Status and challenges of security in distributed computing

Sebastian Lopienski
CERN Deputy Computer Security Officer
(with input from S.Lueders and R.Wartel)

ISGC 2011, 台北 台湾
Fancy learning some Chinese?

女  woman

安  security (woman under a roof)
Status and challenges of security in distributed computing

Sebastian Lopienski
CERN Deputy Computer Security Officer

(with input from S.Lueders and R.Wartel)

ISGC 2011, 台北 台湾
Outline

• Why we are attacked
• Typical attacks
  • ... and defense
• More on virtualization
• ... and cloud computing
Why we are attacked?
Global attention

“I'm contacting you due several security flaws in the structure about the Large Hadron Collider, including the website which seems to be connected somehow with the core of the system and/or the LHC itself. [...] We are interested in solve this issue, and cover this with the press if it wouldn't represent an issue for you.”

[Webpage image showing a news article from Telegraph.co.uk about hackers infiltrating the Large Hadron Collider systems and mock IT security, authored by Roger Highfield, Science Editor, last updated 4:01pm BST 12/09/2008]
How serious are the risks?

Did you notice electricity cables inside the pool?
SSH attacks... since 2008
Patching

Unpatched machine?
Vulnerability management

Critical vulnerabilities:
- CVE-2009-2692
- CVE-2009-2698
- CVE-2009-3547
- CVE-2010-3081
- CVS-2011-1017
- etc.

... all allow for privilege escalation

BTW: is all that software needed?
Protect *and* detect

**Increased sophistication**
- e.g. debug register (Phalanx 2.5f)
- common checkers (rkhunter, chrootkit) don’t detect them

Steal users’ credentials

Install a rootkit
Better authentication needed

Authentication is hard when users are many and distributed
• and SSH passwords or keys are not enough!

One-time passwords (OTP)
• Yubikeys to be used at CERN?
• other: SMS, dedicated OTP mobile apps
Multifactor authN: something you know + something you have

In the future: Federated identities across HEP labs

Steal users’ credentials
Collaboration is crucial

Collaboration between sites - sharing:
  - vulnerability advisories
  - incident information
  - good practices
  - tools
  - policies
  - etc.

Attack other hosts/sites

Steal users’ credentials
Web application security

• Vulnerable Web application are often attacked

• What to do?
  – patch/update (for external software)
  – train developers (for in-house software)
  – limit exposure
  – harden servers
  – use Web application firewalling
  – perform Web application scanning
Web application scanning

Crawl results - click to expand:

- **http://pcitdi72/**
  - Code: 403, length: 398, declared: text/html, detected: application/xhtml+xml, charset: UTF-8 [show trace +]
  - Unknown form field
    1. Code: 200, length: 15
      Memo: comment
  - New 404 signature set
    1. Code: 200, length: 15
      Memo: Apache/2.2.3

- **index.php**
  - Code: 200, length: 950, declared: text/html, charset: UTF-8 [show trace +]
    - Comment
      Memo: response suggests arithmetic evaluation on server side
  - **id=1**
    Memo: injected "<sfi,..." tag seen in HTML
  - **id=2**
    Memo: injected "<sfi,..." tag seen in HTML

- **SQL injection vector**
  Memo: response suggests arithmetic evaluation on server side

- **XSS vector in document body**
  Memo: injected "<sfi,..." tag seen in HTML (from previous scans)
  Memo: injected "<sfi,..." tag seen in HTML

- **HTML form with no apparent XSRF protection**
Virtualization

• **Complexity** doesn’t help security...

  but from the network point of view, a VM is just another host

• Images trusted or provided by users? Image distribution? Patching? Traceability? Forensics?
Cloud Computing

Can you do homework as a service?

From www.cloudtweaks.com / David Fletcher
Experiences with cloud services

• AngelsAndDemons.cern.ch
  – incident? no access to logs
• cern.service-now.com
  – but behind CERN SSO
• gmail.com
  – some prefer it over CERN mailboxes
  – ... and make us partially blind
Clouds and security

From www.cloudtweaks.com / David Fletcher
(Commercial) clouds and security

6.3. Nonexclusive Rights. The rights granted by Amazon in this Agreement with respect to the Amazon Properties, the Marks and the Services are nonexclusive, and Amazon reserves the right to: (i) itself act as a developer of products or services related to any of the products that you may develop in connection with the Amazon Properties or via your use of the Services; and (ii) appoint third parties as developers or systems integrators who may offer products or services which compete with Amazon or your Application.

7. Downtime and Service Suspensions; Security
7.1. Downtime and Service Suspensions. In addition to our rights to terminate or suspend Services to you as described in Section 3 above, you acknowledge that: (i) your access to and use of the Services may be suspended for the duration of any unanticipated or unscheduled downtime or unavailability of any portion or all of the Services for any reason, including as a result of power outages, system failures or other interruptions; and (ii) we shall also be entitled, without any liability to you, to suspend access to any portion or all of the Services at any time, on a Service-wide basis: (a) for scheduled downtime to permit us to conduct maintenance or make modifications to any Service; (b) in the event of a denial of service attack or other attack on the Service or other event that we determine is a threat to our own services or other customers if the Service is not suspended.

7.2. Security. We strive to keep Your Content secure, but cannot guarantee that we will be successful at doing so, given the nature of the Internet. Accordingly, without limitation to Section 4.3 above and Section 11.5 below, you acknowledge that you bear sole responsibility for adequate security, protection and backup of Your Content and Applications. We strongly encourage you, where available and appropriate, to (a) use encryption technology to protect Your Content from unauthorized access, (b) routinely archive Your Content, and (c) keep your Applications or any software updates. We will have no loss of any of Your Content or Applications.

Still 100% responsible for security

Loss of ownership
Loss of availability
Loss of guarantees
Can we use security tools in the cloud?

FAIL
IaaS, PaaS, SaaS... Crime aaS?
Conclusions

• Grid and cloud computing offer increased productivity
• ... but security risks must not be neglected
• A lot of challenges ahead
  – increased sophistication of vulnerabilities & attacks
  – OTP, multifactor authN, federated identities
  – virtualization/image security
  – cloud security
Thank you / 谢谢

Any questions?