Review: Security Model for Wireless Computer in Virtual Lab

Mr. Hemant N. Watane[1], Ms. Snehal A. Lale[2]

[1]Assistant Professor, Department of Information Technology, Sipna College of Engineering and Technology, Amravati, India

[2]Graduate Student, SGBAU, Amravati, India
[1]hwatane@gmail.com, [2]lale1302snehal@gmail.com

Abstract

After reviewing many security models we came to know for effective security model we require Wireless intranet setup, which leads to secure a wireless network of any organization. This paper deals with such a model to secure a wireless computer virtual laboratory through several authentications by supplying authentication parameter at first step. Fingerprint is use to authenticate that a user is not fake one. Specific time slot is allotted for a user, in order to avoid any counterfeiting practice some security question will pose intermittently. Here Structured System Analysis and Design is use. Java programming language is use as front end and MySql is use as backend. This model is quite different from old models which is based on users name, pin or enrollment number

Keywords: *Wireless intranet, virtual laboratory, intermittently*

1. Introduction

Wireless communications constitute a dominant field of modern technology and research. Over the past decades a considerable number of theories, models and techniques have been proposed for literally every aspect of wireless dissemination of information. Every expert in this field is expected to have a deep understanding of milestone studies at least. Furthermore, hands-on experience and familiarization with wireless hardware and expected diversions from theory are vital for successful network planning. However, acquiring such experience comes at a high monetary cost for the related institutes and trainees, given the requirements for actual hardware and maintenance of up-to-date test beds. Virtual labs constitute a promising solution to such issues [1, 2]

Virtual laboratories are software packages that either provide remote access to real test beds [3, 4], or fully simulate them [5, 6]. The former approach allows for experimentation with real hardware and conditions, but limits the number of users that may take advantage of them concurrently. On the other hand, pure software virtual laboratories may be freely downloaded to any PC and be used without restriction. However, care must be taken during the development phase in order to validate the simulation-derived results with actual measurements. This study presents a software-based virtual laboratory environment, which addresses all vital aspects of wireless communications.

To establish a virtual laboratory an Intranet set up is required. Client server computing and the TCP/IP are conceptual technologies, which are used to build such internet based system. Intra-nets are designed to permit users access that has authentication to the internal Local Area Network of an institute. Within an intra-net, Web Servers are installed in the network. Typically we used the common front end to access information stored on those servers is Browser technology.

The word virtual has been applied to computing and IT with various meanings. It is the used of software systems that act as if they were hardware systems (virtual machine, virtual memory, virtual disk, etc) [7]. Virtual Laboratory is simple laboratory in which exercises and tutorial are stored in digital format and accessible by end user

Power of computerized models will use by virtual laboratory, simulations and a variety of other instructional technologies to replace face-to-face laboratory activities [8]. Due to shared resources of computer network, creation of a virtual laboratory does not ensure complete protection [9]. Unauthorized access to wireless and wired networks will occur through number of different methods and intents, some of which include, accidental association, malicious association, non-traditional networks, identity theft, denial of service and network injection [10 ,11].

Deployment of security architecture is now much more essential because it allows for complex and secure interaction of multiple computer systems, communication models and other infrastructures over public and even private networks. To ensure broad security, an institution must address all host systems and networking devices with a strategy that maximizes users ease and productivity, on the other hand blocking security violations [12].

2. Proposed Model

Security issues in the Virtual LABORATORY come from user trying to hack into the wireless intranet, exchanging password or registration number with other users. Introducing biometric authentication technique as fingerprint technology, which will help into Virtual LABORATORY to check out some security issues, because this things we develop security model (software) to secure a Wireless Computer Virtual Laboratory which use users authentication by fingerprint technology [13]. Things that will be performed by model as:

i. Initially it will allow users to give parameters to registered into the Virtual LABORATORY

ii. It will accept biometric samples (fingerprint) and match it with stored samples

iii. It will assign time slots for users of the Virtual LABORATORY

iv. In order to enhance security, it will pose security questions

2.1 Authentication in Proposed System

By using biometric and pop-up screen we will develop model to secure virtual computer laboratory and it authenticates users and then asks some questions which will answer by user during registration to avoid spoofing. That is the proposed model will designed in such a way that for the virtual Laboratory user will be authenticated, identification parameters will be supplied along with security questions and the user's finger print. When 1st time the user logged-on to the Virtual Laboratory, a time slot is given to each access. At the expiration of the allotted time, the user will automatically logged-out, with a prompt requesting from the user whether more time will be needed. If Y, the user will be prompted to login again. If N, the session will terminates finally [14].

3. System Design

The Security model will design and develop which will based on the Java platform as a standard Java desktop, that application can runs on any operating system like window with the appropriate Java Virtual Machine precise to that operating system. The application will have two ends: the client and server application.

The Virtual Laboratory Client can be hosted on the user's computer which is part of a wireless intranet while the Virtual Laboratory Server can be hosted on any computer on the same intranet. The client and server application will interact with the database. The input atmosphere will provide by client interface for Virtual Laboratory users to register and use it by supplying required details to the database and the environment for login to validate user identification for access into the Virtual Laboratory. The server interface provides the atmosphere to administer the monitors processes and session time such as number of connected clients, number of submitted tutorials, number of request, etc

4. Proposed Implementation

Users' authentication parameters, including fingerprints will take from users and stored it in a database. Anytime a user will access the Virtual Laboratory, the user input will re-collect and matched against the database. Access will grant to a user who has passed the authentication. If fail access will denied.

4.1 Input Data

The input data to the system will capture when a student registers to use the Computer Virtual Laboratory. The data required to be supplied form the different fields in the database. The security questions form part of the input data into the system, which after a while into a session will be twisted and post to a user who get grant to access virtual laboratory this is for the user who still the one which was earlier authenticated.

4.2 Login

At login process, the captured data will store in the database against each register user. A user logs-on by supplying user registration number and fingerprints, which will match against the stored fingerprint pattern. The finger print will capture through a fingerprint scanner, hardware device. The renew button will be used if the print was not properly captured and wish to be recaptured. Cancel button is provided to cancelling login operation. If the fingerprint does not match the one stored in the database, the user will see a message "Miss Match Fingerprint. Try once again".

4.3 Session Time

A Virtual Laboratory Administrator, at the Virtual Laboratory server application end, must set the amount of time (in sec) that will elapse before security questions are posted to the user. The default time will be 30 seconds. If a Virtual Laboratory Administrator clicks on Reset Button, the session time will be set to the default. The Virtual Laboratory Administrator can also monitor the number of clients connected, total number of questions requested and total number of tutorials submitted.

5. Conclusions

The major purpose for this paper has been achieved through the use of fingerprints authentication and intermittent pop-up screen for user verification. Reviewing a security model for wireless computer virtual Laboratory has been found effective for user. This method will used in addition to the traditional constraints employed to authenticate users in a virtual Laboratory. These traditional constraints include user name, user registration number etc. The method adopted is different from other methods of securing a virtual Laboratory which are based only on something that the user knows. The proposed model will be superior as it uses biometrics technology for users' authentication and is economical, simple, easy to use and users' friendly.

Acknowledgments

The making of the paper needed co-operation and guidance of a number of people. I therefore consider it my prime duty to thank all those who had helped me through their venture. It is my immense pleasure to express my gratitude to Ms. Snehal A. Lale who provided me constructive and positive feedback during the preparation of this.

I express my sincere thank to my friends whose encouragement and suggestion helped me to complete my work.

References

[1] Rohrig, C. and Jochheim, A., "The Virtual Lab for controlling real experiments via Internet", In Proceedings of the 1999 IEEE International Symposium on Computer Aided Control System Design (Cat. No.99TH8404), IEEE, (**1999**), pp. 279–284.

[2] Coble, A., Smallbone, A., Bhave, A., Watson, R., Braumann, A. and Kraft, M., "Delivering authentic experiences for engineering students and professionals through e-labs", In Proceedings of the 2010 IEEE Global Engineering Education Conference (EDUCON), IEEE, **(2010)**, pp. 1085–1090.

[3] Jochheim, A. and Rohrig, C. (1999), "The Virtual Lab for teleoperated control of real experiments", In Proceedings of the 38th IEEE Conference on Decision and Control (Cat. No.99CH36304), IEEE, **(1999),** pp. 819–824.

[4] Casini, M., Prattichizzo, D. and Vicino, A., "The automatic control telelab: a user-friendly interface for distance learning", In IEEE Transactions on Education, issue 46, vol. 2, **(2003)**, pp. 252–257.

[5] Sancristobal, E., Castro, M., Harward, J., Baley, P., DeLong, K. and Hardison, J., "Integration view of Web Labs and Learning Management Systems", In Proceedings of the 2010 IEEE Global Engineering Education Conference (EDUCON), IEEE, **(2010),** pp. 1409–1417.

[6] Restivo, M., Lopes, Antonio M., Machado, L. and Moraes, R.-M., "Adding tactile information to remote & virtual labs", In Proceedings of the 2011 IEEE Global Engineering Education Conference (EDUCON), IEEE, **(2011)**, pp. 1120–1124.

[7] Border Charles ,38th Technical Symposium on Com-puter Science Education, Covington, Kenturky, USA, **(2007)** ,576-580.

[8] Gercek, G. and Naveed, S.: Designing a Versatile Dedicated Computing Class-room to Support Computer Nerwork Courses: Insights from a case study. Journal of Information Technology Education, Volume 5, **(2006)**, 13 – 26

[9] Peterson, Larry L. And Davies, Bruce S.: Computer Networks, a Systems Approach. Morgan Kaufmann Publishers, 340 Pine Street, Sixth Floor, San Francisco, USA, **(2007).**

[10] Bardwell, J. and Akin, D.: CWNA Official Study Guide (3rd Edition). McGraw-Hill, **(2005)**, page 45.

[11] N. Sickler, E. Kukula and S. Elliot: The Development of a Distance Education Class in Automatic Identification and Data Capture at Purdue University, in World Conference on Engineering and Technological Education, Santos, Brazi,. **(2004).**

[12] Asor, Vincent E.: On Design and Deployment of Information Security Architecture. Proceeding of the Nigeria Computer Society (NCS), Volume 14, **(2003)**, 388 -395

[13] H Watane , Dr. A. D. Gawande & Prof. A. B. Deshmukh, "Implementation of Security Protocol for Wireless Computer in Virtual Laboratory", International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC); ISSN: 2321-8169, Volume 1, Issue 12, **(2013)**.

[14] H Watane, Dr. A. D. Gawande "Implementation of security protocol for wireless computer network" Print ISSN:2249-9423 & E-ISSN:2249-9431, BIOINFO Security Informatics, Volume 2, Issue 1, **(2012)**, Page: 33- 36.