

Security Metrics for Virtual Campuses

Bogdan ZURBAGIU

Academy of Economic Studies, Bucharest, Romania

bogdan.zurbagiu@brd.ro

Abstract: *Because of the great increase in research of technology and the development of new ways of accessing and sharing the information, the communication methods have greatly improved during the last decade. Nowadays, rarely you can find universities that do not have an internet website, which offer multiple ways of remotely accessing data and information related to different scientific fields. The need of reaching as much as possible candidates, located in a multitude of geographical areas, close or far from the headquarters of the academies have determined their development in the internet area, by providing ways of education through e-learning tools, implemented in virtual campuses. The fame and respect of universities with long tradition is maintained by keeping track of technological improvements and adopting distance learning programs, but in the same time the security measures for keeping a high quality standard educational process must be ensured by applying powerful security measures that does not affect the accessibility level.*

Keywords: *security metrics, accessibility metrics, virtual campus, e-learning, security of virtual campuses, fuzzy logic.*

1. Introduction

In the context of ensuring a high level security applied on restricted information, the university's virtual campus managerial board must follow security metrics.

A complex virtual campus can have all the features that are necessary in order to follow classes and graduate without being necessary to be present in the geographic campus of the teaching centre. The problem that arises consists in the need to develop a security strategy that is strong enough to protect the highly confidential information which travels through the internet protocols between students, teachers and administrative staff.

The security level applied to the virtual campus will impact the accessibility of the systems. For example, if the user will need to choose strong passwords, finger print tools and different other authentication mechanisms in the same time, the authentication process will become hard and aggravated. For this reason, the higher the accessibility level will be, the lower the security level will become, and vice versa.

The e-learning systems have the purpose of bringing altogether different users, from different geographic areas, which follow the same objective of obtaining information and knowledge, and sharing them throughout the virtual community.

Students of the e-learning systems follow different courses provided through animated courses, virtual classes or video and audio courses. Using different multimedia technologies, the act of study has become easier; the level of understanding has become suitable and flexible on each one's needs.

The e-learning tools are the core of the virtual campus system. They enable students to follow different curricula according to each one's needs of improvement or study.

2. Virtual campuses

According to [7], “A Virtual Campus, figure 1, refers to the online instrument that provides education programs where college work is completed either partially or wholly online. The term is usually associated with the concept of virtual education that describes online education using virtual courses delivered on the Internet. "Virtual" is used here to characterize the fact that the course is not taught in a physical location, but through some alternative methods.

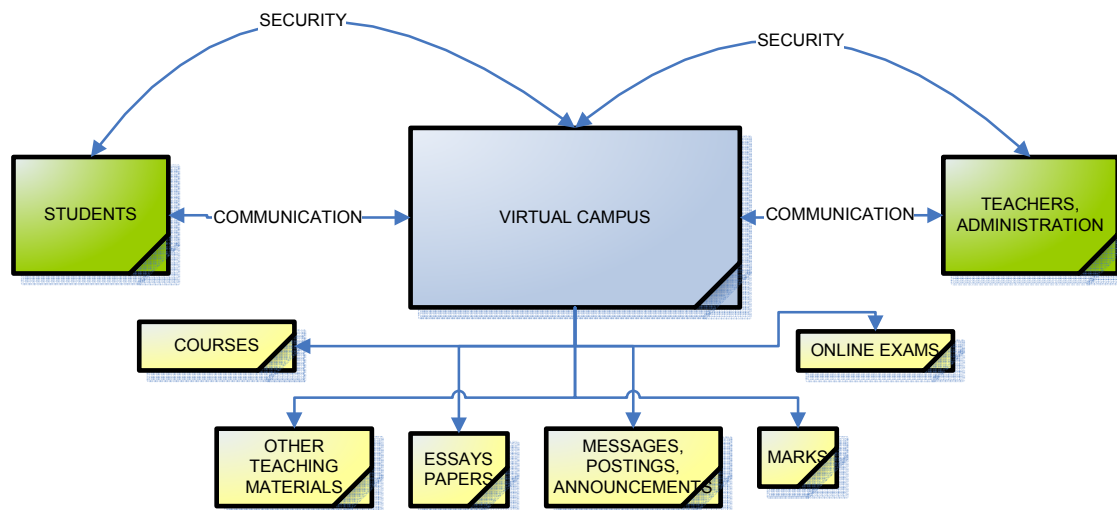


Fig. 1. Virtual campus

The aim of Virtual Universities is to provide access to teaching materials to those who cannot physically attend courses for reasons related to distance or need for flexibility. Students meet rigorous criteria in order to graduate and obtain a diploma. Many virtual institutions are accredited in the same way as traditional universities and operate according to the same academic standards. These universities can grant degrees that will be recognized around the world.”

The e-learning systems provide users the capacity of following online courses, take assessments, get in touch with other students that are part of the same knowledge community, upload papers and receive grades from evaluators.

In the e-learning systems there are mainly 5 types of users: students, teachers, people outside the community, organisations, administrative and management staff.

Students take part to online multimedia courses, participate to online meetings, debate in forums, and take assessments.

Teachers create and upload the educational documents, animated using different multimedia tools or classical format, evaluate the papers input by the students and offer grades that are going to be available on the same platform for students to see.

People outside the online community are usually people that share information related to the performance of the e-learning systems and promote the different functionalities in order to enlarge the number of accessing users and make more visible the performances of the virtual learning tool.

The organizations are interested in recruiting trained staff. For this reason, they get involved in the improvement of the already implemented functionalities and offer support in developing new ones. Usually, they influence the objectives and the curricula of study

according to their own needs. Also, it can be considered as an act of social responsibility to sustain the economy by sponsoring the training of new professionals.

The administrative and management staff takes in charge the achieving of goals, the drawing of objectives. They also moderate the exchanges between students on forums, determine the registration fees and study the labour market demands and adapt the tools functionalities and modules by selecting the teachers and the curricula.

According to [5] “The attacks upon virtual campuses represent any action intended to obtain or to deteriorate classified information. By securing the information, it is meant to ensure the security level imposed in every data processing level and prevent unauthorized access. This will be established through data encryption, during the storage or transmission phase, network traffic protection and severe access control.

Attacks upon virtual campuses concern the stealing of identity and access to classified information, with the purpose of accessing or altering the data. Usually, the security breach takes place during the authorization process, by stealing someone else’s identity. This allows access to the restricted areas of the virtual campus which are specific to a limited number of accounts.

A successful attack affects the reputation of the institution and the integrity of the entire campus, allowing attackers to read emails, to change schedules, to view the questions and answers of future assessments and also to take exams.“

3. Security metrics for virtual campuses

Security metrics are used by virtual campus platform administrator to determine the ideal level of security to be applied. The security level applied in day $t+1$ will be determined on the SMITU level of day t and will determine the security mechanisms used in the virtual campus platform. The security level applied daily (day $t+1$) in the virtual campus platform will automatically adapt depending on the values of the SMITU_{*t*} indicator. The details of the security levels and the measures taken are shown in table 1.

Table 1. Security levels applicability

Security level	Values of SMITU _{<i>t</i>} indicator
SL1	Between 0% and 5%
SL2	Between 5,01% and 10%
SL3	More than 10,01%

Security level SL1 involves the default security measures, allowing the highest level of accessibility, while SL3 will determine the most strict security measures and in the same time the lowest level of accessibility.

$$SMITU_t = \frac{\sum SMIU_{it}}{TNU_t}$$

where:

SMITU_{*t*} (Security Metrics Indicator for Total Users) indicates the average confidence level, showing the average probability that the virtual campus platform is being subject of attacks in day t . It calculated by adding the values of SMIU_{*it*}, for user i in day t , and dividing them to the total number of users.

$SMIU_t$ (Security Metrics Indicator for User) shows the average confidence level when declaring a user as performing unauthorized activities. It is determined by calculating a percentage on the basis of multiple indicators and reflects the level of probability when declaring a user is an unauthorized one that performs different attack activities in day t .

TNU_t represent the total number of users that have accessed the virtual campus platform in day t .

As shown bellow, the $SMIU_{it}$ indicator is calculated based on multiple specific indicators. Each specific indicator will have assigned a level importance.

$$SMIU_{it} = 0,1 * UIP_{it} + 0,3 * EA_{it} + 0,25 * LC_{it} + 0,35 * CI$$

where i = user i ; t = day t ;

UIP_{it} (Unknown IP) – the indicator shows if the user i has connected from an unknown IP address. The virtual campus platform will store the activity of each user and the IP's from where is has connected. The indicator will take value 0 if there was no appearance of the event or 1 of the event has taken place at least once.

EA_{it} (Erroneous Authentications) - this indicator counts the number of erroneous authentications the user has performed before connecting to the virtual campus platform. The indicator will take value 0 if there was no appearance of the event or 1 of the event has taken place at least once.

LC_{it} (Logical Course) – this indicator shows if the user has connected to one of the virtual campus functionalities and did not use the normal path of reaching the functionality. The indicator will take value 0 if there was no appearance of the event or 1 of the event has taken place at least once.

CI_{it} (Code Input) – this indicator will reflect the number of times the user has input code text in different text areas of the virtual campus platform. The indicator will take value 0 if there was no appearance of the event or 1 of the event has taken place at least once.

4. Example

The virtual campus platform of the Academy of Economic Studies in Bucharest has 10 thousand users.

On the 4th February 2010, the user Ion Popescu has connected from an unknown IP address after having indicated 4 times a wrong user/password to the virtual campus platform. After doing so, he has connected to the virtual campus functionalities using the normal path. Also, he has tried 2 times to input PHP code in the open text area.

i = Ion Popescu; t = 4th February 2010;

$UIP_{it} = 1$; $EA_{it} = 1$; $LC_{it} = 0$; $CI_{it} = 1$

$SMIU_{it} = 0,1 * 1 + 0,3 * 0 + 0,25 * 1 + 0,35 * 1 = 0,7$

The $SMIU$ indicator shows with a confidence level of 70% that user Ion POPESCU has performed unauthorized activities on 4th February 2010.

At the level of the Academy of Economic Studies, on 4th February 2010 the SMIU indicators have taken the values reflected in table 2.

Table 2. Occurrence value table

Occurrences	Value
1000	0,1
500	0,3
200	0,25
300	0,35
8000	0

SMITU indicator calculated for 4th February 2010 will have the following values:

$$\text{SMITU} = (1000 * 0,1 + 500 * 0,3 + 200 * 0,25 + 300 * 0,35) / 10.000 = 4,05 \%$$

The conclusion is that the virtual campus platform of the Academy of Economic Studies in Bucharest, with a certainty level of 4,05% has been subject of unauthorized activities on the 4th February 2010. This value will determine a security level value SL1 to be applied on 5th February 2010.

5. Accessibility in virtual campus

Romania's EU accession requires the identification, ownership and solving social problems integrating the various categories of population. Such a special category are persons with disabilities who are unable to use upper limbs or sense of vision.

Virtual universities must take special measures to improve the access to this social category.

In the United States, virtual universities and federal agencies have adopted the contents of Section 508, which sets standards for accessibility, in order to support students with disabilities. [8]

According to the polls in 2000, the U.S., there are a total of 10 million citizens with vision impairments, 1.3 million of them holding a certificate attesting to this. According to surveys 1.5 million U.S. citizens with vision impairments, access and use the Internet.

Universities, especially public ones, must be a structured such material available in the virtual campus, so its use does not require considerable effort from the visitors.

Many renowned universities from the United States and Europe, have implemented the virtual campus, software for identifying and interpreting the text of your website, or standard output device-the standard output device. Interpretation is, then represented to the user by a speech synthesizer.

Also, the font used by some virtual campuses websites are determining non-readability of the text. On a lot of forums there are discussions that the developers of the websites have treated with priority web page layout, and how they combined text with images, ignoring the fact that this social category is not ready scrolling display materials.

The information inside the virtual campus can contain details such as university campus map, photos of buildings on campus and ways to reach them. The purpose of such a process is to help people with disabilities to identify the location and paths of the campus before being indeed within its physical location.

The security applied to a virtual campus has a strong impact on the accessibility of the virtual campus. Multiple examples that reflect the way the security affects the accessibility such as the strong authentication passwords required to the user, strict format of inputted files, strict setup of different tools used to access the platform which may affect the functionality of the other programs the user frequently use.

6. Conclusions

The virtual universities laboratories are in constant use of students for study and tests, video conferencing and streaming. The online laboratories support extensive real time traffic which places a heavy demand on infrastructure as well as the time of the online laboratories operators.

By comparison with the traditional model of distance learning shows a clear difference from the point of view of efficiency, because the learning methods used in the second case are flexible and relate to the method of learning of each individual student the virtual campus.

The complexity of collaboration systems has a great impact on the effectiveness of learning also need a balance between the number of features and complexity of modules, and accessibility of campus in order to achieve optimal results.

Continuous Internet connection increases the vulnerability of the network to threats such as worms and malicious code. Protective measures for the network were therefore essential, but the University needs to find a way of preventing viruses and malicious attacks that would not interfere with student and faculty work and research.

The use of the security metrics brings a great improvement to the way the virtual campus will work because the resources are allocated depending on the security requirements. The security requirements are determined dynamically, they do not require some one's intervention because they are automatically set up. In this way, as soon as the virtual campus security tool will determine an increase of attacks it will use more resources and will decrease the accessibility level, but in the same time, will reduce the protection to minimum level as soon as the level of attacks has decreased.

References

- [1] J. Bobadilla, F. Serradilla and A. Hernando, „Collaborative filtering adapted to recommender systems of e-learning,” *Knowledge-Based Systems*, Vol. 22, No. 4, pp. 261-265, 2009.
- [2] C. Romero, P. Gonzalez, S. Ventura, M. J. del Jesus and F. Herrera, „Evolutionary algorithms for subgroup discovery in e-learning: A practical application using Moodle data,” *Expert Systems with Applications*, Vol. 36, pp.1632–1644, 2009.
- [3] P. Le Beux and M. Fieschi, „Virtual biomedical universities and e-learning,” *International Journal of Medical Informatics*, Vol. 76, No. 5-6, pp. 331–335, 2007.
- [4] C. Bravo, M. A. Redondo, M. Felisa Verdejo and M. Ortega, „A framework for process–solution analysis in collaborative learning environments,” *Int. J. Human-Computer Studies*, Vol. 66, No. 812–832, 2008.

[5] C. Ciurea, "A Metrics Approach for Collaborative Systems," *Informatica Economică Journal*, Vol. 13, No. 2, 2009, pp. 41-49.

[6] C. Ciurea and B. Zurbagiu, „Virtual Campus Collaborative Learning and its Security,” *The Proceedings of the Ninth International Conference on Informatics in Economy*, pp. 6-13, ASE Publishing House, 07-08 May 2009, Bucharest, Romania.

[7] B. Zurbagiu and L. Popescu, „Security of Virtual Campuses – Collaborative Systems”, *The Journal of Applied Collaborative Systems*, Vol. 1, No. 2, 2009, pp. 111-120.

[8] <http://www.section508.gov/index.cfm?FuseAction=Content&ID=80>

Author



Bogdan ZURBAGIU has a background in computer science and is interested in e-learning campus security systems related issues. He has graduated the Faculty of Economic Cybernetics, Statistics and Informatics from the Bucharest Academy of Economic Studies in 2008. He is currently conducting doctoral research in Economic Informatics at the Academy of Economic Studies. Other fields of interest include software metrics, data structures, object oriented programming in C++ and windows applications programming in C#.