Pixel Security

R.Dhinesh[1], N.P.Harikrishna[2], K.R.Lokesh[3], Dr.J.Selvakumar[4]
[1, 2, 3] Dept of computer science Engineering
[3]Assistant Professor, Dept of computer science Engineering
[1, 2] Sri Ramakrishna College of Engineering,
Coimbatore, India

Abstract- *The underlying issues relating to the required and safety of various key words are largely unexplored. However, we know that people generally have difficulty remembering various key words. This reduces security since users reuse the same key word for different systems or reveal other key words as they try to log in. We report on a laboratory study comparing recall of various text key words with recall of various click-based image based key words. In a one-hour session (short-term), we found that participants in the image based key word condition coped significantly better than those in the text key word condition. In particular, they made fewer errors when recalling their key words, did not resort to creating key words directly related to account names, and did not use similar key words across various accounts. After two weeks, participants in the two conditions had recall success rates that were not statistically different from each other, but those with text key words made more recall errors than participants with image based key words. In our study, click-based image based key words were significantly less susceptible to various key word interference in the short-term, while having comparable usability to text key words in most other respects.In this project, a image based key word system with a supportive sound signature to increase the remembrance of the key word is discussed. In proposed work a click-based image based key word scheme called Cued Click Points (CCP) is presented. In this system a key word consists of sequence of some images in which user can select one click-point per image. In addition user is asked to select a sound signature corresponding to each click point this sound signature will be used to help the user in recalling the click point on an image*

Keywords- Cued Click Points (CCP),various key words,image based key words,text key words,click-based image based key words.

I. INTRODUCTION

Special consideration is required to design usable, understandable, and manageable security features. At first glance, it seems like applying standard usability and Human-Computer Interaction principles should suffice, but security constraints make this problematic. Most importantly, some design features that might make a system more usable would also make it less secure. Addressing these security weaknesses can too easily render the software unusable again. Even worse, one might argue that an unusable security system is inherently insecure, since users will then misuse or bypass the security mechanisms. One must also consider how the design affects the observable behaviour of legitimate users, in case such behaviour could be exploited by attackers. The challenge is to design software that is both secure and usable. In this paper, we address an important issue in user authentication software: the memorizing of various key words. Authentication software supports legitimate users in gaining access to systems or resources by verifying their credentials. We focus on key words, the most common form of credentials. The problem with key words is making them easy for legitimate users to remember, but difficult for attackers to guess. Alternatives to key words include physical tokens or biometrics; these also have problems, such as cost, management, and privacy, which we will not address in the paper. As key words are the most common method of authentication, the key word problem is important, and is made worse by the increasing number of users and the number of different systems they access. In particular, users now need to remember not just one key word, but many. This places a significant memory load on users, leading them to choose (and reuse) simple key words that are easy for attackers to guess. Despite this reality, there has been little work investigating the issues relating to various key words. Our current work is motivated by recent proposals for alternative kinds of key words, particularly click-based image based key words [3, 39]. In such systems, the user does not enter a text key word using a keyboard, but instead clicks on particular points on an image. Such image based key words are intended to take advantage of the human ability to more easily recognize and recall images than textual information . We wished to study whether this approach had advantages over text key words when various distinct key words were necessary. We were concerned about the potential for various key word interference, where remembering a key word for one system might affect the user's memory of a key word for another system. As described in the cognitive psychology literature, memory interference is "the impaired ability to remember an item when it is similar to other items stored in memory". Our study was conducted in a laboratory setting

where 65 participants were assigned to use either textual or image based key words. They created six distinct key words for several different "accounts", and later had to recall the key words for each account in a different order than they were created. Twenty-six of those participants also returned after two weeks to test recall of these key words. In the case of image based key words, each account was associated with a different image, so participants had one image per key word. Literature on memory research acknowledges that ceiling effects, such as high success rates that mask differences between conditions, are a problem which must be overcome with careful experimental design in order to get meaningful results. While our study does not mirror real-life usage of key words, the intent of the experiment was to highlight differences in performance. We found that in the short-term, participants had more difficulty recalling various text key words than various image based key words. However, after two weeks, both groups had significant difficulty remembering their key words and there was no statistical difference in success rates. We further found that participants in the text condition could more easily recall their key words when they used insecure key word practices, such as choosing key words that followed a common pattern or that were obviously associated with account names. For example, 40% of text key words were obviously related to their associated account. These results constitute evidence for an important advantage inherent in click-based image based key words – built-in cueing that helps with memorizing – while text key word systems encourage users to adopt insecure coping strategies. In post-hoc analysis, we found that males were more successful than females with image based key words and those males were more likely to use account-related text key words.

II. BACKGROUND AND RELATED WORK

Security is rarely a user's primary task, and typically involves an extra step in addition to the main task, such as having to log in to read one's email. Users need security features to be as non-disruptive as possible, but still need them to work properly to preserve integrity and privacy. A second unusual characteristic of security software is that it attracts illegitimate users of the system who are actively trying to gain unauthorized access. These attackers will take advantage of all information available. Usable security software must therefore offer assistance to legitimate users, without giving assistance to attackers. In particular, this changes the nature of feedback in interaction design, which must inform legitimate users while revealing no useful information to others. With any authentication system where users are expected to recall information to log in, there is a risk of memory interference. Multiple key word interference occurs when users must remember key words for many systems and the memories of the different key words interfere with each other. Studies have shown that users typically create easy-to-guess text key words and reuse these key words across several accounts. When trying to log in, they will cycle through their key words until they find one that works. report that users in their lab study tried an average of 2.43 key words before a correct login. This may be under-reporting the problem, however, because users in their study were only allowed 90 seconds per account. While this trial-anderror approach helps users deal with key word systems and multiple key word interference, revealing all of one's key words at every login can amplify security risks, for example in the presence of key loggers or when key words are sent to phishing sites. We are interested in the image based key word approach. It has been suggested that image based key words may be less susceptible to multiple key word interference since humans have better memory for recognizing and recalling images than text. Many of these have the added advantage of presenting a cue to the user to help trigger the appropriate memory. Cued-recall has been established as an easier memory task thancued recall. With cued-recall, the system provides a cue to help prompt the user's memory of the key word (or a portion thereof). This is a desirable usability feature that reduces the memory load on users. With clickbased image based key words, a key word consists of user-selected click-points on the images presented. Therefore, the images act as mnemonic cues to remember the corresponding click-points. In PassPoints, users are presented with an image, and a key word consists of 5 click-points on the image. To log in, users must select the same 5 click-points in the same order. The system allows for a tolerance area around each click-point so that approximately correct login attempts are accepted. Several user studies and security analyses have been conducted on PassPoints. While these have found PassPoints to be generally usable, security concerns have been raised because users tend to select predictable key words which are exploitable in dictionary attacks. Newer click-based image based key word schemes, such as Persuasive Cued Click-Points address two important security concerns with respect to user selected key words: they offer a significant reduction in hotspots (i.e., areas of the image that have higher probability of being selected by users) and in the use of click-point patterns (such as selecting click-points that form a straight line across the image). These characteristics significantly reduce vulnerability to dictionary attacks. The present paper uses the better-known PassPoints scheme for these interference tests, in order to leverage a more closely-examined and understood key word scheme and to build on existing results on interference between two key words.

III. LITERATURE REVIEW

We concentrate on click-based image based key word schemes where a user clicks on a number of set points in a background image and work is related to guessing attacks on image based key words. In Blonder's proposal user's click on a set of predefined regions. In our proposal user is asked to select a number of images from a set of random pictures. Pass points allow users to click a sequence of some points anywhere on an image with a error tolerance. e, error tolerance can be set to as p=4.An attacker could predict hot spots by using image processing tool for guessing pass points key words and for other images their method guessed 9.1% and 0.9% of key words on two images using an dictionary attack 235 entries compared to key word space 243 key word. Some of the click-order patterns evaluated with human seeded attacks is DIAG and other is LINE and other click based image based key word schemes CCP and PCCP. The major advantage of pass points is its large key word space over alphanumeric key words. The large key word space is significant because it reduces the guess ability of key words

3.1 Survey

Recognition based systems also known as econometric systems or search metric systems generally require that users memorize a portfolio of images during key word creation, and then to log in, must recognize their images. Recognition based systems have been proposed using various types of images. Phishing attacks are somewhat more difficult with recognition-based systems because the system must present the correct set of images to the user before key word entry. Shoulder-surfing seems to be of particular concern in recognition-based systems when an attacker can record or observe the images selected by users during login. For PassFaces, the analysis of user choice by Davis et al.showed that users tend to select attractive faces of their own race; and that users selected predictable sets of faces such that an attacker knowing one face could determine the face most likely to be selected as the next key word part. Because users tend to select predictable images, successful dictionary attacks may be expected, as well as personalized attacks, e.g., if attackers know a user's race or gender. Davis et al. guessed 10% of key words created by male participants in 2 guesses. A major conclusion was that many image based key word schemes, including Faces, may require "a different posture towards key word selection" than text key words, where selection by the user is the norm. As noted in Section (which also mentions user choice issues in the Story scheme [10]), a phishing attack on PassFaces requires a MITM attack Recall based systems In this section two types of picture key word techniques used reproduce a secret drawing and repeat a selection. In these systems, users typically draw their key word either on a blank canvas or on a grid i.e, DAS technique proposed by Jermyn .Passlogix hasalso developed several image based key word techniques based on repeating a sequence of actions. For example, its v-Go includes a image based key word scheme where users can mix up a virtual cocktail and use the combination of ingredients as a key word. Other key word options include picking a hand at cards or putting together a "meal" in the virtual kitchen. However, this technique only provides a limited key word space and there is no easy way to prevent people from picking poor key words (for example, a full house in cards).

3.2 Image based key word Attacks

Brute Force Attack

This type of attack uses an algorithm that produces every possible combination of words to break the key word. Text-based key word contains 94^N number of space where 94 is the number of printable characters (including space) and N is the length. This type of attack has always proven successful against text-based key word because of its ability to check all possibility within the length of the key word. As such, users are advised to select a stronger and complex key word to prevent discovery from brute force attack (Eiji Hayashi, 2008). However, GUA proves to be more resistant to brute force attacks since the attack software needs to produce all possible mouse motions to imitate key words especially when trying to recall the image based key words. One of the reasons that helped is the large key word space present in most image based key words techniques which is not available in the textual variant

Dictionary Attack

This ingenious attack uses words found in the dictionary to check if any were used as key words by the users. Many users' uses weak key words which make it easier for attackers to guess the key word using the image based dictionary attack[6]. Because of image based key word method of using mouse input type recognition, using dictionary attack on GUA would be a waste of time. Dictionary attacks against recognition and cued-recall image based key word systems require more effort upfront than against text key words or recall-based image based key words, since attackers must first collect one or more of a set of images. Images gathered for one system will not help attacks on a second system, unless both systems use the same image set. During recall, it is more difficult and complex to use the automated dictionary method to produce all possibility of a single user pixel of an image than a text-based attack

IV. EXISTING SYSTEM

In the existing system**,** Brostoff and sasse carried out an empirical study of passfaces, which illustrates well how a image based key word recognition system typically operates. Blonder-style key words are based on cued recall. A user pixels on several previously chosen locations in a single image to log in. As implemented by Passlogix Corporation, the user chooses several predefined regions in an image as his or her key word. To log in the user has to pixel on the same regions in effect, cued pixel points (ccp) is a proposed alternative to passpoints. In ccp, users pixel one point on each of 5 images rather than on five points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest pixel-point (at which point they can cancel their attempt and retry from the beginning). It also makes attacks based on hotspot analysis more challenging. Each pixel results in showing a next-image, in Effect leading users down a "path" as they pixel on their sequence of points. A wrong pixel leads down an incorrect path, with an explicit indication of authentication failure only after the final pixel. Users can choose their images only to the extent that their pixel-point dictates the next image. While the predictability problem can be solved by disallowing user choice and assigning key words to users, this usually leads to usability issues since users cannot easily remember such random key words. Number of image based key word systems has been developed, Study shows that text-based key words suffers with both security and usability problems. Multiple key word interference was also examined as part of a field study of PassPoints. In this study, a subset of participants had two distinct key words to remember (on two different images). These participants had lower login success rates than those with only one key word. We are not aware of comparable studies for regular text key words, so it is unknown how this performance decrease compares with text key words. Vu et al. conducted lab studies examining the effect of various text key word restrictions on memorizing when multiple key words were used. Their results include that users with five key words had more difficulty than those who had only three that some users selected key words with obvious connection to their accounts, and that key word restrictions were not sufficient for encouraging secure text key word selection. One proposed solution to the key word problem is to use a key word manager. With a key word manager, users typically have one master key word and the key word manager creates, stores, and enters key words for individual accounts on behalf of the user. The individual key words are typically much more random than what users would select on their own and are thus stronger against attack. However, implementations of some key word managers have usability problems that can leave users even more vulnerable than when they were managing key words themselves.

V.THE PROPOSED FRAMEWORK

In the proposed work we have integrated image signature to help in recalling the key word. No system has been devolved so far which uses image signature in image based key word authentication. Study says that image signature or tone can be used to recall facts like images, text. In daily life we see various examples of recalling an object by the image related to that object enters User ID and select one image frequency which he want to be played at login time, a tolerance value is also selected with will decide that the user is legitimate or an imposter. To create detailed vector user has to select sequence of images and pixels on each image at pixel points of his choice.. Although many variants of image based key words and text key words were available, we began our investigation with regular text key words, where users were free to select any key word, and Pass Points, the pixel-based image based system that had been most closely evaluated to-date.

ADVANTAGE:

- To create detailed vector user has to select sequence of images and pixels on each image at pixel points of his choice. Profile vector is created.
- Users preferred CCP to Pass Points, saying that selecting and remembering only one point per image was easier and image signature helps considerably in recalling the pixel points.
- System showed very good Performance in terms of speed, accuracy, and ease of use.

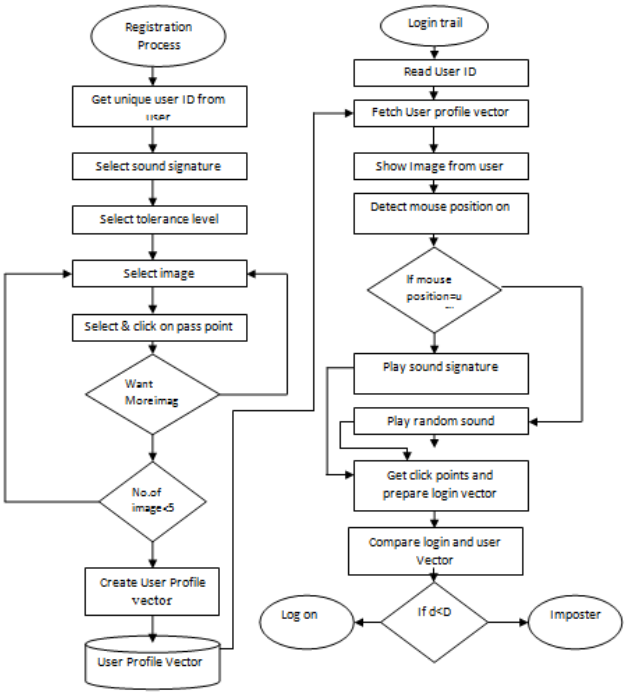
VII. METHODOLOGY FOR THE SYSTEM STUDY

We first conducted a lab study to independently evaluate the usability of pixel-based image based key words. Our methodology differed from the original studies (see below) but still consisted of having users create and confirm a image based key word then log in using that key word. We used a web-based interface developed with ASP .net for this study. Our images were 451x331 pixels in size, the same dimensions as in the Pass Points studies. The original Pass Points studies reported using a 20x20 pixel tolerance square, however it is unclear how this was implemented since it is impossible to accurately centre a 20x20 square on a given pixel. We decided on a tolerance square of 19x19 pixels centred on the original pixel-point. In other words, confirm and login attempts where all points were less than 10 pixels in

any x- or y- direction from their corresponding original pixel-points were considered successful. Since we wanted to perform analysis on the key words collected and the exact points selected, we did not use any discretization methods nor hash the key words before storing them.

In user registration module user enters the user name in user name. When user entered the all user details in registration phase, this user registration data is stored in data base and used during login phase for verification. In picture selection phase there are two ways for selecting picture key word authentication. 1. User defines pictures: Pictures are selected by the user from the hard disk or any other image supported devices. 2. System defines pictures: pictures are selected by the user from the database of the key word system. In picture selection phase user select any image as key words and consist of a sequence of five pixel-points on a given image. Users may select any pixels in the image as pixel-points for their key word. Users must select a pixel-point in the image and proceed on the next image. During system login process, images are displayed normally, without shading or the viewport, and repeat the sequence of pixels in the correct order, within a system-defined tolerance square of the original pixel-points.

VI. SYSTEM FLOW CHART



PASSPOINT METHOD

To improve upon the shortcomings of the Blonder Algorithm, PassPoint was created Passpoint was able to fill in the gaps left by blonder. In this case the image could be any natural picture or painting as well as rich enough so as to have several possible click points. Apart from this the image is not secret and has no other role other than that of assisting the user to remember the click point. Furthermore it is not as rigid as the blonder algorithm which requires the setting of artificial predefined click regions with well-marked boundaries. The authentication process involves the user selecting several points on picture in a particular order. When logging in, the user is supposed to click close to the selected click points, within some (adjustable) tolerance distance, for instance within 0.25 cm from the actual click point Studies indicate that when using the PassPoint system users were easily able to quickly create a valid key word. They found it much harder to know their key words compared to alphanumeric users, hence they had to take a lot more trials and more time to complete the process. Comparatively the login time, in this method is longer than that of the alphanumeric method

VIII. CONCLUSION

Finally, purely automated attacks are arguably much easier for an attacker to prepare especially if large image datasets are used. Corners and centroids of images might be extracted, and used to build a clickorder heuristic graph. Finally, our attacks could be used to help inform more secure design choices in implementing Pass Points-style image based key words. Pass-points key words are most robust than text key words against multiple key word interference. We show that in the short-term, participants could more easily remember multiple click-based image based key words than multiple text key words. Participants in the Text condition made significantly more recall errors and resorted to additional coping strategies such as using account-based key words or cycling through all of their key words when trying to recall their key word. We believe the memory cueing provided by click-based image based key words is at least part of the reason for better user performance and that cueing should be part of any recall-based authentication scheme, where possible. After two weeks, recall of the key words in the text and image based conditions was not statistically different from each other. Given that users were much more familiar with memorizing and recalling text key words, they were better positioned to remember these key words. However, this advantage was offset by the image based key words' built-in memory cue, which is a more secure memory aid than users' typical text key word coping mechanisms. Our results raise an interesting research question for text key words: can cueing mechanisms be (safely) added to text key words in order to achieve the same memorizing advantages seen in click-based image based key words.

V. CONCLUSION

In this paper, comparative studies of different controllers are studied and performance is evaluated according to time domain functions. It is observed that all controllers able to maintain the set point at the desired value but ZN-PID ,Fuzzy based controllers has slight overshoot, Model Reference Adaptive controller has no overshoot and settles quickly. So it conclude that Model Reference Adaptive Controller is the best controller then other controllers

REFERENCES

[1] A. Adams and M. Sasse. Users are not the enemy. Communication of the ACM, 42(12):41–46, 1999.

[2] M. Anderson and J. Neely. Memory. Handbook of Perception and Cognition, chapter 8: Interference and inhibition in memory retrieval, pages 237–313. Academic Press, 2nd edition, 1996.

[3] G. Blonder. Image based key words. United States Patent 5,559,961, 1996.

[4] I. Britton. Freefoto website. http://www.freefoto, accessed February 2007.

[5] B. Burstein, L. Bank, and L. Jarvik. Sex differences in cognitive functioning: Evidence, determinants, implications. Human Development, 23:289–313, 1980.

[6] S. Chiasson, R. Biddle, and P. C. van Oorschot.A second look at the usability of click-based image based key words.In 3rd Symposium on Usable Privacy and Security (SOUPS), July 2007.

[7] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot.Influencing users towards better key words: Persuasive Cued Click-Points. In BCS-HCI '08: Proceedings of the 22nd British HCI Group Annual Conference on HCI. British Computer Society, September 2008.

[8] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot. User interface design affects security: Patterns in click-based image based key words. International Journal of Information Security, 8(5), 2009.

[9] S. Chiasson, P. C. van Oorschot, and R. Biddle.A usability study and critique of two key word managers.In 15th USENIX Security Symposium, August 2006.

[10] L. Cranor and S. Garfinkel. Security and Usability: Designing Systems that People Can Use. O'Reilly Media, edited collection edition, 2005.

[11] D. Davis, F. Monrose, and M. Reiter. On user choice in image based key word schemes.In 13th USENIX Security Symposium, August 2004.

[12] S. Designer. John the Ripper key word cracker.http://www.openwall.com/john/.

[13] A. Dirik, N. Menon, and J. Birget.Modeling user choice in the Passpoints image based key word scheme.In 3rd ACM Conference on Symposium on Usable Privacy and Security (SOUPS), July 2007.

[14] K. Everitt, T. Bragin, J. Fogarty, and T. Kohno.A comprehensive study of frequency, interference, and training of multiple image based key words.In ACM Conference on Human Factors in Computing Systems (CHI), April 2009.

[15] D. Florencio and C. Herley. A large-scale study of WWW key word habits. In 16th ACM International World Wide Web Conference (WWW), May 2007.

[16] A. Forget, S. Chiasson, P. C. van Oorschot, and R. Biddle.Improving text key words through persuasion.In 4th Symposium on Usable Privacy and Security (SOUPS), July 2008.

[17] Free Images.com. Free Image website. http://www.freeimages.com, accessed February 2008.

[18] S. Gaw and E. Felten. Key word management strategies for online accounts. In 2nd Symposium On Usable Privacy and Security (SOUPS), July 2006.

[19] E. Goldstein. Cognitive Psychology.Wadsworth Publishing, 2006.

[20] K. Golofit. Click key words under investigation. In 12th European Symposium On Research In Computer Security (ESORICS), Springer LNCS 4734, September 2007.

[21] S. Komanduri and D. Hutchings.Order and entropy in Picture Key words.In Graphics Interface Conference (GI), May 2008.

[22] R. S. Lockhart. The Oxford Handbook of Memory, chapter 3: Methods of Memory Research, pages 45 – 57. Oxford University Press: New York, NY, 2000.

[23] P. A. Lowe, J. W. Mayfield, and C. R. Reynolds. Gender differences in memory test performance among children and adolescents. Archives of Clinical Neuropsychology, 18:865–878, 2003.

[24] S. Madigan. Chapter 3: Picture memory. In J. Yuille, editor, Imagery, Memory, and Cognition: Essays in Honor of Allan Paivio, chapter 3. Picture Memory, pages 65–89.Lawrence Erlbaum Associates, 1983.

[25] W. Moncur and G. Leplatre. Pictures at the ATM: Exploring the usability of multiple image based key words. In ACM Conference on Human Factors in Computing Systems (CHI), April 2007.

[26] F. Monrose and M. Reiter.Image based key words. In L. Cranor and S. Garfinkel, editors, Security and Usability: Designing Secure Systems That People Can Use, chapter 9, pages 157–174. O'Reilly, 2005.

[27] PD Photo. PD Photo website. http://pdphoto.org, accessed February 2007.

[28] M. Peters. Revised Vandenberg &Kuse Mental Rotations Tests: forms MRT-A to MRT-D. Technical report, Department of Psychology, University of Guelph, 1995.
[29] K. Renaud. Evaluating authentication mechanisms. In L. Cranor and S. Garfinkel, editors, Security and Usability: Designing Secure Systems That People Can Use, chapter 6, pages 103–128. O'Reilly Media, 2005.
[30] A. Salehi-Abari, J. Thorpe, and P. C. van Oorschot.On purely automated attacks and click-based image based key words.In 24th Annual Computer Security Applications Conference (ACSAC), 2008.
[31] L. Standing, J. Conezio, and R. Haber. Perception and memory for pictures: Single-trial learning of 2500 visual stimuli. Psychonomic Science, 19(2):73–74, 1970.
[32] X. Suo, Y. Zhu, and G. Owen. Image based key words: A survey. In Annual Computer Security Applications Conference (ACSAC), December 2005.
[33] J. Thorpe and P. C. van Oorschot.Human-seeded attacks and exploiting hot-spots in image based key words.In 16th USENIX Security Symposium, August 2007.
[34] E. Tulving and Z. Pearlstone.Availability versus accessibility of information in memory for words. Journal of Verbal Learning and Verbal Behavior, 5:381–391, 1966.
[35] M. van Lieshout and A. Baddeley. A nonparametric measure of spatial interaction in point patterns. StatisticaNeerlandica, 50(3):344–361, 1996.