Advanced Authentication Using 3D Passwords in Virtual World

Nisha Salian, Sayali Godbole, Shalaka Wagh

***Abstract*— Providing Authentication to any system leads to provide more security to that system. There are many authentication techniques, such as textual password, graphical password, etc. but each of this individually having some limitations & drawbacks. To overcome the drawbacks of previously existing authentication technique, a new improved authentication technique is proposed. This authentication Scheme is called as "3D passwords". It is multi-password & multi-factor authentication system as it combines a various authentication techniques such as textual password, graphical password etc. Most important part of 3d password scheme is inclusion of 3d virtual environment. A 3d virtual environment consists of real time object scenarios. It is not an actual real time environment, it is just a user interface provided to scheme which looks like a real environment. This authentication scheme is more advanced than any other schemes as we can combine any existing or upcoming schemes. Also this scheme is hard to break & easy to use. In this paper we have introduced our contribution towards 3D Password to make it more secure & more user-friendly to users of all categories. This paper also explains: what is 3D password? , working of 3D password scheme, some mathematical concept related to 3D password, applications of scheme etc. All these concepts are briefly introduced & explained in this paper section wise.**

***Index Terms*— Authentication, Multi-password, Textual Passwords, 3D Password, 3D Virtual Environment.**

I. INTRODUCTION

The authentication system which we are using is mainly very light or very strict. Since many years it has become an interesting approach. With the development in means of technology, it has become very easy for 'others' to hack someone"s password. Therefore many algorithms have come up each with an interesting approach toward calculation of a secret key. The algorithms are such based to pick a random number in the range of 10^6 and therefore the possibilities of the sane number coming is rare. We are provided with many password types such as textual passwords, biometric scanning, tokens or cards (such as an ATM) etc. But there are many weaknesses in current authentication systems. When a person uses textual passwords, he likely chooses meaningful words from dictionary or their nick names, girlfriend, birthdates, etc. which can be cracked easily. And if a password is hard to guess then it is hard to remember also. Users face difficulty in remembering a long and random appearing password and because of that they create small, simple, and insecure passwords that are easy to attack. Graphical passwords are also in use. Their strength comes from the fact that users can recall and recognize pictures more than words. But, their password space is usually very less and they are easy to reproduce if it"s seen when user is performing password. Token based systems can also be used as way of authentication. But smart cards or tokens are susceptible to loss or theft. Biometric scanning is your "natural" signature and Cards or Tokens prove your validity. But users tend to resist biometrics as it is very intrusive and can"t be revoked. Now-a-days as the technology has changed many fast processors and tools are available on internet it has become very easy to crack the traditional authentication schemes. So in this paper, we have introduced 3D password a new generation authentication scheme.

II. RELATED WORKS

Many graphical password schemes have been proposed previously. Blonder introduced the first graphical password schema. Blonder"s idea of graphical passwords is that by having a predetermined image, the user can select or touch regions of the image causing the sequence and the location of the touches to construct the user"s graphical password. After Blonder, the notion of graphical passwords was developed. Many graphical password schemes have been proposed. Existing graphical passwords can be categorized into two categories as follows:

1) recall-based

2) recognition-based. [1][2][3][5]

Recognition-based graphical password is Pass faces. Pass faces simply works by having the user select a subgroup of k faces from a group of n faces. For authentication, the system shows m faces and one of the faces belongs to the subgroup k. The user has to do the selection many times to complete the authentication process. Another scheme is the Story scheme, which requires the selection of pictures of objects (people, cars, foods, airplanes, sightseeing, etc.) to form a story line. Davis et al, concluded that the user"s choices in Pass faces and in the Story scheme result in a password space that is far less than the theoretical entropy. Therefore, it leads to an insecure authentication scheme. The graphical password schema of Blonder is considered to be recall based since the user must remember selection locations. Moreover, Pass Point – is a recall-based graphical password schema, where a background picture is presented and the user is free to select any point on the picture as the user"s password (user"s Pass Point). Draw A
Secret (DAS), which is a recall-based graphical password

Manuscript received February 11, 2015.

Nisha Salian, Department of Computer Engineering, K.J. Somaiya College of Engineering, Vidyavihar.
Sayali Godbole, Department of Computer Engineering, K.J. Somaiya College of Engineering, Vidyavihar.
Shalaka Wagh, Department of Computer Engineering, K.J. Somaiya College of Engineering, Vidyavihar.

schema and introduced by Jermyn et al., is simply a grid in which the user creates a drawing. The user‟s drawings, which consist of strokes, are considered to be the user‟s password. The size and the complexity of the grid affect the probable password space. Larger grid sizes increase the full password space. However, there are limitations in grid complexity due to human error. It becomes very hard to recall where the drawing started and ended and where the middle points were if we have very large grid sizes.[7][8]

III. PROPOSED SYSTEM

Proposed authentication scheme is combination of many other authentication schemes together. 3D password is combination of both recall-based (i.e. textual password, etc) & recognition based (i.e. graphical password, biometrics, etc). so that 3D password is multifactor & multi password authentication scheme. Refer fig. below

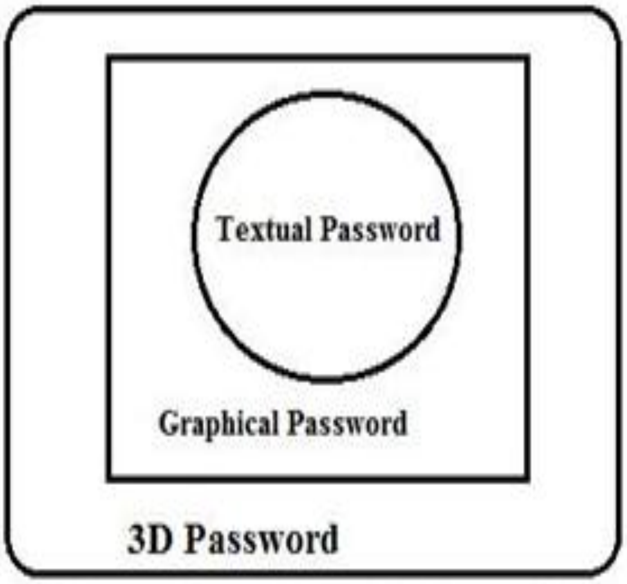

Fig. 3D password as Multi-factor & Multi-password Authentication scheme.

For authentication with 3D password a new virtual environment is introduced called as 3D virtual environment where user navigate, moving in 3D virtual environment to create a password which is based on both the schemes.

We don„t use biometric scheme because biometric having some major drawbacks (like h/w cost is more) So that we have not included biometric authentication in our 3D password scheme. Biometric authentication is efficient over shoulder surfing attack. But other attacks are possible & easy on biometric authentication. Also inclusion of biometric leads to increasing the complexity and cost of scheme & more hardware parts needed.

Figures below shows some snapshots of 3D Virtual Environment of different real time scenarios created in virtual environments. These virtual environments are interactive virtual environment as user can interact with these environments & creates his/her own 3D password easily.

Fig. snapshots of 3D Virtual Environments

Objective of proposed system:

- To provide more secure authentication technique than existing one.
- To design & develop more user friendly & easier authentication scheme and giving user to freedom of selecting more than one password scheme as single system.
- To overcome the drawbacks & limitations of previously existing systems (textual password, graphical password. Etc.).
- New scheme should be combination of recall-, recognition -based authentication schemes.

IV. SYSTEM OVERVIEW

The 3D password is a multifactor authentication scheme. The 3D password presents a 3D virtual environment containing various virtual objects. The user navigates through this environment and interacts with the objects. The 3D password is simply the combination and the sequence of user interactions that occur in the 3D virtual environment. The 3D password can combine recognition, recall, token, and biometrics based systems into one authentication scheme. This can be done by designing a 3D virtual environment that contains objects that request information to be recalled, information to be recognized, tokens to be presented, and biometric data to be verified.

For example, the user can enter the virtual environment and type something on a computer that exists in (x1 , y1 , z1) position, then enter a room that has a fingerprint recognition device that exists in a position (x2 , y2 , z2) and provide his/her fingerprint. Then, the user can go to the virtual garage, open the car door, and turn on the radio to a specific channel. The combination and the sequence of the previous actions toward the specific objects construct the user‟s 3D password. Virtual objects can be any object that we encounter in real life. Any obvious actions and interactions toward the real life objects can be done in the virtual 3D environment toward the virtual objects. Moreover, any user input (such as speaking in a specific location) in the virtual 3D environment can be considered as a part of the 3D password. We can have the following objects:

1. A computer with which the user can type.
2. A paper or a white board that a user can write on.
3. An ATM machine that requires a smart card and PIN.
4. A light that can be switched on/off.
5. A television or radio where channels can be selected.
6. A staple that can be punched.
7. A car that can be driven.
8. A chair that can be moved from one place to another.
9. Any graphical password scheme

Design Guidelines :

Designing a well-studied 3D virtual environment affects the usability, effectiveness, and acceptability of a 3D password system. Therefore, the first step in building a 3D password system is to design a 3D environment that reflects the administration needs and the security requirements. The design of 3D virtual environments should follow these guidelines.

1) **Real-life similarity**: The prospective 3D virtual environment should reflect what people are used to seeing in real life. Objects used in virtual environments should be relatively similar in size to real objects (sized to scale). Possible actions and interactions toward virtual objects should reflect real-life situations. Object response should be realistic. The target should have a 3D virtual environment that users can interact with, by using commonsense.

2) **Object uniqueness and distinction**: Every virtual object or item in the 3D virtual environment is different from any other virtual object. The uniqueness comes from the fact that every virtual object has its own attributes such as position. Thus, the prospective interaction with object 1 is not equal to the interaction with object 2. Refer following scene

Fig. snapshot of 3D Virtual Environment

Therefore, the design of the 3D virtual environment should consider that every object should be distinguishable from other objects. However, having similar objects such as 20 computers in one place might confuse the user. Similarly, in designing a 3D virtual environment, it should be easy for users to navigate through and to distinguish between objects. The distinguishing factor increases the user‟s recognition of objects. Therefore, it improves the system usability.

3) Three-dimensional virtual environment size: A 3D virtual environment can depict a city or even the world. On the other hand, it can depict a space as focused as a single room or office. The size of a 3D environment should be carefully studied. A large 3D virtual environment will increase the time required by the user to perform a 3Dpassword. Moreover, a large 3D virtual environment can contain a large number of virtual objects. Therefore, the probable 3D password space broadens. However, a small 3D virtual environment usually contains only a few objects, and thus, performing a 3D password will take less time.

4) Number of objects (items) and their types: Part of designing a 3D virtual environment is determining the types of objects and how many objects should be placed in the environment. The type of objects reflect what kind of responses that they will receive. For simplicity, we can c

5) onsider requesting a textual password or a fingerprint as an object response type. Selecting the right object response types and the number of objects affects the probable password space of a 3D password.

6) Position of objects/Alignment: The 3D environment should be such that there is no obvious set of movements that the user will tend to make password. For example in following scene, users are more likely to choose 1st 3 computers as password making it easy to guess for hackers.

Fig. snapshot of 3D Virtual Environment

So consider following figure where there is more than one easy to remember password.

Fig. snapshot of 3D Virtual Environment

6**) System importance**: The 3D virtual environment should consider what systems will be protected by a 3D password.

The number of objects and the types of objects that have been used in the 3D virtual environment should reflect the importance of the protected system.

V. WORKING

Consider a three dimensional virtual environment space that is of the size G×G×G. Each point in the three dimensional environment space represented by the coordinates (x, y, z) ∈ [1..G] × [1..G] ×[1..G]. The objects are distributed in the three-dimensional virtual environment. Every object has its own (x,y,z) coordinates. Assume the user can navigate and walk through the three-dimensional virtual environment and can see the objects
and interact with the objects. The input device for interactions with objects can be a mouse, a

keyboard, stylus, a card reader, a microphone…etc. For example, consider a user who navigates through the 3D virtual environment that consists of a ground and a classroom. Let us assume that the user is in the virtual ground and the user turns around to the door located in (9, 16, 80) and opens it. Then, the user closes the door. The user types "ANGEL" into a computer that exists in the position of (10, 5, 25). The user then walks over and turns off the light located in (15, 6, 20), and then goes to a white board located

in (55, 3, 30) and draws just one dot in the (x,y) coordinate of the white board at the specific point of (420,170). The user then presses the login button. The initial representation of user actions in the 3Dvirtual environment can be recorded as follows:[2]

(9, 16, 80) Action = Open the office door;
(9, 16, 80) Action = Close the office door;
(10, 5, 25) Action = Typing, “S”;

(10, 5, 25) Action = Typing, “A”;
(10, 5, 25) Action = Typing, “Y”;

(10, 5, 25) Action = Typing, “A”;

(10, 5, 25) Action = Typing, “L”;

(10, 5, 25) Action = Typing, “I”;
(15, 6, 20) Action = Turning the Light Off;

(55, 3, 30) Action = drawing, point = (420,170)

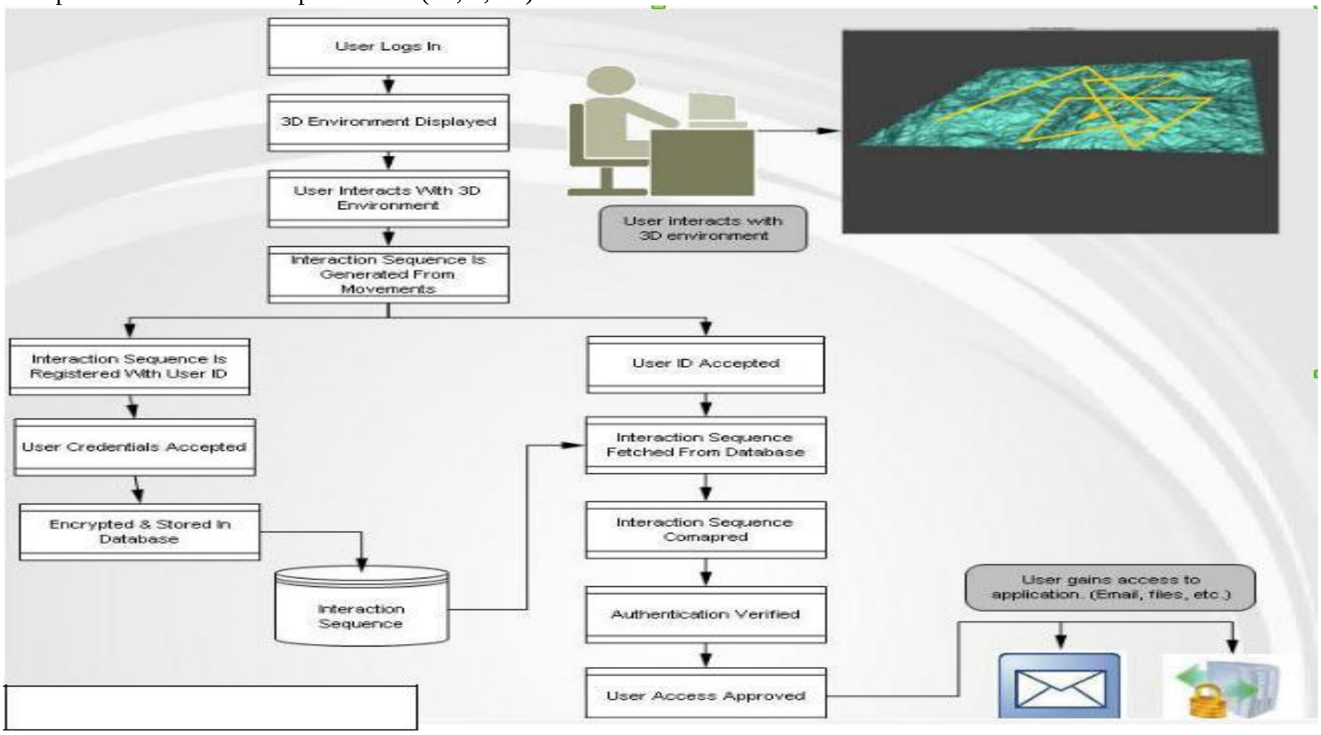
User Logs In
3D Environment Displayed
User Interacts With 3D Environment
Interaction Sequence Is Generated From Movements
User interacts with 3D environment
Interaction Sequence Is Registered With User ID
User Credentials Accepted
Encrypted & Stored In Database
Interaction Sequence
User ID Accepted
Interaction Sequence Fetched From Database
Interaction Sequence Comapred
Authentication Verified
User Access Approved
User gains access to application. (Email, files, etc.)

Fig: Flow diagram of project. [1]

Possible enhancements:

1. Designing customized 3D environments as per user‟s liking
2. Giving option of selecting their environment from more than one possible environment.
3. Continuously adding upcoming authentication schemes
4. For real-time use giving options like forgot password, reset password, etc.
5. Encrypting the passwords of user using various

   encryption schemes like AES
6. Reducing storage size of password using compression techniques.

VI. 3D PASSWORDS DIFFERENTIATORS

- **Flexibility***: 3D Passwords allows Multifactor* The 3-D password has a very large probable pass- word *authentication biometric, textual passwords can be embedded in 3D password technology.*
- **Strength***: This scenario provides almost unlimited passwords possibility.*
- **Easy to Remember**: can be remembered in the form of short story.

Privacy: Organizers can select authentication schemes that respect user‟s privacy.

VII. MATHEMATICAL CONCEPTS RELATED TO 3D PASSWORD SCHEME

3D password is a authentication technique which can be implemented in 3D virtual environment. As every project having problem statement which is relation with mathematical concepts like feasibility study, complexities, set theory etc. this section of paper will explain almost all the mathematical concepts applied while creating 3D password schemes.

A. Time Complexity

For calculating the time complexity of 3D password scheme let„s assume A be the virtual 3d environment plotting, & B is algorithmic processing. From this data available we have come to time complexity of system. Equation (1) gives the time complexity of proposed system. Time Complexity= (1). Where m is time required to communicate with system, & n is time required to process each algorithm in 3d environment.

B. Space Complexity

This system include 3D virtual environment, so that each point in this environment will having 3 co-ordinate values. Any point from 3D virtual environment is represented in the form of (X, Y, Z).Where X, Y & Z are the coordinate values stored for particular point. We are storing three co-ordinate values of each point such as (x1, y1, z1). There for space complexity of proposed system is n3.

VIII. 3-D PASSWORD APPLICATIONS

Because a 3-D password can have a password space that is very large compared to other authentication schemes, the 3-D password‟s main application domains are protecting critical systems and resources. Possible applications include the following.

1) Critical servers: Many large organizations have critical servers that are usually protected by a textual password. A 3-D password authentication proposes a sound re-placement for a textual password. Moreover, entrances to such locations are usually protected by access cards and sometimes PIN numbers. Therefore, a 3-D password can be used to protect the entrance to such locations and protect the usage of such servers.

Nuclear and military facilities: Such facilities should be protected by the most powerful authentication systems.

space, and since it can contain token-, biometrics-, recognition-, and knowledge-based authentications in a single authentication system, it is a sound choice for high-level security locations.

3) Airplanes and jetfighters: Because of the possible threat of misusing airplanes and jetfighters for political agendas, usage of such airplanes should be protected by a powerful authentication system. The 3-D password is recommended for these systems.

In addition, 3-D passwords can be used in less critical systems because the 3-D virtual environment can be designed to fit any system‟s needs. A small 3-D virtual environment can be used in many systems, including the following:[1][2][4]

1) ATMs;
2) Personal digital assistants;
3) Desktop computers and laptop logins;
4) Web authentication

IX. EXPERIMENTAL RESULTS

We have built an experimental 3-D virtual environment that contains several objects. The type of response is graphical passwords. We asked 10 users to experiment with our environment. We asked the users to create their 3-D password and to sign-in using their 3-D password several times over several days.

A. Experimental Virtual 3-D Environment

In our experiment, we have used Unity game engine to build the 3-D virtual environment .We have created two experimental environments. The design of the first experimental 3-D virtual environment represents an art gallery that the user can walk through and the second is shooting game environment.

B. User Study

We conducted a user study on 3-D passwords using the experimental 3-D virtual environments. The study reviewed the usage of textual passwords and other authentication schemes. The study covered almost 30 users. The users varied in age, sex, and education level. Even though it is a small set of users, the study produced some distinct results [9], [11].

We observed the following regarding graphical passwords, 3-D passwords, and other authentication schemes.

1) Most users who use textual passwords of 9–12 character lengths or who use random characters as a password have only one to three unique passwords.

2) More than 50% of user‟s textual passwords are eight characters or less.

3) Almost 25% of users use meaningful words as their textual passwords.

4) Almost 75% of users use meaningful words or partially meaningful words as their textual passwords. In contrast, only 25% of users use random characters and letters as textual passwords.

5) Over 40% of users have only one to three unique textual passwords, and over 90% of users have eight unique textual passwords or less.

6) Over 90% of users do not change their textual passwords unless they are required to by the system.

7) Over 95% of users under study have never used any graphical password scheme as a means of authentication.

8) Most users feel that 3-D passwords have a high acceptability.

9) Most users believe that there is no threat to personal privacy by using a 3-D password as an authentication scheme.

X. CONCLUSION AND FUTURE WORK

In the existing system, Textual passwords and token-based passwords are the most commonly used authentication schemes. Many other schemes are also there like graphical password, biometric authentication scheme etc which are used in different fields. The main goal of this paper is to have a scheme which has a huge password space and which is a combination of any existing, or upcoming, authentication schemes into one scheme. While using 3D password, users have the freedom to select whether the 3D password will be solely recall, biometrics, recognition, or token based, or a combination of two schemes or more. Users do not have to provide their fingerprints if they do not wish to. Users do not have to carry cards if they do not want to. They have the choice to construct their 3D password according to their needs and their preferences. A 3D password's probable password space can be reflected by the design of the three-dimensional virtual environment, which is designed by the system administrator. The three dimensional virtual environment can contain any objects that the administrator feels that the users are familiar with. The 3D password is just introduced means it is in its childhood. A study on a large number of people is required. We are looking at designing different three-dimensional virtual environments that contain objects of all possible authentication schemes. The main application domains of 3D Password are critical systems and resources. Critical systems such as military facilities, critical servers and highly classified areas can be protected by 3D Password system with large three dimensional virtual environments. Moreover, Airplanes and jet fighters, ATM's and operating system's logins can also make use of 3D passwords to provide more secured authentication Finding a solution for shoulder surfing attacks on 3D passwords and other authentication schemes is a field of study.

REFERENCES

[1] Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, Pranjal Rathod,"Secure Authentication with 3D Password ",International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 2, March 2013

[2] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik, "A Novel 3D Graphical Password Schema‖, IEEE International Conference on Virtual Environments, Human-Computer Interfaces, and Measurement Systems, July 2006.

[3] Max-Emanuel Maurer, Rainer Waxenberger, Doris Hausen," BroAuth: Evaluating Different Levels of Visual Feedback for 3D Gesture-Based Authentication ", AVI "12, May 21-25, 2012, Capri Island, Ital © 2012 ACM.

[4] Ms. Vidya Mhaske-Dhamdhere , Prof. G. A. Patil ," Three Dimensional Object Used for Data Security",2010 International Conference on Computational Intelligence and Communication Networks © 2010, IEEE.

[5] Shraddha M. Gurav , Leena S. Gawade , Prathamey K. Rane , Nilesh R. Khochare, "Graphical Password Authentication" , 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies © 2014 IEEE

[6] Karen Renaud, Peter Mayer, Melanie Volkamer and Joseph Maguire , "Are Graphical Authentication Mechanisms As Strong As Passwords?" , 2013 Federated Conference on Computer Science and Information Systems pp. 837–844 © 2013, IEEE

[7] A.B.Gadicha , V.B.Gadicha , ―Virtual Realization using 3D Password‖, in International Journal of Electronics and Computer Science Engineering, ISSN 2277-1956/V1N2-216-222

[8] Duhan Pooja, Gupta Shilpi , Sangwan Sujata, & Gulati Vinita, ―SECURED AUTHENTICATION: 3D PASSWORD‖, I.J.E.M.S., VOL.3(2),242 – 245, 2012.

[9] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords," in Proc. 8th USENIX Security Symp., Washington DC, Aug. 1999, pp. 1–14.

[10]Thorpe and P. C. van Oorschot, "Graphical dictionaries and the memorable space of graphical passwords," in Proc. USENIX Security, San Diego, CA, Aug. 9–13, 2004, p. 10.

[11] A. Adams and M. A. Sasse, "Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures," Commun. ACM, vol. 42, no. 12, pp. 40–46, Dec. 1999