PAKITI

Patching Status System

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

Michal Procházka[1], Daniel Kouřil[1], Romain Wartel[2], Christos Kanellopoulos[3], Christos Triantafyllidis[3]

[1]CESNET, [2]CERN, [3]AUTH

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 +

Security	Other	CVEs	Hostname	OS	Current kernel	Last report	Ops
3	0	3	[redacted]	Scientific Linux 5.5	2.6.18-194.17.4.el5	31.10.10 21:15	X
0	0	0	[redacted]	Scientific Linux 5.5	2.6.18-194.17.4.el5	1.11.10 14:43	X
3	0	3	[redacted]	Scientific Linux 5.5	2.6.18-194.17.4.el5	31.10.10 04:23	X
0	0	0	[redacted]	Scientific Linux 5.5	2.6.18-194.17.4.el5	1.11.10 08:57	X
0	0	0	[redacted]	Scientific Linux 5.5	2.6.18-194.17.4.el5	1.11.10 14:45	X
3	0	3	[redacted]	Scientific Linux 5.5	2.6.18-194.17.4.el5	31.10.10 10:21	X
3	0	3	[redacted]	Scientific Linux 5.5	2.6.18-194.17.4.el5	1.11.10 02:43	X
1	0	8	[redacted]	Scientific Linux 5.3	2.6.18-194.11.4.el5	31.10.10 03:05	X
1	0	8	[redacted]	Scientific Linux 5.5	2.6.18-194.11.4.el5	31.10.10 03:01	X
1	0	8	[redacted]	Scientific Linux 5.5	2.6.18-194.11.4.el5	31.10.10 13:02	X
1	0	8	[redacted]	Scientific Linux 5.5	2.6.18-194.11.4.el5	31.10.10 12:59	X
214	0	122	[redacted]	Scientific Linux CERN 5.4	2.6.18-194.11.3.el5.cve20103081	31.10.10 23:00	X
15	0	30	[redacted]	Scientific Linux 5.5	2.6.18-194.11.4.el5	1.11.10 05:26	X
15	0	30	[redacted]	Scientific Linux 5.5	2.6.18-194.11.4.el5	1.11.10 12:06	X
15	0	30	[redacted]	Scientific Linux 5.5	2.6.18-194.11.4.el5	31.10.10 01:06	X
15	0	30	[redacted]	Scientific Linux 5.5	2.6.18-194.11.4.el5	31.10.10 18:06	X
15	0	30	[redacted]	Scientific Linux 5.5	2.6.18-194.11.4.el5	31.10.10 12:06	X
0	0	5	[redacted]	CentOS Linux 5	2.6.18-194.17.4.el5	1.11.10 10:57	X
2	0	7	[redacted]	CentOS Linux 5	2.6.18-194.17.4.el5	1.11.10 04:14	X
0	0	5	[redacted]	CentOS Linux 5	2.6.18-194.17.4.el5	1.11.10 16:13	X
34	0	65	[redacted]	Scientific Linux 5.3	2.6.18-194.11.4.el5	1.11.10 10:51	X
1	0	24	[redacted]	Scientific Linux 4.7	2.6.9-89.29.1.EL	1.11.10 04:42	X
1	0	24	[redacted]	Scientific Linux 4.7	2.6.9-89.29.1.EL	1.11.10 10:41	X
8	0	140	[redacted]	Scientific Linux 4.6	2.6.9-89.0.16.EL.smp	1.11.10 11:36	X

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

Click to select host | Click to select package | Click to select CVE | Tag: Nagios | View: CVEs

Selected host: [redacted] package: all CVE: all

Host/Package name	*Installed version*	*Required version (Security repository, Main repository)*	*CVEs (Critical, Important, Moderate, Low) Show/Hide CVEs*
[redacted]	*Domain:* [redacted] *Site:* [redacted]	*Os:* Scientific Linux CERN 5.4 (x86_64)	*Kernel:* 2.6.18-194.11.3.el5.cve20103081
acpid	0:1.0.4/9.el5	0:1.0.4/9.el5_4.2	CVE-2009-4033
automake	0:1.9.6/2.1	0:1.9.6/2.3.el5	CVE-2009-4029
automake14	0:1.4p6/13	0:1.4p6/13.el5.1	CVE-2009-4029
automake15	0:1.5/16	0:1.5/16.el5.2	CVE-2009-4029
automake16	0:1.6.3/8	0:1.6.3/8.el5.1	CVE-2009-4029
automake17	0:1.7.9/7	0:1.7.9/7.el5.2	CVE-2009-4029
bind-libs	30:9.3.6/4.P1.el5	30:9.3.6/4.P1.el5_4.2	CVE-2009-4022 CVE-2010-0097 CVE-2010-0290 CVE-2010-0382
bind-utils	30:9.3.6/4.P1.el5	30:9.3.6/4.P1.el5_4.2	CVE-2009-4022 CVE-2010-0097 CVE-2010-0290 CVE-2010-0382
bzip2-libs	0:1.0.3/4.el5_2	0:1.0.3/6.el5_5	CVE-2010-0405
cpio	0:2.6/23.el5	0:2.6/23.el5_4.1	CVE-2007-4476 CVE-2010-0624
cpp	0:4.1.2/46.el5_4.1	0:4.1.2/48.el5	CVE-2009-3736
cups-libs	1:1.3.7/11.el5_4.3	1:1.3.7/18.el5_5.7	CVE-2010-0540 CVE-2010-0542 CVE-2010-1748 CVE-2010-2431 CVE-2010-2941 CVE-2009-2820 CVE-2009-3553 CVE-2010-0302
dbus	0:1.1.2/12.el5	0:1.1.2/14.el5	CVE-2009-1189
dbus-glib	0:0.73/8.el5	0:0.73/10.el5_5	CVE-2010-1172
dbus-libs	0:1.1.2/12.el5	0:1.1.2/14.el5	CVE-2009-1189

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-Criticial

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

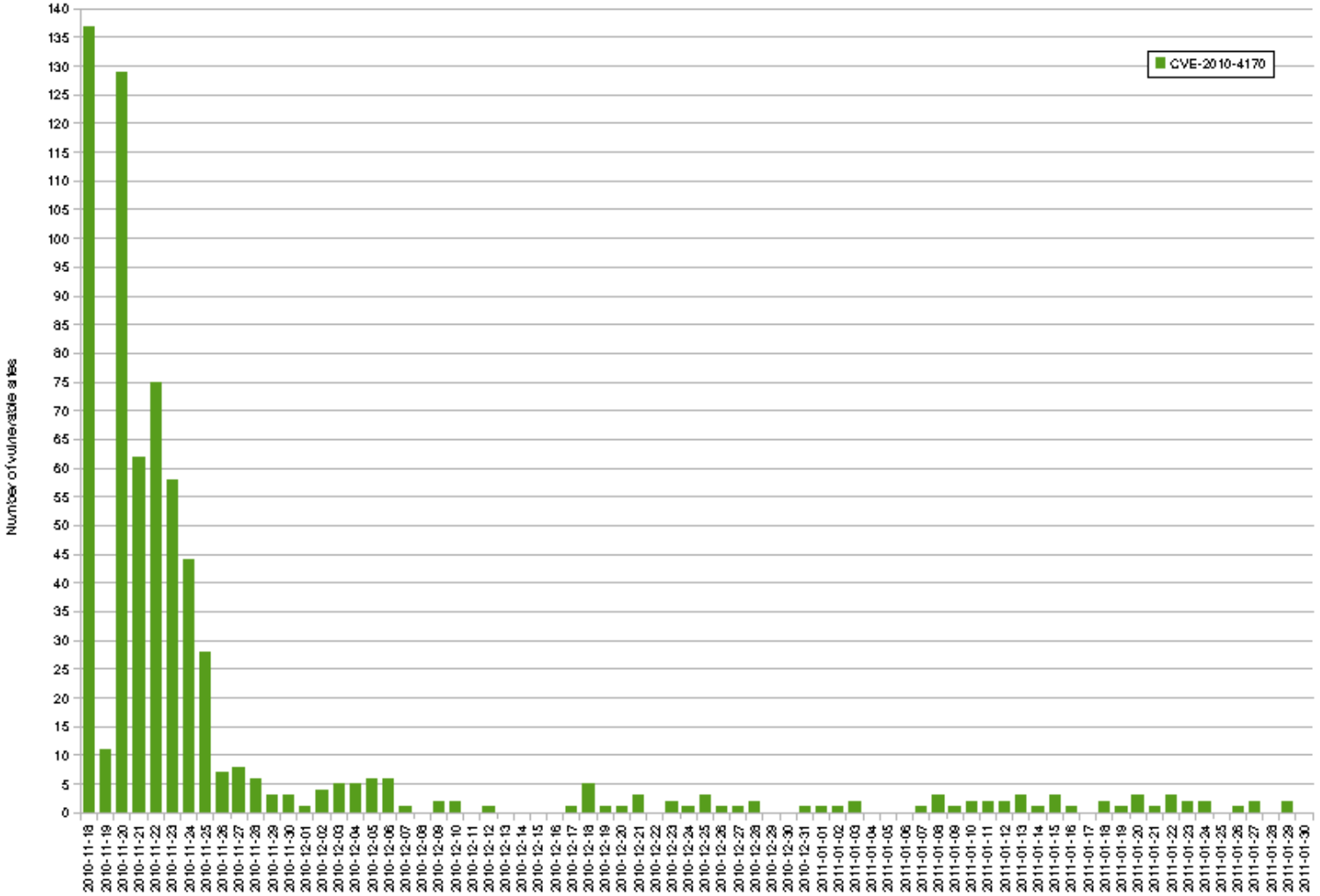
Statistics

- EGI Pakiti monitors around 1600 hosts from 306 sites with average 865 installed packages every day

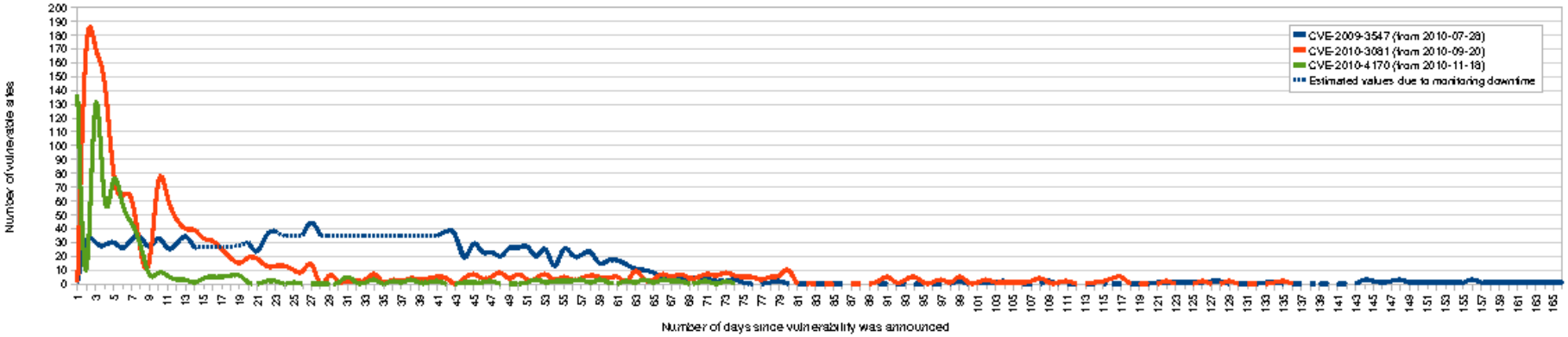
- EGEE
  - First incident, it takes more than month to patch the systems - unacceptable
  - Second incident, more than 14 days – still unacceptable

- EGI
  - Several incidents – less then 7 days to patch the whole infrastructure
  - Continuous monitoring which catches anomalies

CVE-2010-4170 Number of Vulnerable Hosts



Number of Vulnerable Hosts in Days



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