HARDWARE, SOFTWARE AND PEOPLEWARE

UNISA

SAICSIT 2001

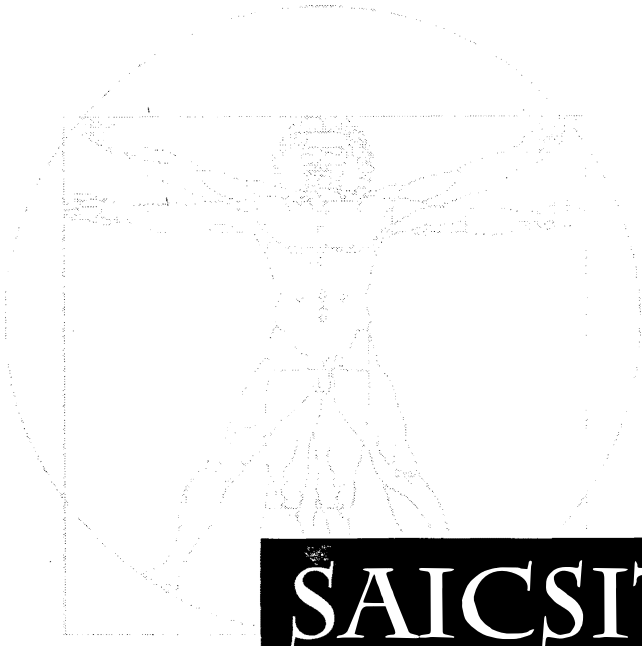
Edited by
Karen Renaud
Paula Kotzé
Andries Barnard

HARDWARE, SOFTWARE AND PEOPLEWARE

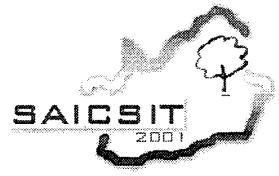
South African Institute of Computer Scientists and Information Technologists Annual Conference

25 – 28 September 2001

Pretoria, South Africa



SAICSIT 2001



Edited by Karen Renaud, Paula Kotzé & Andries Barnard

University of South Africa, Pretoria

Proceedings of the Annual Conference of the South African Institute of Computer Scientists and Information Technologists

First Edition, First Impression
ISBN: 1-86888-195-4

Published by Unisa Press
University of South Africa
P O Box 392, Pretoria, 0003

Cover Design by Tersia Parsons

Editors: Karen Renaud, Paula Kotzé & Andries Barnard

Electronic Publication by the Editors

Printed by Unisa Press
2001

Table of Contents

Abstracts of Electronic Papers

Message from the SAICSIT President

The South African Institute of Computer Scientists and Information Technologists (SAICSIT) was formed in 1982 and focuses on research and development in all fields of computing and information technology in South Africa. Now in the 20th year of its existence, SAICSIT has come of age, and through its flagship series of annual conferences provides a showcase of not only the best research from the Southern-African region, but also of international research, attracting contributions from far afield. SAICSIT does, however, not exist or operate in isolation.

More than 50 years have passed since the first electronic computer appeared in our society. In the intervening years technological development has been exponential. Over the last 20 years there has been a vast growth and pervasiveness of computing and information technology throughout the world. This has led into the expansion and consolidation of research into a diversity of new technologies and applications in diverse cultural environments. During this period huge strides have also been made in the development of computing devices. The processing speed of computers has increased thousand-fold and memory capacity from megabytes to gigabytes in the last decade alone. The Southern African region did not miss out on these developments.

It is hardly possible for such quantitative expansion not to bring a change in quality. Initially computers had been developed mainly for purposes such as automation for the improvement of processing, labour-reduction in production and automation control of machinery, with artificial intelligence, which made great strides in the 1980s, seen as the ultimate field to which computers could be applied. As we moved into the 1990s it was recognized that such an automation route was not the only direction in the improvement of computers. The expansion of processing power has enabled image data to be incorporated into computer systems, mainly for the purpose of improving human utilisation. For most computer technologies of the 1990s, including the Internet and virtual reality, automation was not the ultimate purpose. Humans were increasingly actively involved in the information-processing loop. This involvement has gradually increased as we move into the 21st century. Development of computer technology based not on automation, but on interaction, is now fully established.

The method of interaction has significantly changed as well. The expansion of computer ability means that the same function can be performed far more cheaply and on smaller computers than ever before. The advent of portable and mobile computers and pervasive computing devices is ample evidence of this. The need for users to be at the same location as a computer in order to reap the benefits of software installed on that computer is becoming an obsolete notion. Time and space are no longer constraints. One of the most discussed impacts of computing and information technology is *communication* and the easy accessibility of information. This changes the emphasis for research and development – issues such as cultural, political, and economic differences must, for example, be accommodated in ways that researchers have not previously considered. Our goal should be to enable users to benefit from technological advances, hence matching the skills, needs, and expectations of users of available technologies to their immense possibilities.

The conference theme for the SAICSIT 2001 Conference – *Hardware, Software and Peopleware: The Reality in the Real Millennium* – aims to reflect technological developments in all aspects related to computerised systems or computing devices, and especially reflect the fact that each influences the others.

Not only has SAICSIT come of age in the 21st century, but so has the research and development community in Southern Africa. The outstanding quality of papers submitted to SAICSIT 2001, of which only a small selection is published in this collection, illustrates both the exciting and developing nature of the field in our region. I hope that you will enjoy SAICSIT 2001 and that it will provide opportunities to cultivate and grow the seeds of discussion on innovative and new developments in computing and information technology.

Paula Kotzé
SAICSIT President

Message from the Chairs

Running this conference has been rewarding, exciting and exhausting. The response to the call for papers we sent out in March was overwhelming. We received 64 paper submissions for our main conference and twelve for the postgraduate symposium. We had a panel of internationally recognized reviewers, both local and international. The response from the reviewers was impressive – accepting a variety of papers and *mostly* returning the reviews long before the due date. We were struck, once again, by the sheer magnanimity of academia – as busy as we all are, we still manage to contribute fully to a conference such as SAICSIT.

After an exhaustive review process, where each paper was reviewed by at least three reviewers, the program committee accepted 26 full research papers and 14 electronic papers. Five papers were referred to the postgraduate symposium, since they represented work in progress – not yet ready for presentation to a full conference but which nevertheless represented sound and relevant research. The papers published in this volume therefore represent research of an internationally high standard and we are proud to publish it. Full electronic papers will be available on the conference web site (http://www.cs.unisa.ac.za/saicsit2001/).

Computer Science and Information Systems academics in South Africa labour under difficult circumstances. *The popularity of IT courses stems from the fact that IT qualifications are in high demand in industry, which leads in turn to a shortage of IT academic staff to teach the courses, even when posts are available. The net result is that fewer people teach more courses to more students. IT departments thus rake in ever-increasing amounts of state subsidy for their universities. These profits, euphemistically labelled "contribution to overhead costs", are deployed in various ways: cross-subsidization of non-profitable departments; maintenance of general facilities; salaries for administrative personnel, etc. Sweeteners of generous physical resources for the IT departments may be provided. We have yet to hear of a University in South Africa where significant concessions have been made in terms of industry-related remuneration. At best, small subventions are provided. As a result, shortages of quality staff remain acute in most IT departments – especially at senior teaching levels. What is even worse is that academics in these departments have to motivate the value of their conference contributions and other IT outputs to selection committees, often dominated by sceptical academic power-brokers from the more traditional departments whose continued survival is underwritten by IT's contribution to overhead costs.*[1]

The papers published in this volume are conclusive evidence of the indefatigability and pertinacity of Computer Science and Information Systems academics and technologists in South Africa. We are proud to be part of such a prestigious and innovative group of people.

In conclusion, we would like to thank the conference chair, Prof Paula Kotzé, for her support. We also specially thank Prof Derrick Kourie for his substantial contribution. Finally, to all of you, contributors, presenters, reviewers and organisers – a big thank you – without you this conference could not be successful.

Enjoy the Conference!
Karen Renaud & Andries Barnard

[1] This taken almost verbatim from Professor Derrick Kourie's SACLA 2001 paper titled: "*The Benefits of Bad Teaching*".

Conference Organisation

General Chair
Paula Kotzé

Programme Chairs
Karen Renaud
Andries Barnard

Organising Committee Chairs
Lucas Venter, Alta van der Merwe

Art and Design
Tersia Parsons

Sponsor Liaison
Paula Kotzé, Chris Bornman

Secretarial & Finances
Christa Prinsloo, Elmarie Havenga

Marketing & Public Relations
Klarissa Engelbrecht, Elmarie van Solms, Adriaan Pottas, Mac van der Merwe

Audio Visual
Tobie van Dyk, Andre van der Poll, Mac van der Merwe

Program Committee

Bob Baber – McMaster Univeristy, Canada
Andries Barnard – University of South Africa
Judy Bishop – University of Pretoria
Andy Bytheway – University of the Western Cape
Andre Calitz – University of Port Elizabeth
Elsabe Cloete – University of South Africa
Carina de Villiers – University of Pretoria
Alan Dix – Lancaster University, United Kingdom
Jan Eloff – Rand Afrikaans University
Andries Engelbrecht – University of Pretoria
Chris Johnson – University of Glasgow, United Kingdom
Paul Licker – University of Cape Town
Paula Kotzé – University of South Africa
Derrick Kourie – University of Pretoria
Philip Machanick – University of the Witwatersrand
Gary Marsden – University of Cape Town
Don Petkov – University of Natal in Pietermaritsburg
Karen Renaud – University of South Africa
Ian Sanders – University of the Witwatersrand
Derrick Smith – University of Cape Town
Harold Thimbleby – Middlesex University, United Kingdom
Theda Thomas – Port Elizabeth Technikon
Herna Viktor – University of Pretoria, South Africa
Bruce Watson – Universities of Pretoria and Eindhoven
Janet Wesson – University of Port Elizabeth

Referees

Molla Alemayehu
Trish Alexander
Adi Attar
Bob Baber
Andries Barnard
John Barrow
Judy Bishop
Gordon Blair
Arina Britz
Andy Bytheway
André Calitz
Charmain Cilliers
Elsabe Cloete
Gordon Cooper
Richard Cooper
Annemieke Craig
Thad Crews
Quintin Cutts
Michael Dales
Carina de Villiers
Alan Dix
Dunlop Mark
Elize Ehlers
Jan Eloff
Andries Engelbrecht
Klarissa Engelbrecht
David Forsyth
John Galletly
Vashti Galpin
Wayne Goddard
Alexandré Hardy
Scott Hazelhurst
Johannes Heidema
Tersia Hörne
Chris Johnson
Bob Jolliffe
Paula Kotzé
Derrick Kourie
Les Labuschagne
Paul Licker
Philip Machanick
Anthony Maeder
David Manlove
Gary Marsden
Thomas Meyer
Elsa Naudé
Martin Olivier
Don Petkov
Pekka Pihlajasaari
Nelisha Pillay
Laurette Pretorius
Karen Renaud
Ingrid Rewitzky
Sheila Rock
Markus Roggenbach
Ian Sanders
Justin Schoeman
Martie Schoeman
Elsje Scott
Derek Smith
Elmé Smith
Adrie Stander
Harold Thimbleby
Theda Thomas
Judy Van Biljon
Alta Van der Merwe
André van der Poll
Tobias Van Dyk
Lynette van Zijl
Lucas Venter
Herna Viktor
Bruce Watson
Janet Wesson

Conference Sponsors

Keynote Abstracts

Jiminy: Helping Users to Remember Their Passwords

Karen Renaud[a] Elmé Smith[b]

University of South Africa, Pretoria, South Africa
[a]renaukv@unisa.ac.za [b]smithe@unisa.ac.za

Abstract

This paper presents a novel approach to a familiar problem — that of helping users to choose better passwords, **and** *to remember them. User identification and authentication is an essential aspect of our technologically advanced world, but the difficulty with remembering passwords is well known. This paper presents a mechanism for recording passwords for users by applying a very simple and well-known mechanism to conceal the passwords from casual intruders while facilitating retrieval of the passwords by the authorized user. A prototype implementation of the scheme, named Jiminy, has been developed. The prototype was evaluated with a small number of users. The results of the evaluation are presented here.*

Keywords: *Passwords, Information Security, Human Factors, Memory*
Computing Review Categories: *H.1.2, H.5.2, K.4.1, K.4.2, K.6.5*

1 Introduction

The successful *identification* and *authentication* of a person or an entity wishing to use a computer system, is the first step towards enforcing information security [1, 9, 16]. Each user has a unique user identification (user-id) that ensures that only authorized users gain access to a computer system. Authentication is the process of verifying that an offered user-id really belongs to the person offering that user-id and not to an unauthorized person trying to impersonate the owner of the id [9]. This authentication usually happens by the user having, apart from his/her user-id, some secret (unique) authentication data known or belonging only to the user and the system. This secret authentication data can be categorized as:

- *something the user knows*, such as, for example a password,
- *something the user possesses,* perhaps a physical token such as a smart card,
- *something the user is,* based on biometrics such as fingerprints, or
- a *combination* of the previous three [9, 20].

Some innovative schemes have been proposed, especially in the biometrics category, which utilise mouse usage patterns [11], fingerprints [13], voice identification [4], key stroke latencies [7, 8, 16], word association [23] and ear biometrics [5].

However, most of these schemes require the use of extra equipment which is not always available to the end-user. Passwords are, therefore, still the simplest and the most popular user authentication scheme, because they do not need exclusive devices and are an inexpensive, familiar paradigm that most operating systems support [1, 8, 11, 16, 20].

Confidence in passwords' ability to provide adequate authentication is, however, waning. This is not because of passwords as such, but because of wrongful use of passwords by many users due to the limitations of human memory.

To overcome some of these problems *one-time passwords* have been proposed. A one-time password is one that changes every time it is used. Systems that use one-time passwords assign a static mathematical function to a user, as opposed to assigning a static phrase (as is the case with most conventional password applications). In other words, the system provides an argument to the mathematical function, and the user must then compute and return the function value.

For example, the function $f(x) = x + 1$ can be assigned to a specific user. With this function, the system prompts with a value for x, and the user enters the value $x + 1$. The kinds of mathematical functions used can be very complex, but such functions are limited by the ability of the user to compute the response quickly and easily.

One-time passwords are very secure for authentication, but their usefulness is limited by the complexity of algorithms people can be expected to remember. [20, 21].

In order to gauge the use or abuse of passwords in our organisation we undertook a survey of users' password habits and found that out of 34 respondents 26 used predictable words and names — often the user's own name followed by a number which is incremented each month. Seeley finds that this is not a particularly rare choice of password — it being the one most password-cracking programs search for before trying any others [1, 22]. Only 5 respondents had a special

iar words or names, and 6 wrote their passwords down. Most respondents used passwords shorter than the minimum recommended length of 6 characters. The fact that 76% of the respondents had forgotten their passwords in the past was no surprise but what was surprising was that only 2 of the 'special system' password respondents had not ever forgotten their passwords. Other respondents who had never forgotten their passwords used very predictable passwords, such as the month and year, and it is thus not surprising that the passwords were easy to remember. It is obvious that system security is being compromised and we feel that this group is representative of any employee group in any organisation.

The current password situation is thus at somewhat of an impasse — with employers insisting on the use of non-predictable regularly changing passwords, and employees using easy-to-remember passwords and compromising security by writing them down [17]. This paper will propose a way of resolving this impasse. Section 2 will discuss problems with regard to passwords. Section 3 will propose a solution. Section 4 will give information about the prototype implementation of the proposed solution. Section 5 reports on the evaluation of the prototype and Section 7 concludes.

2 The Problem with Passwords

Many organizations require their employees to change passwords on a regular basis — often once a month. Employees are also often informed of the requirements of a 'strong' password such as the following incomplete list of important password criteria [9, 20]:

1. A password should comprise of at least one of each of the following:
   - a small letter,
   - a capital letter,
   - a non-alphanumeric character (such as @, $ or %), and
   - a digit.
2. A password should also satisfy the following criteria:
   - It should comprise at least 6 characters.
   - It should not be an actual name or word.
   - It should be changed frequently, for example, once a month.
   - It should not be written down.
   - It should not be something directly related to the user, such as, for example, the name of a spouse.
   - It should be as random as possible.
   - Different passwords should be used for different systems.

It is a well-known fact that users have difficulty remembering their passwords, especially if they are required to change them on a regular basis. A newly-changed password is held in the user's working memory. If the user is to remember it for the next occasion, it must be encoded within the long-term memory. For this to happen without the help of some external memory aid one of the following must be true [24]:

- the password must be meaningful or deducible, such as the month and year;
- the password must be rehearsed;
- the password must be based on some fact already encoded within the long-term memory — such as a familiar name; or
- the user must have some special scheme for setting and recalling the password.

The latter entails extra effort and so users will tend to choose one of the other options. If users choose passwords that satisfy all the requirements, without attaching some meaning to the password, they will be likely to forget it. A survey of the system support tasks undertaken at the University of South Africa in January 2001 supported this assertion since a *quarter* of all system administration tasks processed in this month were related to passwords. Many employees had forgotten their passwords after their vacation and from conversations with numerous colleagues one concludes that a significant percentage of the remainder had written their passwords down somewhere in order to retain them.

Furthermore, many users have to remember multiple passwords, that is, use different passwords for different applications. Having a large number of passwords reduces users' memorability and increases insecure work practices, such as writing passwords down [3].

Password-based user authentication, especially for passwords meeting the above-mentioned requirements, penalizes users for the difficulty experienced in remembering sequences. Restrictions introduced to create more secure password content may in fact produce *less* memorable passwords. Users often have weak passwords because strong passwords are long and hard to remember. Security, therefore, does not necessarily improve as password complexity increases, because in reality users will simply write down difficult passwords. Furthermore, password protection weakens with the passage of time as well as improvements in computer performance. Attackers can, therefore, rely on faster and faster computers for guessing passwords, while user memory on the other hand, does not seem to be expanding [1].

It is obvious from this discussion that users have limited memory capacity, which makes it difficult for them to retain passwords until needed [15]. On the other hand, users have particular strengths, such as processing visual information rapidly, coordinating multiple sources of information and making inferences about concepts or rules

from past experiences [19], which can be utilized. We therefore feel that it is possible to come up with a memory assistance scheme which exploits user strengths in order to support them in alleviating their weaknesses and in this way improve and enhance security. The following section will propose our solution.

3 The Solution

To date, research on password security has focussed on designing technical mechanisms to protect access to systems. Since security mechanisms are designed, implemented, applied and breached by people, human factors should be considered in their design [2]. It is simply not possible to eliminate the need for changing passwords. This is because the demands for changing passwords come from employees concerned with safety and security of sensitive information — and human frailty is simply not a factor they consider or care about. However, providing the user with an application to assist in finding a forgotten password is untenable because:

1. the user often cannot get access to the application without the forgotten password, and
2. access to such an application would have to be restricted — probably by means of a password. Due to human factors such a password would tend not to be changed frequently which once again compromises security. In addition, this password, if discovered by an intruder, would give access to *all* of the user's passwords — a very dangerous thing.

This leads to the conclusion that a paper-based mechanism needs to be found. This is difficult to provide since a piece of paper could easily fall into the wrong hands. A paper-based mechanism should therefore record the passwords in a format which will not be understood by anyone except the person who recorded the password. In addition, the mechanism should not be arduous to use because people generally emphasize efficacy rather than efficiency [10, 14] and would probably avoid a complex password-recording scheme.

Our solution does not require users to memorize or to write down long passwords, and does not rely on smart cards or other auxiliary hardware. The solution proposed in this paper is based on the well-known 'Word Search' problems so beloved of travelers everywhere (Figure 1). The puzzler is given a grid populated with characters and a list of words to locate, together with three *implied* templates — horizontal, vertical, and diagonal (Figure 2). To locate the word *PASS*, the puzzler, after some trial and error, applies the diagonal template to the grid (shown in Figure 3). Finding the words in such a grid is not a trivial problem because the profusion of characters in the grid obfuscates the hidden words — hence the attraction of such puzzles to those attempting to while away the hours. Sternberg [24] talks about the role of *distractors* in such grids — non-target stimuli which divert the reader's attention away from the target (the password). The number of targets and distractors influence the difficulty of the task.

This line of thought led to the development of the Jiminy[1] concept — a paper-based mechanism for reminding users of their passwords. The Jiminy approach is a little different from the Word Search puzzle approach, which provides the puzzler with the grid, and the words, and implies the templates. Jiminy, on the other hand, provides a character-filled grid and a set of templates and expects the user to find the hidden password.

Of course the user is faced with the difficulty of remembering where to place the template within the grid in order to locate the hidden password. To make things easier the grid is superimposed over an image so that the user can remember the positioning of the template within the *picture* rather than the position within the *grid*. Improving memory retention by means of the loci method is a well known memory enhancement technique [12]. In addition, *the user* previously provided the password now hidden within the grid and, owing to his or her recognition memory capacity [12, 24], he or she will recognise the previously provided password.

Jiminy is synonymous with a public-key encryption system [20]. A public-key encryption scheme requires the use of two related keys — a private key which is only known to the owner, and a public key which is publicly available. If one encrypts with the public key, then the related private key is required to decrypt the message, and *visa versa*. In Jiminy, the public key is made up of the grid and the templates, whereas the private key is the *position* within the grid which will be used to relocate the password.

Whereas just about anyone can find the words in a common Word Search puzzle with a bit of persistence, the Jiminy scheme makes finding the words dependent on a fore-knowledge of the word itself *and* the location within the grid. It *is* possible for another person to find the word, but it is far more difficult than finding passwords recorded on paper, or guessing familiar names. Jiminy makes accidental identification of passwords much harder by providing users with more than one template — each a different colour. For a grid composed of 20 rows and 26 columns a password composed of 8 characters is surrounded by 552 distractors. An intruder has to match the correct template to the correct position in the grid — which makes finding the password less likely.

4 Jiminy Prototype

A prototype of Jiminy was implemented, using Java, to test the concepts outlined in the previous section. Jiminy takes the user through the following steps to generate the required grid:

1. A background image is identified. At present the Jiminy prototype only accepts JPEG images. This is not necessarily a disadvantage since this is a very popular format.

[1] Named after Pinnochio's conscience — Jiminy Cricket

X	P	O	W	K	L	D	S	S	Q	C	Z
H	H	P	F	E	V	R	J	G	p	A	M
N	U	T	A	Y	W	X	C	V	B	N	M
Q	W	E	R	S	T	Y	U	I	O	P	A
S	D	F	G	H	S	J	K	L	Z	X	C
V	B	N	M	I	Q	W	O	U	A	G	Z
F	D	H	K	B	T	T	O	R	E	X	U
J	I	Z	B	A	R	V	O	R	L	W	A
N	Y	E	H	Y	A	L	K	G	D	D	A

Figure 1: Word Search Grid

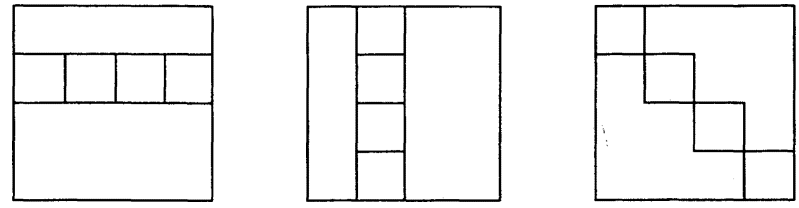


Figure 2: Implied Templates

X	P	O	W	K	L	D	S	S	Q	C	Z
H	H	P	F	E	V	R	J	G	p	A	M
N	U	T	A	Y	W	X	C	V	B	N	M
Q	W	E	R	S	T	Y	U	I	O	P	A
S	D	F	G	H	S	J	K	L	Z	X	C
V	B	N	M	I	Q	W	O	U	A	G	Z
F	D	H	K	B	T	T	O	R	E	X	U
J	I	Z	B	A	R	V	O	R	L	W	A
N	Y	E	H	Y	A	L	K	G	D	D	A

Figure 3: Word Located

2. The user chooses the position of one or more passwords — located according to specific features on the image (see Figure 4).

3. The rest of the grid is then populated with randomly generated distractor characters, obscuring the passwords (see Figure 5). The characters include all small letters, capital letters, non-alphanumeric characters and the ten numeric digits.

4. The user prints the image.

The user is provided with various options so that the eventual grid can be tailored:

1. a set of templates cut out of different coloured cardboard is provided. The user chooses the template to be used for each password embedded in the grid.

2. the user has the option of choosing the colour of the grid to be used for the particular password.

3. the user can pin the template based on any of the four corners — so that many more options for locating the grid are possible.

Jiminy also allows users to generate their own templates and to enter those into the system (see Figure 6). This strengthens the security provided by Jiminy because users can each have different templates.

The grid generated by Jiminy has 20 rows and 26 columns. The templates are 8 squares both ways, so there are 12 x 18 different squares the top left-hand corner of the template can be aligned with (216). With three templates there are therefore 648 different passwords available from one Jiminy grid. Thus an intruder has a 0,1% chance of discovering the right password — especially if the user does not make use of a recognisable word. The biggest obstacle to using unpredictable passwords — remembering them — is alleviated by Jiminy, which will hopefully encourage users to be more security conscious.

5 Evaluation

Evaluation of Jiminy cannot be done within a fixed time period, because one has to make it available to the user to use whenever a password is changed. One cannot predict when a password will be forgotten so the evaluation cannot be hurried. To evaluate, one should make Jiminy available in case a password is forgotten. Jiminy was installed for a number of volunteers and then evaluated from two perspectives:

1. one being the usability of the prototype itself, and

2. the other being evaluation of the Jiminy *concept*.

To this end, volunteers were asked the following questions after a reasonable time had elapsed:

1. whether having Jiminy encouraged them to choose a stronger password.

2. whether Jiminy helped them to remember their password.

3. whether they had written their password down elsewhere.

4. whether Jiminy was easy to use.

All the users found that Jiminy not only helped them to remember their passwords, but that they chose stronger passwords because they had Jiminy. They also did not write down or record their passwords in any other way, which tightens up the currently lax security situation. It was interesting to note that there was a contagiousness about Jiminy. People who had not originally volunteered requested Jiminy because they had forgotten a password, or because they had heard about the experiment and wanted to have the facility available. This suggests that people actually do want to use the password facility properly but are confounded by their own human frailty.

With respect to Jiminy usability we found that users experienced no problems using the prototype. One problem with the use of Jiminy is that users would change network passwords at the beginning of their session and then after waiting for the startup to complete they did not remember to record their password with Jiminy. We intend investigating ways of addressing this problem.

In general we feel that this evaluation has convinced us of the value of the Jiminy methodology, and of the usability of the prototype, and that the Jiminy concept merits further evaluation with a larger volunteer base.

6 Future Work

The ideal time to evaluate Jiminy in South Africa is after the December holidays because most people take a break at this time of year and relax completely and therefore do not think about work-related issues. Making Jiminy available before these holidays would provide a golden evaluation opportunity, one we intend making full use of. Other avenues for future investigation include determining:

1. whether users use the same grid for more than one password;

2. whether users cope with changing grids when passwords change regularly;

3. whether users remember where they placed their passwords within the grid, and which template they used after a long period of time; and

4. whether users use a different image every time they generate a new grid, or whether they use the same image repeatedly.

Answers to these questions will take some time to obtain, since this research depends on the elusive qualities of human memory.

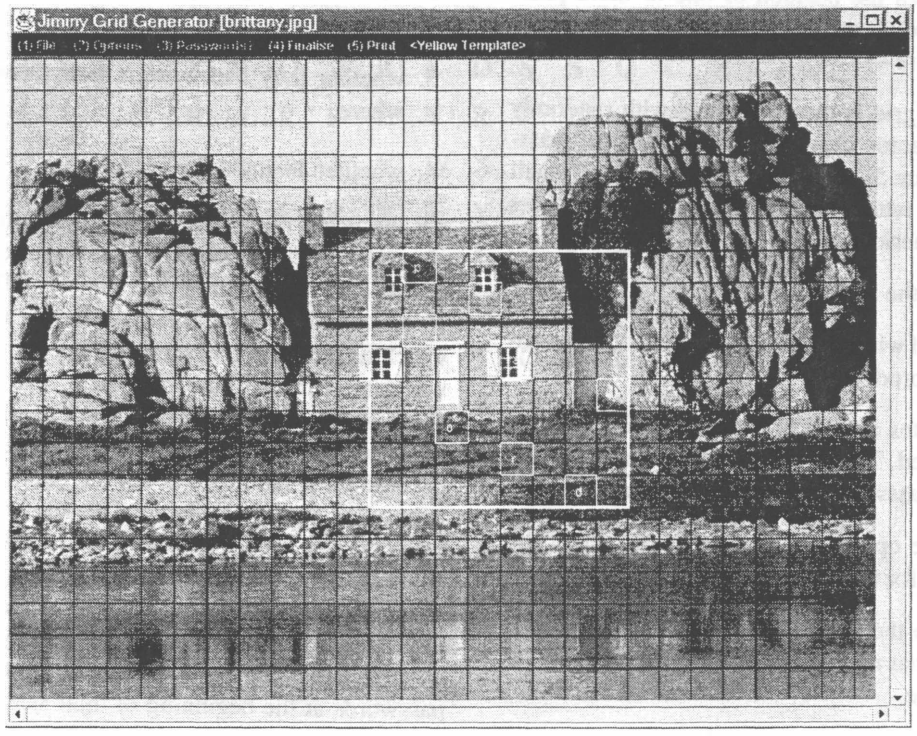


Figure 4: Password Location Chosen

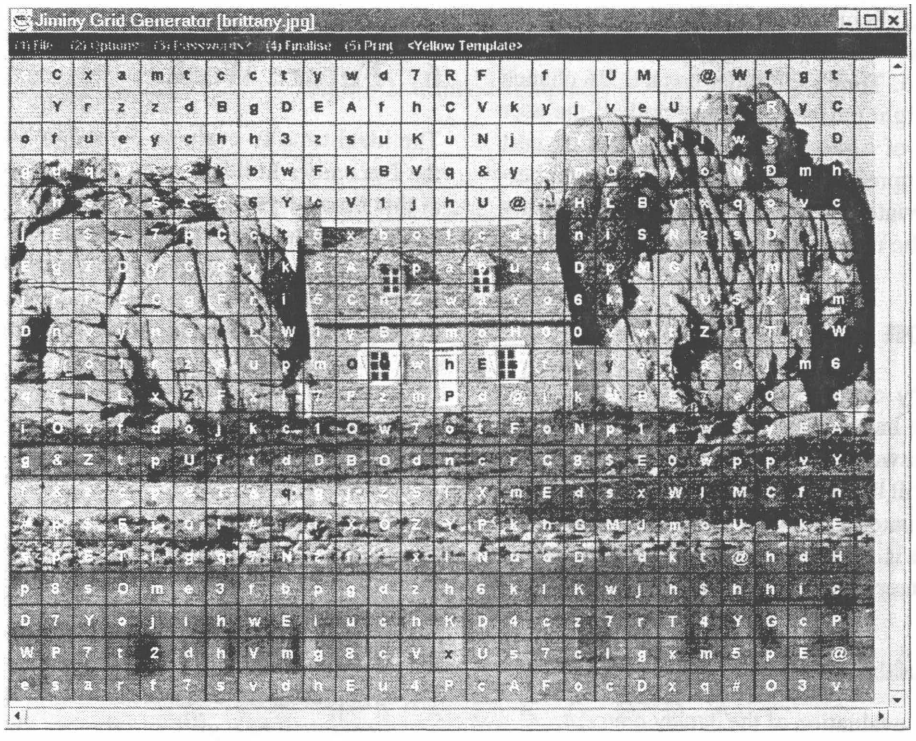


Figure 5: Grid Populated with Characters

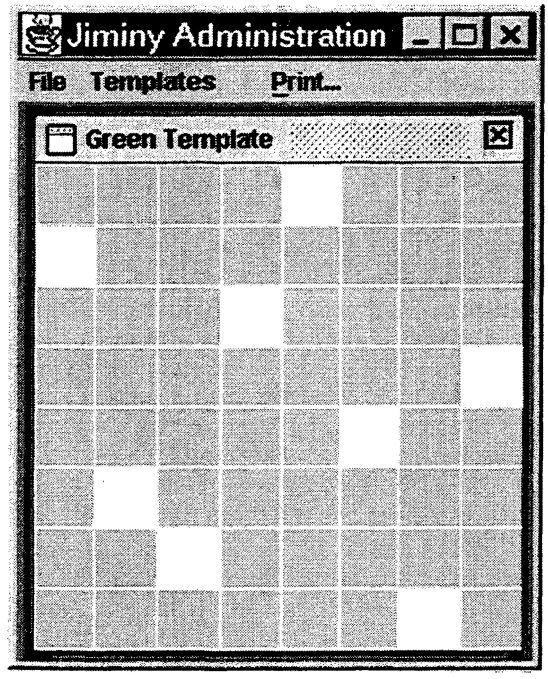


Figure 6: Creating a New Template

and therefore do not think about work-related issues. Making Jiminy available before these holidays would provide a golden evaluation opportunity, one we intend making full use of. Other avenues for future investigation include determining:

1. whether users use the same grid for more than one password;

2. whether users cope with changing grids when passwords change regularly;

3. whether users remember where they placed their passwords within the grid, and which template they used after a long period of time; and

4. whether users use a different image every time they generate a new grid, or whether they use the same image repeatedly.

Answers to these questions will take some time to obtain, since this research depends on the elusive qualities of human memory.

7 Conclusions

The Jiminy approach records passwords on paper in such a way that only the person who originally recorded the password will be able to reliably retrieve it. Even if an intruder gains access to the gridded image, and the templates, it will take a lot of time and effort to find the password. The authorised users, on the other hand, will have no difficulty since their inherent ability to remember location and recognise patterns will assist them in placing the correct template in the right position and recognising their passwords. Even if the user is not certain about where the password is and (s)he has to try a few positions (s)he will recognise the familiar pattern of the previously chosen password. The initial evaluation suggests that Jiminy could prove an invaluable aid to users and play a role in reducing stress both for end-users and system administrators.

We are fully aware that Jiminy does *not* provide a completely secure mechanism which is impervious to attack. What we *do* claim is that Jiminy is superior to traditional mechanisms for remembering passwords — such as writing them down on post-it notes and sticking them close to a workstation.

Acknowledgement

Our thanks to Basil Worrall at the University of Pretoria for kick-starting the prototype.

References

[1] Martín Abadi, T. Mark A. Lomas, and Roger Needham. Strengthening passwords. SRC Technical Note 1997 - 033, DEC , Systems Research Center, December 1997.

[2] A Adams and M A Sasse. Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures. *Communications of the ACM*, 42(12):40–46, December 1999.

TC11 eleventh international conference on information security, IFIP/SEC'95, pages 562–574, London, UK, 1995.

[8] W G de Ru and J H P Eloff. Enhanced password authentication through fuzzy logic. *IEEE Intelligent Systems & their applications*, 12(6), November/December 1997.

[9] J H P Eloff, M Eloff, E Smith, and S H von Solms. *Information Security.* Amabhuku Publications (pty) Ltd., 1st edition, 2000.

[10] L P Goodstein, H B Andersen, and S E Olsen. *Tasks, Errors and Mental Models.* Taylor and Francis, New York, 1988.

[11] K Hayashi, E Okamoto, and M Mambo. Proposal of User Identification Scheme Using Mouse. In Y Han, T Okamoto, and S Qing, editors, *Proceedings of the 1st International Information and Communications Security Conference. Lecture Notes in Computer Science*, number 1334, pages 144–148, 1997.

[12] K L Higbee. *Your memory: how it works and how to improve it.* Prentice-Hall Press, New York, 2nd edition, 1988.

[13] L. Hong and A. Jain. Integrating faces and fingerprints for personal identification. *Lecture Notes in Computer Science*, 1351:I–??, 1997.

[14] P L Klumb. *Attention, Action, Absent Minded Aberrations.* Peter Lang, 1995. European University Studies.

[15] Yoshiro Miyata and Donald A Norman. Psychological issues in support of multiple activities. In D A Norman and S W Draper, editors, *[18]*, chapter 13, pages 171–186. Lawrence Erlbaum Associates, Publishers, Hilldale, New Jersey, 1986.

[16] F Monrose and M K Reiter. Password hardening based on keystroke dynamics. In *Proceedings of the 6th ACM Conference on Computer and Communications Security*, number 1334, pages 73–82, 1999.

[17] Jacob Nielsen. Security & human factors. Web Document. http://www.useit.com/alertbox/20001126.html, November 26 2000.

[18] D A Norman and S W Draper, editors. *User Centred System Design. New Perspectives on Human-Computer Interaction.* Lawrence Erlbaum Associates, Publishers, Hilldale, New Jersey, 1986.

[19] J R Olsen. Cognitive Analysis of People's Use of Software. In *[6]*, chapter 10, pages 260–293. MIT Press, 1987.

[20] C P Pfleeger. *Security in computing.* Prentice Hall, Upple Saddle River NJ, 2nd edition, 1997.

[21] Aviel D. Rubin. Independent one-time passwords. In USENIX, editor, *Computing Systems, Winter, 1996.*, volume 9, pages 15–27, Berkeley, CA, USA, Winter 1996. USENIX.

[22] Donn Seeley. Password Cracking: A Game of Wits. *Communications of the ACM*, 32(6):700–703, June 1989.

[23] Sidney L. Smith. Authenticating users by word association. In *Proceedings of the Human Factors Society 31st Annual Meeting*, Random Access I, pages 135–138, 1987.

[24] R J Sternberg. *Cognitive Psychology.* Harcourt Brace, London, 2nd edition, 1999.