PAKITI
Patching Status System

A Race for Security: Identifying Vulnerabilities on 50 000 Hosts Faster than Attackers

Michal Procházka¹, Daniel Kouřil¹, Romain Wartel², Christos Kanellopoulos³, Christos Triantafyllidis³

¹CESNET, ²CERN, ³AUTH

ISGC 2011, Taipei
Outline

• The problem

• Vulnerability Management

• Pakiti

• Statistics

• Future
The Problem

- Infrastructure is weak as its weakest point
  - One hacked worker node is a big danger for the whole infrastructure

- Attackers usually exploits know vulnerabilities
  - Number of attacks made by real hackers are very low
  - Robot attacks – botnes, script kiddies
  - Software updates are essential

- How to check if a host is properly patched?
  - It is easy on the desktop machine

- How to check this on EGI infrastructure?
Vulnerability Management

- Common Vulnerability and Exposures (CVE)
  - Each vulnerability has assigned an unique number

- Open Vulnerability and Assessment Language (OVAL)
  - Defines conditions under which the vulnerability is applicable

- OS and application vendor software repositories
  - Usually provides at least two repositories, for security updates, for other updates (features, ...)

- Patches shouldn't be applied automatically
Pakiti

- Originally developed by Steve Traylen
  - Current version uses different model for getting and processing the data

- Tool for monitoring patching status on not only distributed infrastructure
  - Provides overview of the software versions on the monitored hosts

- Client-server architecture with lightweight client

- Correlates installed packages with the vulnerability definitions
Pakiti Client

- Bash script running under the user rights
  - In compare to the original version, which requires root privileges

- Gathers the list of installed packages, kernel version and hostname
  - Using generic OS tools to get these data

- Sends data over HTTPs to the Pakiti server(s)
  - Supports server or mutual authentication

- No processing is done on the client
Pakiti Vulnerability Sources

- Pakiti regularly synchronizes its database with the vulnerability sources
  - OVAL definitions (RedHat)
  - vendor's repositories (SL, SLC, CentOS, ...)

- Sources can be configured using web GUI
Pakiti Data Processing

• Each host report is stored in the DB

• Each package version is compared with the version from the vendor's repository and OVAL definitions
  • The results are also stored in the DB

• Synchronous and asynchronous processing
  • Synchronous mode provides results in realtime
  • Asynchronous mode is suitable for large deployments
    • Data are processed on regular basis (e.g. once a day)
Pakiti GUI

- Web based GUI which provides
  - List of hosts
  - List of domains
  - List of sites (EGI case)
  - List of installed packages for each host
  - Required version and list of CVEs for each package if applicable

- Searching hosts by
  - package
  - CVE

- Configuration: sources settings, ACLs
### Pakiti GUI – List of Hosts

**Pakiti** - Patching Status System

**Navigation:** CVE by site | Host by package | Hosts by tags | Hosts | Sites | Settings | Exceptions | CVE Tags | ACL

**Show:** vulnerable, unpatched, all, not reporting

**Order by:** tag | host | time | kernel | os

**Select tag:** all

**Expand all +**

**Tag:** Nagios +

<table>
<thead>
<tr>
<th>Security</th>
<th>Other</th>
<th>CVEs</th>
<th>Hostname</th>
<th>OS</th>
<th>Current kernel</th>
<th>Last report</th>
<th>Ops</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>3</td>
<td></td>
<td>Scientific Linux 5.5</td>
<td>2.6.18-194.17.4.el5</td>
<td>31.10.10 21:15</td>
<td>X</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>3</td>
<td></td>
<td>Scientific Linux 5.5</td>
<td>2.6.18-194.17.4.el5</td>
<td>1.11.10 14:43</td>
<td>X</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>3</td>
<td></td>
<td>Scientific Linux 5.5</td>
<td>2.6.18-194.17.4.el5</td>
<td>31.10.10 04:23</td>
<td>X</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>3</td>
<td></td>
<td>Scientific Linux 5.5</td>
<td>2.6.18-194.17.4.el5</td>
<td>1.11.10 08:57</td>
<td>X</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>3</td>
<td></td>
<td>Scientific Linux 5.5</td>
<td>2.6.18-194.17.4.el5</td>
<td>1.11.10 14:45</td>
<td>X</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>3</td>
<td></td>
<td>Scientific Linux 5.5</td>
<td>2.6.18-194.17.4.el5</td>
<td>31.10.10 10:21</td>
<td>X</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>3</td>
<td></td>
<td>Scientific Linux 5.5</td>
<td>2.6.18-194.17.4.el5</td>
<td>1.11.10 02:43</td>
<td>X</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>3</td>
<td></td>
<td>Scientific Linux 5.5</td>
<td>2.6.18-194.11.4.el5</td>
<td>31.10.10 03:05</td>
<td>X</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>3</td>
<td></td>
<td>Scientific Linux 5.5</td>
<td>2.6.18-194.11.4.el5</td>
<td>31.10.10 03:01</td>
<td>X</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>3</td>
<td></td>
<td>Scientific Linux 5.5</td>
<td>2.6.18-194.11.4.el5</td>
<td>31.10.10 13:02</td>
<td>X</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>3</td>
<td></td>
<td>Scientific Linux 5.5</td>
<td>2.6.18-194.11.4.el5</td>
<td>31.10.10 12:59</td>
<td>X</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>122</td>
<td></td>
<td>Scientific Linux CERN 5.4</td>
<td>2.6.18-194.11.3.el5,cve20103081</td>
<td>31.10.10 23:00</td>
<td>X</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>30</td>
<td></td>
<td>Scientific Linux 5.5</td>
<td>2.6.18-194.11.4.el5</td>
<td>1.11.10 05:26</td>
<td>X</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>30</td>
<td></td>
<td>Scientific Linux 5.5</td>
<td>2.6.18-194.11.4.el5</td>
<td>1.11.10 12:06</td>
<td>X</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>30</td>
<td></td>
<td>Scientific Linux 5.5</td>
<td>2.6.18-194.11.4.el5</td>
<td>31.10.10 01:06</td>
<td>X</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>30</td>
<td></td>
<td>Scientific Linux 5.5</td>
<td>2.6.18-194.11.4.el5</td>
<td>31.10.10 18:06</td>
<td>X</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>30</td>
<td></td>
<td>Scientific Linux 5.5</td>
<td>2.6.18-194.11.4.el5</td>
<td>31.10.10 12:06</td>
<td>X</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>5</td>
<td></td>
<td>CentOS Linux 5</td>
<td>2.6.18-194.17.4.el5</td>
<td>1.11.10 10:57</td>
<td>X</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>7</td>
<td></td>
<td>CentOS Linux 5</td>
<td>2.6.18-194.17.4.el5</td>
<td>1.11.10 04:14</td>
<td>X</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>5</td>
<td></td>
<td>CentOS Linux 5</td>
<td>2.6.18-194.17.4.el5</td>
<td>1.11.10 16:13</td>
<td>X</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>65</td>
<td></td>
<td>Scientific Linux 5.3</td>
<td>2.6.18-194.11.4.el5</td>
<td>1.11.10 10:51</td>
<td>X</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>24</td>
<td></td>
<td>Scientific Linux 4.7</td>
<td>2.6.9-89.29.1.EL</td>
<td>1.11.10 04:42</td>
<td>X</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>24</td>
<td></td>
<td>Scientific Linux 4.7</td>
<td>2.6.9-89.29.1.EL</td>
<td>1.11.10 10:41</td>
<td>X</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>140</td>
<td></td>
<td>Scientific Linux 4.6</td>
<td>2.6.9-89.0.16 El smn</td>
<td>1.11.10 11:36</td>
<td>X</td>
</tr>
</tbody>
</table>
## Pakiti GUI – Host's details

### Pakiti - Patching Status System

**Navigation:** CVE by site | Host by package | Hosts by tags | Hosts | Sites | Settings | Exceptions | CVE Tags | ACL

**Selected host:** [Host's name]

**Tag:** Nagios

**View:** CVEs

### Host/Package name | Installed version | Required version (Security repository, Main repository) | CVEs (Critical, Important, Moderate, Low) Show/Hide CVEs

<table>
<thead>
<tr>
<th>Package name</th>
<th>Installed version</th>
<th>Required version</th>
<th>CVEs</th>
</tr>
</thead>
<tbody>
<tr>
<td>acpid</td>
<td>0:1.0.4/9.el5</td>
<td>0:1.0.4/9.el5_4.2</td>
<td>CVE-2009-4033</td>
</tr>
<tr>
<td>automate</td>
<td>0:1.9.6/2.1</td>
<td>0:1.9.6/2.3.el5</td>
<td>CVE-2009-4029</td>
</tr>
<tr>
<td>automate14</td>
<td>0:1.4p6/13.el5</td>
<td>0:1.4p6/13.el5_1</td>
<td>CVE-2009-4029</td>
</tr>
<tr>
<td>automate15</td>
<td>0:1.5/16</td>
<td>0:1.5/16.el5_2</td>
<td>CVE-2009-4029</td>
</tr>
<tr>
<td>automate16</td>
<td>0:1.6.3/8</td>
<td>0:1.6.3/8.el5_1</td>
<td>CVE-2009-4029</td>
</tr>
<tr>
<td>automate17</td>
<td>0:1.7.9/7</td>
<td>0:1.7.9/7.el5_2</td>
<td>CVE-2009-4029</td>
</tr>
<tr>
<td>bind-libs</td>
<td>30:9.3.6/4.P1.el5</td>
<td>30:9.3.6/4.P1.el5_4.2</td>
<td>CVE-2009-4022 CVE-2010-0097 CVE-2010-0290 CVE-2010-0382</td>
</tr>
<tr>
<td>bzip2-libs</td>
<td>0:1.0.3/4.el5_2</td>
<td>0:1.0.3/6.el5_5</td>
<td>CVE-2010-0405</td>
</tr>
<tr>
<td>cpio</td>
<td>0:2.6/23.el5</td>
<td>0:2.6/23.el5_4.1</td>
<td>CVE-2007-4476 CVE-2010-0624</td>
</tr>
<tr>
<td>cpp</td>
<td>0:4.1.2/46.el5_4.1</td>
<td>0:4.1.2/48.el5</td>
<td>CVE-2009-3736</td>
</tr>
<tr>
<td>cups-libs</td>
<td>1:1.3.7/11.el5_4.3</td>
<td>1:1.3.7/18.el5_5.7</td>
<td>CVE-2010-0540 CVE-2010-0542 CVE-2010-1748 CVE-2010-2431 CVE-2010-2941 CVE-2009-2820 CVE-2009-3553 CVE-2010-0302</td>
</tr>
<tr>
<td>dbus</td>
<td>0:1.1.2/12.el5</td>
<td>0:1.1.2/14.el5</td>
<td>CVE-2009-1189</td>
</tr>
<tr>
<td>dbus-glib</td>
<td>0:0.73/8.el5</td>
<td>0:0.73/10.el5_5</td>
<td>CVE-2010-1172</td>
</tr>
<tr>
<td>dbus-libs</td>
<td>0:1.1.2/12.el5</td>
<td>0:1.1.2/14.el5</td>
<td>CVE-2009-1189</td>
</tr>
</tbody>
</table>
Pakiti CVE Tags

• Tag can be assigned to each CVE
  • Used for further categorization

• EGI CSIRT uses two tags
  • EGI-Critical – the problem must be removed ASAP (7 day deadline)
  • EGI-High – the problem is there, but it is hard to exploit or the software is not installed by default

• Hosts can be categorized by these tags
  • Quick view on the security status of the infrastructure

• EGI CSIRT receives every day an email with list of sites vulnerable to the CVEs tagged as EGI-Critical
Pakiti CVE Exceptions

- Vulnerabilities can be fixed by the local patch
  - Added unique string to the package version
  - Pakiti is then unable to detect these local changes

- Pakiti provides list of all installed package versions for each CVE

- Pakiti administrator can add an exceptions for particular package versions
  - These package versions will be omitted
Pakiti Authorization

- Pakiti recognizes three roles: Administrator, Viewer and Anonymous viewer

- Administrator can view all results and can change the configuration

- Viewer can only see the results for his/her site(s)

- Anonymous viewer can view only results defined by the anonymous link
  - Generated link with limited scope and validity
• EGI Pakiti monitors around 1600 hosts from 306 sites with average 865 installed packages every day

• EGEE
  • First incident, it takes more than month to patch the systems - unacceptable
  • Second incident, more than 14 days – still unacceptable

• EGI
  • Several incidents – less than 7 days to patch the whole infrastructure
  • Continuous monitoring which catches anomalies
CVE-2010-4170 Number of Vulnerable Hosts

![Graph showing the number of vulnerable hosts over time for CVE-2010-4170](image-url)

- **x-axis:** Time (from 2010-11-01 to 2011-03-06)
- **y-axis:** Number of vulnerable hosts

The graph illustrates the trend of vulnerable hosts over the period specified.
Pakiti Proxy Client

• Pakiti can be integrated into the existing monitoring infrastructure (e.g. Nagios)

• Pakiti client prints results to the stdout and then monitoring system transfers them using its own mechanisms to the central monitoring server

• Data are then presented to the Pakiti Proxy Client which then sends them on behalf of the monitored host to the Pakiti server

• Each Pakiti Proxy Client has to be authorized
Pakiti Technology

- Pakiti is written in PHP, so it can be easily changed in order to fit the administrator's needs
- Uses MySQL in non-transactional mode
- Users are autheticated by the Apache web server, Pakiti does only authorization
Pakiti v3

- Reworked from scratch
- Improved performance
- Modular design
- Simplified configuration
- Unified import system for the OVALs and package repositories
- Additional access channels: RPC and CLI
- Additional output formats: CSV, XML
Thank you.

Questions?

michalp@ics.muni.cz

http://pakiti.sf.net
https://pakiti.egi.eu