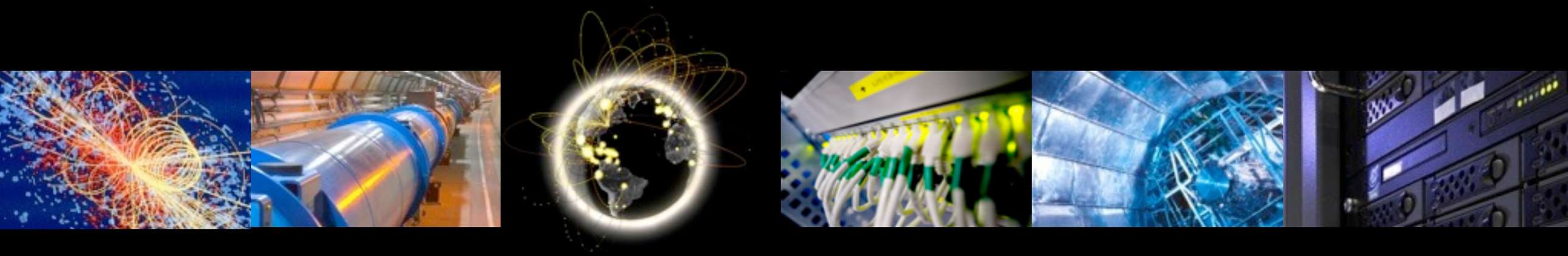
WLCG Group

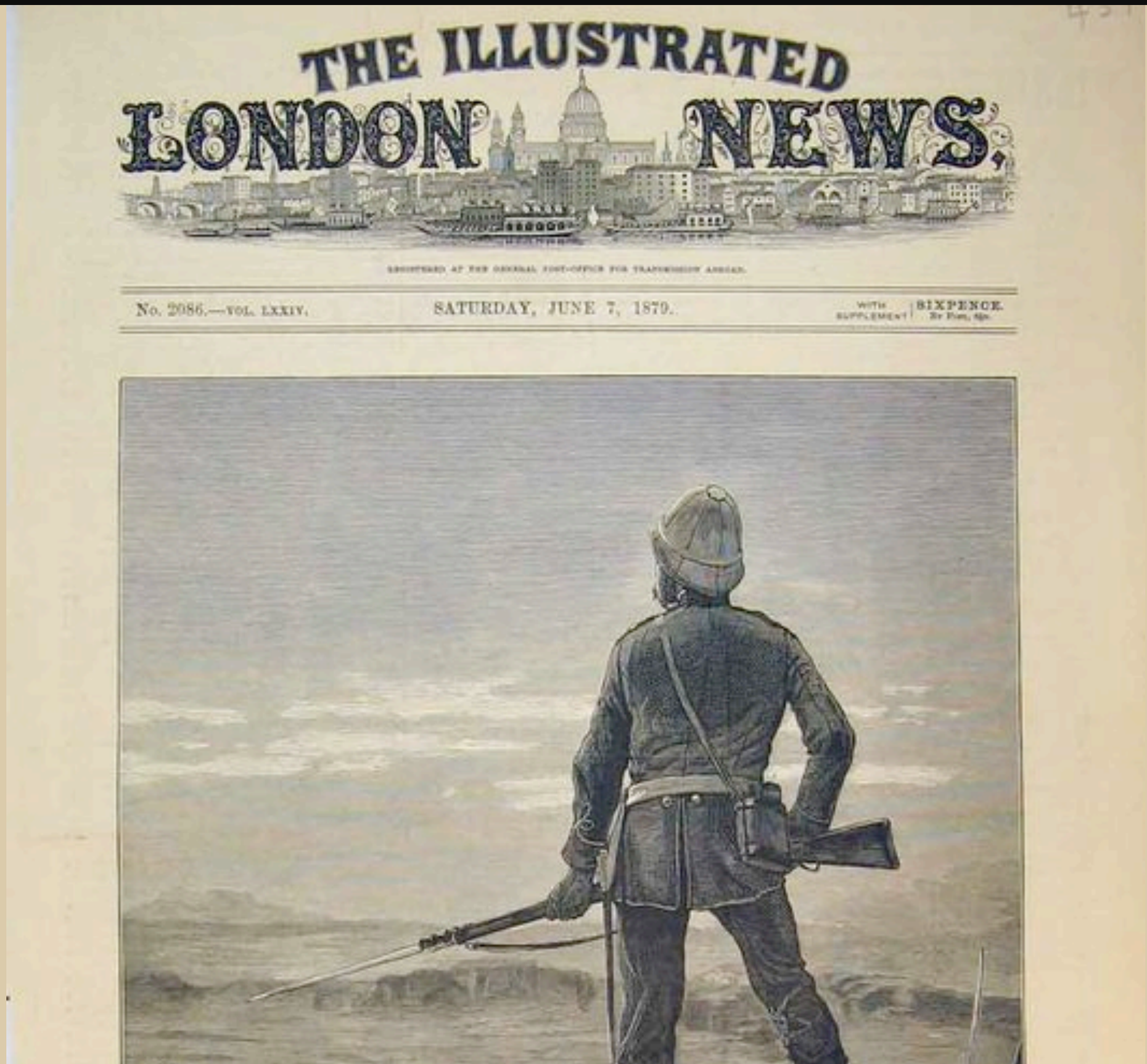
Security update

HEPiX Meeting, Bologna, 15-19 April 2013, R. Wartel



WLCG
Worldwide LHC Computing Grid

News from the front



THE ILLUSTRATED
LONDON NEWS.

REGISTERED AT THE GENERAL POST-OFFICE FOR TRANSMISSION ABROAD.

No. 2086.—VOL. LXXIV. SATURDAY, JUNE 7, 1879. WITH SUPPLEMENT | SIXPENCE. By Post, 6½d.

Some news from (the) Citadel

- ~11730 hosts were discovered compromised with malware
  - Some in HEP!
- Experts from many organisations and countries helped
- CERT Polska played a key role and wrote a public report:
  - http://www.cert.pl/PDF/Report_Citadel_plitfi_EN.pdf
- Citadel inspired by the leaked Zeus code:
  - “Man in the browser” attack: steal login data, bypasses SSL, replace ads on websites, take screenshots, prevents contact with resources mentioning the malware, etc.
  - Zeus believed to have gathered $ 70 Millions from victims
- Business model:
  - Sell a crimeware pack, included a control panel and bot builder
  - Customers need to have their own distribution mechanisms and infrastructure to collect and mind the data back

But most attacks are SSH-based

- Typical SSH attack in the academic community
  1. Use stolen credential to connect to a site
     - Share and collaborate with the community!
  2. Escalate as root as soon as possible
     - Patch as quickly as possible & harden your hosts!
  3. Once root, install a rootkit
     - Run rootkit detection tools and sufficient traceability!
  4. Collect login data
  5. Expand:
     1. Parse data from 4.
     2. Follow users at other sites/hosts
     3. GOTO 1

Ebury: 1990s revisited

- Welcome to Ebury, the new old-style sshd trojan
  - Provides a backdoor mechanism
  - Captures credentials in and out of the infected system

- SANS has a good summary
  https://isc.sans.edu/diary/SSHD+rootkit+in+the+wild/15229
- Trivial to identify with rpmverify, tripwire, Samhain, etc.
  - (Are YOU checking the integrity of your binaries?)
- Actively used since 2011
  - Found mostly on RHEL-based systems
- Does not sound very exciting, but ebury is very interesting!
  - Many versions found (actively maintained malware)
  - Authors made interesting compromises (!)
  - Unique supporting infrastructure

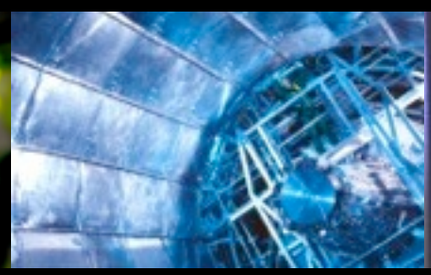
Ebury: 1990s revisited

- The malicious binary
  - Compiled for each victim, with a (unique) hardcoded password
  - Payload initially in sshd, then moved to /lib/libkeyutils.so.*
  - Basic, but reasonably stealth and secure backdoor
  - Some effort was put in obfuscating the code and preventing analysis (rather unusual)
- The malicious infrastructure
  - Malware designed for mass-deployment
  - Carefully designed exfiltration mechanism and supporting infrastructure
- Victims also in the industry sector:
  - http://docs.cpanel.net/twiki/bin/view/AllDocumentation/CompSystem

A paradigm shift








Security: the classic approach

- Something really interesting is happening
- Sites usually build their security architecture around:
  - Strong controls mechanisms
  - Well defined security perimeters
- Then they rely on:
  - Local policies and procedures
  - A small team of security experts (if at all possible)
  - Logs and information collected from their hosts
- Sometime share intelligence or incident information
  - With a small number of trusted peers who have similar issues
  - Always useful to learn best practices and good tools from others
- Goal : keep the attackers outside of the security perimeter
- Very “medieval” approach

Security: a paradigm shift

- Evolution of the controls mechanisms over time
- Access to computing resources is granted to users:
  (Trust : both party agreed to follow a set of policies)
  - Trusted, locally registered (1990s)
  - Trusted, remotely registered at trusted (grid) sites (2000s)
  - Remotely registered users at sites in trusted federations (2010s)
  - Remotely registered users at sites with a good reputation (Facebook, Google, etc.)?
  - Remotely registered users?
  - Remote users?

- What capability can we use to manage this?
  - The ability to terminate access to users not following local policies
  - Authorization and roles

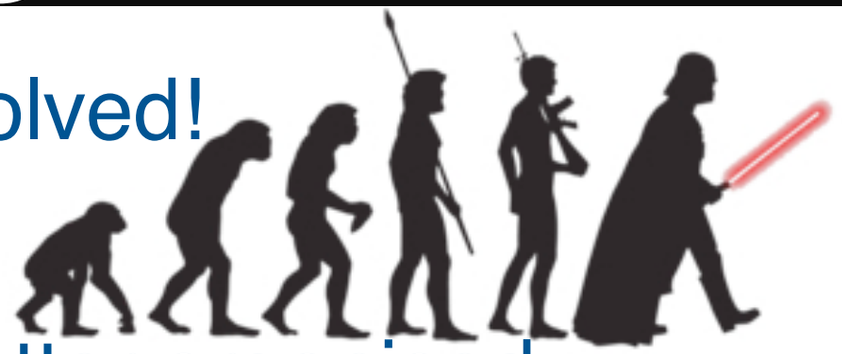
Security: a paradigm shift

- Evolution of the security perimeters over time
- Nobody wants its resources to be used by attackers
  - Build one or more fences to manage this risk
- In order to have a manageable security, it is essential that attackers never:
  - Run any kind of arbitrary code (1990s)
    - All executed code must be legitimate
  - Tolerate previous point, but no root escalation (2000s)
    - There will be malicious users, but they must not be root
  - Tolerate previous point, but root code must be in a VM (2010s)
    - There will be malicious users with root access, but their host will be segregated in VMs we control
  - Tolerate previous point, but all VMs are in a different network (2010s)
    - There will be malicious or untrusted VMs, but they must be isolated

Security: a paradigm shift

- VMs also need access to local resources and they move dynamically
  - Isolation almost impossible
  - Traditional mechanisms (e.g. firewall) provide little benefits
- In our environment, relying simply on controls and security perimeters is bound to fail
- What capability can we use to manage this?
  - Traceability.
  - Traceability is the key asset that must be preserved in the future
    - It defines our ability to contain, resolve and prevent incident
    - It enables legal action to be taken, helps protecting reputation, etc.
  - It is very difficult to implement correctly
    - Need to have sufficient & relevant data, while maintaining privacy
    - Need to store data, but also be able to analyse it later

Security: a paradigm shift



- But our security experts have also evolved!
- More exposed, now better prepared
- As a community, we are now much better organised
  - International information sharing and trust
  - Relevant insight, appropriate experts readily available
  - Precious intelligence sharing across peers
  - A lot of in-depth expertise and know-how gained
  - Strong knowledge on some attack methods and tools
  - Learnt how to deal with the press
- Good connections with the industry and law enforcement
  - Law enforcement also more responsive and interested too
- Landscape is more complex but not necessarily less favorable now

Old vs New

“Good old days”	2013
Local hardening and prompt patching	Local hardening and prompt patching
Local users	User communities and federations
Firewall & ports	Traceability
Malicious users	Malicious organisations
Local expertise	Global intelligence & collaboration
Malicious software	Malicious infrastructures
Local management	Press and media
No escalation possible	Law enforcement may help

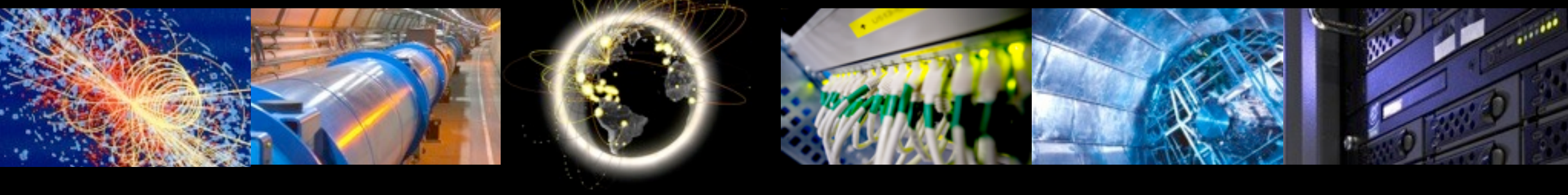
Security: a paradigm shift

- NSA Director: Information-Sharing Critical To U.S. Cybersecurity

  "We don't need to read communications," he said. "We just need the Internet Service Providers and the companies to say, '…you told me to tell you if I saw this coming, I see this coming, I can tell you at network speed, and I can do it in a metadata-like format that eliminates the privacy information and gets you what you need to protect the country and what we need to protect our civil liberties and privacy.'"

  http://www.darkreading.com/threat-intelligence/167901121/security/news/240151955/nsa-director-information-sharing-critical-to-u-s-cybersecurity.html

Recent security work in WLCG



WLCG risk analysis

- WLCG risk analysis
  - Conducted in 2012
  - 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

WLCG Operational Security

- Incidents happen on a regular basis, 10-12 per year
  - 2012 has been a quieter than usual
- 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 HEP sites
    - Attackers being arrested for attacking HEP sites
  - 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

Questions?