The South African Institute of Computer Science
and
Information Technology

Proceedings
of the
The 1997 National
Research and
Development
Conference
Towards 2000

Riverside Sun
Vanderbijlpark
13 & 14 November

Edited by
L.M. Venter
R.R. Lombard
Foreword

This book contains a collection of papers presented at a Research and Development conference of the South African Institute of Computer Scientists and Information Technologists (SAICSIT). The conference was held on 13 & 14 November 1997 at the Riverside Sun, Vanderbijlpark. Most of the organization for the conference was done by the Department of Computer Science and Information Technology of the Vaal Triangle Campus, Potchefstroom University for Christian Higher Education.

The programming committee accepted a wide selection of papers for the conference. The papers range from detailed technical research work to reports of work in progress. The papers originate mainly from Academia, but also describe work done in and for Industry. It is hoped that the papers give a true reflection of the current research scene in Computer Science and Information Technology in South Africa. Since one of the aims of the conference is Research development, the papers were not subjected to a refereeing process.

A number of people spent numerous hours helping with the organization of this conference. In this regard, we wish to thank the members of the Organizing committee, and the Programming committee who had very little time to screen the abstracts and compile the program. A special thanks goes to the secretary of the department, Mrs Helei Jooste, whose very able work was interrupted by the birth of her first child.
Organizing Committee

Conference General Chairs
Prof. J.M. Hattingh (PU for CHE)

Organizing Chair
Prof. Lucas Venter (PU for CHE)

Organizing Committee
Mrs. S. Gilliland
Mr. J.P. Jooste
Mr. R.R. Lombard
Mrs. M. Huisman

Secretariat
Mrs. H. Jooste

Program Chair
Prof A de Waal (PU for CHE)

Program Committee
Prof. D. Kourie (UP)
Prof. C. Bornman (UNISA)
Prof. L.M. Venter (PU for CHE)
# Table of Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>i</td>
</tr>
<tr>
<td>Organizing Committee</td>
<td>ii</td>
</tr>
<tr>
<td>List of Contributors</td>
<td>vii</td>
</tr>
<tr>
<td><strong>Software Objects Change : Problems and Solution</strong></td>
<td>1</td>
</tr>
<tr>
<td>S.A. Ajila</td>
<td></td>
</tr>
<tr>
<td><strong>Liming-like Curve Constructions</strong></td>
<td>26</td>
</tr>
<tr>
<td>M.L. Baart and R. McLeod</td>
<td></td>
</tr>
<tr>
<td><strong>A Model for Evaluating Information Security</strong></td>
<td>27</td>
</tr>
<tr>
<td>L. Barnard and R. von Solms</td>
<td></td>
</tr>
<tr>
<td><strong>Integrating Spatial Data Management and Object Store Technology</strong></td>
<td>31</td>
</tr>
<tr>
<td>S. Berman, S. Buffler and E. Voges</td>
<td></td>
</tr>
<tr>
<td><strong>Metamodelling in Automated Software Engineering</strong></td>
<td>32</td>
</tr>
<tr>
<td>S. Berman and R. Figueira</td>
<td></td>
</tr>
<tr>
<td><strong>Using Multimedia Technology for Social Upliftment in Deprived</strong></td>
<td>33</td>
</tr>
<tr>
<td>L. Bester and E. de Preez</td>
<td></td>
</tr>
<tr>
<td><strong>Extending the Client-Server Model for Web-based Execution of</strong></td>
<td>36</td>
</tr>
<tr>
<td>L. Botha, J.M. Bishop and N.B. Serbedzija</td>
<td></td>
</tr>
<tr>
<td><strong>Access Control Needs in an Electronic Workflow Environment</strong></td>
<td>45</td>
</tr>
<tr>
<td>R.A. Botha</td>
<td></td>
</tr>
<tr>
<td><strong>The Use of the Internet in an Academic Environment to Commercially</strong></td>
<td>51</td>
</tr>
<tr>
<td>Supply and Support Software Products</td>
<td></td>
</tr>
<tr>
<td>B. Braude and A.J. Walker</td>
<td></td>
</tr>
<tr>
<td><strong>Explanation Facilities in Expert Systems Using Hypertext Technology</strong></td>
<td>63</td>
</tr>
<tr>
<td>T. Breetzke and T. Thomas</td>
<td></td>
</tr>
<tr>
<td><strong>Theoretical Computer Science: What is it all about, and is it of any relevance to us?</strong></td>
<td>75</td>
</tr>
<tr>
<td>C. Brink</td>
<td></td>
</tr>
<tr>
<td><strong>Representing Quadrics on a Computer</strong></td>
<td>76</td>
</tr>
<tr>
<td>M.A. Coetzee and M.L. Baart</td>
<td></td>
</tr>
</tbody>
</table>
The Generation of Pre-Interpretations for Detecting Unsolvable Planning Problems
D.A. de Waal, M. Denecker, M. Bruynooghe and M. Thielscher

The Emerging Role of the Chief Information Officer in South Africa
B. Dekenah

A Java-Implemented Remote Respiratory Disease Diagnosis System on a High Bandwidth Network
A. Foster

Early Results of a Comparative Evaluation of ISO 9001 and ISO/IEC 15504 Assessment Methods Applied to a Software Project
C. Gee and A.J. Walker

A Neural Network Model of a Fluidised Bed
M. Hajek

The Effects of Virtual Banking on the South African Banking Industry
M.L. Hart and M. Dunley-Owen

Linear Response Surface Analysis and Some Applications
J.M. Hattingh

Model Checking Software with Symbolic Trajectory Evaluation
A. Hazelhurst

A Risk Model to Allocate Resources to Different Computerized Systems
H.A. Kruger and J.M. Hattingh

Returns on the Stock Exchange
J.W. Kruger

Cardinality Constrained 0-1 Knapsack Problems
M.F. Kruger, J.M. Hattingh and T. Steyn

An Investigation in Software Process Improvement in the Software Development of a large Electricity Utility
M. Lang and A.J. Walker

Design and Implementation of a C++ Package for Two-Dimensional Numerical Integration
D.P. Laurie, L Pluym and Ronald Cools

Algebraic Factorization of Integers Using BDE's
H. Messerschmidt and J. Robertson
Global Optimization of Routes after the Process of Recovery
M. Mphahlele and J. Roos

Using a Lattice to Enhance Adaptation Guided Retrieval in Example Based Machine Translation
G.D. Oosthuizen and S.L. Serutla

Information Systems Development and Multi Criteria Decision Making / Systems Thinking
D. Petkov, O. Petkova

The Development of a Tutoring System to Assist Students to Develop Answering Techniques
N Pillay

Combining Rule-Based Artificial Intelligence with Geographic Information Systems to Plan the Physical Layer of Wireless Networks in Greenfield Areas
K. Prag, P. Premjeeth and K. Sandrasegaran

A Distributed Approach to the Scheduling Problem
V. Ram and P. Warren

More readings than I thought: Quantifier Interaction in Analysing the Temporal Structure of Repeated Eventualities
S. Rock

Ray Guarding Configuration of Adjacent Rectangles
I. Sanders, D. Lubinsky and M. Sears

Developing Soft Skills in Computer Students
C Schröder, T. Thomas

Information Security Awareness, a Must for Every Organization
M. Thomson and R. von Solms

Pla Va: A Lightweight Persistent Java Virtual Machine
S Tjasink and S. Berman

Beliefs on Resource-Bounded Agent
E. Viljoen

Object-Orientated Business Modelling and Re-engineering
M. Watzenboeck
On Indexing in Case Based Reasoning Applied to Pre-Transportation Decision Making for Hazardous Waste Handling
K.L. Wortmann, D. Petkov and E. Senior

Author Index
List of Contributors

S.A. Ajila
Department of Mathematics and Computer Science
National University of Lesotho
Roma, 180
Lesotho

L. Baart
Department of Mathematics
Vaal Triangle Campus of the PU for CHE
PO Box 1174
Vanderbijlpark, 1900

L. Barnard
Faculty of Computer Studies
Port Elizabeth Technikon
Private Bag X6011
Port Elizabeth, 6000

S. Berman
University of Cape Town
Rondebosch, 7701

L. Bester
Faculty of Computer Studies
Port Elizabeth Technikon
Private Bag X6011
Port Elizabeth, 6000

J.M. Bishop
Computer Science Department
University of Pretoria
Pretoria, 0002

L. Botha
Computer Science Department
University of Pretoria
Pretoria, 0002

R.A. Botha
Faculty of Computer Studies
Port Elizabeth Technikon
Private Bag X6011
Port Elizabeth, 6000

B. Braude
Software Engineering Applications Laboratory,
Electrical Engineering
University of the Witwatersrand
Private Bag 3
Wits, 2050

T. Breetzke
Faculty of Computer Studies
Port Elizabeth Technikon
Private Bag X6011
Port Elizabeth, 6000

C. Brink
University of Cape Town
Rondebosch, 7700

M. Bruynooghe
Departement Computerwetenschappen
Katholieke Universiteit Leuven
Celestijnenlaan 200A
B-3001 Heverlee
Belgium

S. Buffler
University of Capetown
Rondebosch, 7701

M.A. Coetzee
Department of Mathematics
PU for CHE
Private Bag X6001
Potchefstroom, 2520

R. Cools
Katholieke Universiteit Leuven
Celestijnenlaan 200A
B-3001 Heverlee
Belgium

E. de Preez
Faculty of Computer Studies
Port Elizabeth Technikon
Private Bag X6011
Port Elizabeth, 6000

D.A. De Waal
Department of Computer Science and Information Systems
PU for CHE
Private Bag X6001
Potchefstroom, 2531

B. Dekenhah
The Board of Executors

M. Denecker
Departement Computerwetenschappen
Katholieke Universiteit Leuven
Celestijnenlaan 200A
B-3001 Heverlee
Belgium

M. Dunley-Owen
Department of Information Systems
University of Cape Town
Rondebosch, 7700

R. Fiqueira
University of Cape Town
Rondebosch, 7701

A. Foster
Department of Computer Science
University of Cape Town
Rondebosch, 7701

C. Gee
Software Engineering Applications Laboratory,
Electrical Engineering
University of the Witwatersrand
Private Bag 3
Wits 2050
The use of the Internet in an academic environment to commercially supply and support software products

B.Braude, A.I.Walker

Software Engineering Applications Laboratory, Electrical Engineering, University of the Witwatersrand, Johannesburg, South Africa

Summary: This paper explores the use of the Internet to supply and support software products within a quality management system. The Software Engineering Applications Laboratory (SEAL) at the University of the Witwatersrand is in the process of developing various software products that will be commercially distributed in the near future. The SEAL has chosen to use the Internet to supply and support these products. The system to be developed for this task has been named the Internet System for the Supply and Support of Software (IS⁴). Issues that have influenced the design of the IS⁴ have been the service processes within a quality management system, the control of the supply and licensing of the supplied products and the transaction processing of the on-line sales. The SEAL is committed to developing and supplying software within a quality management system. Consequently an investigation was undertaken into the quality characteristics and requirements based on the ISO 9001 standard for quality assurance and the ISO/IEC JTC1/SC7 software engineering standards. These quality concerns are being incorporated into the SEAL's quality management system and the development process for SEAL products. To control the supply and licensing of the supplied products, various issues such as unlock keys, Internet based registration, controlled access and hardware control have been investigated. The advantages and disadvantages of each have been investigated. To process the on-line transactions the IS⁴ is being developed to be compliant with recently released 'Secure Electronic Transactions' (SET) standard.

Keywords: software quality management, software engineering standards, secure electronic transactions, Internet commerce

1. Introduction

The Software Engineering Applications Laboratory (SEAL) at the University of the Witwatersrand is in the process of developing various software products that will be commercially distributed in the near future. The SEAL has investigated various means for supplying and supporting these products. The SEAL will use the Internet for this task. An Internet based system was selected due to suitability and advantages of using such a system. The system was named Internet System for the Supply and Support of Software, (IS⁴). Issues that have influenced the design of the IS⁴ have been the service processes within a quality management system, the control of the supply and licensing of the supplied products and the transaction processing of the on-line sales.

The SEAL is an organisation committed to Software Quality and is extensively involved in the development and application of software quality standards and procedures. Some of the applications to be supplied by the IS⁴ are used in the application of software quality standards. One of the initial requirements of the IS⁴ was therefore that the system complies with all the relevant software quality standards relating to the supply and support of software. An investigation was undertaken into the quality standards dealing with the supply and support software and their application in the Internet environment.

An issue that is a major concern in the supply of software products is the prevention of unauthorised duplication and use. In the IS⁴ the product is supplied over the Internet and this problem is compounded further. This issue has been investigated in the design of the IS⁴ and a method developed to prevent the unauthorised use of SEAL software products.

In the design of the IS⁴ various methodologies for conducting business on the Internet have been investigated. VISA International and Mastercard International in conjunction with major software vendors have developed a standard for Secure Electronic Transactions (SET). This standard is in the process of being implemented by the concerned parties. The IS⁴ is being developed to be SET compliant.

The results of these investigations have been taken into account in the development of the IS⁴.
The use of the Internet in an academic environment to commercially supply and support software products

The interface will be accessed using a Web browser on the server.

On accessing the interface the administrator will be presented with a main menu containing links to the various sections. The interface will have the following sections:

a. New Products Section – this will be used to add new products into the system. The administrator will also be able to add ‘User Documentation’ and ‘Cover Information’ as required by ISO 9127 (Refer to section 3.4).

b. New User Section – this will be used by the administrator to add new users to the system. This is required in the case of the user not having web access and manually purchasing a product. This will enable the IS$^4$ to serve as an overall database for recording all users of SEAL products.

c. Register User Section – this will be used to register a non-Internet based customer for a particular product.

d. Approval of Payments Section – in the event of the banking institutions not being able to process the transactions automatically, the administrator will approve transactions in the system after manually processing them.

e. Products Section – used to view and update all the SEAL products in the system and to view transactions for a selected product.

f. User Profiles Section – used to view and update users’ information in the system and to view transactions for a selected user.

g. Transactions Section – used to view all the transactions in the system per time period

3. Software quality issues and their impact on the planned system

The SEAL is committed to supplying and supporting software within a quality management system. The SEAL is an ISO 9001 rated organisation and is involved in extensive research in the field of Software Quality. A number of products to be supplied via the IS$^4$ are related to Software Quality Standards and the application thereof. A number of SEAL customers will therefore also come from a Software Quality environment. It is imperative that the software supplied and supported by the SEAL, be done so in a quality controlled manner and compliant with all the relevant quality standards.

An investigation has been undertaken into the relevant quality standards and into how the requirements of the standards can be addressed in an Internet based supply and support system. The ISO 9000 related series and the ISO/IEC JTC1 SC7 software engineering standards have been investigated.

The investigation examines issues that impacted on, or are part of the supply and support of the software product. The investigation assumes that the organisation developing and supplying the software is already compliant with the standards in the physical environment. The investigation only explores the application of the standards to the supply and support of software using the Internet.

The discussion of each of the standards and the discussion of the applicability of each clause to the IS$^4$ is beyond the scope of this paper. The requirements derived from the investigation into each of the standards are however listed below.


a. The products supplied by the IS$^4$ are to be treated as ‘shrink wrapped’ products. A contract will be developed and will be a non-negotiable contract that is developed by the supplier. Any contract negotiation will have to be conducted outside the scope of the IS$^4$.

b. All documentation supplied via the IS$^4$ must be handled in the same manner as all other organisational documentation, that is in compliance with ISO 9001

c. All product identification and traceability used on the organisational level must be reflected in all products and artefacts supplied via the IS$^4$

d. ISO 9000-3 states that “to protect the integrity of the product and provide a basis for the control of change, it is essential that software items be held in an environment which:

i. Protects them from unauthorised change or corruption

ii. Permits the controlled retrieval of a copy of the controlled master” [1].

e. Precautions must be taken due to the material on which the software is stored, deteriorating. The storage area will be the server on which
The use of the Internet in an academic environment to commercially supply and support software products

<table>
<thead>
<tr>
<th>the product is stored. ISO 9001 and ISO 9000-3 further state that access control must be instituted.</th>
</tr>
</thead>
<tbody>
<tr>
<td>f. Issues that are applicable to replication in the supply of software via the Internet are:</td>
</tr>
<tr>
<td>i. The master and other copies must be identified.</td>
</tr>
<tr>
<td>ii. Disaster recovery plans must be developed.</td>
</tr>
<tr>
<td>iii. The period of obligation of the supplier to supply copies of the respective products must be determined.</td>
</tr>
<tr>
<td>iv. Virus checking must be carried out.</td>
</tr>
<tr>
<td>v. The required documentation to be supplied must be stipulated.</td>
</tr>
<tr>
<td>vi. Copyright concerns must be addressed and agreed to (in the contract).</td>
</tr>
<tr>
<td>vii. The environment must be controlled to ensure repeatability of replication.</td>
</tr>
<tr>
<td>g. Only released products must be made available through the IS^4.</td>
</tr>
<tr>
<td>h. The control of non-conforming product requirements must be followed on the project and organisational levels to ensure that no products are unintentionally released to the IS^4.</td>
</tr>
<tr>
<td>i. Installation of the purchased product falls beyond the scope of the IS^4 and if installation is to be carried out by the supplier, it is to be handled outside the scope of the IS^4. This must be specified in the contract.</td>
</tr>
<tr>
<td>j. Procedures must be developed within the IS^4 to receive and handle (pass on to the relevant party) customer complaints.</td>
</tr>
<tr>
<td>3.2 ISO/IEC 12207 – Software lifecycle processes</td>
</tr>
<tr>
<td>a. The contract is to &quot;address proprietary, usage, ownership, warrantee and licensing rights associated with the reusable off the shelf products&quot; [2].</td>
</tr>
<tr>
<td>b. The delivery and support of the product by the supplier must be specified in the contract and carried out as specified.</td>
</tr>
<tr>
<td>c. It must be specified in the contract that the supplier cannot install the product, assist the acquirer with set-up activities or support of any parallel running activities when the installed software product is replacing an existing system.</td>
</tr>
<tr>
<td>d. The resources and information necessary to install the software product must be determined by the supplier and be made available to the acquirer.</td>
</tr>
<tr>
<td>e. It must be specified in the contract that the developer cannot support the acquirer’s acceptance review and testing of the software product.</td>
</tr>
<tr>
<td>f. The initial and continuing training and support to be provided to the acquirer must be specified in the contract.</td>
</tr>
<tr>
<td>g. The IS^4 must provide a means for the users of purchased products to report problems and request modifications. Once the report is received, the maintainer is to record and track the problem.</td>
</tr>
<tr>
<td>h. The IS^4 must facilitate the communication of change requests between the developer/modifier and the user (acquirer).</td>
</tr>
<tr>
<td>i. The IS^4 must provide for a means to provide feedback to the users.</td>
</tr>
<tr>
<td>j. The IS^4 must provide a mechanism to communicate with the users and provide them with migration information. When the scheduled migration arrives, notification must be given to all concerned. A post-operation review must be performed.</td>
</tr>
<tr>
<td>k. The IS^4 must provide a mechanism to communicate with the users and provide them with retirement information. When the scheduled retirement arrives, notification must be sent to all concerned.</td>
</tr>
<tr>
<td>l. It must be specified in the contract what records of quality assurance activities and tasks shall be made available to the acquirer. The applicable records must be made available via the IS^4.</td>
</tr>
<tr>
<td>3.3 ISO/IEC 9126 – Software product evaluation – Quality characteristics and guidelines for their use</td>
</tr>
</tbody>
</table>

The standard discusses Quality Characteristics that relate to software products. The standard does not discuss the supply and support of software in particular but discusses generic quality characteristics as they apply to all software products.

These characteristics have been investigated and applied to the IS^4 as a software product itself.
The use of the Internet in an academic environment and support software products

3.4 ISO/IEC 9127 - User documentation and cover information for consumer software packages

The software supplied and supported using the IS* is a typical consumer software package except that the traditional physical packaging is not present. Due to the user still obtaining the product as a 'ready-made package' the same information requirements apply.

The standard described two types of documentation:

a. User documentation - "This documentation provides users with all the information they need to install and run the software" [4]. In the traditional sense this documentation is included within the software packaging and therefore the user only has access to this information after purchasing the product. Similarly in the IS*, this documentation need only be provided to the user after the product has been purchased.

b. Cover information - "Its purpose is to enable prospective purchasers to decide on the applicability of the software to their requirements" [4]. This information is traditionally provided on the external product packaging. In the IS*, this information should be available to prospective purchasers prior to purchasing the product.

The standard categorises the information into three categories, namely Essential, Conditional and Optional. The same three categories will apply to the information when supplied by the IS*.

Due to the standard being directly applicable to the IS*, the details of the standard have not been repeated herein. The standard applies as is to the IS*. Refer to Appendix A for the standard.

3.5 ISO/IEC TR 9294 - Guidelines for the management of software documentation

The management of documentation for the IS* and the products supplied using the IS* will be handled on the organisational and project levels.

All the guidelines that are applied to documentation on the organisational and project levels must however be reflected in the documentation supplied by and developed for the IS*.

Documentation developed by the IS* processes may also comply with the guidelines. Ensuring the documentation complies with the organisational and project standards can ensure this compliance.

3.6 ISO/IEC 15504 - Software process assessment

The ISO/IEC 15504 standard is used to assess processes and determine their respective levels of capability. The processes as detailed in the standard have been rated with the required level of capability for the relevant processes that the IS* is to perform. In applying the standard, the processes have been assessed not for the processes of developing the IS* system but for the processes that the IS* will perform when fully functional and complete. The standard has been used to assess the processes that the system will perform but has not described any new processes that need to be incorporated into the system.

4. Internet management of the software supply and licensing

In the supply of tangible products, whether from a tangible or virtual store, unauthorised replication and use is not a concern for suppliers due to the difficulty and cost of replicating the product.

With digital products however, replication is simple and cheap and therefore measures have to be implemented in order to prevent the unauthorised replication and use of the product. In the supply of digital products on physical media (disks and CDs) unauthorised use is controlled to an extent through the localised dispersion of the physical media containing the data. To replicate a CD, one has to have access to another CD containing the data.

In the supply of data over the Internet, the problem becomes a far more serious one. Access to the data is world-wide and methods of obtaining data off the Internet are common (FTP). In order to combat this unauthorised use of data (products), control can be exercised on two levels. Firstly the access to the location to download the data can be restricted and secondly use of the product once obtained can be restricted.

4.1 Access control

Access to download a product can be controlled by:

a. Password protecting the pages used to download the product. Either a unique password for each customer will provide access to the pages or a generic password can be used.

b. Hiding the location (URL) of the Web pages used to download the product and providing the address to customers after the purchase of the product.
The use of the Internet in an academic environment to commercially supply and support software products

The problem with the above methods is that the information necessary to download the product (password or URL) can be passed on to unauthorised people or even be posted on the Internet. Between the options above, the unique password for each customer would be the most preferably as dissemination of access information to unauthorised parties could then be traced to a particular customer.

4.2 Use control

The use of digital products can be controlled through requiring the user to 'unlock' the product before being able to use it. Prior to unlocking the product, use can be fully restricted or limited use can be granted.

The following different types of unlock systems can be used:

a. The product can require the user to input some type of password.

b. The product can require a type of hardware key to be attached to the computer in order to unlock the product.

c. Internet based unlocking

4.2.1 Password key

Password keys can be implemented in a number of ways. Firstly the product can be totally locked prior to insertion of the password key. In this case the product can either require the user to input the key during installation of the product or each time the product is used. The more common method is during installation as this is a once off procedure and thereafter the product can be used normally. The product can only be installed by running the installation procedure and therefore if anyone obtained a copy of the program they would have to run the installation and input the unlock key.

In the situation where limited access to the product is granted prior to insertion of the key, the product is installed and run. Only limited access to product functionality is provided. Once the user obtains the key (after purchase) the key is input into the running application and access to all the functionality is provided. This is a once off procedure and the product is thereafter fully functional every time it is used. If however the product is installed again the unlock key has to be reinserted.

The actual key can be implemented in a number of ways.

a. A single key for use by all users. This implementation is the most simplistic. The main drawback of this implementation is that the key can be distributed illegally on a wide scale without any traceability.

b. A specific key per user per product. This is described in detail in section 4.3.

4.2.2 Hardware key

Hardware keys, commonly known as dongles, are devices that attach to the PC or network on which the software runs. When the product is run, it checks for a specific key and will only run if the key is present. The keys normally attach to the parallel port of the PC. Software protected with hardware keys is practically totally secure.

The disadvantage of a hardware key in the Internet environment is that the hardware key becomes a physical product that has to be delivered and defeats the advantages of digitally supplying the product over the Internet (Refer to section 2.2 above). The use of hardware keys has therefore not be investigated any further in the supply and support of software over the Internet.

Hardware keys may however become a viable option in the future. With the emerging use of smartcards for commerce, the Internet purchasing system may eventually incorporate the use of smartcard readers on PCs for Internet payments instead of users paying with a software based digital wallet. The smartcard could then be used as the hardware key. During purchase the supplier can read the user's smartcard information. This information can then be incorporated into the protection system on the supplied product. After purchase the smartcard would then be used to unlock the product for use. This would alleviate the supplier having to supply a unique hardware key to each customer.

4.2.3 Internet based unlocking

A system can be implemented where the purchased product is automatically unlocked over the Internet. The system would work as follows:

a. The customer would download the product

b. The customer would purchase the product online.

c. The customer would run the product installation. During installation the product would prompt the user for his IS's username and password. Using this information the product would connect to the server and the server would unlock the product by passing it some encryption string.

Siacsit '97
The use of the Internet in an academic environment to commercially supply and support software products

If the system allows each customer purchase to only unlock the product once, it makes the system secure to unauthorised use of the products. This cannot however be used because the customer cannot then reinstall the product in the event of a hardware upgrade, computer failure etc.

Another disadvantage of this system is that the product has to be installed on a machine connected to the Internet. The other methodologies discussed herein allow the product to be downloaded and purchased on an Internet connected machine and then installed on an isolated machine.

This methodology can be carried out with installation on a non-Internet-connected machine as follows, however the disadvantage of a once only installation still holds:

a. The customer downloads the product
b. The customer purchases the product on-line
c. The customer runs the installation program. During installation the program generates a random number.
d. The customer then manually inputs this number into the Internet based purchasing system using his username and password.
e. The Internet system encrypts the number and presents it to the customer. The customer then inputs the encryption number into the application.
f. The application then decrypts the number and if it matches the original random number then unlocks the application.
g. The Internet system will be set to only encrypt one number per customer per purchase.

This method still has the disadvantage of allowing a once only unlocking.

If the server allows for the product to be unlocked multiple times in this manner, the system reduces the methodology of 4.2.1b above.

4.3 Method to be used by the IS

The SEAL uses a control system where it allows the user to download the product and use it with limited features for a limited period. After evaluation the user can decide to purchase the product.

On the IS the user will select the product and purchases it. After the purchase has been processed, the user will be given a product number for that product (a sequential number for each copy of the product purchased) and an unlock key. This key is based on the following being passed through a one way hash function:

a. The registered username which has been input by the customer during registration on the IS
b. The product identification, which is a unique code specific to each product name. This number is hard coded into the application.
c. The product version which is hard coded into the application.
d. The product number as given to the customer. The product number is necessary should a specific user want to purchase multiple copies of the product (a large company).

With this information in hand the user will then open the registration window in the already installed product and input the username, product number and key. The product contains the same hash function and will therefore generate the key. If the generated key matches the input key, the product will open up with full functionality.

Due to the customer requiring access to the product in order to evaluate it prior to the purchase, access control as described in section 4.1 cannot be used.

The only way to bypass this system is for a user of a particular product to pass on his username, product number and key to an unauthorised user for use on the same product. Authorised users will hesitate to do this, especially publicly, as the information is traceable back to the offending customer. This then reduces the control problem back to a localised dispersion problem as has been described regarding the distribution of digital products on physical media.

Once off installations, and Internet based unlocking have not been used due to the disadvantages discussed in section 4.2.3 above.

5. Secure electronic transactions

5.1 Standard transaction process

After a shopper browses an Internet store and selects the products for purchasing, the following is the process for completing the transaction:

a. The customer’s order and payment details are sent to the merchant.
b. An Internet based receipt is then issued to the customer.
c. On receipt of the order and the payment details the merchant passes the payment details to the bank.
The use of the Internet in an academic environment to commercially supply and support software products

d. If available (as is the case with SET) approval is then obtained from the bank.

e. The merchant then supplies the goods to the customer (ships or makes available via the Internet) and charges the customer for the goods.

5.2 Overview of the SET standard

“Visa and MasterCard have jointly developed the Secure Electronic Transaction (SET) protocol as a method to secure payment card transactions over open networks. SET is being published as an open specification for the industry. This specification is available to be applied to any payment service and may be used by software vendors to develop applications.

Advice and assistance in the development of this specification have been provided by GTE, IBM, Microsoft, Netscape, RSA, SAIC, Terisa, and VeriSign” [3].

The SET standard is specified in three books namely a Business Description, Programmer’s guide and Formal Protocol Definition. This discussion only investigates the SET standard on the business level.

Through using well defined procedures, SET uses cryptography to:

• provide confidentiality of information,
• ensure payment integrity, and
• authenticate both merchants and cardholders.

The following implementations or cryptography are used in order to achieve the requirements above:

a. Symmetric key encryption
b. Public key encryption
c. Digital signatures using public keys and message digests
d. Digital Certificates

A detailed description of the use and interactions of the above mentioned cryptographic implementations is beyond the scope of this paper. Refer to reference 1 for more details.

5.3 Advantages of SET to merchants and customers

Currently prior to the availability of SET, there are other methods for carrying out Internet based transactions. These methods are relatively secure but have some disadvantages when compared to SET. Even though the non-SET systems have disadvantages as tabled below, the level of credit card fraud on these systems is far lower than the fraud level in the physical world.

<table>
<thead>
<tr>
<th>Table 2 SET considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>Encryption</td>
</tr>
<tr>
<td>between customer</td>
</tr>
<tr>
<td>and merchant</td>
</tr>
<tr>
<td>Access to payment</td>
</tr>
<tr>
<td>information (credit</td>
</tr>
<tr>
<td>card details)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Integrity of data</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Customer Identity</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Merchant identity</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>System Interoperability</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

5.4 Implementation of a SET compliant system

The following three software components make up a SET system:

a. SET compliant consumer wallets
b. SET merchant software
c. A SET payment gateway connected up to the banks’ credit card systems.

Currently SET software developers are developing the above three software components. Using standard protocols and message formats the three components interact with each other as defined by the SET standard.

The SET payment gateway is set up by or on behalf of a banking institution that signs up credit card merchants. This gateway communicates with the SET merchant software to receive authorisation requests and thereafter for the merchant to capture
The use of the Internet in an academic environment to commercially supply and support software products

payments

The SET merchant software is used firstly to accept customers' purchase requests and reply to the customer's purchase requests. Thereafter it is used to communicate with the payment gateway as described above. The SET merchant software does not contain the software for the store itself. The merchant must set up the store and thereafter the merchant connects the SET merchant software to the on-line store.

The SET consumer wallet is used to submit SET compliant purchase requests to the merchant. SET consumer wallets will be available freely off the Internet or at a minimal charge (depending on the brand.)

Currently the software components have been developed to be SET version 1 compliant. Due to the formal description of protocols and messaging, all three SET components from any software vendor should interoperate with any of the components from any other SET compliant software vendor.

Prior to conducting any SET transactions using the software components described, the merchant and the consumer have to register and obtain digital certificates. The merchant must register with an Acquiring Bank and the consumer must have a credit card issued by its Issuing Bank. Certificates are then issued by Certificate Authorities (CA). The CAs can be the Acquiring and Issuing banks respectively or third parties acting on behalf of these financial institutions. These certificates contain merchant and user details respectively in order for all parties to be identifiable during transactions.

"A certificate is only issued to the cardholder when the cardholder's issuing financial institution approves it. This certificate is transmitted to merchants with purchase requests and encrypted payment instructions. Upon receipt of the cardholder's certificate, a merchant can be assured, at a minimum, that the account number has been validated by the card-issuing financial institution or its agent" [3].

Likewise a certificate is only issued to a merchant with the approval of the merchant's acquiring bank. "These certificates are approved by the acquiring financial institution and provide assurance that the merchant holds a valid agreement with an Acquirer" [3].

The consumer's SET wallet and the merchant's SET software contain functionality to obtain the required digital certificates from the respective CAs.

Once the software and certificates are in place, the merchant can begin with SET compliant transactions.

SET implementations are currently in pilot testing stages with a few banks setting up bank gateways for use with a few merchants and limited customers. After this pilot test phase, more merchants and consumers will be brought into the testing until the gateway is opened up for use by any merchants (subject to standard banking requirements) and all customers. This is planned to take place towards the end of 1997 or early in 1998.

6. Project progress todate

The investigations into the various aspects as discussed in this paper have been carried out. Based on the findings and conclusions of these investigations a Product Functional Specification has been drawn up, as has briefly been discussed in section 2.3. Thereafter the Product Functional Specification has been refined into a High Level Design. Many of the aspects from the investigation into the quality standards have been incorporated into the High Level Design. Based on the High Level Design prototype development of the IS has begun.

The investigation into the quality standards has resulted in requirements being imposed on the SEAL and the development teams responsible for respective products that are to be supplied and supported via the IS. Reference documentation has been developed for future use by the SEAL and development teams when developing products for the IS. This reference documentation has also detailed the encryption system that the supplied products are to use to prevent their unauthorised use.

Discussions have been held between the SEAL, banks and Internet software developers over the implementation of SET in the IS. This has not yet been carried out due to the unavailability of SET for the next few months, as discussed above. However at the earliest availability, the SEAL will be in a position to achieve SET compliance in the IS.

7. Discussion

As has been discussed, the use of the Internet to supply and support software products presents numerous advantages and opportunities to software developers and suppliers. This facility has only recently become a viable option due to the recent
The use of the Internet in an academic environment to commercially supply and support software products

rapid growth in the use of the Internet.

The system as discussed herein meets the initial requirements of the Software Engineering Applications Laboratory in requiring low maintenance and support with minimal human intervention. With the use of SET, the payment mechanism has been totally automated.

The investigation into the Quality aspects of supplying and supporting software products using the Internet has been carried out and the requirements have been incorporated into the IS and the SEAL's development and administrative procedures. The major issues in the supply and support of software that have been influenced by the investigation have been:

a. The information and documentation that needs to be supplied.

b. The contract information that needs to be agreed to by the customer.

c. The feedback mechanism and communication with the customers.

d. The management and security of the system's server.

Various ways of minimising the unauthorised replication and use of the software products have been investigated and a system has been developed for use by the IS. This methodology and system is to be built into the software products that are being developed by the SEAL.

The IS is being developed to be SET compliant. SET will provide major security advantages to the SEAL and the SET standard will be the basis on which Internet commerce will develop into a publicly accepted means of conducting business.

Internet commerce is a very immature field which will continue to grow driven by consumer needs for convenient and secure shopping, merchant needs to securely conduct business in the global market place and banks needs to provide an effective service to meet consumers' and merchants' needs.

Smartcards will further affect Internet Commerce and can further be applied to controlling the use of digital products. Digital wallets will most probably be incorporated into smartcards allowing consumers to conduct secure Internet commerce from locations other than their private computers. Eventually smartcards will be as common as the credit card is today (probably replacing the credit card) and with the customer's digital identification built into the card, smartcards can serve as a means of user verification in preventing the unauthorised use of digital products in the digital market place.

8. References


9. Author contact details

Bruce Braude is currently a postgraduate student in the Department of Electrical Engineering at the University of the Witwatersrand studying towards the degree of MSc in Software Engineering. Bruce's MSc is entitled "Quality Aspects of Software Product Supply and Support using the Internet." Bruce has obtained his BSc (Hons) in Electrical Engineering and has completed further courses in Software Quality Management. During his studies Bruce has been involved in part time Internet and Intranet development for the Software Engineering Applications Laboratory and for commercial institutions. Bruce is a member of the SEAL Management Board and the Young Members Committee of the South African Institute of Electrical Engineers.

Contact details: Bruce Braude, Software Engineering Applications Laboratory, Department of Electrical Engineering, University of the Witwatersrand, Private Bag 3, P O Wits, 2050 Johannesburg. Office Phone: +27-11-716-5379, Fax: +27-11-403-1929, Internet E-mail: braude@odie.ee.wits.ac.za; WWW: http://seal.ee.wits.ac.za/
The use of the Internet in an academic environment to commercially supply and support software products

Alastair Walker is an associate professor in the Department of Electrical Engineering, University of the Witwatersrand. He was responsible for establishing the Software Engineering Applications Laboratory in 1988. The SEAL received an ISO 9001 certification for software development in July 1995. He is a Certified Quality Analyst, and a Certified Software Quality Systems Auditor.

Contact details: AJ Walker, Software Engineering Applications Laboratory, Department of Electrical Engineering, University of the Witwatersrand, Private Bag 3, P O Wits, 2050 Johannesburg, South Africa. Office phone: +27-11-716-5379, Fax: +27-11-403-1929, Mobile: +27-82-452-0933, Internet E-mail: walker@odie.ee.wits.ac.za; WWW: http://seal.ee.wits.ac.za.