A Security Model for Wireless Computer Network

H. N. Watane, Dr. A.D.Gawande, A.B. Deshmukh

Abstract— Implementing security model for wireless computer network we require effective Wireless intranet setup, many models are in working to function. This thing is focused at developing a security model to secure a Wireless Computer network of any institution. The model will develop to secure a Wireless Computer class-room through an authentication server by supplying authentication constraint at registration process, which is used at login for comparison then it will store. Fingerprint is used to make sure that a user is who claims to be. Time duration for access is allotted for a user, after which primary constraint will supplied for re-authentication. While a user is still logged-on, some security questions will pose intermittently to avoid counterfeiting. The methodology used for this research will be Structured System Analysis and Design (SSAD). For coding the program Java Programming Language will use and MySQL as a database. The final result of the system will secure model that guarantees secure access. This is different from the security of other wireless virtual class-room which uses only users name, pin or registration number.

Index Terms—Intermittently, Protocol, Security, Spoofing, Fingerprint, Authentication, Virtual Class-Room .

1 INTRODUCTION

The recent era is of computer based network intelligence. This is feasible through digital computer networks which inter communicate multiple computers and other devices that are based on computer data [1].For connecting these computers wireless technologies are used. Wireless networking is based on the technology which enables two or more computers to communicate using standard network models, and there is no need of network cabling.

Due to the advancements in computer technologies and the World Wide Web, it is now possible to suggest engineer to do class-room projects and assignments on a computer. With wireless intranet and internet access, it is now possible for students to be involved in class-room exercises without being physically present in a traditional class-room setting. Usually class-room pose challenges from many aspects such as funding, space, support staff, etc. subsequently, it becomes necessary to design virtualized class-room to eliminate the problems associated with traditional class-room and in turn offer benefits such as effective utilization of computer class-room resources, easy and quick configuration of multiple environments.

To establish a virtual class-room, an Intranet set up is required. Client server computing and the TCP/IP are conceptual technologies, which will use to build such internet based system. Intranets will design to permit users access that has authentication to the internal Local Area Network of an institute. Within an intranet, Web Servers will install in the network. Typically used technology for the common front end access to the information stored on those servers is Browser technology.

The word virtual has been applied to computing and information technology with various meanings. It is the use of software systems that act as if they were hardware systems (virtual machine, virtual memory, virtual disk etc) [2]. Virtual Class-rooms are class-rooms in which exercises and tutorial will store in digital format and accessible by end user. Power of computerized models will use by virtual class-room, simulations and a variety of other instructional technologies to replace face-to-face class-room activities [3].Due to shared resources of computer network, creation of a virtual class-room does not ensure complete protection [4]. 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, man-in-the-middle attack, denial of service and network injection [5] and [6].

Network computers can have their configuration changed, unauthorized students may log onto the server, other laptops

with wireless Network Interface Cards (NIC) can access the wireless intranet, and students may use a laptop that is unprotected against viruses which may infect other computers causing problems in the Virtual Class-room [7] and [8]. Security issue will be one of the detriments of virtual class-room and therefore securing wireless virtual class-room remains an important issue. Security requirements for transmitting information over a network to overcome Security threats are: privacy and confidentiality, integrity, authentication and non-repudiation [12]. In this paper, the use of biometric authentication for securing a virtual class-room will introduce.

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 [9].

2 USER IDENTIFICATION IN COMPUTER SECURITY MODEL

The major building block of any system's security is a proper user identification/authentication which is a crucial part of the access control system. User identification/authentication of Computer Virtual Class-room will correspond to the traditional method based on:

(i) Something that the user knows (typically a PIN, password etc.)

(ii) Something that the user has (example: a key, a token, a magnetic or smart card, a passport etc.) As traditional methods are based on properties that can be forgotten, lost or stolen. These traditional methods of user authentication unfortunately do not work. Passwords often are easily accessible to colleagues or a users share their passwords with their colleagues to make their work easier.

3 THE PROPOSED MODEL

Security issues in the Virtual CLASS-ROOM 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 CLASS-ROOM to check out some security issues, because this things we develop security model (software) to secure a Wireless Computer Virtual Class-room which use users authentication by fingerprint technology. Things that will be performed by model as:

i. Initially it will allow users to give parameters to registered into the Virtual CLASS-ROOM
ii. It will accept biometric samples (fingerprint) and match it with stored samples
iii. It will assign time slots for users of the Virtual CLASS-ROOM
iv. In order to enhance security, it will pose security questions

3.1 Authentication in Proposed System

By using biometric and pop-up screen we will develop model to secure virtual computer class-room 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 class-room 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 class-room, 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.

3.2 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 Class-room Client can be hosted on the user's computer which is part of a wireless intranet while the Virtual Class-room 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 Class-room 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 CLASS-ROOM. 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

3.3 System Flow Diagram

The general idea of the entire system is represented diagrammatically in figure 1 below:

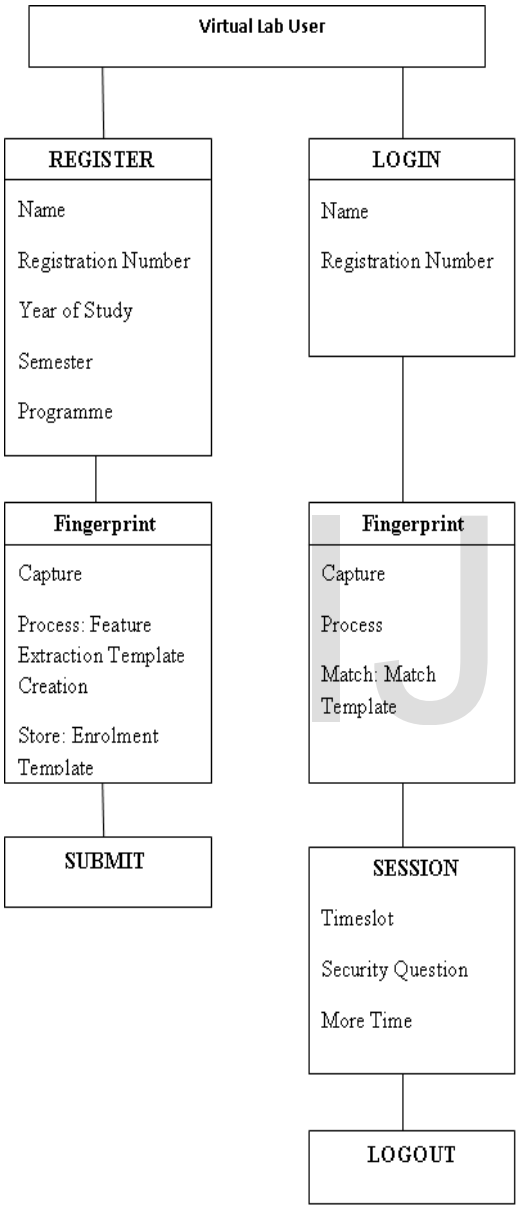

Fig1: System flow diagram

4 IMPLEMENTATION

Users' authentication parameters, including fingerprints will take from users and stored it in a database. Anytime a user will access the Virtual class-room, 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 Class-room. 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 class-room 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 registered 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 Accessing the Server

When a user has successfully logged on into the Virtual CLASS-ROOM, it must supply the name or IP address of the server to be accessed in order to get the questions or submit tutorials. If the server constraint supplied will not valid, the user will receive a prompt.

4.4 Session Time

A Virtual CLASS-ROOM Administrator, at the Virtual CLASS-ROOM 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 CLASS-ROOM Administrator clicks on Reset Button, the session time will be set to the default. The Virtual CLASS-ROOM Administrator can also monitor the number of clients connected, total number of questions requested and total number of tutorials submitted.

During the session time allotted to a user, security questions selected from those answered at registration, will pose from the database to the user; to be sure the user who logs-on is still the one accessing the Virtual CLASS-ROOM. On re-supplying the correct answers earlier given at registration, the user will still be allowed to log-on else the user will be logged-out. At the expiration of the session time, the system will logs out the user with a prompt.

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. Developing a security model for wireless computer virtual class-room has been presented. This method will used in addition to the traditional constraints employed to authenticate users in a virtual class-room. These traditional constraints include user name, user registration number etc. The method adopted is different from other methods of securing a virtual class-room which are based only on something that the user knows. The develop model will be superior as it uses biometrics technology for users' authentication and is economical, simple, easy to use and users' friendly.

REFERENCES

[1] Wohorem, Evans E.: Information Technology in the Nigeria Banking Industry. Spectrum Books Ltd, Spectrum House, Ring Road, Ibadan, Nigeria, 2000

[2] Border, Charles**,** The Development and Deployment of a Multi-user Access Virtualization System for Networking Security and System Administration Classes. Proceedings of the 38th Technical Symposium on Computer Science Education, Covington, Kenturky, USA, 2007, 576 – 580

[3] 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

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

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

[6] 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

[7] Podio, Fernado L. and Dunn, Jeffrey S.: Biometric Authentication Technology: From the Movies to your Desktop, Convergent information Systems Division, 2002

[8] Bubeck, U. and Sanchez, D.: Term Project, Dan Diego State University, 2003

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

[10]Edward N. Udo, Imo J. Eyo, Ini J. Umoeka; Developing a Security Model for a Wireless Computer Virtual Laboratory, 2011

[11]Lammle, Todd: CISCO Certified Network Associate Study Guide (4th Edition). Sybex Inc., 1151 Marina Village Parkway, Alameda, 2004

[12]Leon-Garcia, A. and Widjaja, I: Communication Networks, Fundamental Concepts and Key Architectures. McGraw Hill Higher Education, Boston Burr Ridge, New York, 2000

[13]Tapscott, D.; The Digital Economy. Promise and Peril in the age of Digital Intelligence. McGraw Hill, New York, 1996

[14]Ward, T. **:** Planning an Intranet Model for success Intranet. http://www.presidentdigital.com/articles/intranetarticles/intranet planning-an-intranet-model-for-success. (last visited, June 2009)

First Author H. N. Watane, M.E. student, Department of Computer Science Engineering, Sipna's COET, Amravati-India

Second Author Dr. A. D. Gawande, Head of Department (CSE), Sipna'sCOET, Amravati-India

Third Author A. B. Deshmukh, Department of Computer Science Engineering, Sipna's COET, Amravati-India