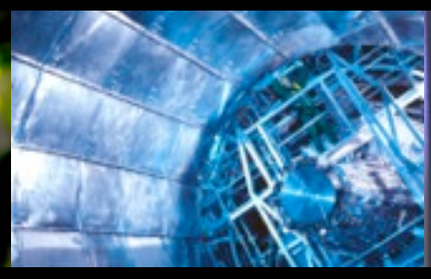
WLCG Group

Summary of WLCG security for 2012

WLCG Security Meeting, 17th December 2012, R. Wartel








WLCG
Worldwide LHC Computing Grid

Operational Security

- Incidents happen on a regular basis, 10-12 per year
- Attacks continue to improve
  - More and more sophisticated
    - For example, Zeus (Windows botnet) used to steal HEP accounts
    - No easy or public mean to detect modern malware
  - No longer a side-effect of being connected to the Internet
    - State-of-the-art malware used against WLCG
    - Attackers being arrested for attacking WLCG resources
  - No reduction of the severity or # of incidents in the recent years
    - Yet most of them follow the same pattern
    - Needs to improve our tools and our practices
    - We have now built the necessary expertise and have experience

WLCG risk analysis

- WLCG risk analysis
  - First task of the Security TEG
  - https://espace.cern.ch/WLCG-document-repository/Boards/MB/WLCG_Risk_Assessment.pdf
  - "Live document"
- Objectives of the document
  - Identify our assets (what we want to protect)
  - Identify the main threats stemming from malicious intents
  - Score and highlight the most important risks
    - Based on likelihood of each threat
    - Based on the typical impact of the realisation of the threat
  - Discuss the risks and how they affect our assets

WLCG risk analysis

- It is the goal of the security teams to protect WLCG assets

Asset	Comments
Trust / collaboration	The trust established between WLCG participants, collaborating infrastructures, external partners and funding agencies, needs to be maintained
Reputation	Reflects the opinion of the general public, funding agencies and participants about WLCG
Intellectual property	It includes both copyrighted material and the result of scientific work conducted on WLCG resources
Data protection	The protection of the data (e.g. personal) collected by, stored at and handled by WLCG resources.
Digital identities	Includes both the credentials and the attributes enabling the authentication and authorization of users and services.
CPU resources	Physical or virtual entities that are consumed through services to enable calculations to be conducted, for example worker nodes
Data resources	Physical or virtual entities that are consumed through services to enable LHC data to be stored
Network resources	Network facilities enabling the different WLCG participants to cooperate and users to access WLCG resources
Services	A service is any computing or software system, which provides access to, information about, or controls tangible assets. This includes the services necessary to the usage, support, operation, monitoring of WLCG as well as the communication and dissemination within and outside the collaboration, such as websites, wikis, etc.
Data integrity	The accuracy, lack of alteration and consistency of stored data (for example scientific data) on WLCG resources

WLCG risk analysis

- Highlighted the need for fine-grained traceability
  - Essential to contain, investigate incidents, prevents re-occurrence
- Aggravating factor for every risk:
  - Publicity and press impact arising from security incidents
- 11 separate risks identified and scored. Top risks:

Risk
Misused identities (“SSH”-type included)
Attack propagation between WLCG sites
Exploitation of a serious OS vulnerability
Threats originating from trust services
Negative publicity on a non-event
Insecure configuration leading to undesirable access
Insufficient protection of information leading to sensitive data leakage
Incidents on resources not bound by WLCG policies
Exploitation of a serious VO/middleware software vulnerability
Data removal/corruption/alteration
DoS from an external organisation

Areas of work

- Important “technical areas” where work is needed
  - Fulfill traceability requirements on all services
    - Sufficient logging for middleware services
    - Improve the logging of WNs and UIs
    - Too many sites simply opt-out of incident response “no data, no investigation -> no work to be done!”
    - Prepare for future computing model (e.g. private clouds)
  - Enable appropriate security controls (AuthZ)
    - Need to incorporate identity federations
    - Enable convenient central banning
- Important “people” issues
  - Must improve our security patching and practices at the sites
  - Collaborate with external communities for incident response and policies
  - Building trust has proven extremely fruitful - needs to continue

Security Controls

- Blocking/banning used mainly for incident response
  - Sites and a "central banning body" (central security operations) should may need to ban users
  - More rarely, the VOs may also want to ban users (in addition to VOMS removal)
  - Normally, the VOs will report incidents/malicious users to the central security operations

- Central banning needed to ensure appropriate incident response
  - Central security operations managing central banning lists
  - Banning conditions are already defined in existing security policies and procedures

Traceability WG

- Main objectives
  - Software: ensure there is enough traceability on the SE and that our services use standard logging mechanisms (syslog)
  - Operations: Recommendations aimed at the sites should be produced to help fulfilling the logging and traceability policy on the WN (whether or not virtualization is used) and UI
- Current status:
  - Started with the discussion on software
    - Questionnaire being prepared for the different software areas
    - Not very active - more participants welcome!
  - Discussion on operations not started yet
    - Probably easier to make progress here
  - Next meeting initially planned for this week, but very few people available to attend :-(

Argus

- "Authentication" cannot be used for banning
  - A user may be deemed malicious without being compromised
- "Authorization" is the appropriate way to ban users
  - Removing a user from VOMS is not sufficient due to long lived proxies.
  - Banning not really workable without central banning

- Central banning deployment proposal:
  - All WLCG sites must implement necessary mechanisms to pull central banning lists from the central Argus instance, for example by deploying Argus locally. The deployment of these solutions should be followed up in the GDB.
  - On the WN, Argus requires gLexec

Virtualization on the WN

- Recommendations aimed at the sites should be produced to help fulfilling the logging and traceability policy on the WN (whether or not virtualization is used)

- A working group should be appointed to conduct this work

Using external clouds

- When VOs use resources not provided by WLCG sites, or sites choose to expand by instantiating off-site cloud VMs, it is currently not possible to do so in such a way that conforms with WLCG security policies
- As specified in the WLCG risk assessment, there are significant concerns in using external cloud providers and additional work is needed to understand the policy issues it raises. There are also operational issues (including procedures and traceability)
- A working group should be appointed to conduct this work and report back to the GDB or MB as appropriate
- In the meantime VOs or sites instantiating external cloud resources should be aware of these concerns and the responsibilities they accept by using these services

Critical proxy extension

- There are two paradigms in use at the moment. The "send a limited user proxy" model of ATLAS, LHCb, and CMS, and the "no user proxy" model of ALICE.
- ALICE can make an extension to their model to pass a "critically limited" proxy which is only valid for use by glexec. This model is much better as far as secure transport of the proxy goes, however it should be verified that there is a persistent site-level link between data and actual user.
- The model for the other three experiments requires care in transport and handling of user proxies, however these proxies can be used to provide the desired link at the storage element between file and payload owner.

Proxy lifetime

- Can we reduce the VOMS proxy lifetimes (currently 3 to 8 days depending on the VO) back to 24h?
  - Consensus: good idea and should be a priority item of work for LS1
  - Technical implications and work needed are yet to be evaluated by each of the VOs.

Pool account recycling

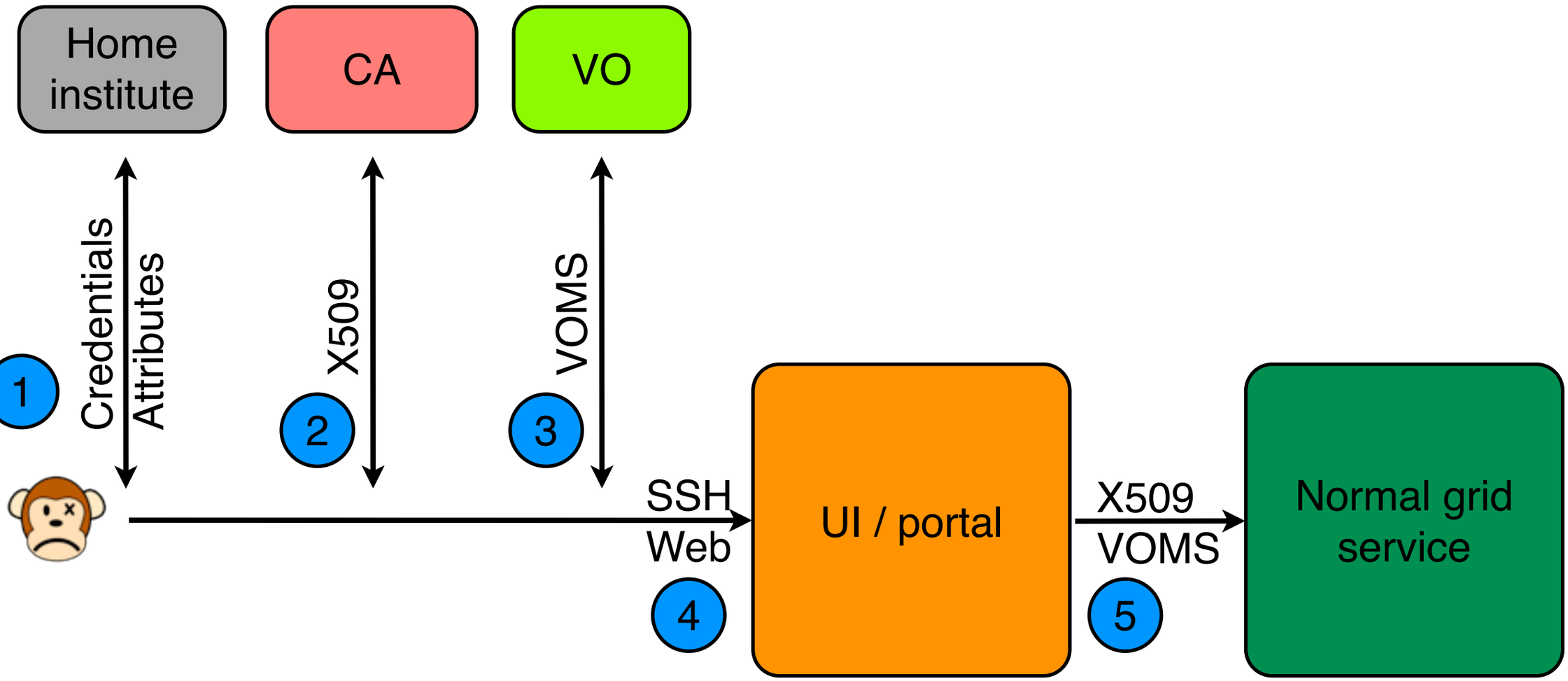
- Pool account recycling
  - Proposal: User accounts on the WN are important for security operations and pool accounts may be recycled only after they have been unused for 6 months.
  - (Unless the account is causing operational issues (too big, etc.)?)
  - It was noted that enabling gLexec on the WN will probably increase the number of necessary pool accounts.
  - VOs should publish the number of pool accounts they need in their VO Card.
  - The situation in OSG was not discussed

Identity Federation

- Federated Identity Management document
  - Common vision, requirements and recommendations
  - https://cdsweb.cern.ch/record/1442597
  - Endorsed by the MB on 5th June 2012

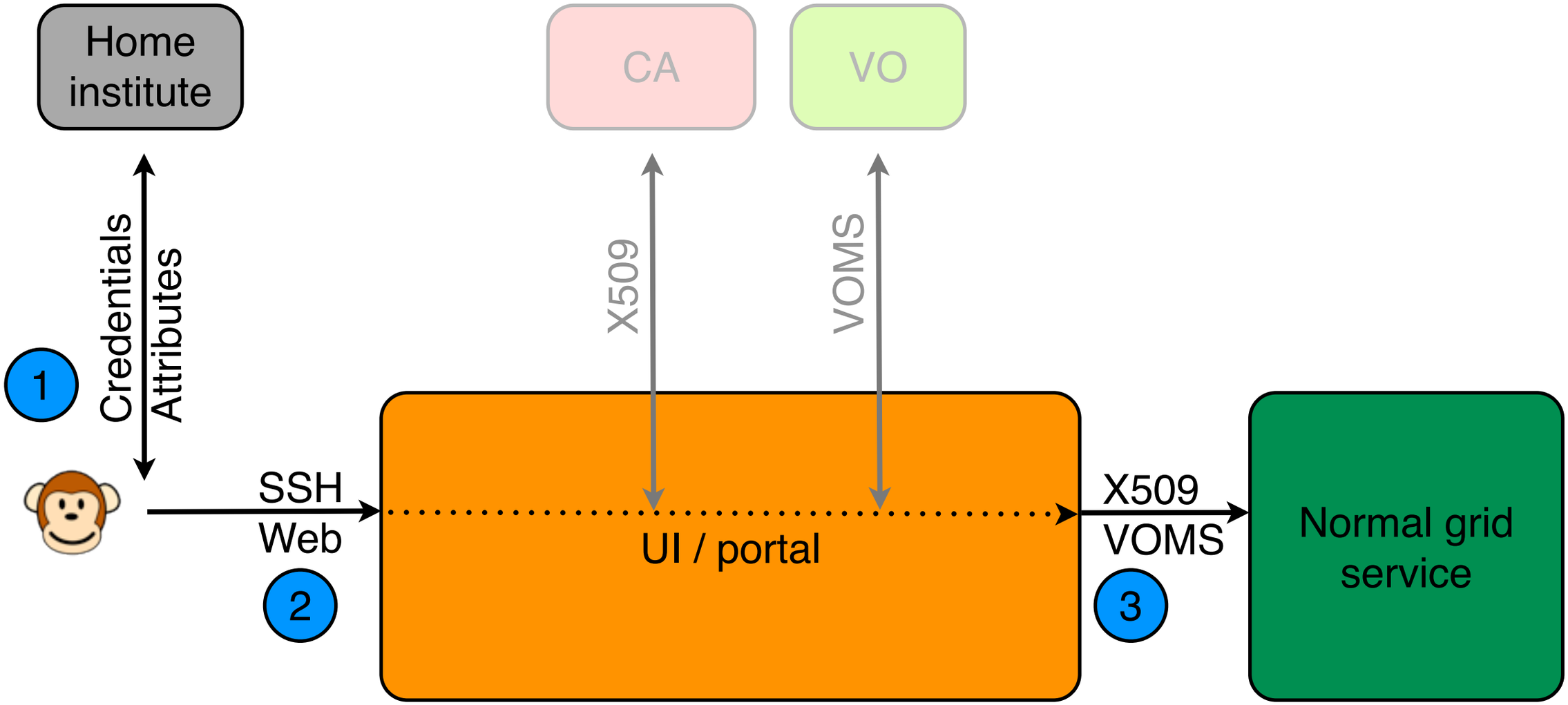
- WLCG planning a non-browser based pilot project
  - a service enabling access to WLCG resources using home-issued federated credentials.

A pilot project for WLCG



Traditional access to grid services

A pilot project for WLCG



Federated access to grid services

Identity Federation Pilot

- Main points agreed so far:
  - Goal of the pilot: a CLI login tool (typically a "voms-proxy-init" or "grid-proxy-init" replacement), able to authenticate users based on their home credentials, create X509 credentials and proxy, and offer to optionally add voms extension
  - As soon as the proof-of-concept options are a bit clearer, we should start investigating levels of assurance, trust and possible IGTF accreditation
  - CILogon and EMI STS (at least) seem to provide valid options to fulfill the described objectives

- Technical discussion “CILogon/EMI STS“ yesterday
  - Should we choose one over the other?
  - Would it be conceivable to have a single, unified pilot relying on *both* CILogon and STS? (Implications and costs?)

Identity Federation Pilot

- Both support SAML ECP (...but very few IdP do...)
- Otherwise very different, need two clients (and a wrapper?)
- Making CILogon and EMI STS compatible?
  - Either CILogon would need to support WS-Trust
  - Or EMI STS would need to support posting the certificate request to the CILogon REST endpoint and support the returned response
  - Both CILogon and EMI STS experts will investigate costs
- Workplan for the next 2 months
  - Setup a pilot EMI STS (at CERN)
  - Review and test the CLI for EMI STS CILogon
  - Conduct a survey to see how many IdP support SAML ECP in EU
  - Review attributes that need to be pulled from the IdPs
  - Start discussions on accreditation and possible operational requirements on the IdPs