP (AIA and Trusted Responders)
  - Jim Basney already has a patch for this!

And now for some of ‘our’ questions

Our Questions!

- are there components that want to integrate with native SAML (or OAuth) federations?
  - – eduGAIN, national federations, ...
- triage of requirements and requests?
  - – how do we do this project-wide?
  - – this should best not be left to the individual development teams ...
- platforms needing release of packaged form?
  - – Add Debian 6, or also 5 & Ubuntu LTS releases?
- what’s the life cycle for released software?

AND NOW YOUR QUESTIONS!