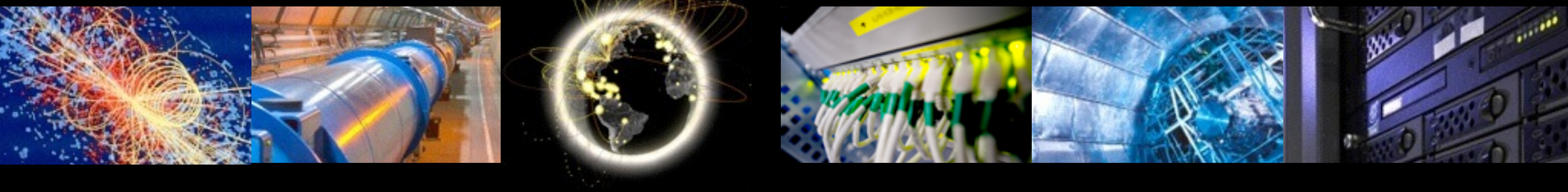
On the importance of Operational Security and Security policies

FIM4R, Frascati, 23-24 April 2014

R. Wartel, CERN



WLCG Worldwide LHC Computing Grid

Welcome!

Offering	Price
Exploit bundle rental: 24 hours 1 week 1 month	 US$25 US$125 US$400
Styx Sploit Pack rental (affects Java and Adobe Acrobat and Flash Player)	US$3,000 per month
Eleonore Exploit Pack v. 1.6.2 (for Microsoft Data Access Components [MDAC], IEpeers, SnapShot, HCP, JDT, JWS, PDF collab,collectEmailInfo, PDF SING, and Java Invoke(chain) 1.5/1.6; average reach of 10-25%)	US$2,500-3,000
Phoenix Exploits Kit v. 2.3.12 (for Internet Explorer [IE] 6 MDAC, Java Deserialize, Java GSB, PDF Collab/Printf, Adobe Flash Player 9 and 10, IEpeers, Java SMB, HCP, PDF/SWF, PDF Open, and PDF Lib TIFF)	US$2,200 per domain
Less popular and less effective bundle	US$25+
XSS exploit for Mail.ru: Active XSS exploit Passive XSS exploit Passive XSS exploit for Rambler.ru and Yandex.ru XSS exploit for Gmail.com	 US$50-150 US$10-35 US$10-50 US$200
SQL exploit for a site with 50,000 visitors a day	US$100
Exploit bundle crypting service: 1-time 1-month subscription (5 times)	 US$50 US$150

Offering	Price
Cheap email spamming service	US$10 per 1,000,000 emails
Expensive email spamming service using a customer database	US$50-500 per 50,000-1,000,000 emails
SMS spamming service	US$3-150 per 100-10,000 text messages
ICQ spamming service	US$3-20 per 50,000-1,000,000 messages
1-hour ICQ flooding service	US$2
24-hour ICQ flooding service	US$30
Email flooding service	US$3 for 1,000 emails
1-hour call flooding service (i.e., typically takes call center services down)	US$2-5
1-day call flooding service	US$20-50
1-week call flooding service	US$100
SMS flooding service	US$15 for 1,000 text messages
Vkontante.ru account database	US$5-10 for 500 accounts
Mail.ru address database	US$1.30-19.47 per 100-5,000 addresses
Yandex.ru address database	US$7-500 per 1,000-100,000 addresses
Skype SMS spamming tool	US$40
Email spamming and flooding tool	US$30

Offering	Price
Bots (i.e., consistently online 40% of the time)	US$200 for 2,000 bots
DDoS botnet	US$700
DDoS botnet update	US$100 per update

Offering	Price
Fake site	US$5-20
Fake WebMoney Keeper	US$50
1-year prepaid phishing domain (e.g., vkOntakte.net.ua and vkontaktu.net.ua)	US$50 each

Offering	Price
Linux rootkit that replaces ls, find, grep, and other commands	US$500
Windows rootkit that operates at the driver level and that allows the download of specially assembled drivers	US$292

Offering	Price
Russian and other Commonwealth of Independent States (CIS) country passport	US$2-5
European passport	US$5
Document rework service	US$15-20
Credit card rework service	US$25

Source: TrendsMicro

Media

Hacker breached data at Harvard University

Information of about 10,000 of last year's applicants are vulnerable

Associated Press
updated 2:46 p.m. ET March 13, 2008

CAMBRIDGE, Mass. - Harvard University is notifying thousands of graduate students and applicants that their personal information may have been exposed by a data breach.

The Ivy League school says a computer hacker gained entry to its server last month.

Harvard says about 10,000 of last year's applicants may have had their personal information compromised, with 6,600 having their Social Security numbers exposed.

USA TODAY

Click to Print

Hacker teams breach powerful research networks

By Anick Desjanun, Associated Press

NEW YORK — Hackers have broken into some of the world's most powerful computer clusters in recent weeks in an apparently coordinated cyberattack targeting research and academic institutions.

Although officials sought Wednesday to downplay the seriousness of the threats, some security experts warned that such a break-in could potentially enable a seriou attack on the Internet.

Stanford University, the National Center for Atmospheric Research, the San Diego Supercomputer Center and the University of Illinois' National Center for

Oxford students hack university network "in minutes"

"We just did it for the kids"

By Jo Best, 19 July 2004 13:30

NEWS Two Oxford University students are facing suspension and a fine after they hacked into the University computer system to s was to access supposedly secure personal details.

The pair used free software that they downloaded and managed to access a database of university pupils' email passwords and oth as well as spy on MSN Messenger conversations and look at some of the CCTV network. Gaining access to the system took only m

Media

- High energy physics also suffered from some attacks + media coverage

NEWS

Watch ONE-MINUTE WORLD NEWS

News Front Page

Africa

Americas

Asia-Pacific

Europe

Middle East

South Asia

UK

Business

Health

Science & Environment

Page last updated at 11:24 GMT, Monday, 15 September 2008 12:2

E-mail this to a friend Printable version

'Big bang' experiment is hacked

Part of the computer system of the Large Hadron Collider (LHC) was hacked into as the world's most powerful physics experiment got under way.

A group calling itself the "Greek Security Team" hacked into a computer connected to the system last Wednesday.

Telegraph.co.uk

Home | News | Sport | Business | Travel | Jobs | Motoring | Telegraph TV

Earth home
Earth news
Earth watch
Comment

Hackers infiltrate Large Hadron Collider systems and mock IT security

ZDNet Government

Richard Koman

Get ZDNet Government via: Mobile RSS Email Alerts Bios: Richard's Bio

Pick a blog category view

September 12th, 2008

Hackers deface LHC site, came close to turning off particle detector

Posted by Richard Koman @ September 12, 2008 @ 8:35 AM

Categories: Security, International, Science

Tags: CERN, Hacker, Content Management System, Hacking, Content Management, Security, Enterprise Software, Software, Richard Koman

TÉ. Des informations confidentielles circulent sur Internet. Une panne informatique permet à n'importe qui d'accéder, privée des physiciens et à

CERN est une véritable passoire

Martin Stoll, «SonntagsZeitung»
Adaptation: Laurent Duvanel

On trouve de tout: des rapports internes, des notes sur des expériences en cours, et une partie de la correspondance privée du CERN. Ces documents sont accessibles via le réseau informati-

ou un manuscrit s
Dans une lettre, un s
que son supérieur lui a
augmentation: «J'ob
mon classement n'est
port avec les témoig
time et de considérat
suis gratifié.». On tro
les instructions de séc

Scientifiques peu attenti

WLCG Worldwide LHC Computing Grid

LCG

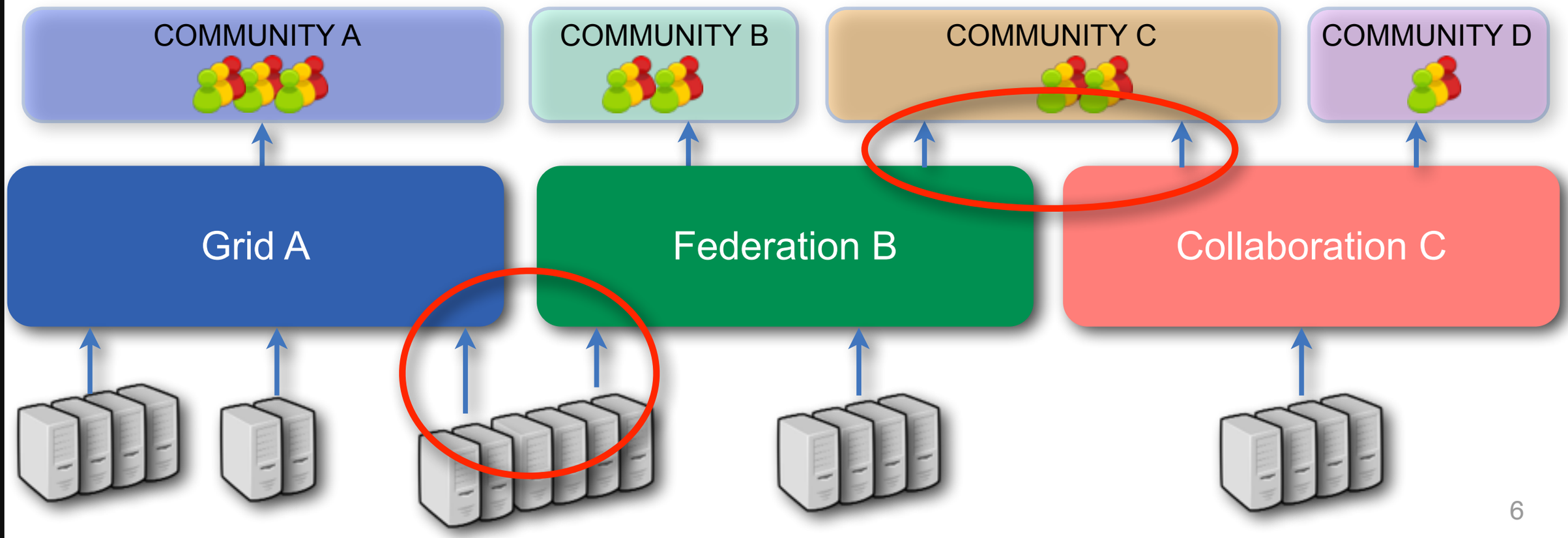
Typical attack

- Typical SSH attack in the academic/research 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

- Payloads: SPAM, phishing, bitcoin, serving malicious iframes, exploit kits, etc.

Attack surface

- Significant increase in collaboration between organizations
  - Shared users
  - Shared resources
  - Transparent access
- Possible incident propagation vector
  - Service providers may share their resources across different unrelated grids and user communities
  - Different infra. may provide services to the same community



Recent/current incidents

- WLCG managed ~80 security incidents in the last 8 years
  - Part of normal operations, business as usual
  - Most incidents are affecting multiple administrative domains

- **Windigo - Global scale - this happens now!**
  http://www.welivesecurity.com/wp-content/uploads/2014/03/operation_windigo.pdf
  - Involves sophisticated Windows, Linux very stealth malware
  - Apache, Nginx and Lighttpd, OpenSSH, etc.
  - Operates across complex fast-flux malicious infrastructure
  - Over 25,000 compromised **servers**
  - 35 milion spam messages per day
  - Many in the academic / research sector!

Soon or later...

- Each community/federation/SP/IdP has been or will be affected by a security incident
- Part of normal operations, just need to ensure
  - It is "cheap" to deal with
  - The overall infrastructure is not affected
- It is essential to prepare for this event to reduce its:
  - Impact (appropriate & timely response, etc.)
  - Likelihood (prevention, etc.)
- Share information
- Report incidents
- We are as strong as our weaker link!

WLCG Worldwide LHC Computing Grid

Inter-federation security

- No minimal requirements on IdPs poses unacceptable risks for our communities
  - **Little/no control over incidents**
  - **Difficult to justify to the funding agencies / media**
- Impossible to impose practices on eduGAIN participants
  - No minimal requirements for IdPs
  - No requirement to help/share/respond during security incidents
  - No process to make sure you will be informed of incidents, compromised IdPs, etc.
  - No incident reporting channel
  - No identity banning process

WLCG Worldwide LHC Computing Grid

LCG

Inter-federation security

- Bilateral agreements needed with all the IdPs/federations
  - Each community will have to repeat this
- IdPs would need to assert their security practices
  - Metadata, manual registry, etc.
- Communities would need to maintain their own channels to collaborate

- Please let us NOT do this

- In order to operate across federations, essential to have:
  - **Strong operational collaboration**
  - **Common policy standards & minimal requirements**

Strong operational collaboration

- Understand the source of incidents to prevent re-occurrence

- People need to trust others have the means to:
  - Respond to email or phone and will collaborate
  - Contact affected users under its governance
  - Deal with confidential information
  - Follow whatever incident response procedure is in place
  - etc.

- Participate in incident response all on a best effort basis
  - Basically: behave as a responsible citizen

- Need common or compatible policies there

Security for collaborations

- Sharing a common security policies is difficult
  - Different funding agencies, scope, internal organisation, terms
- BUT we share services, federations, users, and ultimately we share security incidents
  - Already worked on common incidents with some of you!
- How could we converge?
  - Could we benefit from the experience in the community?
  - NREN CSIRTs have collaborated for many years
  - Several infrastructure, projects, and collaboration are also sharing minimal requirements

Security for collaborations

- SCI started this work some time ago
- EGI, OSG, PRACE, EUDAT, CHAIN, WLCG, and XSEDE

- SCI is developing a framework to
  - Enable interoperation of collaborating infrastructures
  - Manage operational security risks
  - Build trust and develop policy standards for collaborations
  - Especially in cases where we cannot just share identical security policy documents

- http://cern.ch/go/rhP8
  - SCI is not tied to any group, organisation or body

Security for collaborations

- On incident response, each infrastructure must have the following:
  - Security contact information for all service providers, resource providers and communities together with expected response times for critical situations
  - A formal Incident Response procedure. This must address: roles and responsibilities, identification and assessment of an incident, minimizing damage, response & recovery strategies, communication tools and procedures
  - The capability to collaborate in the handling of a security incident with affected service and resource providers, communities, and infrastructures
  - Assurance of compliance with information sharing restrictions on incident data obtained during collaborative investigations. […]

Security for collaborations

- On traceability, each infrastructure must have the following:
  - [TR1] Traceability of service usage, by the production and retention of appropriate logging data, to identify the source of all actions as defined above (cf. document)
  - [TR2] A specification of the data retention period, consistent with local, national and international regulations and policies
  - [TR3] A specification of the controls that the resource provider implements to achieve the goals of [TR1]

Security for collaborations

- Would it be useful to continue and extend this work for inter-federation?
  - Or should we start something new?

- Goals
  - Promote common minimal requirements for all FIM4R communities
  - Jointly find a way that they are followed by the IdPs