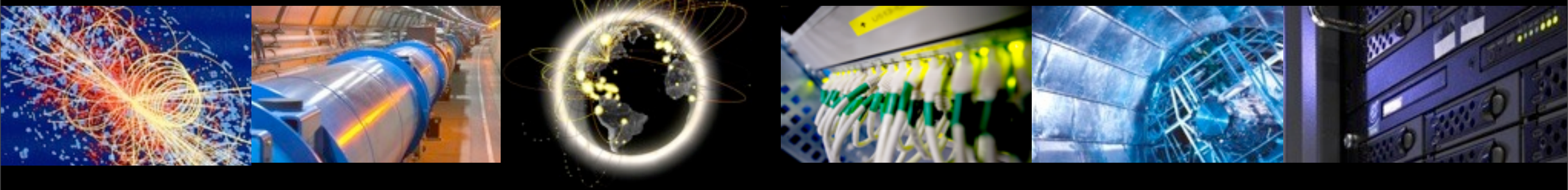
WLCG Group

# CERNVM-FS Security Review



# CERN-VM FS

- CERN-VM FS is a network file system
  - Based on HTTP and Squid proxies
  - Files are distributed over plain-text HTTP
  - Hashes of the files are verified against a list of trusted hashes

- Already used by LCG VOs and other experiments
  - Propagation of software (executables, config) to the sites
  - Probably more in the future

- Is the security of CERN-VM FS in-line with the rest of our middleware components?

# Security review

- Conducted by:
  - Ian Collier <ian.collier@stfc.ac.uk>
  - Jay Srinivasan <jay@nersc.gov>
  - Steve Traylen <Steve.Traylen@cern.ch>
  - Romain Wartel <Romain.Wartel@cern.ch>

- The reviewers would like to THANK the CERN-VM FS team for their patience and collaboration, in particular:
  - Jakob Blomer <Jakob.Blomer@cern.ch>
  - Predrag Buncic <Predrag.Buncic@cern.ch>
  - Artem Harutyunyan <Artem.Harutyunyan@cern.ch>

# Security reviews

- Reviews are useful to help discovering problems before it's too late

# Review focus

- The review focused on:
  - Documentation and packaging
  - Software and infrastructure design
  - Data integrity verification mechanisms
  - Credentials management and segregation between users
  - Central service management at CERN

- NO code review was conducted
- CVMFS is rapidly evolving
- A review does not guarantee that no vulnerability exists in the reviewed software

# Overall results

- CERN-VM FS was designed with security in mind
  - Security model relies on file hashes being verified against a trusted catalog
- Sufficient mechanisms to ensure data integrity
  - Note: no data confidentiality is provided
- Packaging and technologies used enable quick patching
- The signing process is well segregated
  - A rogue VO manager cannot tamper with another repository
- Several findings addressed already by the CERN-VM team
  - https://savannah.cern.ch/bugs/?group=cernvm

# Areas of improvement

- The hashing mechanisms is weak (SHA-1)
  - SHA-1 collisions easier to perform on large amount of data
    - Threat is real but not posing an immediate risk
  - CVMFS team aware of the weakness, plan to integrate the new SHA-3 hash mechanism as it becomes available (in 2012 according to NIST)
  - Probably means a complete re-hash of all files

- A few other details:
  - More “best practice” documentation would be useful
  - Central service being moved to CERN IT
    - Impact on the service?

# Conclusion

- Positive review! Well done CERN-VM FS!
  - Some details can and should be improved
  - No blocking factor or major security issue

- The dev team showed flexibility to address reported issues
  - Good sign should further problems be discovered

- Important to highlight limitations of the features:
  - No confidentiality is provided
  - Read only

  - More details at:

    https://twiki.cern.ch/twiki/bin/view/Main/CernVM-FS-SecurityReview