Cloud security monitoring and vulnerability management

M. Kozlovszky*, L.Kovács*, M. Törőcsik*, G.Windisch*, S.Ács*, D.Prém*, Gy. Eigner*, P.I. Sas*, T. Schubert*, V. Póserné*

* Óbuda University/John von Neumann Faculty of Informatics, Budapest, Hungary
{{kozlovszky.miklos,kovacs.levente}@nik.uni-obuda.hu

Abstract— **Cloud infrastructure becomes the primary business environment for all types of enterprises during recent years. In cloud computing security is a fundamental concern, loss of control and potential lack of trust prevent large set of potential customers to immerse in the cloud world. One of the major key problem is how one can test, monitor or measure the underlying Cloud infrastructure from user/customer space. We have developed a solution which is able to examine the infrastructure, from security point-of-views. We offer a clear, adaptable, concise and easy-to-extend framework to assess the underlying cloud infrastructure. Our developed solution is generic and multipurpose it can act as a vulnerability scanner, and performance benchmarking tool at the same time. It is virtualized, it is agent based and collects assessment information by the decentralized Security Monitor and it archives the results received from the components and visualize them via a web interface for the tester/administrators. In this paper we present our virtualized cloud security monitor and assessment solution, we describe its functionalities and provide some examples of its results captured in real systems.**

Keywords: Cyber Defense and cloud vulnerability assessment, Information Security

I. INTRODUCTION

1) Aim

Over recent years the adoption of new technologies (such as unified communications, server virtualization, high-speed networking and cloud services) created a hard task by operational teams responsible to manage and secure corporate networks and data centers. Instead of just diagnosing and troubleshooting problems now they need to cope with the communication over increased bandwidth and protection of fully virtualized data centers. Our general goal is to provide assistance for system administrators building up sustainable and less vulnerable infrastructure and survive cyber-attacks. For this aim we have created an IT security audit framework for distributed computing systems (DCIs) in order to assess, evaluate and decrease their vulnerability level.

In Section I. we provide information about existing security monitoring solutions. In Section II we give description about the design of the Cloudscope modular cloud evaluation and monitoring framework and show the security module of the solution with various integrated Vulnerability Assessment Tools. At the end of our paper we conclude and explain directions of our future work.

B. Vulnerability trends

The software evolution (e.g.: size, functionality set) generally increases complexity in the software stack. It is hard to protect even a single PC node infrastructure against malicious attacks. This problem multiplies significantly if the infrastructure is heavily distributed, contains thousands of cores, and serves hundreds of people. During recent years the amount of explored network vulnerabilities are increasing constantly with about 500 NVTs per month [1].

Cloud computing technology is rapidly spreading within the IT world. Companies worldwide migrate their infrastructure to cloud infrastructure. However there are lots of known potential security problems with multi-tenant, always available, online, distributed and shared systems:

- caused by the technology and complexity itself,
- caused by site/software stack setup,
- caused by end-user behavior.

Due to the massively virtualized, up-scaled environment and the homogeneity of the infrastructure a successful break-in method is very likely become instantly applicable against other similar cloud environments. Usually it takes non-zero time to find the vulnerability, initiate alarm and document protection by the incident response teams. As a consequence a valid vulnerability can be likely reusable and provide a vast gain for the potential intruders on a short term basis.

C. Existing best practices

Cyber security is one of the major driving force behind cloud infrastructure and service evaluation. IT security organizations and groups such as CSA [2] (Cloud Security Alliance), ENISA [3] (European Network and Information Security Agency), the Cloud Computing Interoperability Group, and the Jericho Forum [4] are actively doing cloud ecosystem evaluation mainly from security, and data control point of view. The U.S. government initiated the FedRAMP [5] (Federal Risk and Authorization Management Program, and this is basically a risk management program for large outsourced and multi-agency information systems. It defines the entire assurance process for cloud instances, provides compliance evaluation for individual governmental agency applications and also authorizes federal IT services. There are worldwide de facto audit standards of enterprise financial and infrastructure-related internal controls: such as the Statement on Auditing Standards No. 70 report usually referred to as SAS 70 [6], the SSAE 16 [7] and SOC reports [12] and the CSA guide [8].

978-1-4799-0830-1/13/$31.00 ©2013 IEEE

D. Generic security monitoring solutions

Several types of monitoring tools have been designed and implemented for large scale distributed systems with different goals. We can categorize these monitoring solutions by their focused targets such as availability, functionality, performance/load and security, however in the following we will focus only on some of the available vulnerability/security monitoring solutions.

1) Grid Site Software Vulnerability Analyzer

Grid Site Software Vulnerability Analyzer (GSSVA) [9] by MTA SZTAKI is a monitoring tool which collects status information of the distributed computing infrastructure (DCI) machines, analyzes the information gathered and compares the results using an external information repository to find the existing security problems. It can automatically explore the installed Linux packages of the computing elements (CE) and worker nodes (WN). It is using a modified status monitoring system as a basis software called PAKITI[10]. PAKITI, is basically a patching status monitoring tool, which can be used for infrastructure security status monitoring. GSSVA collects the list of the installed software packages on the nodes and matches the gathered information with the security database (coming from an external repository). Fig. 1 shows the high level schematic system overview of GSSVA.

It is using HTTP or HTTPS protocol to communicate and provide a graphical user interface for its users. GSSVA is an official IT security software tool of SEE-GRID-SCI project's infrastructure monitoring solution.

2) OpenVAS

OpenVAS - Open Vulnerability Assessment System [11] is an open source vulnerability scanner and vulnerability management solution. Beside that it is also a framework, which contains several services, tools and a continuously increasing number of (about 30.000) Network Vulnerability Tests (NVTs).

3) Advanced Vulnerability Assessment Tool

Advanced Vulnerability Assessment Tool (AVAT) [1] by MTA SZTAKI supports various DCIs (e.g.: grids such as ARC and gLite and clouds). The DCI interface module contains the middleware specific commands to copy and run the vulnerability scanner and to gather the results of the investigations.

Fig. 2 presents the high level schematic system overview of AVAT. The included OpenVAS package contains a modified and precompiled OpenVAS vulnerability scanner. AVAT stores the vulnerability scan results and reports it to the DCI resource administrators. AVAT is used within the HP-SEE project to assess vulnerability on its available supercomputing infrastructure.

4) Nessus

Nessus [13] by Tenable Network Security Inc. provides centralized management of multiple vulnerability scanners and real-time vulnerability, log, and compliance management. Since 2005 the software is not open source anymore. OpenVAS is its follow up open source project.

5) Nexpose and Metasploit

Nexpose [14] by Rapid7 Inc. provides a full scale (from single user, up to enterprise level) vulnerability management solution. It was among the fist software solutions, which received USGCB (United States Government Configuration Baseline, and EAL3+ certificates Common Criteria Certification for Evaluation Assurance level Augmented [15]. It supports automatic asset discovery, scanning and remediation on virtualized environments. Metasploit [16] is an open source vulnerability scanner solution, focusing mainly on penetration testing. Recently the two software solutions are combined closely together.

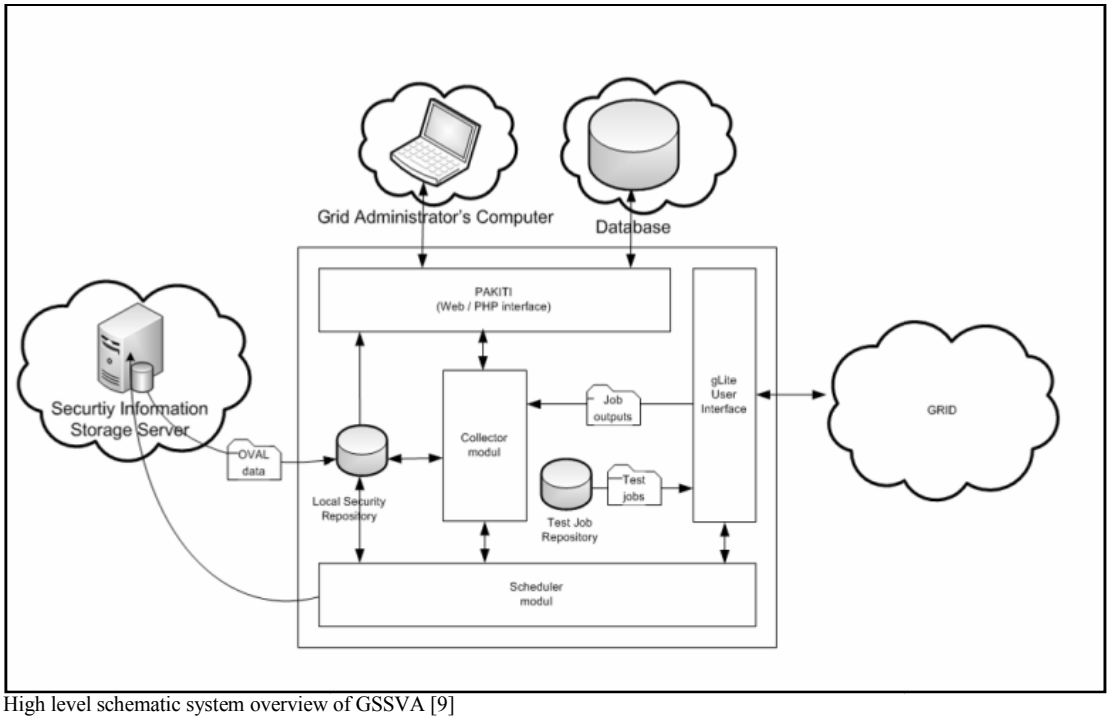

Figure 1. High level schematic system overview of GSSVA [9]

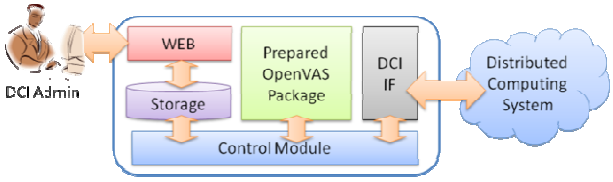

Figure 2. High level schematic system overview of AVAT [1]

Metasploit is a handy solution to validate security risks, audit IT infrastructure and verify vulnerabilities with simulated penetration tests.

6) Microsoft Baseline Security Analyzer

The Microsoft Baseline Security Analyzer (MBSA) [17] is a freeware tool designed to determine security state most of the MS based environment in accordance with Microsoft security recommendations and offers specific remediation guidance. It is a standalone security and vulnerability scanner designed to identify common security misconfigurations and missing security updates. Its availability and importance decreased during recent years.

7) Qualys Guard

Qualys Guard [18] by Qualys Inc. helps organizations with globally distributed data centers and IT infrastructures to identify their IT assets, collect and analyze large amounts of IT security data, discover and prioritize vulnerabilities, recommend remediation actions and verify the implementation of such actions.

8) NetIQ Security Manager

NetIQ Security Manager by NetIQ [19] is a Security Information and Event Management (SIEM) solution that provides host-focused security, supports automatic security activity reviews, log collection, threat management, incident response, and change detection. It is capable to do change detection and file integrity monitoring, privileged-user monitoring, log management, analysis and query-based forensics.

II. COMBINED INFRASTRUCTURE VULNERABILITY SCANNING - CLOUDSCOPE

Centralized vulnerability assessment solutions for distributed systems are only focusing on some fragments of the whole IT security picture and feature-rich frameworks (e.g.: OpenVAS, Metasploit) could not work easily in multi-administration domains frequently used in such DCIs.. To overcome these issues we designed our IT software security solution - Cloudscope - to combine the benefits of various IT security software tools and frameworks. Moreover, we combined existing vulnerability scanner and monitoring tools (such as GSSVA used on girds /EGI and SEE-GRID-SCI/, and AVAT used on HP-SEE supercomputing infrastructure and on private clouds) and tried to use these solutions in an integrated way.

We have developed a modular software, which is combining various software solutions and able to examine the infrastructure, from security point-of-views. We offer a clear, adaptable, concise and easy-to-extend framework to assess the underlying DCI infrastructure. Our developed solution is generic and multipurpose it can act as a vulnerability scanner and has support for asset discovery at the same time. It is virtualized and collects assessment information by the decentralized Security Monitor and it archives the results received from the components and visualize them via a web interface for the testers/administrators. In our Vulnerability Management module we are able to measure vulnerability parameters of a certain DCI. We are using parallel the integrated security measurement applications.

A. Vulnerability assessment

Previously we have identified security assessment parameters, which helps us to gather objective measurement data from the examined infrastructure [20]. Our solution collects information about security status using various external software tools, and matches the gathered information with security data. It is using HTTP and HTTPS protocol to communicate and provide security information via the graphical user interface. The framework is capable to test various virtualized and non-virtualized DCIs (such as grids, clouds, normal/HPC clusters), and due to its own virtualized environment it can be used as a generic security assessment tool to evaluate even non-virtualized critical infrastructure.

B. Internal architecture

Cloudscope is trying to remain middleware, virtualization technology and OS independent. The vulnerability testing module orchestrate remotely the loosely coupled various scanning tools. These tools are gathering the information and store their results internally.

All integrated virtualized security scanner software works in an agent-like way, separately. Both the client side (which contains the vulnerability/security probes and scanners) and the server size (which contains the local data collectors of each individual probes and scanners) are virtualized. Each plug-in is controlled remotely.

The user can initiate a vulnerability scanning task on the web front-end (Fig. 3). Firstly an XML based worklist is generated according to the user's security scanning aim. This worklist with a large set of configuration parameters forwarded to the virtualized security monitoring client automatically. Each pre-defined work task of the worklist runs separately on the VM and the vulnerability scanners examining the infrastructure individually.

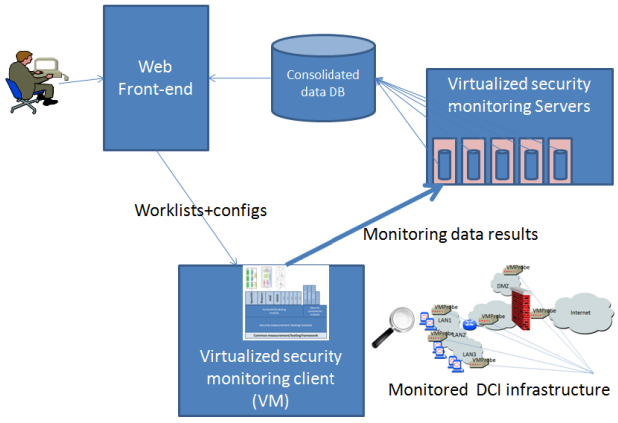

Figure 3.: Cloudscope, combined infrastructure vulnerability scanner (schematic overview)

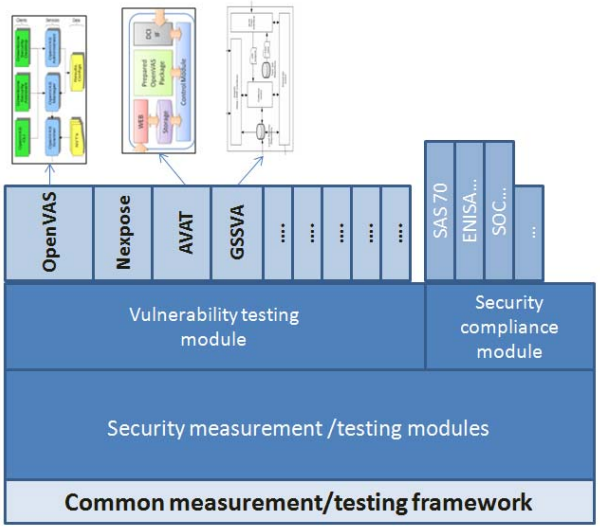

Figure 4. Internal module structure of Cloudscope

The results are forwarded automatically by the scanners to their own virtualized servers. Cloudscope extracts the relevant security results and stores into a consolidated database. This consolidated database is connected together with the centralized web front-end, where the user can see the annotated data of the vulnerability scanners. Our solution is capable to check not only single spot problems, but able to examine multi-point vulnerability tests if needed. The internal architecture of the data collection framework is modular and enables easy integration of all kind of measurement tools (Fig. 4).

We post-process and evaluate the collected data on the centralized server side of the framework and provide feedback on the web user interface about the examined system.

Inside our developed security assessment framework standard DB (MySQL) and Web server (Apache based) solutions have been used. The framework is open source, and there are no restrictions to re-implement and/or adapt it to other community needs. Dependencies on proprietary or commercial products are optional, due to the loosely coupled external tools.

III. CONCLUSIONS

In this paper, we discussed the major vulnerability sources in distributed computing infrastructures and we presented some of the recently used monitoring solutions and vulnerability frameworks for DCIs. We have designed and implemented a software solution - Cloudscope -, which is a modular security assessment framework and based on various existing security scanner solutions. We have incorporated a large number of external security solutions in a virtualized manner and build up a centralized security system monitoring user interface to show security assessment results for the users in a unified way.

The vulnerability testing module orchestrates remotely all the loosely coupled scanning tools (PAKITI, GSSVA, AVAT, OpenVAS).

Each of these software solutions has been already used successfully by us to evaluate different type of DCIs (for example SEE-GRID-SCI's grid infrastructure /GLite based/, MTA SZTAKI's cloud infrastructure (Open Stack, Open Nebula based/, HP-SEE's supercomputing infrastructure /ARC based/. Using our framework, the combined vulnerability scanner tool set revealed a large number of valid security problems and vulnerabilities with high impact on the examined infrastructures. With the forwarded detailed reports existing vulnerabilities have been eliminated by the local experts/administrators. The feedbacks received from the regional DCI administrators (from HP-SEE - supercomputing infrastructure, SEE-GRID-SCI – grid infrastructure, and various cloud service providers) proved, that it is a handy tool to make DCIs more secure. The proposed software can easily (re)used for other DCIs and authors are jointly working with various DCI communities to open up the vulnerability service for a large set of critical infrastructure user community, for other projects and for large IaaS cloud infrastructure providers.

As future work we are planning to include into Cloudscope additional software components to evaluate security compliance. We are also planning to further expand the security/vulnerability assessment tool set of the framework.

ACKNOWLEDGMENT

The research leading to these results has received funding from the European Social Fund and the hungarian TÁMOP-4.2.1.B-11/2/KMR-2011-0001 "Kritikus infrastruktúra védelmi kutatások" project. Authors would like to thank for the helpful technical support of the Laboratory of Parallel and Distributed Systems (LPDS) at MTA SZTAKI. Levente Kovács is supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences.

REFERENCES

[1] Sándor Ács, , Miklós Kozlovszky; Advanced Vulnerability Assessment Tool for Distributed Systems; HP-SEE User Forum 2012, BoA. pp. 46,Belgrade, Serbia, October 17-19, 2012

[2] Cloud Security Alliance – CSA; https://cloudsecurityalliance.org/; February 2013

[3] European Network and Information Security Agency – ENISA; http://www.enisa.europa.eu/ ; February 2013

[4] The Opengroup Jericho Forum; http://www.opengroup.org/getinvolved/forums/jericho ;February 2013

[5] The Federal Risk and Authorization Management Program (FedRAMP); www.fedramp.gov ; February 2013

[6] http://sas70.com/ , February 2013

[7] http://ssae16.com/SSAE16_overview.html , February 2013

[8] https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/ , February 2013

[9] Acs, S., Kozlovszky, M., and Balaton, Z.: Automation of security analysis for service grid systems: PARENG2009, The First International Conference on Parallel, Distributed and Grid Computing for Engineering, Pécs, Hungary, 2009.

[10] http://pakiti.sourceforge.net/ , February 2013

[11] The OpenVAS website, http://www.openvas.org , 2013 February

[12] http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/SORHome.aspx; February 2013

[13] http://www.tenable.com/products/nessus , February 2013

[14] http://www.rapid7.com/products/nexpose/ , February 2013

[15] http://www.rapid7.com/company/news/press-releases/2012/usgcb-cyberscope.jsp, 2012. November 10.

[16] http://www.metasploit.com/ , February 2013

[17] http://en.wikipedia.org/wiki/Microsoft_Baseline_Security_Analyzer , February 2013

[18] http://www.qualys.com/enterprises/security-compliance-cloud-platform/ , February 2013

[19] https://www.netiq.com/products/sentinel/ , February 2013

[20] M. Kozlovszky, M. Törőcsik, T. Schubert, V. Póserné; IaaS type Cloud infrastructure assessment and monitoring , MIPRO 2013 may, Opatija, Croatia