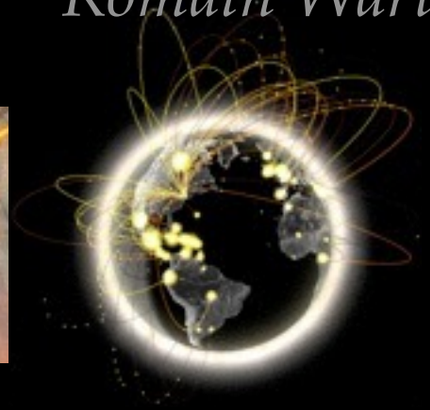
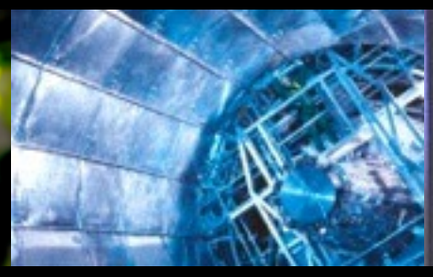
New paradigms for academic computing security

Romain Wartel, WLCG Workshop 2016, 1 Feb 2016, Lisbon








WLCG
Worldwide LHC Computing Grid

Short summary

- See past GDB and HEPiX talks on underground economy, nation-state attacks and cybercrime evolution.
- 5 years ago:
  - Attacker mostly small groups or specific individuals
  - Linux/Grid world isolated from “Windows” malware, phishing, etc.
  - Prevention & monitoring key strategy
  - Secure services
- 2016:
  - Attackers mostly global organised groups. Or nation-states.
  - Intrusions via phishing/social engineering
  - Threat intelligence (know what to look for) is key strategy
    - Almost all our intrusions are detected because a contact tells us (intelligence). We need to have good contacts!
  - Defendable services

Proposed strategy

Protecting grid services…
… by shifting emphasis away from grid and services:

- Increase our focus on people (& our relationships)
- Reach out globally: the non-WLCG part of our sites, security vendors, NRENS, peer projects, federations, etc.
- Get high quality intelligence (requires trust!)
- Build the ability to make good use of it

Detailed strategy: all of us

WLCG participants and WLCG itself should consider a strategy addressing how to:

1. Involve security vendors in monitoring/incidents/forensics
   - Appliance? Service? Partnership?
     "We are keen on working with you guys, because you have large network and you are favorable target for advanced attackers."

2. Obtain indicators of compromise (threat intelligence)
   - Establish a solid network of security contacts?
   - Outsource and hire a security vendor (jointly or alone)?
   - Build the technical means to use them (SoC infrastructure, storage, etc.)
     - Do we need a working group for this?
     - Should we work on a "HEP appliance", like the NSF is the US?

3. Involve law enforcement for serious breaches
   - Attackers rarely decide they have had enough data/money…

4. Continue to raise the bar
   - Make it as difficult and expensive possible to break-in

Detailed strategy: management

- Treat WLCG security is a global issue
  - Not limited to WLCG/HEP sites
  - Including: operations, traceability, incident handling, policies
  - Continue to invest in global trust frameworks
  - Continue to contribute to global efforts against cybercrime
    - Focus on major threats that are known to cause significant damage to WLCG participants (Dridex, etc.)
- Main strategy for the VOs
  - Focus on traceability and controls (blocking) in priority
  - Participate more actively in the incident response process
- Shift security emphasis from services to people
  - Next big breach likely via phishing, unlikely via SSH/grid 0-day

Detailed strategy: incident response

- Leverage WLCG's incident response contacts globally
  - Not solely rely on EGI CSIRT and OSG Security team
  - Reinforce cooperation with federations, eduGAIN, security vendors, private sector, etc.
  - Propose an academic security trust group to share threat intelligence
- Update WLCG's incident response workflow
  - Centrally coordinated forensics and analysis - to help support the many sites with limited forensics expertise
  - Sites will would simply fulfil "traceability" requests *(unless they have expertise to do more)*
  - Involve more directly the WLCG/EGI operations team (already the case in OSG) and VOs
- Prepare for possible funding for serious cases?
  - Security vendor
  - Travel expenses of WLCG experts, etc.