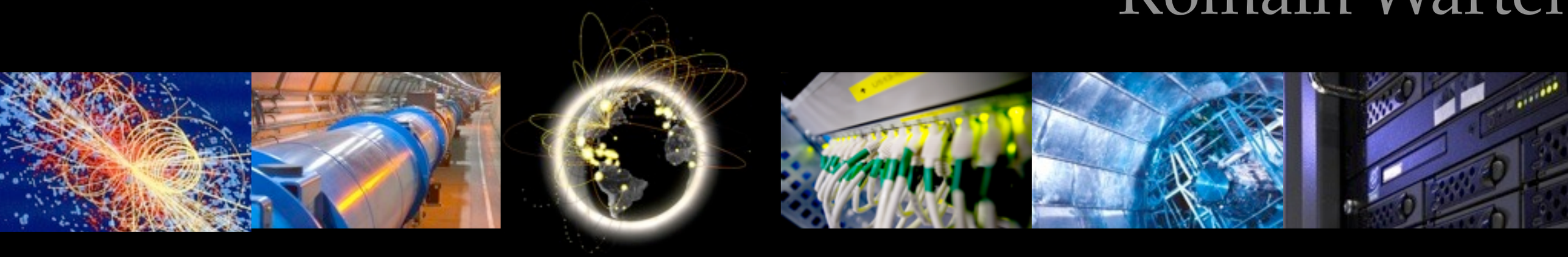
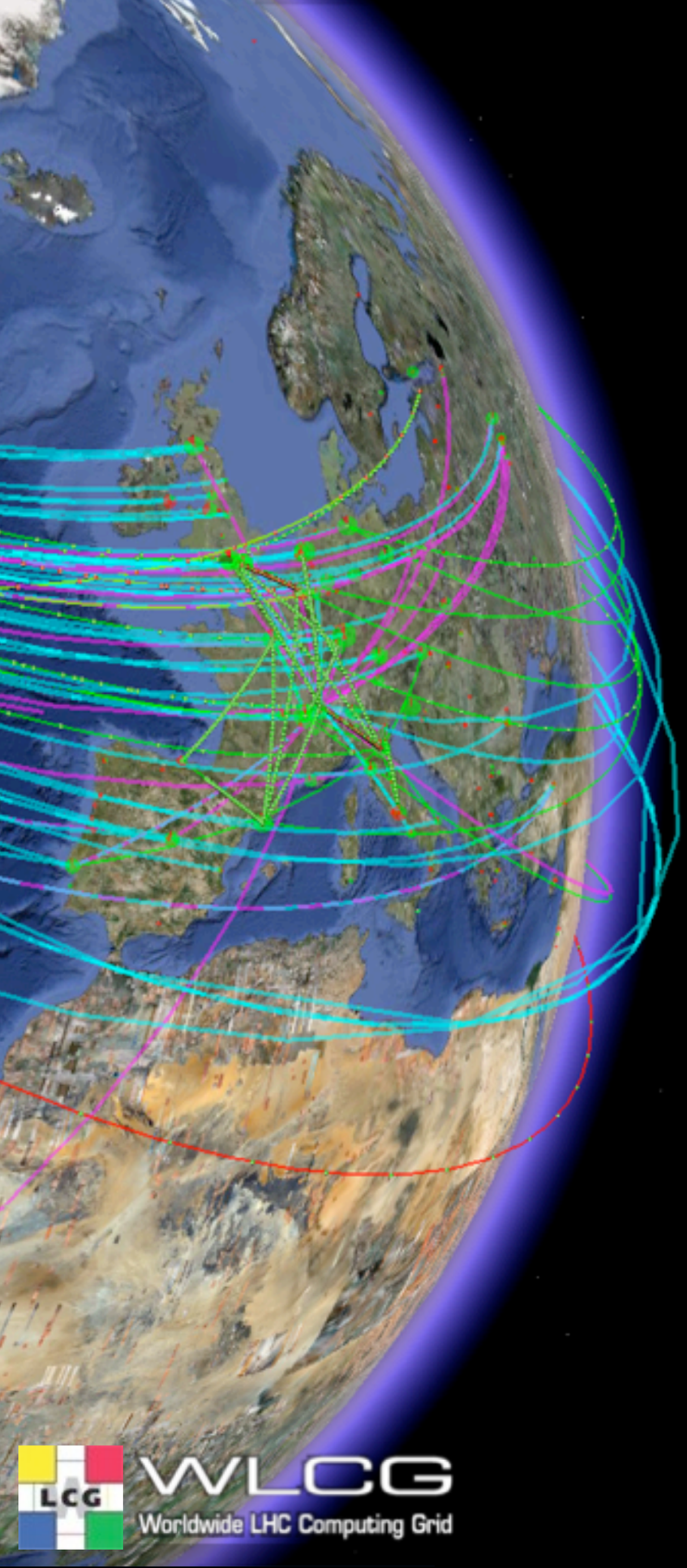
WLCG Group

Security update

Romain Wartel



WLCG
Worldwide LHC Computing Grid

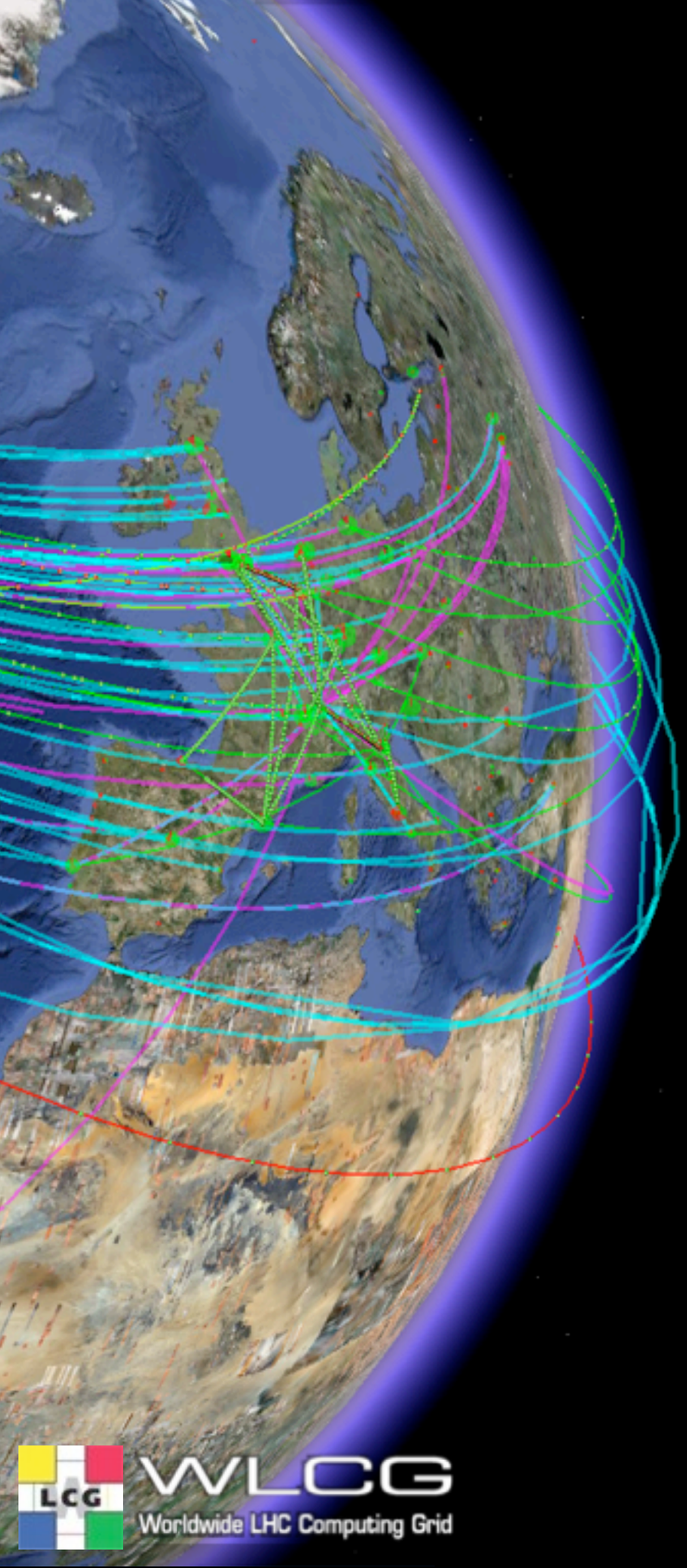


On reputation and the media

WLCG
Worldwide LHC Computing Grid

Reputation

- "Computer security" aims at protecting different assets:
  - Service availability
  - Data integrity or corruption
  - Confidentiality
  - Reputation
- For online services, reputation is everything
  - Trust
  - Do business
  - Keep existing customers, acquire more
- Reputation is fragile
  - Need to take great care of it while managing security
    - Both to prevent attacks and to recover from them
  - Affected by an incident echoed in the press?
    - Cooperating with partner sites is essential



Recent attacks

WLCG
Worldwide LHC Computing Grid

RSA SecurID tokens

Open Letter to RSA Customers

Open Letter to RSA Customers

http://www.rsa.com/node.aspx?id=

Home > Programs

Open Letter to RSA Customers

Arthur W. Coviello, Jr.

Like any large company, EMC experiences and successfully repels multiple cyber attacks on its IT infrastructure every day. Recently, our security systems identified an extremely sophisticated cyber attack in progress being mounted against RSA. We took a variety of aggressive measures against the threat to protect our business and our customers, including further hardening of our IT infrastructure. We also immediately began an extensive investigation of the attack and are working closely with the appropriate authorities.

Our investigation has led us to believe that the attack is in the category of an Advanced Persistent Threat (APT). Our investigation also revealed that the attack resulted in certain information being extracted from RSA's systems. Some of that information is specifically related to RSA's SecurID two-factor authentication products. While at this time we are confident that the information extracted does not enable a successful direct attack on any of our RSA SecurID customers, this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack. We are very actively communicating this situation to RSA customers and providing immediate steps for them to take to strengthen their SecurID implementations.

We have no evidence that customer security related to other RSA products has been similarly impacted. We are also confident that no other EMC products were impacted by this attack. It is important to note that we do not believe that either customer or employee personally identifiable information was compromised as a result of this incident.

Our first priority is to ensure the security of our customers and their trust. We are committed to applying all necessary resources to give our SecurID customers the tools, processes and support they require to strengthen the security of their IT systems in the face of this incident. Our full support will include a range of RSA and EMC internal resources as well as close engagement with our partner ecosystems and our customers' relevant partners.

We regret any inconvenience or concern that this attack on RSA may cause for customers, and we

RSA SecurID tokens

RSA hacked, data exposed that could 'reduce the effectiveness' of SecurID tokens -- Engadget

RSA hacked, data exposed that ...

http://www.engadget.com/2011/03

RSA hacked, data exposed that could 'reduce the effectiveness' of SecurID tokens

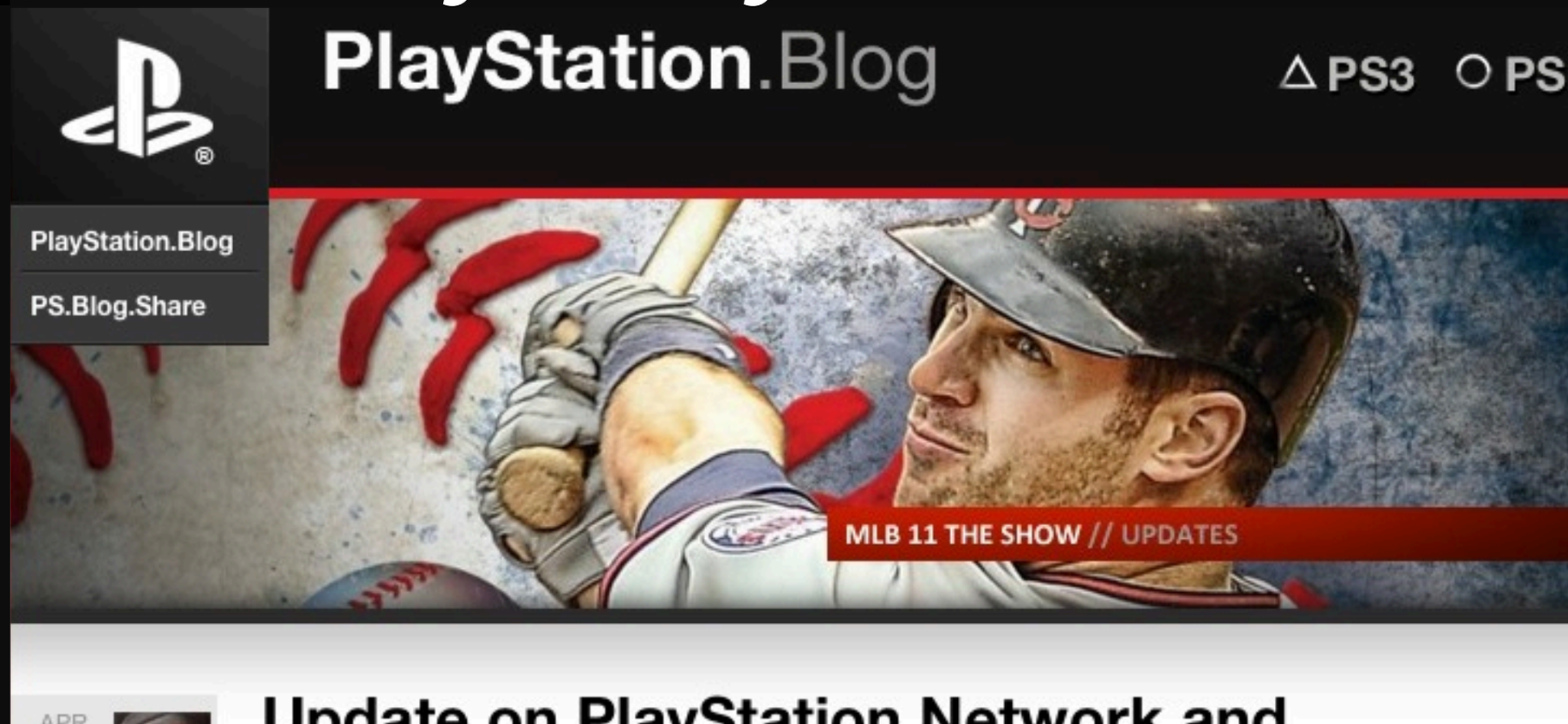
By Tim Stevens posted Mar 18th 2011 8:49AM

If you've ever wondered whether two-factor authentication systems actually boost security, things that spit out pseudorandom numbers you have to enter in addition to a password, the answer is yes, yes they do. But, their effectiveness is of course dependent on the security of the systems that actually generate those funny numbers, and as of this morning those are looking a little less reliable. RSA, the security division of EMC and producer of the SecurID systems used by countless corporations (and the Department of Defense), has been hacked. Yesterday it sent out messages to its clients and posted an open letter stating that it's been the victim of an "advanced" attack that "resulted in certain information being extracted from RSA's systems" -- information "specifically related to RSA's SecurID two-factor authentication products."

Yeah, yikes. The company assures that the system hasn't been *totally* compromised, but the information retrieved "could potentially be used to reduce the effectiveness of a current two-factor authentication

- SecurID's effectiveness now reduced
- Can't upgrade tokens
- Customers probably need to replace all units?
- How many will choose SecurID again?

Sony Playstation Network



APR 26 2011

Update on PlayStation Network and Qriocity

+ Posted by Patrick Seybold // Sr. Director, Corporate Communications & Social Media

Thank you for your patience while we work to resolve the current outage of PlayStation Network & Qriocity services. We are currently working to send a similar message to the one below via email to all of our registered account holders regarding a compromise of personal information as a result of an illegal intrusion on our systems. These malicious actions have also had an impact on your ability to enjoy the services provided by PlayStation Network and Qriocity including online gaming and online access to music, movies, sports and TV shows. We have a clear path to have PlayStation Network and Qriocity systems back online, and expect to restore some services within a week.

We're working day and night to ensure it is done as quickly as possible. We appreciate your patience and feedback.

Valued PlayStation Network/Qriocity Customer:

We have discovered that between April 17 and April 19, 2011, certain PlayStation Network and Qriocity service user account information was compromised in connection with an illegal and unauthorized intrusion into our network. In response to this intrusion, we have:

- 77 millions accounts compromised
- Personal details
- Credit cards
- Service completely down since 19th April

Sony Playstation Network

Sony PlayStation Security Flaw ...

https://www.nytimes.com/2011/04

The New York Times

Video Games

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION | ARTS

ART & DESIGN | BOOKS | DANCE | MOVIES | MUSIC | TELEVISION | THEATER

CRITIC'S NOTEBOOK

PlayStation Security Breach a Test of Consumers' Trust

By SETH SCHIESEL
Published: April 27, 2011

SIGN IN TO E-MAIL
PRINT
REPRINTS

When Sony designers made the PlayStation 3, they lavished attention on the hardware. And when their shiny new machine was finished, Sony executives basically said, "Hmm, we'd better figure out an online system for this thing." So they tacked one on.

Enlarge This Image

Thomas Peter/Reuters

Sony lavished attention on the PlayStation 3 hardware, creating the online part last.

Related

It shows.

On Tuesday I was among the more than 70 million customers of Sony's PlayStation Network and Qriocity music and video service to receive an appalling e-mail essentially saying that everything the company knew about us — where we live, when we were born, our log-ins and passwords, and possibly more — had been ripped off. As an admission of online ineptitude, it could hardly be more thorough.

It could get worse.

"If you have provided your credit card data through PlayStation Network or Qriocity," Sony said, "out of an

Sony Playstation Network

PSN Users Reporting Hundred of Dollars Stolen From Them | VGN365

PSN Users Reporting Hundred o...

http://vgn365.com/2011/04

PSN Users Reporting Hundreds of Dollars Stolen From Them

Published on April 26, 2011, by Jim - Posted in PS3 44

After the shock announcement regarding Sony saying that every single PlayStation Network account may have been compromised, reports are starting to come in pointing towards the fact that PSN users are having hundreds of dollars stolen from their account this past weekend.

One PlayStation Network user, Josh Webb, emailed us after seeing the news regarding a user having $600 taken from him, stating:

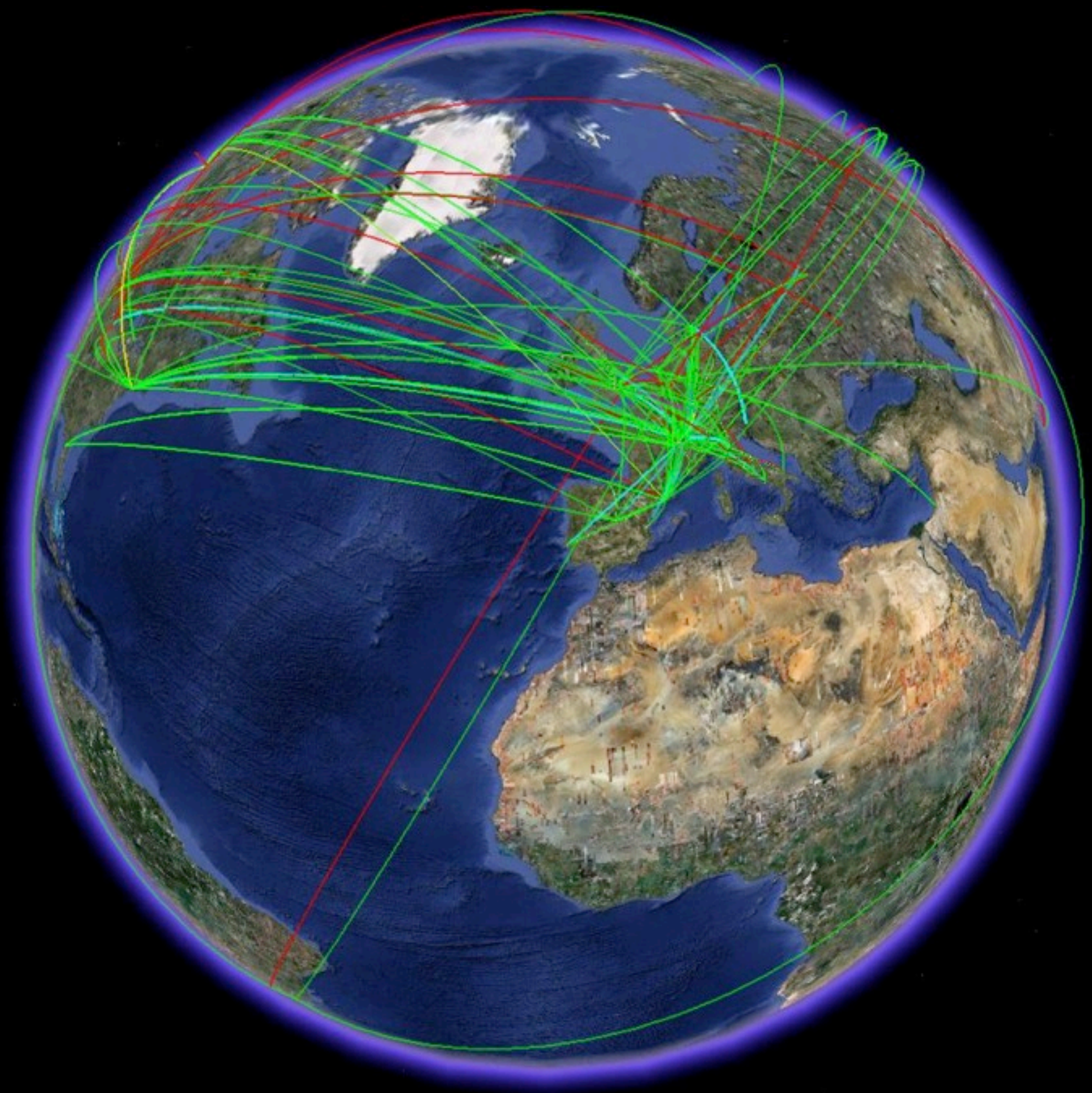
> *A total of $300 was taken from my debit card on Saturday. However, my bank called me*

Newpapers also get attacked

HEPiX/Academic community

- 4 security incidents handled in WLCG since last meeting
  - 1 Web application attack
  - 3 involving SSH
- SSH remain the primary intrusion vector
  - Passwords+Keys: sniffed/copied and re-used by attackers
  - The vast majority of Linux incidents at CERN results from compromised account at other sites

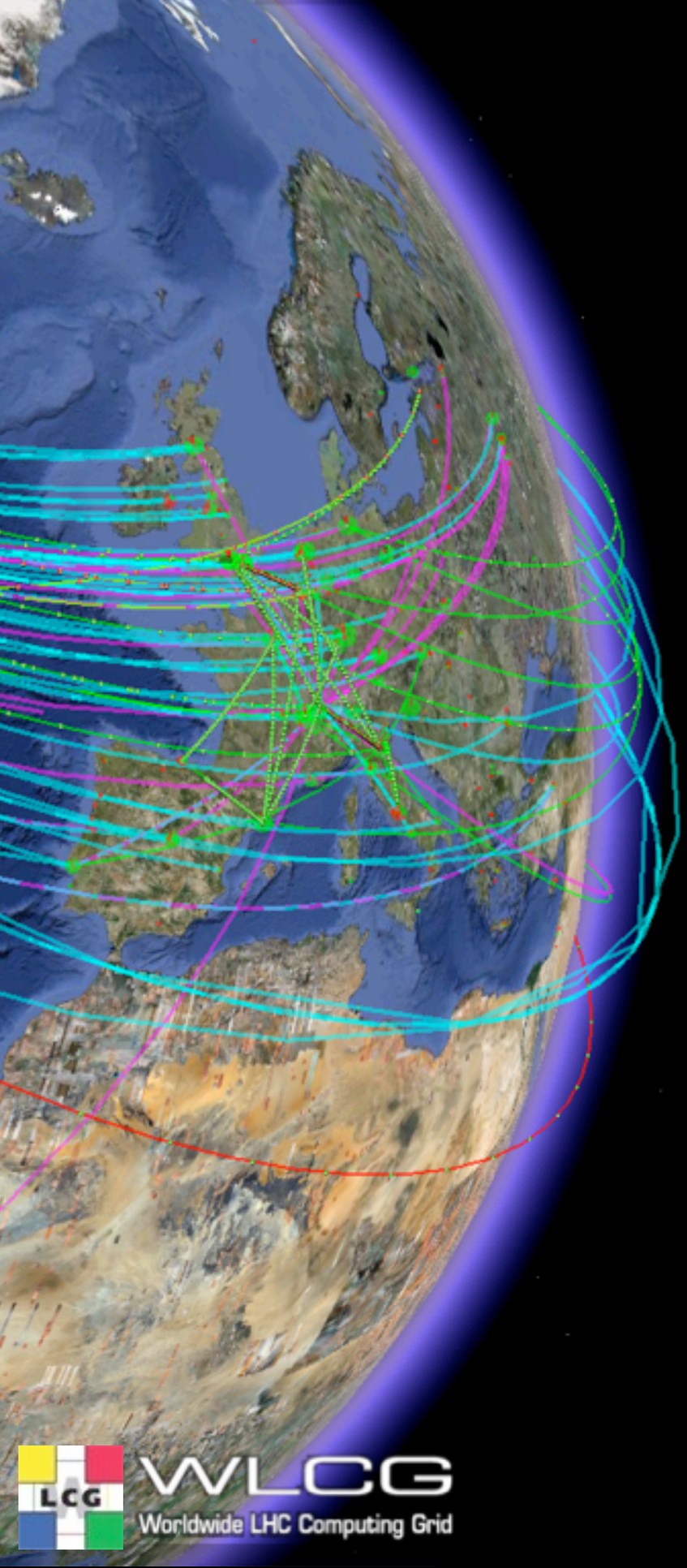
HEPiX/Academic community



WLCG
Worldwide LHC Computing Grid

HEPiX/Academic community

- 4 security incidents handled since last meeting
  - 1 Web application attack
  - 3 involving SSH
- SSH remain the primary intrusion vector
  - Passwords+Keys: sniffed/copied and re-used by attackers
  - The vast majority of Linux incidents at CERN results from compromised account at other sites
  - Pilot Yubikey service at CERN seen as a success
    - Further tests are currently being conducted with other groups in IT
- Identity federation
  - Will quite likely have an impact on such SSH incidents
    - Better traceability and unified blocking of compromised accounts?
    - Workflow remains TBD
  - Identity Federation Workshop - 9-10 June 2011, CERN
    - https://indico.cern.ch/conferenceTimeTable.py?confId=129364



(Not so) recent Linux rootkit trends

WLCG
Worldwide LHC Computing Grid

Rootkits

- Kernel-level rootkits
  - Modify kernel structures (syscall table, IDT, etc.)
  - Malicious codes is loaded directly in the kernel
    - Loadable Kernel Modules
    - Direct /dev/mem access (patch kernel on-the-fly)
  - Reference implementation (SuckIT) proposed in Phrack in 2001
    - http://www.phrack.org/issues.html?id=7&issue=58
    - Not new!
  - Phalanx 2 used against the academic community

Rootkits

- Debug Register Rootkit (DR rookits)
  - Use CPU Debug Registers to alter system behavior
    - No modification of the kernel structures (system call table etc.)
    - Just place a breakpoint at a key point, linked to a malicious handler
  - Described in Phrack in 2008
    - http://www.phrack.org/issues.html?issue=65&id=8
  - Reference implementation (DR. rootkit) proposed by Immunity
    - http://www.immunitysec.com/resources-freesoftware.shtml
  - Variants used against the academic community since 2010

Rootkit checkers

- Signature-based:
  - rkhunter, chkrootkit, etc.
  - Very efficient against known versions of rootkits
  - Very easy to use
  - Not so efficient if the rootkit is open source or maintained
    - E.g. There are at least 10+ Phalanx updates
- snapshot and check:
  - Samhain, Tripwire, Zeppoo, the99lb, etc.
  - Good results, but often require significant work
- Little/no public rootkit checkers would detect DR rookits
  - OSSEC's rootcheck could detect a sample discovered last year (hidden process + wrong link count on the filesystem)

Strategy?

- Good ways to manage these risks at a reasonable cost?
  - Strict access control of users (multifactor is a significant help)
  - Tight security patching policy
  - Periodic reinstallation of the nodes
  - Prevent users to escalate as root (system hardening)
  - Implement in-depth monitoring of the system
  - Detailed log trails (remote syslog)
  - Good incident response capability
  - Ability to manage incidents as part of normal operations

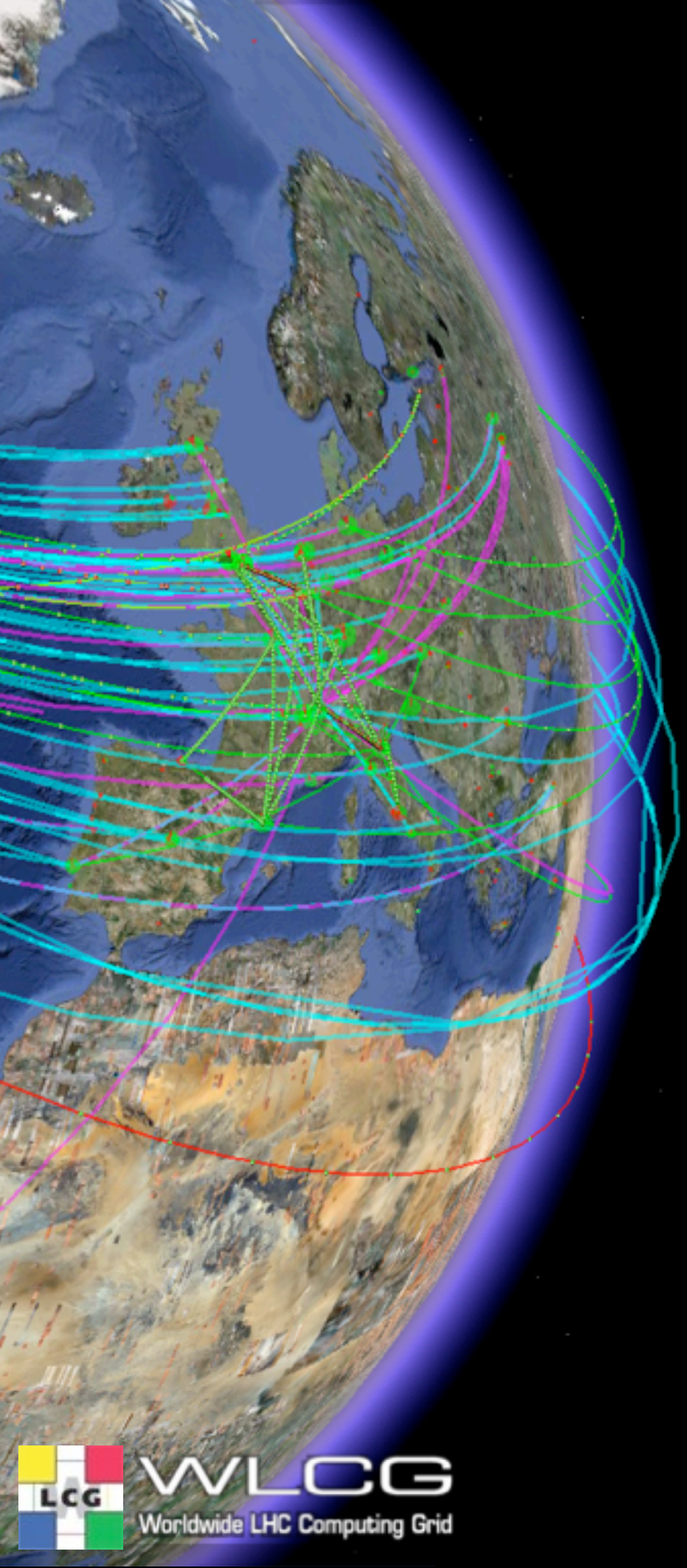
- As secure as the weakest link!

TTY hijacking

- TTY hijacking a growing concern
  - Again, not a new technique
  - Works when the attacker has root access on the client:
    - Wait for the victim to SSH to a remote site
    - Victims authenticate with password (+Yubikey) (+Blood sample)
    - SSH session is open and active with the remote site
    - Attacker hijacks the session and connects interactively with the remote site
  - Recent versions of Phalanx feature a built in TTY hijacker
    - Several implementations in the wild (Dirtty, etc.)
  - No real protection against TTY Hijacking

TTY hijacking

Demo



Virtualisation

WLCG
Worldwide LHC Computing Grid

Virtualisation

- Virtualisation brings no major changes to the security model

Virtualisation

- Two main approaches from the security point of view?
- Virtualised infrastructure
  - Transparent to the user (e.g. virtual batch nodes)
  - Typically a local service
  - Image must be trusted
  - The security of this image should be identical to any other host
    - Patching, hardening, privileges dropping, monitoring, access control, traceability, etc.
  - Good integration with the traditional fabric management tools essential to ensure security

Virtualisation

- Virtualised payload
  - Image may be provided by users (e.g. “Atlas WN image”)
  - Aimed at being shared across multiple sites
  - The security of this image should be identical to any other binary
    - No control over it, don’t trust it, maybe malicious and must be contained
  - May provide additional segregation between users
  - But may involve greater exposure:
    - Difficult/impossible to patch - must rely on users
    - More code, additional complexity compared to traditional binaries
      - More prone to vulnerabilities
  - Probably a good idea to retain control over the access to the VMs
    - Authentication remains under the control of the site
    - E.g. via dedicated SSH gateways

Virtualisation

	Virtualised infrastructure	Virtualised payload
Needs to be trusted?	YES	NO
Needs to be controlled?	YES	NO
Expected to be malicious?	NO	YES
Sharing with other sites?	NO (?)	YES

Virtualisation

- Also at risk of being affected by (security) incidents at the cloud services provider
  - A small loss for Service-Now may be a disaster for some customers

Amazon's Cloud Crash Disaster Permanently Destroyed Many Customers' Data

Henry Blodget | Apr. 28, 2011, 7:10 AM | 52,330 | 53

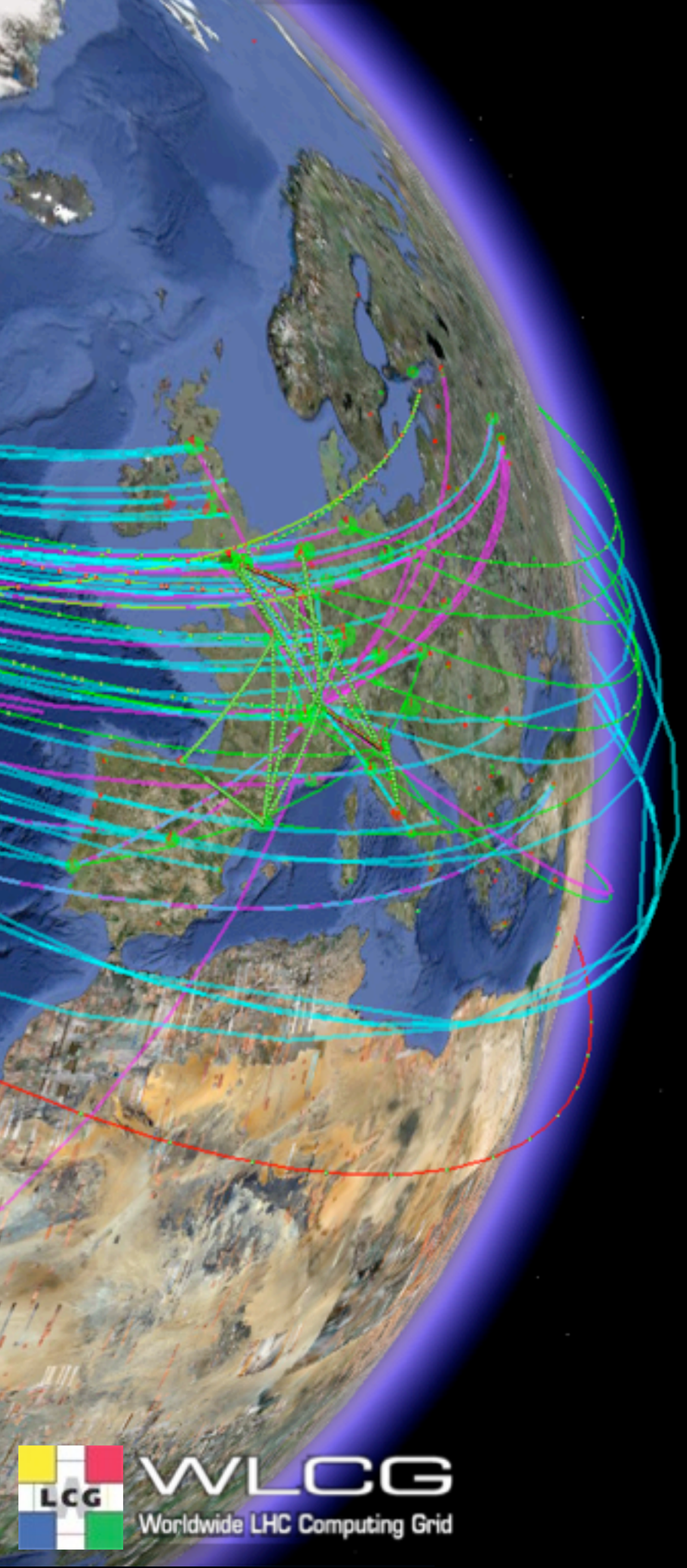
Tweet Email A A A

In addition to taking down the sites of dozens of high-profile companies for hours (and, in some cases, days), Amazon's huge EC2 cloud services crash permanently destroyed some data.

The data loss was apparently small relative to the total data stored, but anyone who runs a web site can immediately understand how terrifying a prospect any data loss is.

(And a small loss on a percentage basis for Amazon, obviously, could be catastrophic for some companies).

Um...



Questions?

WLCG
Worldwide LHC Computing Grid