Guaranteeing High Availability of the „Secure Exam Environment“ (SEE)

Gabriele Frankl[1], Peter Schartner[2] and Dietmar Jost[2]
[1]*Department of eLearning, Alpen-Adria-Universität Klagenfurt, Universitätsstrasse 65-67, 9020 Klagenfurt, Austria*
[2]*Department of Applied Informatics, Alpen-Adria-Universität Klagenfurt, Universitätsstrasse 65-67, 9020 Klagenfurt, Austria*

Keywords: Secure Online Testing, Secure Exam Environment, Security, High Availability, Monitoring.

Abstract: Online exams are an increasingly popular form of assessment. Compared to written exams they reduce the marking workload and offer advantages such as enhanced objectivity, assessment that includes software specific to the course and thus increased constructive alignment with teaching and learning processes. To conduct large-scale online exams without the physical restrictions of (often extremely small) computer rooms, we implemented the “Secure Exam Environment” (SEE) in 2011. The SEE enables online testing in any lecture hall with electricity and LAN sockets using students’ own devices (and loan devices if needed) while blocking access to unauthorized files or internet pages. Assessment is conducted via Moodle and additional software (e.g. Eclipse or GeoGebra) can be used as well. As of November 2017 we have conducted 1,297 such online exams with 47,930 students and are able to test up to 220 students concurrently. To maintain quality of service we developed a monitoring solution to control the growing complexity of the technical infrastructure of the SEE. The monitoring solution aims to detect failures sufficiently early to guarantee a high level of availability and to gather data to further improve the SEE.

1 INTRODUCTION

Student and teacher involvement in assessment, including digitally-enhanced assessment, remains an essential part of contemporary learning (Gibson & Webb, 2015). Assessment channels students’ energies, heavily influences student behavior, shapes students’ experiences and generates feedback with opportunities for reflection (Marriot, 2009; Müller & Bayer, 2007; Sharpe & Oliver, 2007). Despite a growing number of alternative assessment strategies, written exams and summative assessment continue to be the primary methods of assessing factual knowledge at schools, universities as well as in several business areas, leading to a huge grading workload if conducted with paper-and-pencil exams. eExams result in noticeable time and money savings (Anakwe, 2008) due to the automatic delivery, storage and(semi-)automated scoring of (semi-)standardized question types, along with the improved readability, structure and clarity of typed open-text answers. The greater efficiency of eExams provides students with instant grading and – if supported by lecturers – feedback (Hewson, 2012). Furthermore, online exams provide greater flexibility compared to traditional testing methods (Anakwe, 2008). Moreover, since today's students are more used to typing than to extensive handwriting (Hewson, 2012), online exams prevent hand pains and bad handwriting related to paper-and-pencil exams. In addition, eExams restrict the halo-effect which occurs when different handwriting styles influence the lecturer when grading. Online exams enable each question to be evaluated on its merits without being influenced by other answers provided by the student and thus subjective construction processes. Hence, online exams enhance objectivity. Additionally, eExams bring further advantages such as improved correction possibilities, the establishment of a question pool or opportunities for statistical analysis of questions, improving the quality of questions over time.

Furthermore, the shuffling of questions and answers, the automatic selection of questions out of a sufficiently large enough question pool as well as the opportunity to create questions including variables which are assigned different values for each student decreases the likelihood of cheating. Another and very promising advantage of online exams is the opportunity to include additional software and

Frankl, G., Schartner, P. and Jost, D.
Guaranteeing High Availability of the "Secure Exam Environment" (SEE).
DOI: 10.5220/0006751801300136
In *Proceedings of the 10th International Conference on Computer Supported Education (CSEDU 2018)*, pages 130-136
ISBN: 978-989-758-291-2

multimedia in the examination environment. According to Biggs and Tang (2011) and their concept of "constructive alignment", coherence between all phases and elements of the learning process is essential for high quality education. Intended learning outcomes, teaching/learning activities, assessment tasks as well as grading should support one another (Biggs & Tang, 2011; Müller & Schmidt, 2009). Thus, the software tools used for teaching and learning – e.g. mathematical or statistical calculations and analysis, programming, literature essays - should be used during the examination process as well. Being able to use specific software and multimedia in electronic exam environments paves the way to promising (hands-on) performance assessments too.

Despite all the positive aspects of eExams mentioned so far, we found a lack of technical solutions for conducting secure online exams for larger audiences. The problems we encountered were computer rooms that were simply too small as well as a lack of consideration for the security requirements which inevitably arise in the context of (electronic) exams: confidentiality, privacy, integrity, authenticity, accountability, and availability. The first five aspects are commonly addressed through cryptography (e.g. encryption of transmitted and stored data, network-based security mechanisms like firewalls, and authentication of messages and users), whereas the last one is provided by physical and logical redundancy and continuous monitoring of the IT system. This includes the continuous monitoring of the infrastructure (hardware, software and network) which is a preventive measure to help detect issues before they cause any major problems.

To overcome the existing shortcomings, we implemented the Secure Exam Environment (SEE). After a depiction of the SEE, this paper will focus on the low-cost monitoring solution (see Ratan, 2017 for a list of open-source monitoring tools) that guarantees high availability of our Secure Exam Environment. In the case of the SEE, the monitoring checks not only the availability of the service (i.e. Moodle-server) per se, but also the quality of service (QoS) including network-related parameters like available bandwidth and latency (similar to the approach in Zeng et al., 2009). Further information concerning the other security requirements mentioned above can be found in Frankl et al. (2017).

2 THE SECURE EXAM ENVIRONMENT (SEE)

The Alpen-Adria-Universität Klagenfurt (AAU) launched the Secure Exam Environment (SEE) for online testing in 2011 (Frankl et al., 2011) with the aim of supporting large class sizes, as well as modern teaching and testing strategies, while working within budgetary and organizational constraints. By making use of the students' existing personal computers (laptops), the SEE increases efficiency since ordinary lecture halls can be used for large scale online testing as well as effectiveness since the students are presumably familiar with their own devices.

The SEE disables access to students' own files and data as well as to other internet sites. Loan devices are offered for those who do not own a laptop. As a result, institutional asset requirements as well as the associated maintenance costs are minimized. We are currently able to test up to 220 students simultaneously.

Furthermore, the SEE facilitates the integration of different software tools and programmes, which are increasingly used for teaching and learning (e.g. Eclipse, GeoGebra), into the exam environment, fostering pedagogical coherence (Biggs & Tang, 2011).

The actual exams are presented as quizzes, a key component of the Moodle learning management system (LMS) utilised by the AAU.

In contrast to other electronic exam environments (e.g. SoftwareSecure, 2017), we avoid the use of special equipment and encourage students to use their own device. However, accessing the Moodle server directly via a web browser running on the student's OS is an insecuret approach. In this case, blocking connections to Wikipedia or other online resources may be simple, but cheating by using materials stored on the local hard drive is rather easy. Since we do not want to force students to install additional software (such as lockdown modules) on their personal laptops, we have to use our own operating system (OS) in order to restrict the access to the local resources and programmes that are prohibited during the exam. We decided to boot this OS via the Preboot eXecution Environment (PXE) protocol over a local area network (LAN), since the handling of USB sticks or DVDs is very error-prone, time-consuming and inflexible, especially when additional software is needed, and the usage of WLANs is too insecure and interference-prone. Clearly, this requires that the client is able to boot via the network.

In order to support a very broad range of (private) laptops, our solution is designed as a minimal Linux

system. At the moment, this OS is realized using Fedora and Knoppix, which enables us to boot Legacy or UEFI devices (both Apple and PC). In order to restrict the access to external resources, we implemented corresponding firewall rules. Since Moodle as an LMS not only provides exam features but also chatting capabilities and course related material, a solution was needed to prevent access to such resources and activities during exams. Running an ordinary web browser in centOS – even when restricted with firewall rules – would not have completely solved the cheating problem. Fortunately, the Safe Exam Browser (SEB – see Safe Exam Browser, 2017) is fully supported by Moodle-core. The SEB is more restrictive than an ordinary browser, since it prevents students from opening other programmes or additional web browser windows during the exam and ignores certain key combinations or clicks. So by limiting access to the exam page only, cheating by exploiting Moodle's features is no longer possible. However, the SEB is only available for Windows XP, Windows 7 and MAC OS X. Therefore, we boot a minimized Windows 7 as a virtual machine on the minimized Linux system via VirtualBox (see Virtual Box, 2017) (see Figure 1). Additionally, proprietary software which only runs on Windows systems is still widespread in the educational sector. On the one hand, the reliance on a virtual machine is a drawback in terms of performance, on the other hand, it adds flexibility regarding the management of the virtual machine image. Furthermore, hardware driver management is done completely in Linux, which is known for its broad, driverless hardware support especially for older devices. The selection of the allowed programmes during the exam (in addition to the SEB) is set via a configuration file, which is retrieved from an Intranet Service. In the GUI of this service, administrators are able to configure the exam (e.g. only Calculator or Calculator and Excel or GeoGebra or Eclipse and PDFs allowed).

Starting an online exam using the SEE begins by booting a minimized Linux from the LAN, then the minimized Linux automatically starts the Windows 7 virtual machine (VM), Window 7 automatically starts the SEB, the SEB automatically connects to the homepage of the AAU's learning management system Moodle, and finally users have to log in to Moodle and select the exam.

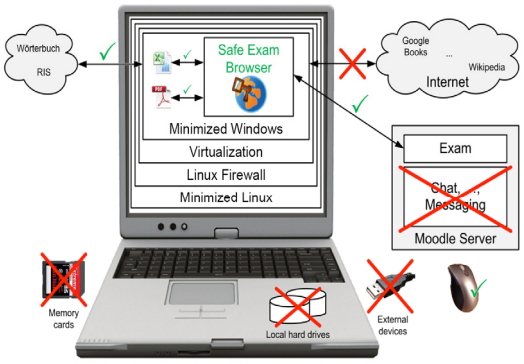

Figure 1: The operating principle of the Secure Exam Environment (SEE).

3 MAXIMIZING THE AVAILABILITY OF THE SEE

The availability of an exam environment is an issue of critical importance. Even a short downtime of the SEE could prevent hundreds of students from taking exams which might be urgently needed to get marks or certificates, take new courses, finish modules, classes or studies, get financial aid for higher education studies or even get a new job. Furthermore, students tend to be quite nervous before an exam and a technical glitch would undoubtedly increase stress and erode trust in the exam environment. Thus, perception of the SEE's reliability (from both for examiner's and examinees' viewpoint) depends on the availability of the (information) technology during the exam (Sharpe & Oliver, 2007).

During the SEE boot process, the SEE-servers (and the personal computers with which the exams are written) have to operate properly as well as the network including the switches in the lecture halls. At the time of writing, the SEE depends on the online connection between the SEB and the Moodle-server. Thus, the availability of the SEE can be affected by hardware failure, network drop outs or service outages. Analyzing and identifying failures when a breakdown occurs usually costs a lot of time, which is at a premium while conducting an eExam. Thus, a continuous monitoring solution of the various IT components involved - e.g. servers and computer networking technologies – to prevent failures and optimize the availability of the SEE is mandatory, particularly considering the SEE is based on various hardware components which are administered by different departments of the University.

Drop outs of components or services or deviations from thresholds within defined time intervals result in alerts, allowing support staff to react to and resolve issues immediately, leading to crucial time-savings within the failure identification process. Monitored components and services include the availability of the SEE-servers (implemented with centOS) including CPU and storage, as well as DHCP, NFS, TFTP and HTTP services; the availability of the administration backend of the SEE including the corresponding HTTP service; the availability of Moodle including HTTP-access, as well as end-to-end-tests in the lecture halls with minimal computers (Raspberry Pi); the availability of the network (connection between SEE-server, clients and Moodle), and end-to-end performance tests within the network with low-cost probes (Raspberry Pi).

3.1 Monitoring the High-availability SEE-host and Including Services

The availability of the server, providing the SEE for network boot, as well as services like DHCP, NFS, HTTP und TFTP is one of the key requirements of online testing with the SEE.

We operate the SEE-server as a high availability and stable system by running multiple redundant SEE-servers. Using DRBD/Heartbeat or Pacemaker/Corosync in a failover setup (to define one server as the master server and the other one as slave) enables us to switch from one server to the other automatically in case of a failure or manually in case of scheduled maintenance. Thus, a new update can be safely implemented within the system by installing it on one server and, after careful testing, on the other and thus the production system.

While monitoring the services mentioned above, we log CPU utilization, RAM and hard disc usage, and the status as well as the utilization of the network interface. Additionally, we periodically check for pending updates, especially security updates, to eliminate failures or prevent hack-attacks on the system and improve performance. Controlling upcoming updates enables us to schedule maintenance periods efficiently around exams.

3.2 Measuring Network Performance

Measuring the run-time of the network including the connection between the SEE-server, clients and Moodle during an eExam in real time generates significant data about the latency and utilization of the network. The open source software SmokePing is a suitable tool for measuring and visualising the round-trip-time (RTT) of Linux-based systems by defining the specific hosts as well as relevant external hosts which are reachable via ICMP. By default, every five minutes twenty ICMP-packages are transmitted to each specified host and used to calculate RTTs. The median for each interval of measurement is shown in Fig. 2, with green indicating no packages were lost while red indicates 19 out of 20 packages were lost. Each single RTT is shown as smoke in the graph.

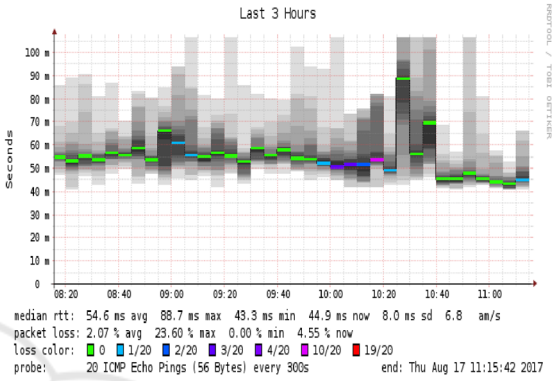

Figure 2: RTTs of a host, measured with SmokePing.

Package loss is a signal for capacity overload of the main host or related hosts, or for a failure or an erroneous configuration of a network device. Black ‘smoke’ at an interval of measurement shows the range of fluctuation of the RTT. Increased smoke indicates a high variation of the RTT per ping and thus capacity overload of the network. The combination of SmokePing and probes (Raspberry Pi’s) placed in the SEE-network enables us to monitor all servers and network devices and thus to recognise network bottlenecks and failures at an early stage.

3.3 Maximizing Availability of the Network Connection

In order to maximise network availability, we only use wired LAN connections at this point in time. Despite recent developments, WLAN remains too error prone and, additionally, a malicious user could easily perform a denial-of-service (DoS) attack on the WLAN access points and hence prevent all users from taking the exam. To achieve such an attack, a battery-powered pocket-sized WiFi jammer could be mounted close to or in the room where the eExams take place.

To ensure the maximum stability of the network system, the network department of our university provides high redundancy within the network-core, distribution-switches, firewalls and the border-router,

as well as load sharing via the Border Gateway Protocol (BGP) in a multihomed environment and redundant cables. In addition, the equipment used in the core and distribution layer are high-end components.

3.4 Infrastructure

The availability of our Secure Exam Environment (SEE) is affected by the infrastructure in which the SEE components are embedded. One critical issue is an Uninterruptible Power Supply (UPS) for the SEE-server as well as for the network to protect the system from power failures. The UPS also guards against over and undervoltage and is backed by means of batteries (short-term power failures) and a diesel generator (long-term power failures).

Another important topic is the geographical distribution of the (redundant) hardware components. The two SEE-servers are located in different areas of the university and thus, in the case of an extended power failure, fire or flooding, it is unlikely that both servers will be affected.

3.5 Backups

One indirect approach to guarantee the availability of the SEE-servers, and thus the SEE, is frequent, well organized backups. In case of an outage like hardware failure, the SEE-server must be restored to the most recent valid state. An up-to-date, functioning backup reduces the mean time to repair (MTTR). A well-organized backup-strategy includes the evaluation of functionality of the frequently executed backups as well as the documentation and frequent testing of the backups and training of the responsible staff. Furthermore, it should be guaranteed that spare hardware (like hot-swappable harddisks and power supplies and spare network components) is on hand in case of serious hardware failure.

3.6 Monitoring the Availability of the Administration Backend of the SEE Including the Corresponding HTTP Service

The administration backend is another key component of the SEE, offered via web interface and used by the supporting staff to activate any additional software (e.g. a calculator or Eclipse) for an exam. The administration backend is accessible only via a URL https://backend.spu.aau.at. A periodical check of the HTTP server's reachability is performed which monitors the HTTP status code. If the wrong status code is returned from the backend, an alarm is sent to the service team. Additionally, it is possible to check the server's response times. Longer response times could be an indicator of network outages or a server problem.

3.7 Centralized Monitoring of All SEE-Components and Services

Deviations from threshold values of all components and services of the SEE are reported at regular intervals. Every outage triggers an alarm (via e-mail or SMS) which, together with centralized monitoring, helps the service team to rapidly identify the cause of a failure, saving additional time.

3.8 Optimizing the SEE based on Monitoring Data

The constant monitoring of all components and services of the SEE offers the opportunity for (trend) analysis (also see section 5.1 "Further developments") as a basis for the continuous optimization of the systems' performance.

3.9 Loan Devices

Loan devices serve two purposes within the SEE: Firstly, it cannot be assumed that all students have a portable device, and secondly, they may substitute a student's personal device in the case of technical problems or breakdowns during the exam. The AAU currently has approximately 100 laptops serving as loan devices for students.

3.10 Reliability

At the time of writing, the SEE depends on the online connection between the SEB and the Moodle-server. As a result, users cannot save current results or proceed to the next question during a network failure. Thus, the temporary storage of the answers (during network failures) remains a problem. Fortunately, Moodle saves the last answer received and the progress of each examinee. Therefore, the examinee may simply continue the exam from the point where the error occurred after potential network problems are solved. In the worst-case scenario, the last answer of the examinee is lost. Similarly, laptop failure is not a severe problem because all previous answers are stored on the server and the student can simply continue his or her exam on one of our loan devices.

4 TECHNICAL OBSTACLES AND CHALLENGES

One of the current restrictions of online exams is the necessity of a network connection. As WLAN is still prone to failure, LAN is the best option, especially for larger groups of students. This results in another challenging aspect, namely that lecture halls require LAN and power sockets near at least every second seat. Unfortunately, not all lecture halls fulfill these requirements and retrofitting is extremely expensive. The obstacle with the LAN sockets could be overcome with access points, however running laptops purely on battery power is risky.

New generations of laptops, requiring continuous adaptation of the SEE, remain a persistent challenge. For example, we had to invest significant effort to support UEFI as a new interface between the hardware and the OS. Moreover, some manufacturers no longer offer PXE or Net-Boots on their devices, forcing us to find workarounds. Furthermore, as many new laptops come without Ethernet-sockets, we must support adapters within the SEE.

5 EXPERIENCES WITH EEXAMS AT THE AAU AND FURTHER DEVELOPMENTS

In June 2011, we began offering online exams with the SEE. Table 1 shows the growth of eExams conducted with the SEE at the AAU over the last six years.

Table 1: The progression of eExams with the Secure Exam Environment (SEE), * in progress.

2011	2012	2013	2014	2015	2016	2017 *	Total
288	2,717	7,475	7,082	8,954	10,391	11,023	47,930

5.1 Further Developments

Further developments in monitoring will include the integration of the students' devices and the loan devices into the monitoring concept and predictive maintenance (for details refer to Sasisekharan et al., 1994; Susto et al., 2015; Hashemian & Bean, 2011)). In more detail, we will pursue the following ideas:

- By gathering and analysing the devices' log-files whenever they are connected to the SEE, *students' devices* and the *loan devices* may be directly integrated into the monitoring system. This will help to keep the loan devices up-to-date, because a problem detected on a single device (currently in use) can (automatically) be fixed on all other instances of the same model. A similar process can be applied for the students' devices: a problem detected with one device can either trigger an update of the SEE (e.g. with respect to drivers) or a warning for other students using the same model. In the long-term, the log-data may be included in a predictive model.
- The goal of *Predictive Maintenance* is to determine the condition of equipment (servers, laptops, and network-infrastructure like switches and cabling) in order to predict when maintenance should be performed in order to avoid failures. This is contrary to the classical approach, where maintenance is either triggered by a concrete failure (aka the break-fix model [20]) or on an interval-based approach which often causes unnecessary costs. In short, predictive maintenance promises time and cost savings and a higher level of availability.

Currently, we are only able to execute one eExam with specific settings, e.g. additional software, at the same time. Therefore, we are developing a boot environment which enables us to run eExams with various additional software simultaneously by recognizing the identity of the student and transmitting the proper exam environment. Furthermore, the support of newer devices without LAN ports is in development. In the future, we also intend to provide a WLAN access point. Finally, like every software solution, the SEE needs constant security and compatibility updates.

6 CONCLUSION

eExams extend the possibilities for assessment in terms of quality and especially efficiency. However, the transition from paper-based to electronic exams raises "new" security-related problems. Traditional paper-based exams handled requirements like confidentiality, privacy, integrity, authenticity, accountability, and availability in a straight-forward manner: simply preventing access to the empty and completed exams guarantees their confidentiality, the paper and well established organizational and

personnel processes do the rest (privacy, integrity, authenticity, accountability, and availability). For eExams all the aforementioned aspects have to covered by complex mechanisms, particularly technical ones. In this paper, we first briefly presented the secure exam environment (SEE) used at the Alpen-Adria-Universität Klagenfurt (AAU) and then presented our low-cost monitoring system that helps us to achieve a high quality of service level with respect to the availability of the SEE. We also discussed technical obstacles and challenges of the SEE and possible future work concerning the monitoring system.

REFERENCES

Anakwe, B., 2008. Comparison of Student Performance in Paper-Based Versus Computer-Based Testing. In: *Journal of Education for Business* (October), 13-18.

Biggs, J., Tang, C., 2011. *Teaching for Quality Learning at University*. McGraw Hill, Berkshire.

Fluck, A., 2011. eExaminations Strategic Project Final Report for Academic Senate, University of Tasmania. Meeting 1/2011, cited in Fluck, A., Hillier, M.: *Innovative assessment with eExams*. Paper presented at the *Australian Council for Computers in Education (ACCE) conference*, 29 September – 2 October, Brisbane, Queensland (2016).

Frankl, G., Schartner, P., Jost, D., 2017. The „Secure Exam Environment“: E-Testing with Students' Own Devices. In: *Tomorrow's learning: Involving everyone learning with and about technologies and computing*, Springer, 179-188.

Frankl, G., Schartner, P., Zebeding, G., 2011. The "Secure Exam Environment" for Online Testing at the Alpen-Adria-Universität Klagenfurt/Austria. In: *World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education. Association for the Advancement of Computing in Education* (AACE), Hawaii.

General Electric Company, 2013. *Beyond the break-fix model: predictive services to leverage GE's record $229 billion backlog.* GE Reports, October 18,http: //www.gereports.com/beyond-the-break-fix-model.

Gibson, D. C., Webb, Mary, E., 2015. Data science in educational assessment. In: *Education and Information Technologies* (20, Issue 4), 697–71.

Hashemian, H.M., Bean, W.C., 2011. State-of-the-Art Predictive Maintenance Techniques, In: *IEEE Transactions on Instrumentation and Measurement*, Vol. 60, No. 10.

Hewson, C., 2012. Can Online Course-Based Assessment Methods Be Fair and Equitable? Relationships between Students' Preferences and Performance within Online and Offline Assessments. In: *Journal of Computer Assisted Learning*, (28, Issue 5), 488-498.

Marriott, P., 2009. Students' Evaluation of the Use of Online Summative Assessment on an Undergraduate Financial Accounting Module. In: *British Journal of Educational Technology*, (40, Issue 2), pp. 237-254.

Müller, F. H., Bayer C., 2007. Prüfungen: Vorbereitung - Durchführung - Bewertung. In: Hawelka, B., Hammerl, M., Gruber, H. (eds.), *Förderung von Kompetenzen in der Hochschullehre.* Asanger, Kröning, 223-237.

Müller, A., Schmidt, B., 2009. Prüfungen als Lernchance: Sinn, Ziele und Formen von Hochschulprüfungen. In: *Zeitschrift für Hochschulentwicklung* (4 No.1), 23-45.

Ratan, V., 2017. *An Overview of Open Source Tools for Network Monitoring*, http://opensourceforu.com/2017/04/overview-open-source-tools-network-monitoring

Safe Exam Browser (SEB), http://www.safeexambrowser.org/news_en.html, last accessed 2017/08/16.

Sasisekharan, R., Seshadri, V., Weiss, S.M., 1994. Proactive Network Maintenance Using Machine Learning, in *Workshop on Knowledge Discovery in Databases* (KDD94), pp. 453-462.

Sharpe, R., Oliver, M., 2007. Designing courses for e-learning. In: Beetham, H., Sharpe, R. (eds.): *Rethinking Pedagogy for a Digital Age. Designing and delivering e-learning*. Routledge, London and New York.

SoftwareSecure, http://www.softwaresecure.com/, last accessed 2017/08/16.

Susto G.A., Schirru, A., Pampuri, S., McLoone, S., Beghi, A., 2015. Machine Learning for Predictive Maintenance: A Multiple Classifier Approach, In: *IEEE Transactions on Industrial Informatic*, Vol. 11, No. 3.

Virtual Box, http://ww.virtualbox.org, last accessed 2017/08/16.

Zeng, W., Wang, Y., 2009. *Design and Implementation of Server Monitoring System Based on SNMP*, International Joint Conference on Artificial Intelligence 2009