The African Journal of Computing & ICT
Volume 5. No. 3. May, 2012

All Rights Reserved
© 2012

Published for the Institute of Electrical & Electronics Engineers (IEEE)
Nigeria Section Computer Chapter

By

The Trans-Atlantic Management Consultants
2580 Fairham Drive
Baton Rouge LA, USA
CONTENTS

i. Table of Contents

ii. Editorial Board

iii. Managing Editor’s Introduction

TABLE OF CONTENTS

1-6 A Platform for Solving Transportation Problems Using an Interactive System for Optimal Solution.
C.U. Onianwa & F.I. Sadiq
Ambrose All University, Ekpoma, Nigeria

7-14 An Activity Ontology for a Water Production Company
V.B. Oyekunle
Lead City University, Ibadan, Nigeria

11-16 Employing Response Time Constraints To Mitigate CAPTCHA Relay Attack
C.U. Onwudebelu & C. Ugwuoke
Salem University, Lokoja, Nigeria

15-22 Review on Number Portability in Global System For Mobile
J.N. Odii & J.C. Onuoha
The Federal University of Technology, Owerri, Nigeria

23-30 On the Role of Linguistics in The Detection and Prevention of Cybercrimes in Nigeria
F.U. Balogun, O. Abu (Esq), E.I.G. Balogun & O.O. Aramide
Auchi Polytechnic, Auchi, Nigeria

31-36 A Model for Intelligent Motion Detection in Live Video Streaming Systems.
Olufade, F.W. Onife., Oladeji, P. Akomolafe & Ademola, S. Olaniyi
University of Ibadan, Nigeria

37-48 A Model Checking Framework For Developing Scalable Antivirus Systems
E. Osaghae & S.C. Chiemeke
University of Benin, Benin City, Nigeria

49-56 Just another Harmless Click of the Mouse ? - An Empirical Evidence of Deviant Cyber Space Behaviour Using an Online Trap
P. Danquah, O.B. Longe & F. Totimeh
Pentecost University Collec & The Accra Institute of Technology, Accra, Ghana.

57 Call for Papers

58 Publication Template
Editorial Board

Editor-in-Chief

Prof. Dele Oluwade
Senior Member (IEEE) & Chair IEEE Nigeria – Computer Chapter.
Dean - College of Information & Communication Technology
Salem University, Lokoja, Nigeria

Editorial Advisory Board

Prof. Gloria Chukwudebe - Senior Member & Chairman IEEE Nigeria Section
Engr. Tunde Salihu – Senior Member & Former Chairman  IEEE Nigeria Section
Prof. A.B. Sofoluwe – Vice Chancellor, University of Lagos, Nigeria
Prof. Adenike Osofisan - University of Ibadan, Nigeria
Prof. Amos David – Universite Nancy2, France
Prof. Clement K. Dzidonu – President Accra Institute of Technology, Ghana
Prof. Adebayo Adeyemi – Vice Chancellor, Bells University, Nigeria
Prof. S.C. Chiemeke – University of Benin, Nigeria
Prof. Akaro Ibrahim Mainoma – DVC (Admin) Nasarawa State University, Nigeria
Dr. Richard Boateng – University of Ghana, Ghana.
Prof. Lynette Kvaszny – Pennsylvania State University, USA
Prof. C.K. Ayo – Covenant University, Nigeria
Dr. Williams Obiozor – Bloomsburg University of Pennsylvania, USA
Prof Enoh Tangjong – University of Beau, Cameroon
Prof. Sulayman Sowe, United Nations University Institute of Advanced Studies, Japan
Dr. John Effah, University of Ghana Business School, Ghana
Mr. Colin Thakur - Durban University of Technology, South Africa

Managing/Production Editor

Dr. Longe Olumide PhD
Southern University and A & M College, Baton Rouge, USA
University of Ibadan, Ibadan, Nigeria
Managing Editors Introduction.

The ICT strides continues - so are the challenges

Events within the last one year showed that Computing and ICT will continue to dominate popular discussions all over the world. What with new advances in mobile developments, tele-medicine, drones for fighting battles and new concerns about viruses that can now close down nuclear plants. We live in a time that can be considered as a watershed of mixed blessings brought about by accelerated developments in computing, ICTs and their applications.

The African Journal of Computing & ICT stands at the nexus of providing a platform for contributions to discourses, developments, growth and implementation of Computing and ICT initiatives. We provide a voice for scholars from the developing countries and other nations across the world to contribute to the solution paradigm through timely dissemination of research findings as well as new insights into how to identify and mitigate possible unintended consequences of ICTs.

In the last year, we have experienced tremendous impact and acceptance across the globe. This is evidenced by the H-Index of some of our authors ranking as high as 7 based on cited works in the journal. Our impact factor has also grown beyond the 1.7 in 2011 to 2.8 during the first quarter of this year, 2012. In particular is the interest expressed in the Journal by African scholars in Diaspora. Thanks to our authors and reviewers and the Editorial board for continuously striving to provide submissions, insights and comments that has helped improve the quality of the Journal. We have also continued to experience increased interest evidenced by the volume of submissions that we received recently from Asia, America, the United Kingdom and many parts of Africa that are now scheduled to appear in future issues. Surely, the Journal is repositioning itself among the league of impactful Journals in Computing, information systems/science, Information and Communication Technology and other allied fields globally.

The African Journal of Computing & ICTs is now indexed in the Cabells Directory of Scientific Journa, Google Scholar, IS Publication Indexing, ScienceCentral.com, Database of Computer Science Journals, Docstoc Database/Indexing and the SCRIBD Research Database. Other indexing schemes are being pursued to further increase access to the journal contents. We remain committed to excellence in publishing and desire that the Afr, J of Computing and ICT be a prime avenue for the dissemination of cutting edge research report by Africans, for Africa and all lovers of research and development all around the world. We will promote indigenous Computing and ICT development through the dissemination of cutting edge research and development report.

This March, 2012 issue of the African Journal of Computing & ICT contain ten (10) articles that have been subjected to rigorous peer review by experts in the subject domain. The articles articulate issues of research and development related to computational informatics and mathematical modelling, computer and cyber security, e-Learning and multimedia-based pedagogy, data mining and knowledge management, management of ICT units, grid computing and open source mobile platform system design. While welcoming you to peruse this March, 2012 Edition of the African Journal of Computing and ICTs, we encourage you to submit your manuscript for consideration in future issues of the African Journal of Computing and ICTs.

Have a rewarding reading

Thank you

Longe Olumide Babatope  PhD
Managing Editor
African Journal of Computing & ICTs
Fulbright SIR Fellow
International Centre for Information Technology & Development
Southern University System
Southern University
Baton Rouge
Louisiana, USA

E-mail: longeolumide@fulbrightmail.org
A Platform for Solving Transportation Problem Using an Interactive System for Optimal Solution

C.U. Onianwa (Ph.D) and F.I. Sadiq (MCPN,MNCS)
Department of Computer Science
Ambrose Alli University, P.M.B 14, Ekpoma.
fatai_aau@yahoo.com charlesonianwa@yahoo.com

ABSTRACT
Transportation problem is one of the major areas of application of linear programming. In this paper, we discussed the concept of transportation system and the method of solving transportation problems. We developed a model for the transportation system in Ambrose Alli University (AAU), Ekpoma though private but provides an optimal transportation framework for decision making in the University transportation division. In developing the software, we used Microsoft Visual Basic 6.0. The optimal solution arrived at showed that the management can operate at a minimum cost if they utilize the routes as presented in the study: Main campus to Alli Square conveying an average of 90 passengers per day, Main campus to Market Square with an average of 150 passengers, Basic Medical Sciences to Alli Square with an average of 15 passengers, Basic Medical Sciences to Mousco junction with an average of 150 passengers and Basic Medical Sciences to Opoji junction with an average of 85 passengers. Consequently, the cost of transportation on these routes are ₦30, ₦30, ₦20, ₦20, and ₦30 respectively per journey. An online application was also developed using North-West Corner (NWC) rule to automate the analysis of the System.

Keyword: Transportation problem, Route, Linear programming, Software, Optimal solution

1. PRELIMINARIES
Transportation is a vital part of the everyday life of every urban citizen. Even the very young, the very old, the sick and the shut-ins are beneficiaries of a good transportation system or victims of a poor one. Efficient transportation stimulates the economy of any state. The condition of transportation services and facilities improves or detracts from living and working conditions, enhances or harms the environment of the area, and heavily influences the general desirability of the community. In most studies of transportation, the following questions are asked for the transportation system to be in the best possible condition in an area. They are:

- do you receive numerous complaints about congestion and accidents caused by a poor transportation system?
- are industry and commerce concerned about delays in their shipments caused by inadequate transportation facilities?
- are industry and commerce rejecting your community because of a poor transportation system?
- has enough been done to take care of transportation problems in your community?
- and finally, has timely improvements been made?

2. RELATED WORKS
Jurgen [5] noted that the main task of scheduling is the temporal assignment of activities to resources where a number of goals and constraints have to be considered. Scheduling problems can be found in several different application areas, e.g., the scheduling of production operation in manufacturing industry, computer processes in operating systems, aircraft crews, etc. Scheduling covers the creation of a schedule of the activities over a longer period (predictive scheduling) and the adaptation of an existing schedule due to actual events in the scheduling environment.

However, scheduling also has a very important interactive dimension because we always find humans involved in the scheduling process that have to decide, interact or control. Among the decisions to be taken by the human scheduler are, e.g., introducing new orders, canceling orders, changing priorities, setting operations on specific schedule positions. These decisions have to be regarded within the scheduling process. But, Reed [7] stated that a key problem manager’s face is how to allocate scarce resources among various activities or projects.
Therefore, an essential tool for doing this is the linear programming method. Thus, Linear programming, is a method of allocating resources in an optimal way. It is one of the most widely used operation research tool and has been a decision-making aid in almost all manufacturing industries and in financial and service organizations. These resources are known as decision variables.

2.1 Transportation Problem

Chung et al [2] presented a poly-log-competitive deterministic online algorithm for the online transportation problem on hierarchically separated trees when the online algorithm has one extra server per site. Using metric embedding results in the literature, one can then obtain a poly-log-competitive randomized online algorithm for the online transportation on an arbitrary metric space when the online algorithm has one extra server per site. Sheng et al [8] analyzed a transportation problem with discontinuous piecewise linear cost function and developed a genetic algorithm to solve it. Their genetic algorithm exhibits better optimization effect on solution quality and efficiency than the matrix encoding genetic algorithm. Their genetic algorithm utilizes the structure of spanning tree in the basic feasible solution and the possible values of the non-basic variables are restricted to the flow bounds.

The compact coding representing the basic feasible solution is another important factor. In addition, the genetic algorithm developed in their paper can be applied to solve the fixed charge transportation problem as well. Zijian et al [10], focused on the computing complexity dealing with hub and spoke system, proposed a new reliable combination optimization method, named ACO (ant colony optimization) algorithm, to solve the container transportation network problem for marine transport system. To prove its utility, they compared the proposed method with the result by Dijkstra algorithm through a simple example. The result shows ACO algorithms is of a credible and excellent probability accumulation searching method. In general, it’s known that there exist four factors in an optimization problem of container transportation, namely economical efficiency, speediness, security and inventory cost [4]. Yuichi et al [9], considered the problem of transporting a long object such as a ladder through a degree corner in a corridor using two omni directional robots that do not necessarily have identical characteristics. A distributed algorithm is presented in which each robot computes its own motion-based on the current and goal positions of the ladder, the locations of the walls and the motion of the other robot observed indirectly through the link between the robot and the ladder. They evaluate the performance and robustness of the algorithm using extensive computer simulation by changing several parameter values that act as the key characteristics of the robots including the maximum speed.

Table 1: Passengers

<table>
<thead>
<tr>
<th>Locations/Services</th>
<th>Ali Square</th>
<th>Market Square</th>
<th>Mousco Junction</th>
<th>Opoji Junction</th>
<th>Supply</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main Campus</td>
<td>60</td>
<td>100</td>
<td>30</td>
<td>50</td>
<td>240</td>
</tr>
<tr>
<td>Basic Medical Sciences</td>
<td>45</td>
<td>30</td>
<td>20</td>
<td>35</td>
<td>150</td>
</tr>
<tr>
<td>Demand</td>
<td>105</td>
<td>150</td>
<td>50</td>
<td>85</td>
<td></td>
</tr>
</tbody>
</table>

For the above problem, all units available must be supplied. How likely it is that supply always will equal demand? For practical purposes, it doesn’t matter as long as supply is adequate to meet demand. We can ignore the surplus and treat the total supply as equal to the requirement.

3. PROBLEM STATEMENT

In Ambrose Alli University, (AAU) Ekpoma the transportation unit is faced with the optimal administration of transportation solution in a bid to reducing the cost of transportation for staff and students to and from campus while in the process considering the convenience of the passengers. In this paper, we model the transportation system in Ambrose Alli University, (AAU) Ekpoma. The outcome of the model was finally automated with the process of analysis of the system. The study used the North-West Corner (NWC) rule to obtain the initial basic feasible solution of the system that can serve as a guide for the unit.

3.1 Research Direction

This paper reported the findings of a result in an undergraduate research, that developed an automated transportation problem using AAU Ekpoma as a case study, the purpose which focused on the following:

- to aid administration minimize the total transportation cost within the school environment
- to help administration analyze the various transportation situation at a very fast rate
- to facilitate the decision making process on transportation at all levels
4. MATERIALS AND METHOD

We considered some routes and collected data from the routes. The collection of data was done for some period of time after which average of the observations was determined. This idea was to enable us know the routes to include in our modeling. The modeling of the transportation took effect as soon as the data collection was completed. The model was used to develop an algorithm that eventually transformed into the use of visual basic programming language at the end to design software that is usable in solving problems related to the transportation matters in the university. The available routes include Main campus to Alli square, Main campus to Market Square, Main campus to Mousco junction, Main campus to Opoji junction, Basic Medical Sciences to Alli square, Basic Medical Sciences to Market Square, Basic Medical Sciences to Mousco junction, and Basic Medical Sciences to Opoji junction.

4.1 Mathematical model of the transportation problem

The mathematical modeling of this transportation problem is nothing but a special linear programming problem in which the objective function is a minimize cost of transportation subjected to the demand and supply constraints.

Let $d_i =$ Number of passengers (staff and students) available to be transportation from the origin $i$.

$S_j =$ Number of passengers that is required to be at a destination $j$.

$C_{ij} =$ The transportation cost per passenger from the origin $i$ to destination $j$.

$X_{ij} =$ Number of passenger from origin to destination $j$.

Mathematically, the problem is:

Minimize $\sum \sum x_{ij} C_{ij}$

$\sum x_{ij} d_i i = 1, 2, \ldots, m$

$\sum x_{ij} s_j j = 1, 2, \ldots, n$

$\sum x_{ij} \geq 0$ for all $i$ and $j$

From equation 1, it can be understood that we have two sources of supply namely main campus and Basic Medical Sciences to four demand destination namely; Alli square, Market square, Mousco junction and Opoji junction. With this in mind, we now formulate transportation problem.

### Table 2: Cost of transportation

<table>
<thead>
<tr>
<th>Routes</th>
<th>Alli Square</th>
<th>Market Square</th>
<th>Mousco Junction</th>
<th>Opoji Junction</th>
<th>Supply</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main Campus</td>
<td>30</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>240</td>
</tr>
<tr>
<td>Basic Medical Sciences</td>
<td>20</td>
<td>30</td>
<td>20</td>
<td>30</td>
<td>150</td>
</tr>
<tr>
<td>Demand</td>
<td>105</td>
<td>150</td>
<td>50</td>
<td>85</td>
<td></td>
</tr>
</tbody>
</table>

The total transportation cost:

Minimize $z = 30 x_{11} + 30 x_{2} + 30 x_{3} + 40 x_{14} + 20 x_{23} + 30 x_{22} + 20 x_{23} + 30 x_{24}$

Subject to:

$x_{11} + x_{12} + x_{13} + x_{14} = 240$

$x_{21} + x_{22} + x_{23} + x_{24} = 150$

$x_{11} + x_{21} = 105$

$x_{21} + x_{22} = 150$

$x_{31} + x_{32} = 50$

$x_{41} + x_{42} = 85$

$x_{ij} > 0$
5. DESIGN IMPLEMENTATION

The software design for the model used Microsoft Visual basic 6.0. The development was possible due to the proper understanding of the formulation as well as the development of the mathematical model of the problem. The major step that was followed to solve the problem also played a vital role in the development, but the key issue is actually the process of translating mathematical algorithm into visual basic symbolic instruction code and the design of the interface to achieve the goal of the study. System analysis approach was followed and sample data presented in our methodology was used to test run the software developed. The results for input and output during testing are presented in Figures 1 to 4.

Fig 1: Transportation problem software introduction page
Source: Okoruwa [6]

Fig 2: The transportation problem input page
Source: Okoruwa [6]

Fig 3: Transportation problem with test data with (NWC).
Source: Okoruwa [6]

Fig 4: The transportation problem output on computation using the test data.
Source: Okoruwa [6]
5.1 System Installation
Before the software can be used, the executable file name “aigbibhalu.exe” need to be installed having installed visual basic programming language 6.0, for the application to effectively run, the system must met the following requirements;

Minimum hardware requirements
a. Pentium III computer system or more
b. 233 MHZ processor clock speed
c. 64 MB RAM or more
d. 200MB free hard disk space or more

Minimum software requirements
The software will work well on Microsoft Windows 2000, XP, Vista operating systems. No additional framework is needed on any of this operating system for the application to run effectively.

6. FINDINGS
The transportation problem in all the routes from campus to various locations such as Basic Medical Sciences, Alli Square, Market Square etc, are often computed by estimation but the data collected were entered into the interface and the results obtained. More accurate results were equally obtained using the North West Corner rule that gave the optimal solution of 11050.

Based on our findings, it is recommended that the management in transportation unit should always carryout survey periodically to find out if there are variations in the distributions of passengers in their routes. Data obtained in surveys should be analyzed with this application to obtain current optimal solution for the current transportation situation and compare it with previous one. If any alteration is made to the number of routes, then the system will need to be modified to meet the specified routes.

7. CONCLUSION
This study on the transportation problem in Ambrose Alli University Ekpoma was mainly to identify the transportation routes and then structure the system to obtain a model that will enable the management to operate at minimal cost. We went further to develop an application that will help the management to analyze the AAU transportation problem as fast and effectively as possible. As a result of this the management can operate at a minimum cost.

REFERENCES
AUTHOR'S BRIEFS

Dr. Charles Uche Onianwa has been at Ambrose Alli University, Ekpoma, Nigeria since 1988 and has been engaged in teaching and research. Born at Asaba, Delta State, he attended St. Patrick's College, Asaba between 1973-1978 and 1978-1980 and the University of Benin, Benin City. He hold a Bachelor, Master of Science and an MBA degrees from the same University between 1980-1984, 1985-1987 and 1990-1995 respectively. He also holds a Doctor of Philosophy (Ph.D) degree in Mathematics from Ambrose Alli University, Ekpoma with specialization in numerical computing. He is a member of several professional organizations including the Nigeria Computer Society, Nigerian Institute of Management and the Research and Development Network. He is a fellow, Chartered Institute of Administrator and Strategic Institute for National Resources and Human Development. His primary research interests are in Numerical computing, Hardware maintenance and Information Technology where he has authored a number of books and published academic papers.

Mr. Fatai Idowu SADIQ is a Lecturer at Ambrose Alli University, Ekpoma, Nigeria. He obtained his B.Tech. Maths./Computer Science in 1998 at Federal University of Technology, Minna. Master of Technology in Computer Science in 2005 at Federal University of Technology, Akure, MBA and PGD in Education at Ambrose Alli University, Ekpoma in 2004, 2010 respectively. He has recently obtained Master of Philosophy (MPhil) in Computer Science in 2012 from the University of Benin, Benin City, Edo State. Nigeria, with a view to proceed for Ph.D. in the same field. He is a member of Nigeria Computer Society (NCS), Computer Professional and Registration Council of Nigeria (CPN). IEEE Computer Society. His research interest is mobile computing applications for electronic learning and Information and Communication Technology (ICT) for Development. He has published number of papers in both local and International journals.
An Activity Ontology for a Water Production Company

V. B. Oyekunle
Department of Computer Science
Lead City University
Ibadan, Nigeria
bolanleoyekunle@yahoo.com

ABSTRACT
The key success of a business process is the ability to manage between processes within an enterprise and between enterprises. To remain competitive, enterprises must become increasingly agile and integrated across their functions. Activity ontology plays a critical role in this integration, enabling better designs for enterprises, analysis of their performance, and management of their operations. The goal of this paper is to create an activity ontology for water production processes that has the ability to deduce answers to queries that require relatively shallow knowledge of the domain. This activity ontology will provide a sharable representation of knowledge that minimizes ambiguity and maximizes understanding of the production activities. This kind of representation is of importance because it will be able to provide sophisticated support to automated decision making; it does not only answer queries with what are explicitly represented in the Knowledge Base, but also answer queries to what is implied in the Knowledge Base. The project was implemented using Prolog, a logic programming language and it was tested by posing a set of competency questions.

Keywords: Activity Ontology, Knowledge Base, Formal Representation, Competency questions.

1. INTRODUCTION

An activity is the basic transformational action primitive with which processes and operations can be represented; it specifies how the world is changed [12]. Thus in this paper, the focus is on how the production activities of water production company can be modeled. The activity ontology for the production activities would provide a framework that would break down the steps involved in the different activities and the time interval for each activity. In enterprise modelling, we want to define the actions performed within an enterprise, and define constraints for plans and schedules which are constructed to satisfy the goals of the enterprise. This leads to the following set of informal competency questions;

a. Temporal projection: Given a set of actions that occur at different points in the future, what are the properties of resources and activities of different intervals?

b. Planning and Scheduling: What sequence of activities must be completed to achieve some goal? At what times must these activities be initiated and terminated?

c. Time-Based Competition: We want an ontology that minimizes the cycle time for a product. This is essentially the task of finding a minimum duration plan that minimizes action occurrences and maximizes concurrency of activities.

Activities are defined to occur over intervals of time and cannot be reduced to some set of properties holding at instantaneous points in time. In an enterprise, activities take place over time. These time points can be point based, interval-based or point-interval-based. In this paper, we want to see how practicable are the Allen’s interval temporal logic of Actions and Events using Water Production Activities.

This paper therefore aims at developing an activity ontology in form of knowledge representation that includes facts and axioms that support deduction for the activities of water production, the ontology will be able to deduce answers to some given queries. These queries are the common sense queries that require the knowledge based system to have extensive knowledge and reasoning capabilities. Ontologies are widely used as technique for representation and reuse of knowledge. Ontology can be viewed as a shared conceptualization of a domain that is commonly agreed to by all parties. It is defined as ‘a specification of a conceptualization [11]. ‘Conceptualization’ refers to the understanding of the concepts and relationships between the concepts that can exist or do exist in a specific domain.
The primary goals for developing ontology is not only to enable reuse of domain knowledge but also to share common understanding of the structure of information among people or software agents, to make domain assumptions explicit, to separate domain knowledge from the operational knowledge and to analyze domain knowledge in an enterprise context, they reflect the relevant knowledge based on enterprise-specific concepts and their relations. This activity ontology can be considered as building blocks for demand-oriented information supply in networked organizations.

Drinking water can be produced from any natural sources like ground water, lakes and rivers (surface water) or sea water. Drinking water standard are set by the world health organization/NAFDAC. Drinking water must be free of suspended solids, microorganism and toxic chemicals. The quality of drinking water is assessed not only in terms of health but also in terms of taste. One of the solution for improving the taste of water is to reduce the amount of environmental organic materials, which are difficult to eliminate with traditional treatment processes due to their high solubility. The more organic materials there are in water the higher the microbiological risk and the more necessary the chlorination treatment becomes, organic materials and chlorine jointly deteriorating the taste of water in the supply systems, the easier it is to reduce chlorination and therefore unwanted effects, not only in terms of taste but also with regard to disinfection by-product. Water properties differ from one area to another, some of these properties are; Hardness, Alkalinity, pH level, Conductivity etc. these properties differ from one area to another area and any drinking water produced must be in accordance with the NAFDAC specifications.

2. RELATED LITERATURE

Ontology as a specification of conceptualization is defined by logical theory, axioms of which constrain predicate interpretations. Nikola Guarino uses notions of domain space and conceptual relationships. Several projects are known that create ontologies to define a given subject domain and share this knowledge among users for more coordinated interaction in domain. TOVE [8] and Enterprise [16] create ontologies for commerce and production organization, CIDOC [4] develops an ontology for museums and cultural heritage, PHYSSYS [2] creates an ontology in the area of physical systems. The project SYNTHESIS uses ontologies for semantic interrelating of object-oriented specifications.

Project Ontoseek and Plinus use ontologies for information retrieval. There are many projects where ontologies help to detect similarities and redundancies in natural language information [5]. Ontologies are used for context definition in a subject domain. Determination of exact difference between contexts helps to solve a problem of viewing onto an information resource from another context or changing of resource moving from one context to another [6].

Using shared ontologies, establishing correspondence of data to ontological definitions; enhancing ontologies for new tasks allow to achieve correct interoperability between different information systems [7]. The web needs ontologies for relating web-information to concepts of ontologies. The project SHOE [14] proposes to support HTML-pages by additional tags, which relate the information to ontological definitions. The TOVE Ontology currently spans knowledge of activity, time and causality, resources and more enterprise oriented knowledge such as cost, quality and organization structure. The TOVE Testbed provides an environment for analyzing enterprise ontologies; it provides a model of an enterprise and tools for browsing, visualization, simulation and deductive queries. The goal of the TOVE Enterprise modelling project is to create a common sense Enterprise model. By common sense we mean that an enterprise model has the ability to deduce answers to queries that require relatively shallow knowledge of the domain.

2.1 Computer Integrated Manufacturing Open System Architecture (CIMOSA)

CIMOSA incorporate an event-driven, process based modelling approach with the goal to cover essential enterprise aspects in one integrated model. The main aspects are the functional, behavioural, resource, information and organizational aspect. For each of the aspects, modelling constructs are available. This enables to model the aspects of business processes independent from each other. CIMOSA provides a formal language for the modelling, which is specified in BNF form. Furthermore, CIMOSA aims at the execution of business processes also, not only the modelling of those. The goal is to drive an information infrastructure with the processes modelled.

2.2 PERA(The Purdue Reference Architecture)

PERA was developed as an endeavor in enterprise modeling for a computer-integrated manufacturing (CIM) factory by the Purdue Laboratory for Applied Industrial Control at Purdue Laboratory University. The functional descriptions of the tasks and functions of the enterprise are divided into two major streams: (1) Information (including decision and control) and (2) Manufacturing, or customer service.

2.3 Classes of Models for Ontology Construction and Reasoning

Ontological modelling in information technologies has undergone considerable evolution. Models and languages used for ontology construction and reasoning can be classified as follows.

2.3.1 Verbal Models

Informal linguistic models are often used for specification of ontologies [3]. In such models ontological concepts are defined by verbal definitions like in an explanatory dictionary. Some kinds of basic relationships may be established between concepts. A glossary of terms in some subject domain, a thesaurus with its concepts and relationships defining natural language terms may be considered as ontologies.
2.3.2 Logic-Based Models
In contrast to verbal models, logic based ontologies are defined formally and have an ability of formal reasoning. One of the first logic-based ontological models was Ontolingua [11]. Predicative expressions in Ontolingua are represented in the KIF language, which is based on the first order logic. KIF is highly expressive and due to that it is not tractable for automatic inference. Development of ontologies in this model is regulated by special technique for adding of unambiguous specifications [7]. Ontolingua has been intended as an intermediate language for heterogeneous ontologies interchange.

Ontological model uses a train model as its basis. The open knowledge Base connectivity (OKBC) API is considered as a key enabler in the distributed ontology repository architecture. The OKBC model serves as an inter-lingua for ontology that is being communicated using OKBC. Ontology interchange language, OIL is the first ontology representation language in W3C standards that is properly grounded. It is an evolution of existing proposals such as OKBC, XOL, RDF (Resource Description framework). OIL is the first web-based representation language intended for ontology definition with the formal semantics and reasoning services provided by a description logic.

2.3.3 Structural (Object) Models
Several approaches are known to apply structural (Object) data models to define ontologies. A mediator ontological language (MOL) may depend on a subject domain and is to be defined at the media for consolidation phase. On the other hand, for different information sources different ontological models (languages) can be used to define their own ontologies. Reversible mapping of the source ontological models into MOL is needed for information sources registration at the mediator.

2.3.4 Hybrid Models
To enrich an expressive power of the ontological model, there might be a need to use a facilities of verbal, logic-based or structural models in one and the same ontology. For instance, this project uses a hybrid model. The ontological model has verbal facilities making possible to define ontological or glossary concepts, classifier categories. At the same time, it is defined as logic-based type.

3. METHODS AND FORMAL REPRESENTATION
Actions and Events in Interval Temporal Logic
In order to adequately represent actions and events, one need an explicit temporal logic [1] and that approaches with weaker temporal model such as state spaces (e.g. STRIPS-based approaches) and the situation calculus, either cannot handle the problems.

3.1 Properties of Actions and Events
Properties of action and events that are essential to any general representation:

a. Actions and events take time, while some events may be instantaneous, most occur over an interval of time – During this time, they may have a rich structure. Because events are extended in time, different events and actions may overlap in time and interact.

b. The relationship between actions and event and their effects is complex. Some effects become true at the end of the event and remain true for some time after the event. Other effects only hold while the event is in progress. Other effects might start to hold sometime after the event has started and stop holding before it finishes.

c. Actions and events may interact in complex ways when they overlay or occur simultaneously.

d. External changes in the world may occur no matter what actions an agent plans to do, and may interact with the planned actions.

e. Knowledge of the world is necessary incomplete and unpredictable in detail, thus prediction can only be done on the basis of certain assumptions.

In this paper, the following steps are carried out;

a. Purpose identification and requirement specification-concerns to clearly identify the ontology purpose and its intended uses, that is, the competence of the ontology. To do this, we use competency questions.

Fig 1: Stages in the ontology development process.
b. Ontology capture, the goal is to capture the domain conceptualization based on the ontology competence. The relevant concepts and relations were identified and organized.

c. The formalization activity aims to explicitly represent the conceptualization captured in a formal language. In this project, first order logic is the preferred formalism, since it embeds less ontological commitments.

d. Finally, the ontology was evaluated using Prolog to check whether it satisfies the specification requirements and ontology competence. It should be noticed that the competence questions plays an essential role in the evaluation of the completeness of the ontology, especially when considering its axiom.
3.2 Language Definition
The language used is the interval temporal logic of Action and Events, subset of first order predicate calculus. Standard symbols for quantifiers are used; universal (\(\forall\)) and Existential (\(\exists\)).

The connectives used are;
- Negation (\(\neg\))
- And (\(\land\))
- Or (\(\lor\))
- Implies (\(\rightarrow\))
- Conditional implication (\(\iff\))

Time relations used are;
- Meets (\(i, j\)) - Interval ‘\(i\)’ meets interval ‘\(j\)’.
- Before (\(i, j\)) - Interval ‘\(i\)’ is before interval ‘\(j\)’.
- After (\(i, j\)) - Interval ‘\(i\)’ is after interval ‘\(j\)’.
- Equal (\(i, j\)) - Interval ‘\(i\)’ is equal to interval ‘\(j\)’.
- Overlaps (\(i, j\)) - Interval ‘\(i\)’ overlaps interval ‘\(j\)’.
- Cover (\((i, j, k)\)) - Interval ‘\(i\)’ covers interval ‘\(j\)’ and ‘\(k\)’.

Specification in First Order Logic – Axioms

A.  \(V t1,t2,t3\) Pump(st1, st2, t3) Level(st2full, Pre2(e)) Level(st2empty, Pre2(e)) \(\land\) Levels(st2comp_filter, t3) Level(st2, eff1(e)) Level(st2full, eff2(e)) Level(st2, empty, eff2(e)) Water flows(st2, st1, t1) Level(st1full, eff1(e)) Level(st1full, eff2(e)) Meets(time(pre1(e)), time(pre2(e))) Meets(times)(pre1(e), time(e3)) Overlap(time(e1), time(e3)) Cover(time(e1), time(pre1(e)), time(e3)).

Water is pumped from storage tank (\(st1\)) to storage tank (\(st2\)) if \(st1\) is full and \(st2\) is empty, these are the two preconditions. There exist activities (\(e1\)) and (\(e2\)) such that \(e1\) is the opening of tap for \(st1\) and \(e2\) is the process of water flowing from \(st1\) to \(st2\) and the effect of these is that the level of \(st1\) will now be empty while that of \(st2\) will be full. The time relations are shown as below.

B. \(\forall e1,t\) Treatment(e1, t) Sedi(e1, pre1(e1), t1) A Fill(e2, pre2(e1), t) A Steril(e2, pre3(e1), t) A Before(t1, t2) A Overlaps(t1, t2) A Covers(t1, t2).

For all water treatment, there exist sedimentation, filtration and sterilization.

B1. \(\forall e1,e2\) Sedi(e1, t1) A Fill(e2, t2) A Dissolve(CaCO3, t3) A Comp_filter(st2, t4) A Cover(t1, t2, t3).

For Sedimentation to occur, there is going to be addition of Calcium Carbonate, which will take time interval \(t2\) to dissolve. Sodium Hydroxide will take time interval \(t3\) to dissolve and Buffer Solution will take time interval \(t4\) to dissolve. The time relation is as shown.

\[B2. \ V e, t \ A Waterflows(st1, comp_filter, t) \ A Waterflows(st2, carbon_filter, t) \ A Waterflows(st2, micro_filter, t) \ A Waterflows(st2, ultralight, t) \ A After(st2, t) \ A Overlap(st2, t2) \ A Overlap(st2, t3) \ A Cover(st2, t4)\]

For filtration and sterilization to occur, sedimentation tank \(st2\) will be opened for water to flow from it through composite filter, then through carbon filter and then micro filter, for the process of filtration. After the water has been filtered, it needs to be sterilized by flowing through the ultraviolet light. The time interval is as shown.

C. \(\forall e, t\) Bottlemaking(e, t) \(\exists\) Heating(e1, t) A Blowing(e2, t) A Meets(st1, st2).

For all bottle making activities, there exists heating and blowing activities, and the two activities meet.

\[C1. \ V e \ A Heating(e) \ A Blowing(e, t) \ A Meets(st1, st2) \ A Cover(st1, st2)\]

For all heating activity, there exists perform of a particular size and heating machine such that the heating machine is heated within time interval \(t1\) and immediately the perform is passed through the heated machine. The end product is the heated perform.

\[C2. \ V e \ A Blowing(e, t) \ A Heating(e, t) \ A Meets(st1, st2) \ A Cover(st1, st2)\]

For all blowing process, there exists heated perform and blowing machine, such that mould of size(s) is set into the blowing machine and the heated perform is put inside the blowing machine which in turn is being pressed. The end product is the bottle.

D. \(\forall e, t\) Bottlemaking(e, t) \(\exists\) Heating(e1, t) A Blowing(e2, t) A Meets(st1, st2) A Cover(st1, st2)
For every sachet water production, there exists subactivities; set, pass through, fill, seal, cut, and pack. Film(f) is set into Automated machine(a) and the film is passed through the ultraviolet light to be sterilised. The function of the automated machine is to fill, seal and cut. The factory workers(w) pack the sachet water(s) in number of 20 inside the packing nylon(n). The time relation is as shown.

Further_treatment(e₁,t₁) Ʌ Bottlewashing(e₂,t₂) Ʌ Feeding(e₃,t₃) Ʌ Capping(e₄,t₄) Ʌ Labelling(e₅,t₅) Ʌ Auto_pack(e₆,t₆) Ʌ Meets(t₁,t₂,t₃,t₄,t₅) Ʌ Cover(t₆,t₈).

For every bottle water activity, there exists subactivities; further treatment, bottle washing, feeding, capping, labelling and autopack.

Microfilter(m) Ʌ Ozonator(o) Ʌ ReverseOsmosis(r) Ʌ Waterpass_through(m,t₁) Ʌ Waterpass_through(o,t₂) Ʌ Waterpass_through(r,t₃) Ʌ Overlap(t₁,t₂,t₃) Ʌ Cover(t₆,t₈).

Bottle water process involve insertion of covers(c) by factory workers(f) on the automated capping machine(a), arranging bottles(b) on the washing machine(w) and washing of these bottles by the washing machine, feeding of these bottles by the feeding machine(j), capping of these bottles by automated capping machine(k), labeling by the factory worker and packing of these filled bottles by the automated shrink machine(v).

Dispenser(d) Ʌ Factory_worker(f) Ʌ Treated_waterTank(t₈) Ʌ Fill(f,d,t₉) Ʌ Cap(f,d,t₉) Ʌ before(t₈,t₉) Ʌ Cover(t₉,t₁₀).

For all dispenser water production, there exists raw material, dispenser, factory worker and treated water tank, the factory worker fill the dispenser from the treated water tank and the factory worker then cap the dispenser. The time interval is as shown.

4. RESULTS AND DISCUSSION

Informal Competency Questions
Motivating scenarios are problems which are encountered in the specified industry. Given the motivating scenario, a set of queries will arise. TOVE consider these queries to be requirements that are in the form of questions that an ontology must be able to answer. These are the informal competency questions, since they are not yet expressed in the formal language of the ontology.

Ideally, the competency questions should be defined in a stratified manner, with high level questions requiring the solution of lower level questions. These competency question do not generate ontological commitments, rather they are used to evaluate the ontological commitment that have been made.

4.2 Competency Questions
1. What steps are involved in a particular process?
2. Which activity comes first?
3. What is the total time taken for a particular process to complete?
4. What are the low level activities involved in achieving the high level activity?
5. What is the time interval for each low level activity?
6. What are the raw materials used for each activity?
7. The window below shows the available set of options, these 8. options have been linked for the system to answer each competency question

Fig 3: Options Interface
Choose an option
1. Overall Process
2. Sedimentation
3. Filtration and Sterilization
1

There are two stages
1. Sedimentation: Sedimentation takes place between time interval
   1235, 1514
   It involves addition of
   A. co2 into tank2 between inteval 1235, 1237
   and this will dissolve in tank2 between interval 1237, 1340
   B. NaOH into tank2 between interval 1341, 1345
   and this will dissolve in tank2 between interval 1345, 1369
   C. into tank2 between interval 1400, 1405
   and this will dissolve in tank2 between interval 1405, 1514
2. Filtration and Sterilisation: here sedimented water from tank2 will pass through three different filters
   a. composite_filter within the time interval 1528, 1580
   b. carbon_filter within the time interval 1530, 1570
   c. micro_filter within the time interval 1540, 1520
   d. Finally water will be sterilised by passing through ultra_light within time interval 1561, 1531

Fig 5: Interface showing water treatment activities

Bottle Making

bottle is made from the raw material preform, of particular size_s,
within time interval 1030, 1936.
The first stage is to set mould of a particular size_s into blowing_machine
within time interval 1830, 1850.
The second stage is to heat up the heating_machine
within the time interval 1900, 1930.
The next stage is to pass preform of a particular size_s, into heating_machine
within time interval 1930, 1932.
The fourth stage is to remove preform of a particular size_s,
from heating_machine within interval 1932, 1933.
The next step is to immediately put preform of a particular size_s,
removed from heating_machine into,
blowing_machines within time interval 1933, 1934.
Preform still inside blowing_machine press blowing_machine,
within time interval 1934, 1935.
The end product is The bottle of size_s,
within interval 1935, 1936.
True

Fig 6: Interface showing bottle making activities

To know about the processes involved in sachet water production and the raw materials involved, enter option 4 and press enter.

4. Sachet Water Production

sachet_water is the end product of Sachet Water Production
automated_filling_machine is a machine that:
fill
seal and
cut
The raw material used is film The time interval taken to produce sachet water using a pack of film is 2001, 2149
The first stage is to set pack of film into automated_filling_machine within interval 2001, 2033
The next stage is to sterilise film by passing it through ultra_violet_light within time interval 2034, 2140
Next, automated_filling_machine will now fill film within time interval 2142, 2147
The next stage is to automated_filling_machine will seal film within interval 2144, 2144
automated_filling_machine will then cut film into equal sizes within time interval 2146, 2146
The end product of this production is sachet_water within time interval 2147, 2147
The final package is done by the factory_workers using nylon
True

Fig 7: Sachet water production activities

5. CONCLUSION

An activity ontology has been built using the water production company. It achieves the principal aim of capturing domain knowledge in a generic way, and it provides a shared understanding of the domain, which may be reused and shared across applications and groups. It provides a standard ontology for water production company, thereby minimizing ambiguity and maximise understanding of the production activities. Also the set of competency questions developed and tested showed that it would effectively serve as the core of an organisation. In addition, it also helps in the storage of water production knowledge for those people that have no experience in the field.

REFERENCES


[16] Uschold, M., King, M. Towards a Methodology for Building Ontologies. Workshop on Basic Ontological issues in knowledge sharing, held in conjunction with IJICAL-95, Montreal, August 20-25, 1995.

Author’s Brief

Mrs. V.B. Oyekunle lectures at the Department of Computer Science, Lead City University, Ibadan, Nigeria. She holds B.Sc Electrical and Electronics Engineering from Obafemi Awolowo University, Ile-Ife; and M.Sc Computer Science from University of Ibadan. She is a doctoral student at the department of Computer Science, University of Ibadan, Nigeria. Her interest is in the area of Artificial Intelligence, Ontology and Information System.Modelling. She can be reached at the Department Of Computer Science, Faculty Of Information Technology and Applied Science, Lead City University, Ibadan, Nigeria. E-mail bolanleoyekunle@yahoo.com
A Review On Number Portability In Global System For Mobile

1J.N. Odii & 2J.C. Onuoha
Department of Computer Science
Federal University of Technology
Owerri, Imo State
1jnodii@yahoo.com 2chiomajaco@yahoo.com

*Correspondence Author

ABSTRACT
This work looks into the monopoly associated with some telecommunication regulatory agencies inability to mandate the implementation of Mobile Number Portability (MNP) and its effects on subscribers who cannot retain their directory numbers when switching over to another service provider for reason best known to them. Many operators have claimed that Mobile Number Portability (MNP) is unnecessary and is an unwarranted expense, using assertions that the sector is highly competitive. Some mobile operators have gone to considerable trouble to make MNP difficult and have discouraged customers from exercising this right. They have suggested alternatives such as personal numbering and Universal Personal Telephony (UPT). However, these are not substitutes for MNP, but are expensive, value-added services. MNP should therefore strongly be encouraged by governments and Regulatory Agencies to recognize that Mobile Number Portability (MNP) is an essential part of the competitive framework and should be made legally binding on all operators and service providers.

Key word: Mobile number portability, universal personal telephony, mobile subscriber, service provider

1. INTRODUCTION

Technology has influenced the telecommunication industry in so many ways. Mobile data, Wi-Fi and 3G networks are few of these technologies that will continue to have great influence of the telecoms industry in general. But there is one new capability that gives subscribers greater flexibility and mobility which has been mandated and implemented in so many countries – Number Portability (NP). Number Portability gives subscribers the ability to change service providers and keep his/her dial-able number. To make this seemingly simple concept a reality, a whole host of new technologies, network upgrades, new business processes, laws and regulations, and cost models need to be addressed.

The list of countries that have adopted number portability is growing; and the technologies needed to support number portability continue to evolve. More importantly, the increase in number portability awareness among subscribers has resulted in an increased expectation by consumers that taking their numbers with them when changing service providers should be seamless and trouble free [6].

The Telecommunications Act of 1996 (TA 96) tore down most of the significant barriers to unfettered competition in telecommunications. However, the inability of end users to retain their telephone numbers when changing service providers or types could potentially dissuade consumers from making such a change, threatening to hinder industry competition and growth. Congress’ addition of Section 251 (b)(2) to TA 96 addressed this obstacle by defining number portability, requiring that all carriers deploy it, and setting deadlines for implementation. Federal Communications Commission (FCC) Docket No. 95-116 (In the Matter of Telephone Number Portability) and subsequent FCC orders and reconsiderations reinforced Congress’ mandate and set the machinery in motion to implement number portability [5][7].

The actions of both Congress and the FCC enabled consumers and businesses to choose new providers, services, and locales while retaining their phone numbers, thereby fostering competition in the telecommunications industry. To ensure standardization across platforms for all participants, the FCC instructed the North American Numbering Council (NANC) to determine which number portability method to employ. Several options were investigated. The location routing number (LRN) method was chosen because it appeared to be the most efficient and is now successfully implemented in the wireline environment. The NANC then created the Local Number Portability Working Group (LNPA-WG) and empowered it to select the appropriate technology, create standards, determine operational processes, and develop and implement a deployment strategy [3][4].
To fulfill its responsibilities, the LNPA-WG was granted the authority to convene appropriate subcommittees as needed. Subcommittees created include the National Number Pooling and Slow Horse groups, as well as the Wireless Number Portability subcommittee, which defines integration issues between the wireless and the wire line industries. NeuStar was named the Number Portability Administrator and operates the Number Portability Administration Center (NPAC). Regulators have mandated that number portability be implemented before the regional Bell operating companies (RBOCs) are allowed to offer long distance service within their regions. Conversely, interexchange carriers (IXCs) and competitive local exchange carriers (CLECs) require local number portability (LNP), also called service provider portability, to gain a competitive foothold in the local loop [2][8].

This ability to enter local markets on a competitive basis is considered key to fair and open competition and is directly addressed in FCC Docket No. 95-116. CLECs are taking advantage of opportunities created by LNP to compete with incumbent local exchange carriers (ILECs). In 1999, the local service market—the primary market identified by CLECs—represented over $109 billion in total revenue, and CLECs garnered 5.8 percent of that revenue, according to the FCC. (VeriSign Communications Services, 2004) This penetration is largely predicated on the ability of current ILEC customers to change service providers without changing their phone numbers. Some CLECs have reported that over 90 percent of their subscriber growth was directly enabled by number portability. Wireline LNP has been implemented within the top 100 MSAs in the United States, as mandated, and is gradually being adopted outside of these areas[1][5].

The FCC order also set an aggressive implementation schedule for the wireless industry. However, the Cellular Telecommunications Industry Association (CTIA), acting on behalf of the wireless community, asked for and received deadline extensions. The FCC’s current mandate requires that wireless carriers, including cellular and personal communications service (PCS) carriers, implement service provider portability by November 24, 2003 [10]

2. PRINCIPLES OF IMPLEMENTING NUMBER PORTABILITY

2.1. Mandates for the Implementation of Number Portability in Nigeria

The proposition for the mandated for the implementation of Mobile Number Portability was first raised by the Vice Chairman of the Nigerian Communications Commissions (NCC) Engr. Ernest Ndukwe during the public lecture held at the NCC secretariat (11th June 2007). During the lecture, he made the mandate for the implementation of MNP known the various telecommunication operators in Nigeria and December 31st 2007 was fixed for the implementation. However, the plan for the implementation on Mobile Number Portability in Nigeria failed due to various constrains from cost and infrastructure. The process is still on and would be implemented soonest [7]

2.2 Number Portability Defined

Number portability gives a telephone subscriber (fixed or mobile) the ability to change service providers but keep the same dial-able phone number. Sometimes, the porting of a number may require a different phone; the new phone is programmed with the “old” phone number [9]

2.3 Types of Number Portability

There are basically three types of Number Portability currently being implemented around the world presently which includes, Service Provider Portability (SSP) or Local Number Portability (LNP), Location Portability (LP) and Service Portability (SP).

2.3.1 Service Provider Portability (SSP)

The most commonly deployed number portability type, service provider portability enables end users to retain their telephone numbers when changing service providers.

2.3.2 Location Portability (LP)

Location portability is the ability of end users to retain their telephone numbers when moving from one location to another (between areas serviced by different central offices). In this instance, a telephone number could be associated with a device, independent of location. It would allow customers to keep their numbers when they move to locations outside of the original rate center. Until very recently, no requirements have been designated or mandated for location portability in the USA. (Note: In August 2005, the Federal Communication Commission (FCC) mandated a 90-day waiver for location number portability to help victims displaced by Hurricane Katrina in Mississippi, Alabama and Louisiana.)

2.3.3 Service Portability

This is the ability of end users to retain the same telephone number as they change from one service to another. The new service can be offered by a new operator or can be within the same operator network. For example, a subscriber shifts subscription to a VoIP service provider, or from a code division multiple access (CDMA) or time division multiple access (TDMA) network to a global system for mobile communications (GSM) network or vice versa [6].

2.4 Forms of Number Portability

Number Portability can take one of the following forms: Fixed – to – Fixed Porting. This is the porting of a fixed line number into another fixed line, Mobile – to – Fixed Porting. This involves the porting of a mobile phone number to a fixed line, Fixed – to – Mobile Porting. This porting of a fixed line number to a mobile phone and Mobile – to – Mobile Porting, This is the process of porting a mobile phone number to another mobile phone [6].

2.5 Key Network Elements in a Number Portability Domain
Listed below and shown in Figure 6 are several key network elements in a number portability domain:

- **NP server**: maintains the number portability database (NPDB) and provides routing instructions, for example the Tekelec EAGLE® 5 Integrated Signaling System (ISS).
- **Donor network**: network from where the number originally came.
- **Originating/initiating network**: network from where the call originated.
- **Subscription network**: network in which the subscriber is presently being served.
- **Recipient network**: network to where a number is ported.
- **Transit network**: network between two networks (where signaling is transported prior to arriving at the recipient network) (Tekelec Co. 2007).

### 3. ARCHITECTURE AND METHODOLOGY

#### 3.1 Three Steps to Porting a Number

Different countries have implemented NP differently. These differences are primarily because of the disparities among regulatory agency philosophies, existing infrastructure and methods employed by operators to meet the mandate. Although there is a variety of ways to implement these steps, in all cases, there are three basic steps to porting a number from the “old” service provider (OSP) to the “new” service provider (NSP):

- **Port Initiation**: The subscriber has to initiate the port by letting an operator know of his/her intent.
- **Exchange of Porting Information**: The OSP and NSP must communicate with each other specific about the port, including the subscriber information, exact date and time, and of course, the phone number.
- **Network Routing Schemes**: Once the number has been ported, calls made to that phone number must be “re-routed” to the NSP.

#### 3.2 Step One: Port Initiation

To start the porting process, a subscriber needs to contact an operator to request the port. There are two basic approaches for this process used around the world which includes, **Donor Initiated** in which the subscriber goes to his/her current operator or OSP to request to port “out” and **Recipient Initiated** in which the subscriber goes to the NSP to request to port “in” his/her number.

**3.2.1 Donor Initiated**

In this model the donor operator or OSP starts the porting process. The subscriber contacts their current service provider and indicates their desire to change service providers and port their number.

The OSP then initiates the administrative process with the NSP. In some places, the subscriber is given an authorization code or document showing they are eligible for porting (note: eligibility is determined by fulfillment of the contract or ability to break the contract). The subscriber has a set period of time (e.g. up to 30 days in the U.K.) to determine a desired service provider and present the written authorization. The NSP then coordinates the port with the OSP, using contact information provided in the written authorization form. In other cases, the OSP contacts the NSP directly upon initiation by the subscriber. This assumes that the subscriber has already selected a new service provider. In both of these cases, the net result is that the subscriber must initiate the porting process through the current service provider.

**3.2.2 Recipient Operator Initiated**

In this model the porting process starts when the subscriber contacts a desired new service provider (NSP) (recipient operator) to initiate the porting process. The subscriber contacts a retail point of sale (a kiosk, a Web site, a retail center, an authorized agent, etc.) and provides information regarding his/her current operator (OSP), such as account number. The NSP then begins the administrative process and must validate the subscriber-provided information with the OSP. At this point, the OSP still has the ability to reject the port, based upon agreed valid reasons, such as incorrect subscriber information.

**3.3 Step Two: Exchange of Porting Information**

Regardless of the method chosen for port initiation, the OSP and NSP must exchange information for validation and port coordination. This information exchange is commonly referred to as inter-carrier communications or inter-operator communications (IOC) [1].

In the case of fixed-to-fixed porting, the amount of information in the IOC can be several pages, including circuit and trunk information, physical locations of various network elements, as well as subscriber information. In the case of mobile-to-mobile porting, the data in this exchange can be as simple as: subscriber name and billing address, account number, the phone number to be ported and the date and time of port. There are several different methodologies used around the world to accomplish IOC. One such example is a fully automated exchange through a single central clearinghouse.

This method uses a pre-determined format for the data and can be completed in minutes. This fully automated exchange is “kicked-off” by one operator’s back-office system (e.g. a billing system or a customized gateway) and is responded to automatically by the other operator’s back-office system. Another automated approach involves entering the porting information into a GUI. The information is then exchanged through a centralized clearinghouse with the other operator. In both of these cases, software systems play a major role in validating the port, expediting the changeover in service providers, and tracking the porting process end-to-end.
In some countries, a manual approach is used, often using facsimile or e-mail to exchange information. There are trade-offs to both approaches. The automated solution results in less errors and a much faster overall porting experience for the subscriber. This automation comes at a cost – software systems need to be developed, and modifications to operators’ existing back-office systems need to be made to exchange the information. The manual approach can be troublesome – faxes can be lost, e-mails can be deleted, and in both cases, humans need to interpret and input the information into various systems. And of course, a manual approach results in a much longer porting process.

3.3.1 Port Timing
The time it takes to complete a port varies as widely as the differences in the implementation of the process – from as little as two and a half hours to as lengthy as 30 days, with extreme examples of four months. How long should the process take? There is no right or wrong answer; but generally from a subscriber’s perspective, a shorter timeframe is better. The answer to this question, in part, needs to be determined by the regulatory agency and in part, by the operators.

3.3.2 Cooperation between Operators
Typically competitors do not communicate, never mind cooperate. But in the case of number portability, competitors need to cooperate to accomplish the porting process. The degree to which the operators cooperate has a direct correlation to the reliability and overall porting speeds. And although two operators may be competitors, there is incentive to cooperate – the OSP assisting the NSP in porting a subscriber will benefit next time the roles are reversed. Furthermore, two cooperating competitors can decrease the cost of porting for both operators.

This cooperation includes agreement on the forms to be exchanged, the method and protocol to be used for the exchange, timeframes for acknowledgement of the requests and responses, information to be used to validate the port request, valid reasons for rejection, hours / days of the week and holiday schedule to be observed in the porting processed, etc. The need for cooperation is obvious – the degree to which competing operators agree to cooperate varies greatly by country, and even among operators within a single country. However, we have observed that those operators most willing to cooperate find that their ports go through quickly and reliably, resulting in a better porting experience for the subscriber.

3.4 Step Three: Network Routing Schemes
After the IOC process has been completed and the port is in effect, calls made to the ported number must be re-routed – i.e. an incoming call must find its way to the NSP. The routing information used prior to the implementation of porting would route the call to where it always went – the OSP. Although there are many variations and hybrids, routing of incoming calls in a ported environment can be categorized into three basic methodologies or schemes such as Onward Routing (OR), Query on Release (QoR) and All Call Query (ACQ).

A description of the call processing for each of these schemes follows, but first a brief explanation of the roles of the operators in the following diagrams. The originating network typically refers to the network that places or originates the call, but for purposes of this document, it could refer to the network prior to the terminating network. If the call originates in another country, the network denoted by “originating network” in these diagrams would be the long distance carrier. If the call was originated by a mobile operator that subverts all calls to the local PTT or local LEC, then that PTT or LEC would take on the role denoted by “originating network” in these diagrams. This role is referred to as the “N-1” network, i.e. the network one prior to the terminating network.

The donor network is the network from which the number was ported. The donor switch is the switch to which the number range is assigned, and to which, by default, calls are routed. The new network is the network to which the number has been ported. Although the following diagrams are simplified, there could be more than one donor and/or new network, if the subscriber has ported, and then ported again.

3.4.1 Onward Routing (OR)
In the OR scheme, calls generated from an originating network are routed just as if there was no porting, that is, according to the path indicated by the dialed digits. The donor network checks against an internal database, notes that the number has been ported, determines to which network the call should be routed, and then routes (“trunks”) the call to the new network. The internal database may be a stand-alone database, shared by all switches belonging to that donor operator, or may be switch-resident, and only contain information about numbers ported out of that switch. This method has been referred to as a “call forwarding” scheme and has some positive aspects and some drawbacks.

Most switches have some call forwarding capability, therefore this method is a very quick and relatively simple to implement. It does not involve a centralized database, as does the other methods, and therefore does not require close cooperation among competitive operators. This scheme does require the setup of multiple call segments; this scheme can become very inefficient with regard to transmission facilities (i.e. circuits and trunks) and switch resources (i.e. cards, racks, and memory) – all expensive components in an operators network. Furthermore, a donor network that loses subscribers may incur costs for additional transmission facilities and switch resources to handle the routing for subscribers that it has lost – not a good position to be in.

3.4.2 Query on Release (QoR)
In the QoR scheme, the originating network first routes the call as if porting had not happened. The donor network checks if the number was ported, and if so, the call is released back to the originating network. Note that the donor network does not keep track of where the subscriber has ported, just that the number is not resident on the switch.
The originating network queries a centralized database, determines the revised routing to the new network, and re-routes the call correctly. With QoR, circuits are allocated to the donor network but are released immediately rather than remain tied up for the length of the call, as in OR. And although the donor network is still involved in each call, its involvement is minimized. This method therefore is more efficient in terms of circuit and transmission facilities. But a new network element is needed – a centralized database. This requires that all operators agree on a process by which the centralized database is updated and maintained – typically by agreeing on a third party to own and operate the database. Also, the costs to own and operate the centralized database must be borne by all the operators.

A special note on a hybrid model, proposed on paper but not seen implemented, known as Call Drop Back or Return to Pivot (RTP). As in OR, in RTP the donor operator maintains an internal database, which is used to look-up new routing information. The call is released back to the originating operator along with the new routing information that is also passed back to the originating operator. The originating operator in turn uses the routing information provided by the donor network to reroute the call. Therefore a centralized database is not needed, and a circuit from the donor operator to the new operator is not required. However, major changes to the signaling protocol are required. However, major changes to the signaling protocol are necessary to make this scheme happen, which is the major reason it has not been widely adopted. OR is efficient when a limited number of ported numbers exist, by comparison, QoR becomes more cost effective as porting becomes more common. But as porting becomes even more prevalent in a country; QoR is less efficient than All Call Query.

### 3.4.3 All Call Query (ACQ)

In the scheme known as ACQ, the originating network does not route calls to the donor network; in fact, once a number has been ported, the donor network is not involved at all. The originating network queries a centralized database and the call is re-routed to the new network. There are two forms of ACQ – in one, literally all calls are queried; in the other, the line range in which the number belongs is checked to see if that line range is eligible for porting prior to the database query. In reality, where ACQ is used, most operators query all calls to simplify administration. As in QoR, there is a process to update and maintain the database and a third party to own and operate the database.

All the operators must agree upon this. And as in QoR, the costs to own and operate the database must be borne fairly by all the operators. As porting volumes increase, QoR becomes the most efficient scheme for call routing. In some cases, countries have started with OR when porting volumes were low, and have migrated to ACQ as volumes have increased. In some countries, QoR and ACQ coexist, and the choice of implementation is left to each operator [6].

### 3.5 Process Overview: Porting a Number

This involves:

- **a)** When the recipient operator wins the business of one of the donor operator’s customers it enters porting information into its operations support system (OSS), at the point of sale (POS) (i.e., retail store, affiliate retailer, web, etc.).
- **b)** 2. Next, a port request is sent from the recipient operator to the donor operator via the inter-operator communications (IOC) process.
- **c)** 3. Upon acceptance and acknowledgement by the donor operator, a port request response is returned from the donor to the recipient via the IOC. Alternatively, the donor operator can ask for a delay or further information from the recipient operator instead of accepting the port request. Note that the recipient operator cannot port the number if it does not receive a mobile port response from the donor operator.
- **d)** 4. The recipient operator’s OSS provisioning system feeds the porting information to a SOA system. Ideally the IOC process and SOA process should be integrated with the POS system so data does not have to be re-keyed at various stages in the porting process. This will save money and increases accuracy.
- **e)** 5. The recipient operator sends a notification of the porting subscription request to the NPAC, specifying the date and time when porting should occur.
- **f)** 6. The NPAC sends a notification of the porting request to the donor operator’s SOA. This starts a two-hour timer at the NPAC. The donor operator has one hour to respond. Then the recipient operator has another hour to confirm the subscription request.
- **g)** 7. The donor operator’s SOA forwards a porting subscription request to the NPAC, specifying the date and time to stop billing for the number. Note that the donor operator may, at its own discretion, notify the customer that it has received a notice to discontinue service and will be porting the number to the recipient operator and that it will send a final bill and expects prompt payment. This action will increase the donor operator’s costs but may help it collect final payments and prevent some porting mistakes. For the donor operator, this should kick off the process of making final payment arrangements with the end user. For example, if the customer is breaking a contract to leave, the donor operator may want to make the subscriber aware that it will be billing him or her for this. This may also be a good time to determine why the customer is leaving. Did they leave over service quality, cost or another reason? Is there anything you can do to win back their business? These are questions an operator may want to ask in order to solve the underlying problems before losing additional customers.
- **h)** 8. The donor operator’s SOA notifies the NPAC that it has received the porting request and confirms the date and time of the change.
4. BENEFITS OF NUMBER POTABILITY

Regulatory agencies mandate NP because it is good for consumers. It eliminates a particular barrier unique to the telecommunication industry, that is, the ownership of the phone number. However, additional reasons to mandate and implement NP include market, regulatory and operator benefits.

4.1 Consumer Benefits

NP clearly benefits the consumer. At the individual subscriber level, the biggest impact to changing phone numbers is not to the subscriber, but to those individuals in the subscriber’s circle of friends, family and acquaintances. Updating written address books, changing programmed contacts lists, remembering the new number, are all unnecessary burdens. For a business the scope of changes forced by a change in phone number is even more considerable: business cards, stationary, print advertising, Web sites, signage, the sides of delivery vehicles, and invoices. All the changes that affect a business contribute to the reason why a business, in general, would not change service providers if it means also changing phone numbers.

4.2 Market Benefits

With the advent of NP comes a more competitive marketplace. Without a doubt, the mobile industry is already a highly competitive industry. However, by lifting of the last remaining barrier to what some would consider a completely free market, operators become even more focused on subscribers. Rather than continuing price wars, in countries where MNP has been implemented, operators tend to start consumer loyalty programs, improve customer service, reduce hold times, increase outbound calling programs, focus on renewal incentives, work to improve network coverage, roll-out additional differentiated services such as Wi-Fi agreements, push-to-talk service, 3G, and other customer-pleasing new functionality.

4.3 Regulatory Benefits

The infrastructure developed for NP has been used to solve other problems in some countries. Where directory number resources (i.e. number ranges) were being exhausted, the infrastructure to make NP possible was also used to allow numbering plan administrators to assign numbers in a more efficient manner (to assign a block of 1000 numbers to an operator rather than a block of 10,000 numbers). In another example, in countries where the mandate for NP also included fixed-to-mobile as well as mobile-to-fixed porting, the regulatory agency could encourage greater competition to incumbent fixed operators. With fixed-to-mobile portability mandated, mobile operators become a competitor to fixed service, since the subscriber can change from fixed to mobile easily, and of course, keep the same directory phone number.

4.4 Operator Benefits

On the surface, it would seem that NP is a financial and implementation burden to operators; and with the increased competition comes lower prices and hence lower margins. And certainly, some operators have argued that the implementation of number portability is cost prohibitive and would be bad for consumers since the cost of implementing NP would have to be paid for by subscribers, and could ultimately put the operator out of business. However, some operators have used the mandate for NP as an opportunity to gain market share and target high ARPU subscribers as well as multi-line business customers. As with any market where a barrier to competition is lifted, some of the free market agents will gain and some will lose. In the U.S., operators who took a proactive stance in preparing for NP were able to increase net additions in the face of increased competition. This was through a combination of customer service improvements, network improvements, targeted advertising, focus on fixed-to-mobile porting (also known as displacement), and to a lesser degree, more competitive rate plans. The graph shows that when comparing fourth quarter 2002 (prior to the implementation of MNP in the U.S.) with fourth quarter 2003 (MNP was implemented Nov 24, 2003) some operators managed to increase their subscriber base, some operators found themselves in negative net additions position, while some stayed relatively neutral. (Syniverse Tech. 2006).

5. CONCLUSION

One of the tenets that have been observed is that number portability is inevitable. As subscribers become aware of NP in other countries, they too begin to ask, “Why can’t I keep my number when I change service providers?” NP lifts a barrier to competition, which is unique to the telecommunications industry. And increasing competition is always in the best interest of consumers.

The principle of number portability is fully applicable to mobile telecommunications. Many operators have claimed that Mobile Number Portability (MNP) is unnecessary and is an unwarranted expense, using assertions that the sector is highly competitive. Some mobile operators have gone to considerable trouble to make MNP difficult and have discouraged customers from exercising this right. They have suggested alternatives such as personal numbering and Universal Personal Telephony (UPT). However, these are not substitutes for MNP, but are expensive, value-added services. MNP should therefore strongly be encouraged by governments and Regulatory Agencies to recognize that Mobile Number Portability (MNP) is an essential part of the competitive framework and should be made legally binding on all operators and service providers.
Mobile Number portability is a fundamental prerequisite for true competition in the telecommunications sector. Without this facility users are locked into their existing suppliers and can change operator with disruption and large expense. Businesses have to reprint letterheads and business cards. They may also have to repaint Lorries and vans. A change of number, whether in business or by an individual, requires others to change the number stored in their mobile phones, PDAs, software on personal computers, in fax machines and so on. Consequently, it is increasingly difficult because others must effect the change.
REFERENCES
7. Thisday Newspaper (11th Aug. 2006) Mandate for the implementation of Number Portability in Nigeria, Dailies, Thisday Publication, pg 7A

Author’s Brief

Onuoha Jacinta Chioma is on Faculty at the Department of Computer Science, Federal University of Technology, Owerri, Imo State, Nigeria. Her research interest is Modeling, Analysis and Rendering in heterogeneous Information and Social Networks Systems. She is a member of Nigeria Computer Society and also a member of Organisation for women in Science for Developing World (OWSDW). She can be contacted by phone on +2348037394691 and through E-mail: chiomajaco@yahoo.com.

Mrs Juliet N. Odii is on Faculty at the Department of Computer Science, Federal University of Technology, Owerri, Imo State, Nigeria. Her research interest is Computer Networks. She can be contacted by phone on +2348035373137 and through E-mail: jnodii@yahoo.com.
On the Role of Linguistics in the Detection and Prevention of Cybercrimes in Nigeria

Femi U. Balogun  
Department of Languages - School of General Studies  
Auchi Polytechnic, Auchi, Nigeria  
unufem@yahoo.com

O. Abu (Esq)  
Department of Humanities and Social Sciences  
Auchi Polytechnic, Auchi, Nigeria

Edmund I. G. Balogun  
School of Information Technology  
The American University of Nigeria,  
Yola, Adamawa State, Nigeria  
edmundbalogun@yahoo.co.uk

Olusegun O. Aramide  
National Teachers' Institute (NTI)  
Igarra, Edo State  
Applied Linguistics/Communication Arts  
e-mail: aramidedu@gmail.com

ABSTRACT
A linguist is not a policeman nor is linguistics a law enforcement agency. Linguistics is simply the scientific study of language while a linguist is someone concerned with such study. Since the commission of crime necessarily involves, among others, the use of language, this paper, theoretical in nature, argues that linguistics has a role to play in the detection and prevention of cyber crime in Nigeria. This it does by looking at: what is cybercrime? How is it committed and by whom? How can it be prevented with the aid of linguistics? The paper rounds off with some suggestions.

Key words: Cybercrime; Linguistics; Human Computer Interaction (HCI), Computer-Mediated Communication (CMC)

1. INTRODUCTION
Since the industrial revolution of the 18th century Europe, the world has not stopped witnessing one form of revolution or the other in different areas of human endeavour. One of such revolutions currently taking place in the world is the information technology revolution occasioned by the information explosion of the modern times. This revolution, like a coin, and every other one before it, has two sides to it – the good and the bad.

With the aid of different types of computers ranging from the old mainframes, desktops, laptops, PDAs to ipad, iphones, etc, and the inception of the internet, the world has been reduced to a global village. Thus, business has become simplified; distances between nations have been reduced or even closed and access to hitherto inaccessible information has been made possible. The advent of the internet, in particular, has revolutionized communication in many ways; it changed the way people communicate and created new platforms with far-reaching social impact.

Significant avenues include but are not limited to SMS Text Messaging, e-mails, chatgroups, virtual worlds and the web (Crystal, 2005). This is a good side to the coin of information technology revolution of the modern times; many more certainly exist. Cybercrime which manifests as spam, fraud, obscene or offensive content, etc, belongs to the bad side of the coin. It is a global phenomenon that is threatening the economy of nations.
For instance, most ironically, the internet online business services such as e-commerce, e-banking which ought to be a blessing to mankind as it exposes people to a lot of opportunities in various fields of human endeavour, is fast turning a source of discomfort and regret as a result of atrocities being perpetrated through it. In Nigeria, it is becoming pervasive. Its category, victims, and nature are endless just as its perpetrators are many and varied.

This has forced Ehimen and Bola (2010:95) to lament that “cybercrime in Nigeria is difficult to prove as it lacks the traditional paper audit trail, which requires the knowledge of specialists in computer technology and internet protocols.” Cybercrime has had some adverse social and economic consequences on the country just as it has projected a bad image of the country. Security especially of lives and properties and of the nation as a whole, is everybody’s business. It is not that of the law-enforcement agents alone, even though it is their primary responsibility.

But since the “prevention of cybercrime requires the cooperation of all the citizens and not necessarily the police alone who presently lack specialists in its investigating units to deal with cybercrime” Ehimen and Bola (2010:93), this paper argues that linguists, especially applied linguists, are some specialists who also have a role to play in the task of combating cybercrime. Consequently, the paper examines what cybercrime is, how it is committed and by whom, how it can be detected and prevented with the assistance of linguistics.

2. WHAT IS CYBERCRIME

Every generation, since the history of man, has always had its peculiar problems and challenges. During the voyages of exploration in the 14th century when sea transportation was in vogue, sea piracy was a common phenomenon. Today that computers are everywhere and with the inception of the internet, cybercrime, like sea piracy of old, is on the rampage posing a serious challenge to this generation. It is sparing no one, no matter the age, sex or nationality. If one is not perpetrating it, one is falling a victim; if one is not falling a victim, one is a relation or a friend of a victim. Many people and agencies, consequently, have attempted to define cybercrime in various ways.

Their definitions do not seem to differ much from each other, however. Chaubey (2009: 135) defines cybercrime “as the use of computer and the Internet by criminals to perpetrate fraud and other crimes against companies and consumers”. Chaubey (2009) quoting Grant Adamson (2003) states that cyber crime is a broadly used term to describe criminal activities committed on computers or the Internet. Some of it is punishable by the laws of various countries, whereas others have a debatable legal status.

According to Ehimen and Bola (2010:94) quoting Taylor (1999):

"Cybercrime or computer crime can broadly be defined as a criminal activity involving an information technology infrastructure: including illegal access or unauthorized access; illegal interception that involves technical means of non-public transmissions of computer data to, from or within a computer system; data interference that include unauthorized damaging, deletion, deterioration, alteration or suppression of computer data; systems interference that is interfering with the functioning of a computer system by imputing, transmitting, damaging, deleting, deteriorating, altering or suppressing data; misuse of devices, forgery (ID theft), and electronic fraud.

A generalized definition of cybercrime may be “unlawful acts wherein the computer is either a tool or target or both.” Chaubey (2009) quoting Nagpal (2002) explains that the computer may be used as a tool in the following kinds of activity – financial crime, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, cyber defamation, cyber stalking. The computer may however be target for unlawful acts in the following cases: unauthorized access to computer/computer, system/computer networks, theft of information contained in the electronic form, e-mail bombing, data diddling, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking, theft of computer system, physically damaging the computer system.

Chaubey (2009), again, quoting Townsend (2004) states that the concept of cybercrime is not radically deferent from the concept of conventional crime. They both include conduct whether act or omission which causes breach of rules of law and counterbalanced by the sanction of the state. Life is about a mix of good and evil so is the internet. For all the good it does us, cyber space has its dark sides too. Unlike conventional communities though, there are no policemen patrolling the information superhighway, leaving it open to everything from Trojan horses and viruses to hacking, cyber stalking, trademark counterfeiting and cyber terrorism. (Chaubey, 2009: 6) Cybercrimes may be financial or otherwise. Financial cybercrimes include: Online auction trade; Identity theft; Nigerian scam; Internet gambling and Digital forgery. Others are: Phishing; Software piracy; Sale of illegal articles; Hacking; Online business opportunity schemes; Virus dissemination; Credit card fraud; Spoofing; Online investment schemes; Cyber money laundering; Violation of copyrights and Pornography.

3. CYBER CRIME UNDER NIGERIAN LAW

There is no specific legislation on cybercrime in Nigeria. As a result, what therefore constitutes cybercrime is not defined in any written law in Nigeria. This has been a major impediment against the successful eradication and/or curtailment of the menace in Nigeria against the backdrop that section 36(8) of the
The 1999 Constitution of the Federal Republic of Nigeria expressly provides that:

No person shall be held to be guilty of a criminal offence on account of any act or omission that did not, at the time it took place, constitute such an offence.

It further provides that “no penalty shall be imposed for any criminal offence heavier than the penalty in force at the time the offence was committed.”

The above provisions are part of the Fundamental Rights guaranteed under Chapter IV of the Nigerian Constitution. What is currently used in Nigeria, to fight the menace of cybercrime are related provisions in other penal legislations in Nigeria like the Criminal Code Act, the Advanced Fee Fraud and Other Fraud Related Offences Act 2005, the Economic and Financial Crimes Commission (Establishment, etc) Act 2004 etc.

3.1 The Economic and Financial Crimes Commission (Establishment, Etc) Act 2004

The Act contains 47 sections. Section 6 (b) of the Act imposes on the commission the responsibility of investigating all financial crimes including advance fee fraud, money laundering, currency counterfeiting, illegal charge transfers, futures market fraud, fraudulent encashment of negotiable instruments, contract scan and most importantly computer credit card fraud, etc. Section 6 (c) of the Act also charges the commission with the responsibility of co-ordination and enforcement of all economic and financial crimes laws and enforcement functions conferred on any other person or authority. Furthermore, Section 6 (e) of the Act charges the commission with the responsibility of adopting all measures that would ensure the eradication of all forms of economic and financial crimes in Nigeria.

3.2 The Corrupt Practices and Other Related Offences Act 2005

The Act contains 56 sections. The relevant provisions are those contained in Section 16 and 17 of the Act. Section 16 deals with fraudulent receipt of property while section 17 prescribes penalties for offences committed through postal system. Section 16 provides as follows:

Any person who receives anything which has been obtained by means of any act constituting a felony or misdemeanor, or by means of any act done at a place outside Nigeria, which if it had been done in Nigeria would have constituted a felony or misdemeanor and which is an offence under the laws in force in the place where it was done, knowing the same to have been so obtained, is guilty of a felony.

Section 17 of the Act provides that if the offence by means of which the thing was obtained is a felony, the offender shall on conviction be liable to imprisonment for three (3) years, except the thing so obtained was postal matter, or any chattel, money or valuable security contained therein, in which case the offender on conviction be liable to imprisonment for seven (7) years.

3.3 The Advanced Fee Fraud and Other related Offences Act 2005

The Act contains 18 sections. Section 1 of the Act deals with obtaining property by false pretence. The section provides that:

1. Notwithstanding anything contained in any other enactment or laws, any person who by any false pretence, and with intent to defraud:
   (a) Obtains, from any other person, in Nigeria or in any other country, for himself or any other person;
   (b) Induces any other person, in Nigeria or in any other country, to deliver to any person;
   (c) Obtains any property, whether or not the property is obtained or its delivery is induced through the medium of a contract induced by the false pretence, is guilty of an offence under this Act.

2. A person who by false pretence, and with the intent to defraud, induces any other person, in Nigeria or in any other country, to confer a benefit on him or on any other person by doing or permitting a thing to be done on the understanding that the benefit has been or will be paid for is guilty of an offence under this act.

3. A person who is guilty of an offence under subsection (1) or (2) of this section is liable on conviction to imprisonment for a term of not less than ten years without the option of a fine.

Section 4 which deals with fraudulent invitation provide that a person who by false pretence, and with the intent to defraud any other person invites or otherwise induces that person or any other person to visit Nigeria for any purpose connected with the commission of an offence under this act is guilty of an offence and liable on conviction to imprisonment for a term of not less than seven years without the option of a fine.

Section 5 of the Act states that:

1. Where a false pretence which constitutes an offence under this act is contained in a letter or other document, it shall be sufficient in a charge of an attempt to commit an offence under this act to prove that the letter or other documents was received by the person to whom the false pretence was directed.

2. Notwithstanding anything to the contrary in any other law, every act, or thing done or omitted to be done by a person to facilitate the commission by him of an offence under this act shall constitute an attempt to commit the offence.

It is noteworthy that “other document” as used in section 5 (2) is interpreted in section 5 (3) to include a document transmitted through a fax or telex machine or any other electronic or electrical device, a telegram and a computer printout (emphasis ours).
Section 11A of the Act places a duty on any person or entity providing an electronic communication service or remote computing service either by e-mail or any other form to obtain from the customer or subscriber:

(a) Full names;
(b) Residential address, in the case of an individual; and
(c) Corporate address, in the case of corporate bodies.

The failure by any customer or subscriber to furnish the information specified above or with the intent to deceive, supplies false information or conceals or disguises the information required above commits an offence and is liable on conviction to imprisonment for a term of not less than three years or a fine of ₦100,000 and forfeiture of the equipment or facility used in providing the service.

Section 11B of the Act provides that any person or entity who in the normal course of business provides telecommunications or internet services or is the owner or person in the management of any premises being used as a telephone or internet café or by whatever name called shall:

(a) Be registered with the Economic and Financial Crime Commission;
(b) Maintain a register of all fixed line customers which shall be liable to inspection by any authorized officer of the commission; and
(c) Submit returns to the commission on demand on the use of its facilities.

Under section 11B (2) any person whose normal course of business involves the provision of non-fixed line or global system of mobile communications (GSM) or is in the management of any such service, is required to submit on demand to the commission such data and information as are necessary or expedient for giving full effect to the performance of the functions of the commission under the Act. Persons specified under subsection (1) and (2) of section IIB are required to exercise utmost duty of care to ensure that his services and facilities are not utilized for unlawful activities. Finally, where a person or entity has been convicted for more than once under the Act he shall have his operational license revoked or cancelled.

Thus, from the foregoing, nowhere is specific mention made of cybercrime. This led Ehimen and Bola (2010: 97) to conclude that:

Nigeria is a place where computers can be used to commit all sorts of crimes without prosecution, as there is no law on cybercrime. The Nigerian police simply lack internet policing capability. Nigerian law enforcement agencies are basically technology-illiterate; they lack computer forensics training and often resort to conducting police raids on Internet service sites mainly for the purpose of extortion.

4. WHO COMMITS CYBERCRIMES IN NIGERIA AND HOW

Perpetrators of cybercrimes in Nigeria are many and various. They include the following category of persons: disgruntled employees; teenagers; political hacktwists; professional hackers; business rival; ex-boy/girl friend; divorced husband/wife, etc (www.cybercellmumbai.com). These cybercriminals are commonly referred to, in Nigeria, as “yahoo boys”. Yahoo boys ply their trade in cybercafés, private offices/homes and in recent times, with the availability of various modems and blackberry, iphone, ipad, they can carry on their criminal activities from anywhere and at any time.

In 2009, for instance, one of the writers of this paper, a student at American University of Nigeria, (AUN), while working online with his laptop suddenly received a mail purportedly sent by Interswitch, the company handling ATM business in Nigeria. He was requested to supply his PIN number and other vital information for the purpose of upgrading his ATM card. He complied innocently, ignorant that it was a fraud. A while later, he received an alert on his mobile phone that One hundred thousand Naira (₦100,000.00), was withdrawn in quick succession from his account. This is one way in which the “yahoo boys” or cybercriminals ply their trade. This particular type of cyber crime – phishing was becoming too prevalent in Nigeria that the EFCC had to rise up to the challenge. Some of the criminals were arrested and the crime has reduced. This is how it was reported:

A Youth Corps member, who is serving in the Finance and Supply section of Ibadan South East Local Government has been arraigned by the Economic and Financial Crimes Commission (EFCC) for allegedly defrauding some new generation banks to the tune of ₦4 million. The 28 year old corps member (name withheld), who graduated from the Federal University of Agriculture, Abeokuta, Ogun State has since been dragged before an Ibadan High Court to answer a 50-count charge (Nigerian Tribune 2009, May 14).

Cybercriminals in Nigeria, otherwise known as “yahoo boys” could be university graduates or secondary school leavers who are computer-literate and can browse the net. They use a combination of methods to trick their victims, who are unlucky, greedy, gullibly unskilled and inexperienced, into releasing vital information about themselves and businesses before proceeding to strike. It is either they are hacking, spoofing, phishing, spamming or defaming, threatening. Recently, it was reported in a national daily (Nigerian Tribune) that the mobile telephone line of Justice Ayo Salami, the president of the Court of Appeal was hacked into. According to Adewole (2011), “Justice Ayo Salami reportedly opened his defence by claiming that his mobile telephone line was ‘spoofed’ to speak with chieftains of the Action Congress of Nigeria (ACN) before, during and after the governorship appeal judgements in Ekiti and Osun States”
Although this claim was refuted by the mobile telecommunication company (MTN) allegedly used in the crime, it shows how ‘hacking’ and ‘spoofing’ have become common in Nigeria. Copyright/software piracy is no less common. Ewelukwa-Ofodile (2010) had lamented that the Nigerian entertainment industry is presently threatened by high rate of copyright piracy. Mumbai Police reveals that retail revenue loses worldwide are ever-increasing due to this crime, which is done in various ways as end-user copying, hard disk loading, counterfeiting, illegal downloads from the internet, etc.

(www.cybercellmumbai.com)

4.1 The Nigerian Scam
The Nigerian Scam also known as 419 scam is named after its Nigerian Criminal Code, section 419 revised and expanded with the issuance in April 1995, of the Presidential Decree No. 13 titled Advanced Fee Fraud and other Fraud Related Offences Decree 1995 in which recipients of an unsolicited e-mail are asked to provide a safe bank account for the transfer of frozen or illegal funds.

Quite often, the scammers will ask for a financial contribution in order to bribe official or to cover a processing fee. Once this initial money is collected, the scammers either disappear or clean out the victim’s bank account. A similar example of internet fraud involves the victim’s supposed winning of a previously unknown foreign lottery. The scammers promise to forward the winnings in exchange for a substantial processing fee.

The “419” scam has circulated for years through snail mail, fax and e-mail. It has become so prevalent that even the US secret service, which refers to it as the Nigerian Advance Fee Fraud, has dedicated an entire section to it on its financial crimes division page. It also calls it the fastest growing epidemic division page. It also calls it the fastest growing epidemic

4.1 The Nigerian Scam
The Nigerian Scam also known as 419 scam is named after its Nigerian Criminal Code, section 419 revised and expanded with the issuance in April 1995, of the Presidential Decree No. 13 titled Advanced Fee Fraud and other Fraud Related Offences Decree 1995 in which recipients of an unsolicited e-mail are asked to provide a safe bank account for the transfer of frozen or illegal funds.

Quite often, the scammers will ask for a financial contribution in order to bribe official or to cover a processing fee. Once this initial money is collected, the scammers either disappear or clean out the victim’s bank account. A similar example of internet fraud involves the victim’s supposed winning of a previously unknown foreign lottery. The scammers promise to forward the winnings in exchange for a substantial processing fee.

The “419” scam has circulated for years through snail mail, fax and e-mail. It has become so prevalent that even the US secret service, which refers to it as the Nigerian Advance Fee Fraud, has dedicated an entire section to it on its financial crimes division page. It also calls it the fastest growing epidemic


The hoax e-mail, which has many variants, appears to be sent out by a deposed African official or a relative or one. Messages ask its recipients for assistance in transferring or handling a sizeable sum of money, offering a corresponding share for such service. This scam e-mail has victimized many individuals, some of whom have given up millions of dollars and their personal safety for lure of promised lure. But it’s not just 419 but a host of other such tempting offers that often leave a hole in your pocket – if, i.e., you are naïve enough to fall into this well-oiled trap, (Ashish, 2006, quoted in Chaubey, 2009).

As for the infamous 419 scam, it is advance fee fraud scheme that has been in existence through regular mail for more than 20 years and has multiplied after the advent of internet. Thousands of people receive 419 e-mails every month. Although the Nigerian government claims to be cracking down on them, it is commonly believed that they are actually protecting the culprits. Well, to start with it is alleged that it is the Nigerian government officials themselves who are the kingpins. Secondly, the 419 scam is estimated to be the third largest source of revenue for the Nigerian economy.

This is just too large a business for it to crack down on. (Nigerian Advance Fee Fraud, Department of State Publication 10465, Bureau of International Narcotics and Law Enforcement Affairs, April 1997). Not only are there many cases of people who have had their bank accounts drained by 419. There are also cases where they have been lured into actually travelling. Enforcement agencies report that some of the people have not left that country alive. If in response to one of these letters, you wire-transfer or mail money to the Nigerians, then you’re probably just lucky to have been this stupid but will be worse off if you try to investigate so as to protect your investment. Persons who have travelled overseas to investigate or consummate this scam have made a tragic mistake. Violence and threats of physical harm have been employed to pressure victims.

Once you are overseas, there are a variety of ways the Nigerians will get you. Typically, the Nigerians will bribe the Customs officials when you arrive so that you do not have to pass through them. This is the first huge mistake the victims commit. You are now a foreigner in Nigeria without a passport – a very serious offence. The scammers then threaten to turn you in to authorities or you are told to cough up money. Even after you have paid them the money, the local police are about as likely to extend this extortion racket themselves with the result that you will not get out of the country until they have gotten every last dime out of you, and maybe not even then. The key to the continuing Nigerian model success is the ingenuity and adaptability of the scammers. When victims realized that wiring money overseas was not a good idea, the scammers started recruiting US residents as go-betweens. They asked the victims to send the money to US addresses thereby circumventing suspicion. In the wake of all the above, the law and the law-enforcement agents (police) seem incapable of stamping out completely the menace of cybercrime.

5. DETECTION AND PREVENTION OF CYBERCRIMES: LINGUISTICS TO THE RESCUE

Quite expectedly, any discussion of cybercrime would be thought to involve law, legislations and computers only. Linguistics as a field of study would hardly be thought to have any role to play whatsoever. Balogun (1998:75) reports that Banjo (1983) was well aware of this low esteem in which the subject was held when he lamented that “even from the point of view of relevance, the discipline of linguistics remains even to the highly educated individual throughout the world, as an esoteric subject.”

Today, however, notes Balogun (1998), it would be wrong to hold such a simplistic notion. This is because “linguistics now shares with other sciences a concern to be objective, systematic, concise and explicit in its account of language” (Crystal, 1987). This being the case, it can be argued that linguistics – the scientific study of language – must have a role to play in the detection and prevention of cybercrimes.
This argument is further strengthened when it is recalled that cybercrimes are committed by human beings against human beings by means of language, among others. Besides, since the beginning of Human Computer Interaction (HCI) leading to Computer-Mediated Communication (CMC) and Internet-Mediated Communication (IMC), experts have acknowledged that linguistics has a contributing role in it, in terms of web interface and usability (http://en.wikipedia.org).

In every field of human activity that involves the use of language, linguistics is thus, necessarily relevant. This relevance and pervasive nature of linguistics in all fields of human endeavours, according to Balogun (1998) can be compared only to the relevance of electricity to the life of man. Crystal (1987:412) had pointed out that since university teaching of linguistics emerged during the 1960s, the following branches of linguistics enquiry have been established:

- Anthropological linguistics; Applied linguistics; Biological linguistics; Clinical linguistics; Computational linguistics; Educational linguistics; Ethno linguistics; Geographical linguistics; Mathematical linguistics; Neurolinguistics; Psycholinguistics; Sociolinguistics; Statistical linguistics; and Theo linguistics.

Needless to say that many more branches such as Forensic Linguistics and Internet Linguistics keep evolving. With a field as relevant and pervasive in human endeavours as linguistics, it only remains to highlight how it can assist in the detection and prevention of cybercrime in Nigeria. Language, the main raw material of the linguist, happens to be what cybercriminals deploy to commit their crimes using mechanical devices of computers. This has led to the evolution of Internet linguistics which is concerned with new language styles and forms that have arisen under the influence of the internet and other new media, such as short message service (SMS) and text messaging (Crystal, 2005).

Insights gained from studying the emerging language on the internet can help in improving the conceptual organization, transmission, translation and usability of messages. This will help in detecting the genuineness or otherwise of transmitted messages. For example, trained Internet linguists are able, using available software, to determine whether a received e-mail is worthy of receiving attention or not. With accepted professional advice from them, crimes can be detected and prevented.

Richards and Schmidt (2002:102) report that “computer languages have many interesting formal properties, but do not have the functional properties associated with natural languages.” This might lead to the erroneous conclusion that computer languages are not amenable to a linguistic study. Indeed, they are. Areas and topics in internet linguistics such as stylistic diffusion, which involves the study of the spread of internet jargon and related linguistic forms into usage, language change, conversation discourse, which explores the changes in patterns of social interaction and communicative practice in the net prove that computer languages whether BASIC, FORTRAN, COBOL ALGORITHM are amenable to a linguistic study. This study, in turn, equips one to be able to detect cybercrimes like spam, scam, etc.

As new software and packages are daily being produced to checkmate the activities of cybercriminals, internet linguists can be relied upon for expert advice and guidance. One such product recently launched in Nigeria is the Symantec Endpoint Protection 12 (SEP12). “This product is designed to detect and block sophisticated new threats earlier and more accurately than any other security product in the IT market” (Nigerian Tribune, 2011, July 28 pg. 20).

Apart from Internet linguists, there are the Forensic linguists who also play very invaluable roles in the detection and prevention of cybercrimes. Richards and Schmidt (2002:207) explain that Forensic linguistics “is a branch of applied linguistics that investigates issues of language in relation to the law”. While it is important that countries harmonize their legal frameworks to combat cybercrime and facilitate international cooperation, it is doubtful if this can succeed without the involvement of forensic linguists. This is why it is suspected that the ITU Toolkit for cybercrime legislation which aims to provide countries and reference material that can assist in the establishment of harmonized cybercrime laws and procedural rules could have involved them. It was reported that “the sample language provided in the toolkit was developed after a comprehensive analysis of the most relevant regional and international legal frameworks currently present. The toolkit language is consistent with these laws and is intended to serve as a guide for countries desiring to develop, draft or modify their own laws” (http://www.itu/ITU-D/cyb/cybersecurity).

6. CONCLUSION

It is a fact that as society grows and becomes more complex, human activities, whether social, political, economic or technological are bound to become more sophisticated. This is why sophisticated technology has today brought with it increasing sophisticated criminals who are using computer systems, networks and computers for illegitimate ends, chief among which is cyber crime, which, today, poses the biggest challenge for police, prosecutors and legislators.

This theoretical paper, examining what cyber crime is, how it is committed and by whom in Nigeria, posits that linguistics – the scientific study of language – can play a vital role in the detection and prevention of cyber crimes. Experts in the branches of linguistics called internet linguistics and forensic linguistics (both branches of applied linguistics) with their knowledge of internet protocols, cryptography can assist in the development of software that can detect logic bombs, Trojan horses and known viruses and consequently, help to prevent cyber crimes, especially hacking. The paper does not lay any claim to exhaustiveness.
7. RECOMMENDATIONS

1. It is very interesting to note that Nigeria has recently created a ministry of Information and Communications Technology (ICT). The ministry should set up a department for training people, especially the police in cyber forensics.

2. Like India, where the police are trying to be cyber crime savvy and hire people who are trained in the area, (Chaubey, 2009), Nigeria should sponsor people to specialize in Internet linguistics and Forensic linguistics as experts in these fields are currently almost non-existent.

3. Some Nigerian Universities and polytechnics should be designated centres of Applied Linguistic Research where emphasis should be on training Internet linguists, Forensic linguists and law with a view to catching up with the increasing sophistication of cyber criminals.

4. Nigeria should take steps to harmonize her legal framework with other countries to facilitate international cooperation to effectively combat cyber crimes.

5. It is recommended that the following famous ten commandments of Computer Ethics (Chaubey, 2009: 32) be taught and learnt before being allowed to own and operate a computer or even a cyber café in Nigeria. They are:
   
   a. We shall not interfere with other people’s computer work and respect the right of privacy of information of other people.
   b. We shall not snoop around in other people’s computer files.
   c. We shall not use a computer to steal something, means the computer cannot be used to perform theft.
   d. We shall not use a computer to bear false witness.
   e. We shall not copy or use proprietary software for which you have not paid.
   f. We shall not use other people’s computer resources without authorization or proper compensation.
   g. We shall not appropriate other people’s intellectual output.
   h. We shall think about the social consequences of the program you are writing or the system you are designing.
   i. We shall always use a computer in ways that ensure consideration and respect for your fellow humans.
   j. We shall not use a computer to harm other people i.e. we shall not use the computer in the way that it will cause harm to other peoples.

The above commandments which are mere admonitions and not laws have no force. Nigerian National Assembly should legislate on them and possibly convert them to laws with appropriate and commensurate sanctions. This will go a long way in preventing cyber crimes in Nigeria.

6. Finally, Chaubey (2009: 179) in his recommendation on prevention of cyber crime states: “last but not the least, suggestion is that of identification of citizens … it has to be realized that identification of citizens in certain areas such as cyber crime is equally necessary.” This is where the internet and forensic linguists who are experts in Voice – identification and handwriting – verification come in. If the IT industry enlists the expertise of these professionals, detection and prevention of cyber crimes will be greatly enhanced.

REFERENCES

1. Adewole, L. (2011, June 2). NJC Probe: My line was hacked to call ACN Chieftains. Nigerian Tribune.


Author’s Brief

Femi U. Balogun is a Chief Lecturer in the Department of Languages, School of General Studies, Auchi Polytechnic, Auchi, Edo State, Nigeria. He is currently Director, Polyconsult, Auchi Polytechnic and a doctoral degree student of Applied Linguistics/Communication. He can be reached thru e-mail at unufem@yahoo.com

Olusegun O. Aramide is a Senior Tutor and Co-ordinator at the National Teachers’ Institute (NTI) Igarra, Edo State, Nigeria. He was a part-time lecturer at Auchi Polytechnic. He is a doctoral degree student of Applied Linguistics/Communication. His e-mail: aramidedu@gmail.com

Ahmed O. Abu, Esq is a Senior Lecturer in the Department of Humanities and Social Sciences, Auchi Polytechnic, Auchi, Edo State, Nigeria. He is currently the Head, Legal Unit of the Polytechnic.

Edmund I. Balogun is a Senior in the School of Information Technology at the American University of Nigeria, Yola, Adamawa State, Nigeria. He is majoring in Information Systems with concentration in Database and Web Integration. With a vast knowledge in internet policies, system analysis, and enterprise resource planning, he is currently carrying out a research on "Human Computer Interaction: Eradicating Complexities in Interface Designs." His e-mail: edmundbalogun@yahoo.co.uk
A Model for Intelligent Motion Detection in Live Video Streaming Systems

Olufade, F.W. Onifade., Oladeji, P. Akomolafe & Ademola, S. Olaniyi
Department of Computer Science,
University of Ibadan, Ibadan
fadowilly@yahoo.com; akomspatrick@yahoo.com; oademola2000@yahoo.com

ABSTRACT
Latest technologies aimed at combating burglary, thefts and wanton destruction are the video surveillance and monitoring systems. With these technologies, it is possible to monitor and capture every inch of the target area. The ability to recognize objects and humans, to describe their actions and interactions from information acquired by sensors is essential for a visual surveillance system. This paper focuses on an object-location-based (OLB) approach to crime and public safety that seek to simultaneously address the interconnected relationships between people and their environments. This work establishes a framework for detecting the motion in a live streaming video and once motion has been detected in the live stream, the system will alert the user of suspicious activity and capture the live streaming video thereby providing a near-real time monitoring of lives and properties on the move a possibility. It is aimed at increasing the efficiency of security guards performing surveillance operation on lives and properties.

Keywords: Motion, Detection, System, Monitoring, object-location-based, Video, Crime, Surveillance.

1. INTRODUCTION

Intelligent visual surveillance systems deal with the real-time monitoring of transient objects within a specific environment. The primary aims of these systems are to provide automatic interpretation of scenes and to understand and predict the actions and interactions of the observed objects based on the information acquired by sensors. The main components of processing in an intelligent visual surveillance system are: moving object detection and recognition, feature extraction, tracking and system indication.

Recent interest in surveillance in public, military and commercial scenarios is increasing the need to create and deploy intelligent or automated visual surveillance systems. In scenarios such as public transport, these systems can help monitor and store situations of interest involving the public, viewed both as individuals and as crowds. Current research in these automated visual surveillance systems tend to combine multiple disciplines such as signal processing, telecommunications, management and socio-ethical studies. Nevertheless there tends to be a lack of contribution from the field of system engineering to the research [5].

The increasing demand for security by society leads to a growing need for surveillance activities in many environments. The demand for remote monitoring for safety and security purposes has received particular attention, especially in the following areas:

- Transport applications such as airports [9] and maritime environments [11].
- Remote surveillance of human activities such as attendance at football matches [14].
- Public places such as banks, supermarkets, homes, department stores and parking lots [15–16].

As people become more and more security savvy, they will demand real protection for their property. The new digital video systems will have to raise the required security to a new level. They should make the customers feel good. Scare off a few troublemakers, and those who do try to beat the system should face a far greater risk of getting caught. Hence, the new digital video surveillance systems should be able to provide a high sense of security. The peace of mind can only be achieved when the person is assured that he will be informed of any thefts of his property while they are in progress. He would also feel more secure if he can be guaranteed that the surveillance system that he uses will not only give him evidence against the perpetrators but also try to stop the thefts from taking place in the first place. Therefore, to achieve such kind of security Motion Detection in the live video stream is implemented. The motion detection systems will not only be monitoring the areas of interest but will also keep an active lookout for any motion being produced [1].

African Journal of Computing & ICT Reference Format:

ISSN 2006-1781
The rest of this work is as follows: in section II, we give related works, while section III has the model development and methodology. Section IV presents the result discussion and the work is concluded in section V.

2. RELATED WORKS

The technological evolution of video-based surveillance systems started with analogue CCTV systems. These systems consist of a number of cameras located in a multiple remote location and connected to a set of monitors, usually placed in a single control room, via switches (a video matrix). Video surveillance began with simple closed circuit television monitoring (CCTV). As early as 1965, there were press reports in various countries across the world suggesting police use of surveillance cameras in public places. When video cassette recorders hit the market, video surveillance became really popular.

Analog technology using taped video-cassette recordings meant surveillance could be preserved on tape as evidence. A complete analog video-surveillance system consisted of a camera, monitor, and VCR. The old tube camera was only useful in daylight, and the VCR could only store eight hours of footage at best. The drawback was that after a while, owners and employees of such a system would become complacent and not change the tapes daily or the tapes would wear out after months of being re-used. There was also the problem of recording at night or in low light.

While the concept was good, the technology hadn’t yet peaked. The next step was the Charged Coupled Device camera (CCD), which used microchip computer technology. In the 1990’s video surveillance made great strides in practicality by the introduction of digital multiplexing. When digital multiplexer units became affordable, it revolutionized the surveillance industry by enabling recording on several cameras at once (more than a dozen at time in most cases) [1].

Three key factors brought on the popular use of the digital video recorder. They are:

- The advancement in compression capability, allowing more information to be stored on a hard drive. (Round-the-clock surveillance produces a lot of information.)
- The cost of a hard drive, which has dropped dramatically in recent years.
- The storage capacity of a hard drive, which has increased dramatically in recent years.

Digital video surveillance made complete sense as the price of digital recording dropped with the computer revolution. Rather than changing tapes daily, the user could reliably record a month's worth of surveillance on hard drive. The images recorded digitally were much clearer than the often grainy images recorded with analog that recognition was immediately improved for identification purposes.

Digitally stored images can also be enhanced in various ways (add light, change colors, reverse black and white) to make crucial determinations. With videotape, what you see is what you get. It’s against this backdrop that this research is carried out to bring into play a mobile monitoring of lives and properties of subscribers of the proposed system.

Some of the approaches for moving objects detection use simple intensity comparison to reference images so that the values above a given threshold identify the pixels of moving objects [8]. A large class of approaches is based on appropriate statistics of colour or gray level values over time at each pixel location. (e.g. the segmentation by background subtraction [10], eigenbackground subtraction [12], etc). Other models used a statistical model of the background instead of a reference image [13].

3. MODEL DESCRIPTION

A model description of our system is shown below. The webcam captures the live video feed in real time. This live feed is plugged into the server which redisplays the original live feed in real-time, whilst doing image processing in the backend.

Hierarchically, the operational system model can be described in the following ways:

**Capturing the live video feed through a webcam (motion sensor equipment):** To detect motion we first have to capture live video frames of the area to be monitored and kept under surveillance. This is done by using a web cam which continuously provides a sequence of video frames in a specified speed of FPS (frames per second).

**Comparing the current frames captured with previous frames to detect motion:** For checking whether any motion is present in the live video feed, we compare the live video frames being provided by the web cam with each other so that we can detect changes in these frames and hence predict the occurrence of some motion.
Storing the frames on the memory if motion is detected: If motion is detected, the video recorder in commence recording such motion so that the user can view it in the near future. This also helps the user in providing a legal proof of some inappropriate activity since a video coverage can be used as a proof in the court of law.

Indicating through an alarm when the motion is detected: This is the novel part of the development. We believed there should be provision for real-time monitoring of such live feed in other to intimate the user of any impending danger. To this end, once an intrusion is detected by the system, the indication system which is included in the software will trigger an alert which could be in form of an SMS or MMS sent to the user with pictures of sample threat. This helps in preventing any kind of breach of security at that moment of time.

3.1 System Architecture
The detection of motion essentially requires the user to perform two major steps. They are: acquisition of the video data in which the motion is to be detected and the later step is to actually device an algorithm by which the motion will be detected. The video stream is stored or acquired as a series of frames occurring in an ordered sequence one after the other. Algorithm for detection becomes imperative because other factors/moving objects like dogs and other domestic animals/pets might trigger unnecessary movement with the set space. The system is developed in such a way that once a snap-shot is taken, it is compared to existing, predefined images in the database for validation before further actions. This eliminate the false-positive response that could result from pets but take into cognizance the issue of “creeping-human” with a bid to disguise or fool the system. Keeping the work objective in mind, we present the basic system architecture as shown below.
4. DISCUSSION

The system architecture which we developed was adapted from [6], describes how the system component interacts and work together to achieve the overall system goals. It describes the system operation, what each component of the system does and what information is exchanged. The system is initialized to take a snapshot of an image which is referred to as Old. With the system’s inbuilt timer, the next image taken will be referred to as Current. If there exists a difference in the Old and Current images’ RGB values, the motion is said to occur which is detected by the sensors.

Here motion detection algorithm is based on frame difference calculation in terms of RGB values and brightness threshold values stored in byte arrays. The algorithm compares two consecutive frames Old and Current, pixel by pixel to generate a difference value. If the difference value is greater than a fixed value (randomly taken), then motion is detected. Else if, there is no difference between previous and current frame’s byte arrays then Old is set to Current. The process repeats according to the program’s set timer.
Table 1: System Architecture Description

<table>
<thead>
<tr>
<th>S/N</th>
<th>FEATURE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Object Detection/capture</td>
<td>A digital image is produced by a security camera</td>
</tr>
<tr>
<td>2</td>
<td>Image processing and analysis</td>
<td>Re-sampling in order to assure that the image coordinate system is correct. Noise reduction in order to assure that sensor noise does not introduce false information.</td>
</tr>
<tr>
<td>3</td>
<td>Feature extraction</td>
<td>Frame Differencing with binary thresholding to remove stationary objects. Regions of interest (ROI) such as blobs.</td>
</tr>
<tr>
<td>4</td>
<td>Object Recognition</td>
<td>Motion History Image (MHI) to store blobs movement pattern. MHI is stored in a cyclic buffer - a single, fixed-sized array as if it were connected end-to-end</td>
</tr>
<tr>
<td>5</td>
<td>Object tracking</td>
<td>Using the MHI extracted from the image to determine the movement between images.</td>
</tr>
</tbody>
</table>

Below, we discuss the methodology by elaborating on the following key techniques used in developing the system:

On capturing a frame, gray scaling is used to convert colour images to its grayscale equivalent. The grayscale image shows the effective brightness or luminance of the colour image. The conversion, to a shade of grey from a colour image, is established by calculating the effective brightness or luminance of the colour. This value is then used to create the shade of grey that corresponds to the desired brightness. Frame difference is used when the still part of an image needs to be separated from the moving part of the image. During the frame differencing process a binary threshold value needs to be used to get rid of unwanted noise whilst preserving the foreground. Setting the threshold to the correct value is important so that we get acceptable results in blob tracking.

The motion history image is the final component for blob tracking. This method focuses on accumulating and recognizing entire object patterns rather than focusing on detailed features. The advantages of this approach are the low use of memory and blazingly fast yet descriptive representation of capturing motion on a per blob basis. It has coordinates that can be used to measure the width and the height of the blob component. The relative angle at which the blob is traversing is also measured. The MHI is created by layering images over successive image regions. This system can be embedded in home monitoring systems which are gaining interest in recent years. This system can be used to detect motion in target areas. It prevents users from making blunders which can arise as a result of missing footage when monitoring several screens. It can also be used to prevent car hijacking in various parking stations. Once unusual movement is detected by the system, the system indicator triggers an alarm. Such monitoring keeps the heart of users at rest knowing full well that their properties are secured. The video recorder commences recording once motion has been detected. This recorded video can be used as an evidence in the court of law.

5. CONCLUSION

This paper presents the framework for the design of a video monitoring and detection system. This system mainly provides an efficient method for surveillance purposes and is aimed to be highly beneficial to an individual or organization. As a future work, extended efforts are being made to enhance the security provisions. Works can also be done to ensure that the video coverage is saved on multiple storage devices in real time, in case of damage. This will serve as a backup.
REFERENCES


[4] Dane Brown, Mr James Connan, Mr Mehrdad Ghaziasgar (2010): Suspicious Activity Detection; mini-thesis Department of Computer Science; University of the Western Cape


A Model Checking Framework For Developing Scalable Antivirus Systems

E. Osaghae
Department of Computer Science
University of Port Harcourt
Port Harcourt, Nigeria.
edgarbros@yahoo.com

S.C. Chiemeke PhD
Department of Computer Science
University of Benin
Benin City, Nigeria
schieemeke@uniben.edu.ng

ABSTRACT
Conventional antivirus products rely on signature matching technique to detect malicious programs. Signature matching technique needs constant connection to the internet so that the antivirus companies can send new updates to their clients’ computers antivirus database, and the database may be very large to the extent that it slows down the computer performance. This method therefore fails to detect new and unknown viruses. We propose and implemented a model checking framework as a novel technique to improve static malware detection. Model checking technique is employed to determine behavioural patterns of an executable program on assembly programming level. Deterministic finite automata technique is used to extract the set of Application Programming Interface (API) functions used for malicious activities, which has been identified by the model checking technique. Naïve Bayes technique is used to identify only API functions used by a virus program based on self-modification, self-referential and self-replication. Chi square techniques is used to identify Trojan, worm and unknown malicious attributes from the codes already examined by the Naïve Bayes technique. We implemented the proposed framework by developing a scalable antivirus system called “Intellect” using c++ 2008 programming language and the results of detection is sent to a file. We tested one hundred benign files, one hundred viruses, one hundred Trojan horses and one hundred worms. Preliminary results from our test runs shows that the antivirus is efficient at detecting viruses, Trojans, worms and unknown malicious programs.

Keywords: Virus detection, Model checking, Naïve Bayes, Deterministic Finite Automata, and Chi Square.

1. INTRODUCTION

The internet is proliferated with more computers being connected to it on daily basis although, this is an improvement to the world of information technology and there is also a dark side: malware. Malware is becoming increasingly common and poses a major threat to individuals and businesses, as it is employed by both criminals and vandals to steal valuable information, commit fraud, send junk mail or attack computer systems (Bohne, 2008). A study between 2004 and 2007 showed that antivirus companies required an average of six (6) hours to analyze and extract a signature from a newly discovered virus and add it to their signature database. In 2006, a Federal Bureau of Investigation (FBI) survey reported computer viruses as the number one cause of financial loss for American companies.

Kaspersky labs reported a strong rise in the number of new viruses and momentum in the second half of the year with email worms topping the list. Despite this growing problem, antivirus companies continue to use signature databases as their primary tool for virus detection. In 2006, Kespersky labs averaged 10,000 new record updates to its signature database per month and 200 new malware samples per day. Even after solutions have been released it is unknown how much time passes until all end user signature databases are updated. It is clear that antivirus companies will continue to improperly and slowly handle the ever growing virus problem using signature databases as the centerpiece for detection (Morales, 2008).

Microsoft operating system applications are the targets of many viruses because the operating system is widely used compared to other operating systems. There are about 60,000 viruses known for Windows, 40 or so for the Macintosh, about 5 for commercial Unix versions, and perhaps 40 for Linux. Most of the Windows viruses have caused widespread monetary damages. Two or three of the Macintosh viruses were widespread enough to be of importance, none of the Unix or Linux viruses became widespread because most were confined to the laboratory (Granneman, 2003).
An antivirus system is a software product that essentially safeguards computer data and instructions against destruction or modification by viruses and other malicious programs (Alessandro, 2009). Malicious program contains malicious code which is any code added, changed, or removed from a software system to intentionally cause harm or subvert the computer system’s function. A computer virus is a malicious program that reproduces itself by injecting its codes into existing programs thereby infecting it, and propagate to other programs when executed (Gaddam, 2008; Kolter and Maloof, 2006). A Trojan horse is also a malicious program that is non-replicated program which enters a computer system by disguising or embedding itself inside another legitimate program however, each Trojan has its own characteristics that make it different from other Trojans.

A worm is another type of malicious program that reproduces itself just like a computer virus however, the only difference is that it does not attach itself to other existing program. A worm uses network resources to infect other computer systems in a network (Raghunathan, 2007). A program that does not contain any malicious code is called a benign and it would not corrupt or damage the computer system in any way (Sathyanarayanan et al, 2008). Currently, most widely used antivirus software uses signature-based and heuristic-based algorithms to recognize a virus file. Signatures are short strings of bytes which are unique to the programs and can be used to identify particular viruses in executable files however, signature-based method is expensive, slow and they are not effective against modified or unknown virus (Alessandro, 2009).

Heuristic-based recognition tends to provide protection against new and unknown viruses, this kind of virus detection is usually inefficient and inaccurate. Heuristic-based virus detection is better than signature-based detection because, it is preventive in nature and it also has the ability to detect viruses before they infect any file (Varun et al, 2009). Although, virus prevention is better than virus cure (detection before infection), but virus prevention still has a lot of challenges. For a prevention system to be effective, it must address both challenges comprehensively: accuracy and performance. Accuracy is concerned with both false positives as well as false negatives of the virus detection mechanism, while performance is the ability to function efficiently without degrading the computer system (Koller, 2008; Alessandro, 2009).

In spite of the research improvements made by antivirus communities, computer viruses still pose a major threat to computer resources because they expose vulnerability of a computer system. However, the goal of this research is to apply deterministic finite state automata Model checking technique, Naïve Bayes and chi-square techniques to accurately extract viral Application Programming Interface (API) attributes in order to build a proposed intelligent virus detection system tagged “Intellect Antivirus”. The antivirus was implemented in C programming language, tested using 100 viruses, 100 Trojans and 100 Worms.

The results of the detection were compared with 44 updated antivirus products using the virus total website (www.virustotal.com). After analyzing the comparison of the antivirus products, it revealed that the proposed antivirus is an accuracy detector.

2. ANTIVIRUS SOFTWARE DETECTION TECHNIQUES

There are two main usage models when running anti-virus software they are on-demand, and on-access. The on-demand model involves the user specifying which files to scan then, the anti-virus software will usually be running for a period of time, scanning numerous files. The on-access model can be thought of as a daemon process that monitors system level and user-level operations then intervenes (scans), when a predefined event occurs. An alternative strategy involves behavior blocking, wherein the behavior of a binary is analyzed and the rate of connections to a new host is limited. In the area of anti-virus software characterization, the Antivirus-Test group has published online results of measuring the overhead associated with different anti-virus software products (Uluski et al, 2005).

When virus detection and analysis unit finds a known virus in the file, it will be sent to virus removal or quarantine unit. Here the viruses, which can be removed i.e., healed, are removed, however, there are some virus definitions on which healing is not possible therefore, these files will be quarantined. Quarantining an infected file means to move the file into an area where it cannot cause more harm. A more advanced virus detection method is to invite the virus to attack computer files in a simulated virtual machine. The success of implementing a virtual machine and opening it to all vulnerabilities is in monitoring the activities occurring in the virtual environment. Activity monitor will continuously track the virus activity in the virtual environment and it will create an activity log of the happenings inside virtual environment (Kekre et al, 2009; F-PROT antivirus SDK, 2005).

Most current anti-virus mechanisms use virus pattern matching to detect viruses but their limitation is, they can only detect those viruses for which patterns have been collected. Namely, without a specific virus pattern, a new virus can be neither detected nor removed and the problem becomes compounded, when the viruses and their variants have different virus patterns (Shakeel, 2009). A proactive method or mechanism must be developed to tackle the problem caused by known and unknown viruses. Most virus-related research focuses directly on virus files, investigating specific virus patterns in the files, the structure of the virus file and the behavior of the virus, which are all related at a low level to operating system and hardware architecture (Lin and Chen, 2006).
that simple obfuscation techniques foil commercial programs for virus detection. However, this challenges have prompted some researchers to investigate learning methods for detecting new or unknown viruses, and more generally, malicious code (Kolter and Maloof, 2006).

3. RELATED WORK

Sathyanarayan et al (2008) proposed a behavioural detection method based on chi-square technique to detect general malware family, using the malware critical API calls. The results from the statistical comparison were used to formulate the malware detection algorithm using the program behaviour model. The signatures were based on the characteristics of the entire malware class created by determining their similar behaviors. The merit of this research is that details on the detection of individual malware such as virus were reported and the results showed that the false negative rate of detection is zero. The drawbacks of this method is that its accuracy depends on constant training of the malware samples and in some cases, it still experiences high false positive alarm for virus samples detection.

Lisitsa and Webster (2008), developed a supercompilation technique to detect metamorphic viruses. Supercompilation technique can be used to prove if two programs are equivalent, this is useful for virus detection, if signature of a virus family is found in one of its variants, and other programs are checked for the same signature. The advantage of this technique is that false positive alarms are unlikely, or even impossible. The disadvantages are: (i) The supercompilation algorithm cannot normalize all equivalent programs to the same syntactic form, (ii) False negatives are possible because some codes are not analyzable by the supercompiler, (iii) Formal prove for correctness of the detection by supercompilation has not been established, (iv) The detection is a prototype, it has not yet been implemented and tested.

Sekar et al (2001) built a detection system based on finite state automata to learn the normal behaviour of a benign program and raise detection alarm when a contrary behaviour is noticed. To implement the detector, uninfected program would be trained to obtain its normal behaviour then, recorded for subsequent verification. In a subsequent execution, when there is a deviation from the initial execution path recorded, the detection alarm of the system would be triggered. The advantages of the detector are: (a) False positive detection rate using Finite State Automata is very low, (b) Space and runtime overhead of Finite State Automata-learning is minimal, (c) Finite State Automata approach is effective in detecting attacks. The disadvantages are: (i) This method can not learn the behaviour of a program that has too many transitions, (ii) The arguments of a function calls could not be included in the Finite State automata and (iii) The system is designed for Linux operating system. However, observing system calls for Linux operating system cannot be used to judge system calls for other operating systems.

Gao et al (2004) introduce a model of system call behaviour called execution graph. Execution graph is the monitoring and training of the system calls made by a program, in other to extract function call structures and build a similar graph that would be equivalent to the Control Flow Graph (CFG) generated by the program. The advantage of the system is that it accepts only system call sequences that are consistent with the control flow graph of the program. The drawback is that it is maximal, given a set of training data, meaning that any extensions to the execution graph could permit some intrusion to go undetected.

Dai et al (2008) developed a malware detector that would intercept the API calls made by an arbitrary executable program at runtime. The classifications of malicious programs are based on the sequential order which the set of API calls were made and the type of parameters passed to them. The problems with the detection system are the detector is a proposed system, it has not yet been implemented and the detector can only monitor API function calls imported from kernel32.dll and cannot detect malicious programs whose API function calls are imported from other system functions such as ntdll.dll.

Kinder (2005) developed a model checking technique for detecting email worms which uses the CopyFile and GetFileModuleName API functions. Model checking technique is an efficient method to verify the concordance of systems to specifications, such as proving the correctness of protocols in concurrent environments. The problem with this technique is that it is a prototype and has not yet been implemented, and the computational effort to implement this technique is very high (Kinder, 2005).

Abdulalla et al. (2010) developed a malware detection system that was inspired from the co-stimulation process of human immune system. The model developed could improve the accuracy of detection systems, because it checks the suspected files with two groups of API. The advantages are:

1. Improving false alarm rate for detection system.
2. Improving the prediction rate for unknown malware, as the system will not depend on a threshold value or other probability application.
3. Minimizing the cost of computation for detection systems.
4. Building direct detectors that do not need optimization (Abdulalla et al., 2010).

Murugen and Kuppusamy (2011) analyzed malware code at assembly language level by first disassembling the code and then subjecting it to analysis. From the analysis of the disassembled executable code, they observed that Application Programming Interface (API) system function calls take in sets of arguments and return the results of the functions through an eax register. The malicious program being examined makes use of the following set of API functions namely, CreateFileW, SetFilePointer, ReadFile, GlobalAlloc, CloseFile, WriteFile, GlobalFree, WinExec, DeleteFileW and ExitProcess.
They observed that CreateFileW was first used to read from a file and later used to create a new file whereby the contents of a memory location is copied into it. SetFilePointer and ReadFile functions were called twice in order to enable the malicious program being opened to read some sections of its own code with the help of GlobalAlloc function. DeleteFileW function was used by the malicious program to delete a temporary file that was created and had been used, and WinExec was used to run a newly replicated portion of the malicious (Murugen and Kuppusamy, 2011). Although the analysis of the malicious program was able to show which system functions it used, for it could not identify the particular malicious program (virus, worm or trojan) used in these system functions.

<table>
<thead>
<tr>
<th>MS-DOS Header</th>
<th>MS-DOS Stub</th>
<th>PE Header</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATA Directory</td>
<td>Section Table</td>
<td></td>
</tr>
</tbody>
</table>

**Fig 1. The Portable Executable file format**

### 5. RESEARCH DIRECTION

The antivirus companies use the signature-based technique as their primary analysing method for detecting the presence of viruses and other malwares in portable executable files. However, there are some problems in using this technique:

i. Signature-based technique is unable to detect obfuscated versions of known viruses.

ii. Antivirus researchers have not been able to automate static analysis process for building signature-based technique of antivirus products.

iii. In static analysis, no single virus analyzing tool can perform other tools functions.

iv. The existing heuristic detectors cannot distinguish between detected viruses and other malware samples during detection processes.

v. Existing antivirus programs contain a large database with a lot of signatures which may degrade computer performance when searching for match of a signature with that in a program being examined.

We set out to reprogram Microsoft Dumpbin disassembler to have features of other static analysis tools. The intention is to develop a mathematical models that can help identify the presence of viruses, worms and Trojan horses in an executable program. A momodel checking specifications is also developed for the proposed intelligent virus detection models. The proposed framework is then implemented by developing a scalable antivirus system called “Intellect Antivirus System” without a database and an Internet update.

The Windows executable file format is called the Portable Executable (PE) and it consists of five main sections as shown in figure 1. Every PE file starts with the MS-DOS header section which contains a pointer to the PE header section. MS-DOS Stub section is provided for legacy reason and this section informs the user that this file cannot be run in DOS mode, when the user attempts to run it with DOS command. The PE header contains important information needed to run the executable such as: the base address of the PE File, the address of the entry point, and the number of sections in the section table (Eilam, 2005).

The section table is divided into individual sections to store the file contents. The executable code is stored inside the code section (.text section). Program's data (for example, global variables and initialized variables) are stored inside the data section (.data section). As a result, data section contains important strings that can assist in reversing. Program'sidata (imported system functions used to access operating system resources) are stored inside the idata section (.idata section). As a result, idata section also contains important API functions that can assist in reversing an executable file. Each section has different access rights (readable, writeable, or executable) that are based on the settings available inside the section header. The last section is the directory section which consists of 16 directories holding information about PE file. Usually a few directories are present inside the PE file, such as the import table, export table, debugging information, and import address table (Eilam, 2005).

The challenges faced by Windows operating system when offering Win32 services to executable is how to differentiate between the set of system calls made by either a Benign or a malicious program. Benign and malicious programs may use the same set of API system calls, and the only way to differentiate the motive behind the usage of API system calls, is the type of parameters passed to the API function calls. Another way is how subsequent API function calls utilize the results passed by set of functions, before it was called. With regards to this, Windows operating system does not have a routine which checks the type of parameters passed to the import API system functions. It would be a great accomplishment, if there is a way, Windows operating system can be enhanced to check for malicious attributes with regards to the types of parameters passed to the set of API function calls made by executable programs.
5.1 Our Approach
In this research, the following research approaches were used:

i. A close study of the Windows operating system that uses 32-bit registers for its processor.

ii. An in-depth study of antivirus software products and their virus detection techniques in existing literature.

iii. The Dumpbin disassembly tool of Microsoft Visual studio was redesigned, implemented and applied to this research.

iv. An ultimate Packer for eXecutable (UPX) unpacking software product was used as plug-ins to unpack an executable program before sending it to a Disassembler tool.

v. A Model checking technique was used to extract interdependencies of some parameters passed by system call functions to determine malicious attributes in a disassembled program.

vi. The Deterministic Finite State Automata technique was used to extract the specific malicious attributes from an executable program.

vii. The Naïve Bayes technique was used to extract the virus attributes from the results generated by the Deterministic Finite State Automata technique.

viii. The chi square technique was used to extract the worm and Trojan attributes from the results generated by the Naïve Bayes technique.

ix. The results of malicious programs generated by using the techniques, were evaluated with some existing antivirus software products.

The system being designed is called Intelligent Computer Virus Detection System (ICVDS) and it is tagged as “Intellect Antivirus Product”, which is displayed in Figure 2. ICVDS would run directly on Windows portable executable (PE) code and would scan any Windows portable executable (PE) file codes for its set of API calls, which are classified as a file either as virus, Trojan, worm, unknown malicious program or benign program. It consists of the following components: unknown programs, Unpacking, API Function Disassembling, Finite Automata Transition Mapping Engine and Statistical Classifier Engine. The Finite Automata Transition Mapping Engine is further divided into two sections namely, **API call transition section** and **API intelligent section**. The Statistical Classifier Engine is further divided into two sections namely, **Separator Section** and **Virus Behaviour Profiling section**.

i. **The unknown programs**: is a file that is portable executable (PE) code format, which is expected to be analyzed.

ii. **Unpacking**: is a section which tries to unpack the packed or encrypted executable program about to be examined for malicious attributes.

iii. **The API Function Disassembling**: helps decompose the executable binaries into assembly codes so that an idea of the system resources used by benign or malicious executable can be got.

iv. **API call transition section**: the functionality of this section is to map the sequential order in which the set of API functions calls were made. The observation of this order would help determine if an executable program is a benign or a malicious program. The Deterministic Finite State Automata technique is used to extract and determine if the executable file contains a malicious code or it is a benign file.

v. **API intelligent section**: the functionality of this section is to extract the viral attributes from malicious code already identified by the API call transition section. The Naïve Bayes method is use to compute the attributes of self-modification, self-referential and self-replication in order to identify a virus.

vi. **Separator Section**: the functionality of this section is to ensure that the already analyzed executable file in the Deterministic Finite Automata Transition Mapping Engine are separated and accurately supplied to virus behaviour profiling section.

vii. **Virus Attribute Behaviour Profiling Section**: this is also an intelligent section which profiles the API calls made by Trojan program to differentiate the set of API calls made by worm program. It carries out this functionality by interacting with the virus profiling storage and if a Trojan or worm program is found, it is responsible for removing it.

viii. **API Behavioural Storage**: this component would be responsible for temporary storing the set of API calls made by an executable program and at the same time, stores the patterns of viral or other malicious API calls, based on their common features (self-modification, self-referencing and self-replication).

ix. **Virus Attribute Profiling Database**: this component is responsible for storing the profiles that would differentiate a Trojan attribute from a worm attribute.

Microsoft Windows operating system contains Application Programming Interfaces (API) that is a set of software functions, used by an application program for providing access to a system’s resources. These set of important API calls are present in kernel32.dll and ntdll.dll and these API calls are made by some Win32 executable programs. The detection process of intelligent computer virus detection system starts with the unknown program enters the feature extraction phase and it is being examined for malicious code. In the feature extraction phase, the unpacking section tries to unpack a packed unknown program and then move the unknown program to the API function disassembling section. The API function disassembling section disassembles the API Function Call of the unknown windows executable program to determine it set of API functions and the parameter passed to them.

If the disassembling process fails then the unknown program is either packed with unknown packer software, damaged or protected and the unknown program is detected as a special type of malicious program. When the unknown program is not packed, damaged or protected, it is passed to the API Call Transition Section of Finite Automata Transition Mapping Engine, which contains API Call Transition Section and API Intelligent Section.
The API call transition section makes use of deterministic finite automata (DFA) to map all API calls made by the unknown program into the API behaviour storage. In addition, the API call transition section learns and represents the sequential order in which a malicious API calls are made. The API Intelligent Section takes the responsibility for extracting the virus features of self-modification, self-reference and self-replication from a set of API calls made by a malicious program. It would extract these features with the help of Naïve Bayes technique, which would mine the API calls already mapped by the API call transition section. The automata pattern would be designed to match the API calls which would signify the presence of a malicious action by transiting through all the API calls made by the unknown executable program. This malicious API patterns are used to define the structure of a virus attribute based on self-modification, self-referencing and self-replication which are stored in the behavioural storage. When the deterministic finite automata transition mapping engine has finished processing the API calls made by the unknown program, if it matches the set of API calls defines as the API calls for a virus attribute, stored as patterns in the API behavioural storage, the unknown program would be detected as a virus program and removed from the system.

When the unknown program’s API calls did not match the virus APIs, then, the unknown program is believed to be free from virus but would be subjected to another check in the statistical classifier engine. In the statistical classifier engine, the analyzed executable program and its API calls are sent to the separator section in the engine. The function of separator section is to make sure that the API calls and the unknown program are supplied separately to the virus behaviour profiling section. While the separator section is necessarily is to ensure that an already examined unknown program which has been identified to contain a malicious code and it is not a virus, should be further subjected to more analysis in order to determine if it is a worm or a Trojan without re-disassembling it a second time. The virus profiling storage contains the critical API calls, with the minimum requirement to match the unknown program containing a Trojan, worm or unknown malicious code.

---

**Fig 2: Framework for Intelligent Computer Virus Detection**

- **FEATURES EXTRACTION PHASE**
  - Unknown programs → Unpacking → API Function Disassembling
  - Failed Disassembling → Successful Disassembling

- **DETECTION PHASE**
  - Deterministic Finite Automata Transition Mapping Engine
  - API Intelligent Section
  - API Call Transition Section
  - Analyzed executable program and their API calls
  - Statistical Classifier Engine
  - Virus behaviour Profiling section
  - Virus Profiling Storage
  - Virus Attribute
  - Benign
  - Packed/
    Damaged/
    Protected

- **High false positive error corrected**
- **High false negative error corrected**
- **Virus detected are reported**
The virus behaviour profiling section test the membership of a given set of API calls made by the unknown program, and compare it with the pattern stored in the virus attribute behaviour profiling storage.

The Statistical Profiling Algorithm
(i) Define \( P_i = (P_1, P_2) \) ................. equation 1.

To be the set of profiles of samples in the malicious attribute where a virus attribute has been identified from the classes \( C_1, C_2, C_3 \).

Define \( T = (T_1, T_2, T_3, ..., T_n) \) ................. equation 2.

To be tested samples of a generalized virus attributes belonging to the classes \( C_1, C_2, \) and \( C_3 \) respectively.

Define \( B \) to be the set of API function calls used to identify a benign program.

Define \( M \) to be the set of API function calls used to identify a malicious program.

(ii) Get the program incomplete API function used, which belongs to either Trojan horse or worm program and has been separated by the separator section.

(iii) Compute chi-square for each attribute class

\[
X_i^2 = \frac{(A_i - V_i)^2}{V_i}
\]

\( A_i \) is the number of observed malicious attribute and \( i \) is 2; trojan and worm.

\( V_i \) is the number of expected worm or Trojan attribute is suppose to have.

(iv) Compute degree of membership \( \sigma_i = \sum X_i^2 \).

(v) Compute the degree of freedom = number of attributes - 1

Degree of freedom = \( 2 - 1 = 1 \)

(vi) Compute threshold value \( \sigma_i \), where the null hypothesis judgment would be based upon, by reading the degree of freedom from probability level of 0.5 from the chi square table. A significant level of 0.90 was selected which means that 90% of the time, \( X^2 \) is expected to be less than or equal to \( \sigma_i \).

We have \( X^2_{0.90} = 1.386, \sigma_i = 2.71 \).

\[
X^2_{0.90} \leq 2.71.
\]

(viii) Compute the classification strategy:

\[
\begin{align*}
\exists & i, \ 1 \leq i \leq 2, \ \sigma_i \geq \sigma_i \\
\Rightarrow & T \in B_i \\
\end{align*}
\]

Otherwise,

\[
\forall i, \ 1 \leq i \leq 2, \ \sigma_i < \sigma_i \\
\Rightarrow T \in M.
\]

The virus attribute behaviour profiling section makes use of chi-square technique to measure the difference between the proportions of the critical API calls made by a Trojan from the critical API calls made by a worm. The mechanics of the proposed intelligent virus detection engine is strictly a management process whereby, deterministic finite state transition mapping engine has the ability to detect viruses infected programs and malicious programs which are not viruses are subjected to another test in statistical classifier engine. On the other end, the statistical classifier engine detects critical API calls made by Trojan, worm and unknown malicious infected programs. When an executable program is malicious-free it is reported in the deterministic finite state transition mapping and statistical classifier engines as a benign program. The Structure System Analysis and design methodology was used to develop the proposed antivirus.

6. IMPLEMENTATION

The hardware requirements necessary for the deployment of the system are Processor type of Pentium M processor with 1.70GHz and size of 598MHz, memory size of 504 MB of RAM space and hard disk space of 37.2GB. Software requirements are Microsoft Windows XP Professional operating system and Microsoft visual C++ 2008 Express Edition. Application development tools are VMware Workstation 6.0, Ultimate Packer for eXecutable version 3.7.0.0 and Microsoft Dumpbin Disassembler.

We install the VMware Workstation 6.0, Internet modern software, Ultimate Packer for eXecutable and Microsoft Dumpbin Disassembler tools from their CD packs and follow the instructions displayed during the installation processes. A folder is created (named Intellect Antivirus) and all these installed software products including the proposed antivirus software tagged “Intellect”. To run the antivirus software, the VMware workstation is installed executed, Intellect Antivirus folder is installed inside the VMware environment and then Intellect Antivirus folder icon is double-clicked on the desktop, inside the VMware environment. After double-clicking the Intellect Antivirus icon, an input screen appears which requires a file name as input to the antivirus software. To test the application, either a benign, virus, Trojan or worm filename is entered and the result of malicious detection is sent to an output file. The results of the type of malicious programs detected are displayed in table 1.
Table 1: Selected Malicious Files

<table>
<thead>
<tr>
<th>Malicious file</th>
<th>Benign Detection</th>
<th>Virus detection</th>
<th>Trojan Detection</th>
<th>Worm Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Benign file: Dumpbin.exe</td>
<td>√</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Virus file: Virus.win32.cabinfector</td>
<td>X</td>
<td>√</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Trojan file: Trojan-dropper.win32.apent</td>
<td>X</td>
<td>X</td>
<td>√</td>
<td>X</td>
</tr>
<tr>
<td>Worm file: Worm.win32.ladex.a</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>√</td>
</tr>
</tbody>
</table>

Key: X: no detection, √: Detection.

From the results displayed in table 1, it shows that Intellect Antivirus software accurately detected the various types of malicious files from samples files used.

6.1 Implementation Results

We tested the accuracy of Intellect Antivirus by testing it on 100 benign programs copied from a newly installed Windows XP operating system, 100 viruses, 100 Trojan horses and 100 worms downloaded from VX Heaven website (www.vx.net.org).

Table 2 shows the summary of the detection results produced by Intellect Antivirus software and the relevant columns of the table are:

(i) SR1 means the number of self-referential attributes recorded during the detection.
(ii) SR2 means the number of self-replication attributes recorded during the detection.
(iii) SM means the number of self-modification attributes recorded during the detection.
(iv) Tr means the number of Trojan attributes recorded during the detection.
(v) No-Dis means the number of executable files that could not be disassembled during detection.
(vi) Mal-C means the number of known malicious code attributes detected.
(vii) Unk-M means the number of unknown malicious code detected.
(viii) Packed-M means the number of packed or protected malicious code detected.
(ix) Error means the number of files that could not be examined for malicious attribute by the intellect antivirus.
(x) HC means the number of executable files that whose header section were coded.
(xi) T means true identification of a malicious category (virus, Trojan or worm).
(xii) B means set of benign executable file that missed detection.
(xiii) Pi means unknown packer identified in malicious programs.
(xiv) M/S means set of Benign executable programs wrongly identified as suspicious or malicious programs.

Table 2: Features detected in Malicious executables

<table>
<thead>
<tr>
<th>s/n</th>
<th>SR1</th>
<th>SR2</th>
<th>SM</th>
<th>Tr</th>
<th>Wo</th>
<th>No-Dis</th>
<th>Mal-C</th>
<th>Unk-M</th>
<th>Packed-M</th>
<th>Error</th>
<th>HC</th>
<th>T</th>
<th>Pi</th>
<th>M/S</th>
</tr>
</thead>
<tbody>
<tr>
<td>Benign</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>97</td>
<td>0</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>s/n</th>
<th>SR1</th>
<th>SR2</th>
<th>SM</th>
<th>Tr</th>
<th>Wo</th>
<th>No-Dis</th>
<th>Mal-C</th>
<th>Unk-M</th>
<th>Packed-M</th>
<th>Error</th>
<th>HC</th>
<th>T</th>
<th>Pi</th>
<th>M/S</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viruses</td>
<td>9</td>
<td>7</td>
<td>1</td>
<td>21</td>
<td>9</td>
<td>7</td>
<td>23</td>
<td>9</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>3</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Trojans</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>1</td>
<td>9</td>
<td>77</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Worms</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>7</td>
<td>8</td>
<td>7</td>
<td>70</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

During the running of malicious files used for this experiment, we observed how these files used certain features described in table 2.

i. Self-Referential Feature (SR1): it was observed in the results shown in table 2 that only virus files used for this experiment exhibited the self-Referential feature and the number of virus files which showed this feature is 6 files, as shown in table 2. No Trojan or worm files used in this experiment showed self-referential features.

ii. Self-Replication Feature (SR2): similar to the SR1 feature, only virus file exhibited this feature with a total number of 6, while neither Trojan nor worm file has this feature.

iii. Self-Modification Feature (SM): in this experiment, we are only interested in examining a virus file for this...
feature and for this reason, we did not record the feature for Trojan and worm. It was only 1 virus file which exhibited this feature.

iv. Trojan horse Feature (Tr): in this experiment, we observed that virus file scored the highest number to exhibit this feature with a score of 21, Trojan has 5 while worm has 8.

v. Worm Feature (Wo): we observed that virus set of files has the highest number of file which exhibit this feature with a total of 9, Trojan has 3 and worm has 8.

vi. Executable code Not-Disassembled Feature (No-Dis): worm files have the highest number of malicious with this feature, with a total of 11, while virus and Trojan has the same number, which is 8.

vii. Known Malicious code feature (MAL-C): Trojan files use more of this feature with the number of 30, and 16 viruses and 24 worms also use this feature.

viii. Unknown Malicious code feature (Unknown-M): virus files use more of this feature with the number of 10, and 5 trojans and 1 worm files also use this feature.

ix. Packed or protected feature (Packed-M): virus files also uses more of this feature with the number of 5, and 1 trojans and 1 worm files use this feature.

x. Error in Executable (Error): virus files use more of this feature with the number of 3, and no Trojan file uses this feature and 1 worm files use this feature.

xi. Header Section code feature (HC): worm files use more of this feature with the number of 26, and 2 Trojan file use this feature and no virus file uses this feature.

xii. True Positive feature (True): 3 Trojans and 3 worms files show their true nature of their malicious categories and no virus files showed their true nature without combining features of other malicious categories.

xiii. Benign Executable feature (Benign): 3 virus and 3 Trojans were missed during detection, only 1 worm file was missed during detection.

a. Benign: from the results shown in table 2, it shows that intellect antivirus was able to detect 97% of the benign programs tested on it and recorded a false alarm of 3%. This false alarm is attributed to three registry files in the system files used.

b. (Virus: from the results displayed in table 2, it was observed that viruses has 3% of true virus attributes, 9% of self-referential attribute, 7% of replication attribute, 21% of Trojan attributes and 9% of worm attributes.

c. Trojan horse: it was further observed that Trojan score 3% of true Trojan attribute, 5% of Trojan code mixed with other code, 0% of virus attributes and 1% of worm attributes.

d. Worm: it was observed that worm recorded 3% of true worm attribute 8% of worm code mixed other malicious code, 7% of Trojan attribute and 0% of virus attributes.

The result of detection displayed in table 2 further shows that registry programs can exhibit sometimes malicious behaviour and these registry benign programs can exhibit unknown malicious and header coded behaviour. Among all the malicious programs tested on the proposed antivirus, it reveals that most of the malicious programs were detected under the category of malicious code while the least was the unknown packer category. It is very clear from this research which we have earlier confirmed during the experimental stage that Trojans and worms do not exhibit self-referential and self-replication attributes used by virus programs.

6.2 Post Implementation Evaluation

We carried out a post implementation Evaluation of proposed Intellect antivirus product with 44 updated antivirus software products. The evaluation was carried out by using the same set of malicious programs tested on Intellect antivirus to test the efficiency of the 44 antivirus products using virus total website (www.virustotal.org) and the detection results are compared with the ones got from the proposed intellect antivirus. The malicious detection results got from the 44 updated antivirus products and results from intellect antivirus is displayed in table 4.

3. The relevant columns of table 3 are:

i. ANTIVIRUS are set of antivirus that participated in the malicious testing.

ii. VIRUSES, TROJANS, WORMS are results of detection (Det.) or no-detection (No-Det) recorded for viruses, Trojans and worms used in the testing.

iii. DET.AVG is the average detection rates of viruses, Trojans and worms recorded during the testing process.

iv. Database Present is to indicate an antivirus product taking part in the testing contains a viral signature database.

v. Internet Update is record if an antivirus product needs an internet update to remain effective.

From the results displayed in table 3, it shows that the kasperkey recorded an average of 100 percent detection score and no-detection score of 0 percent. SUPERAntisyware scored the lowest with 8 percent detection score and no-detection score of 98 percent compared with other antivirus products used for the testing. The proposed Intellect Antivirus product recorded an average detection of 98 percent, no-detection of 2 percent, requires no signature database and no internet update. The increasing number of malicious signature database during antivirus update, and its size in megabytes (millions of bytes) and the time taken to compare each malicious signature with every executable file can degrade the performance of a computer system. When there is a cut in internet connection for few days, can render an antivirus ineffective and this can pose serious risk to the computer system safety.

The best eleven antivirus products which recorded the highest detection rate is ranked according their order of detection rates and this is displayed in table 4.
Table 3: Detection results of some Malicious programs

<table>
<thead>
<tr>
<th>S/n</th>
<th>ANTIVIRUS</th>
<th>VIRUSES Det, No-Det</th>
<th>TROJANS Det, No-Det</th>
<th>WORMS Det, No-Det</th>
<th>DET. AVG Det, No-Det</th>
<th>Database Present</th>
<th>Internet update</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>AhnLab-V3</td>
<td>88, 12</td>
<td>97, 3</td>
<td>93, 7</td>
<td>92.7%, 7.3%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>2</td>
<td>AntiVir</td>
<td>99, 1</td>
<td>98, 2</td>
<td>98, 2</td>
<td>98.7%, 1.3%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>Antiy-AVL</td>
<td>61, 39</td>
<td>77, 23</td>
<td>85, 15</td>
<td>74.3%, 25.7%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>4</td>
<td>Avast</td>
<td>100, 0</td>
<td>95, 5</td>
<td>97, 3</td>
<td>97.3%, 2.7%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>5</td>
<td>Avast5</td>
<td>100, 0</td>
<td>95, 5</td>
<td>98, 2</td>
<td>97.7%, 2.3%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6</td>
<td>AVG</td>
<td>100, 0</td>
<td>99, 1</td>
<td>98, 2</td>
<td>99%, 1%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>7</td>
<td>BitDefender</td>
<td>100, 0</td>
<td>97, 3</td>
<td>100, 0</td>
<td>99%, 1%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>8</td>
<td>CAT-QuickHeal</td>
<td>74, 26</td>
<td>76, 24</td>
<td>85, 15</td>
<td>78.3%, 21.7%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9</td>
<td>ClamAV</td>
<td>49, 51</td>
<td>69, 31</td>
<td>79, 21</td>
<td>65.7%, 34.3%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>10</td>
<td>Commtouch</td>
<td>98, 2</td>
<td>75, 25</td>
<td>98, 2</td>
<td>90.3%, 9.7%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>11</td>
<td>DrWeb</td>
<td>100, 0</td>
<td>98, 2</td>
<td>99, 1</td>
<td>99%, 1%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>12</td>
<td>Emsisoft</td>
<td>81, 19</td>
<td>81, 19</td>
<td>88, 12</td>
<td>83.3%, 16.7%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>13</td>
<td>Esafe</td>
<td>75, 25</td>
<td>43, 57</td>
<td>72, 28</td>
<td>63.3%, 36.7%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>14</td>
<td>eTrust-Vet</td>
<td>98, 2</td>
<td>86, 14</td>
<td>97, 3</td>
<td>93.7%, 6.3%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>15</td>
<td>F-Protes</td>
<td>96, 4</td>
<td>96, 4</td>
<td>100, 0</td>
<td>97.3%, 2.7%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>16</td>
<td>F-Secure</td>
<td>85, 15</td>
<td>97, 3</td>
<td>95, 5</td>
<td>92.3%, 7.7%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>17</td>
<td>GData</td>
<td>100, 0</td>
<td>99, 1</td>
<td>99, 1</td>
<td>99.3%, 0.7%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>18</td>
<td>Ikarus</td>
<td>100, 0</td>
<td>100, 0</td>
<td>95, 5</td>
<td>98.3%, 1.7%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>19</td>
<td>Jiangmin</td>
<td>78, 22</td>
<td>93, 7</td>
<td>96, 4</td>
<td>89%, 11%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>20</td>
<td>K7Antivirus</td>
<td>97, 3</td>
<td>96, 4</td>
<td>98, 2</td>
<td>97%, 3%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>21</td>
<td>Kaspersky</td>
<td>100, 0</td>
<td>100, 0</td>
<td>100, 0</td>
<td>100%, 0%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>22</td>
<td>McAfee</td>
<td>99, 1</td>
<td>99, 1</td>
<td>99, 1</td>
<td>99%, 1%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>23</td>
<td>McAfee-GWL-Ed.</td>
<td>100, 0</td>
<td>99, 1</td>
<td>98, 2</td>
<td>99%, 1%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>24</td>
<td>Microsoft</td>
<td>93, 7</td>
<td>93, 7</td>
<td>94, 6</td>
<td>93.3%, 6.7%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>25</td>
<td>NOD32</td>
<td>97, 3</td>
<td>93, 7</td>
<td>99, 1</td>
<td>96.3%, 3.7%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>26</td>
<td>Norman</td>
<td>99, 1</td>
<td>92, 8</td>
<td>96, 4</td>
<td>95.7%, 4.3%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>27</td>
<td>nProtect</td>
<td>29, 66</td>
<td>34, 86</td>
<td>74.3%, 25.7%</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>Panda</td>
<td>100, 0</td>
<td>93, 7</td>
<td>93, 7</td>
<td>96.7%, 3.3%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>29</td>
<td>PC Tools</td>
<td>97, 3</td>
<td>98, 2</td>
<td>97, 3</td>
<td>97.3%, 2.7%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>30</td>
<td>Pervx</td>
<td>13, 87</td>
<td>21, 79</td>
<td>2, 98</td>
<td>12%, 88%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>31</td>
<td>Rising</td>
<td>77, 23</td>
<td>75, 25</td>
<td>79, 21</td>
<td>77%, 23%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>32</td>
<td>Sophos</td>
<td>100, 0</td>
<td>95, 5</td>
<td>96, 4</td>
<td>97%, 3%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>33</td>
<td>SUPERAntiSpyware</td>
<td>2, 98</td>
<td>8, 92</td>
<td>14, 86</td>
<td>8%, 92%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>34</td>
<td>Symantec</td>
<td>93, 3</td>
<td>99, 1</td>
<td>96, 4</td>
<td>97.3%, 2.7%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>35</td>
<td>The Hacker</td>
<td>24, 76</td>
<td>82, 18</td>
<td>89, 11</td>
<td>65%, 35%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>36</td>
<td>TrendMicro</td>
<td>94, 6</td>
<td>86, 14</td>
<td>93, 7</td>
<td>91%, 9%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>37</td>
<td>TrendMicroHouse</td>
<td>94, 6</td>
<td>86, 14</td>
<td>93, 7</td>
<td>91%, 9%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>38</td>
<td>VBA32</td>
<td>64, 36</td>
<td>61, 39</td>
<td>91, 9</td>
<td>72%, 28%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>39</td>
<td>VIPRE</td>
<td>91, 9</td>
<td>92, 8</td>
<td>95, 5</td>
<td>92.7%, 7.3%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>40</td>
<td>VirusBuster</td>
<td>93, 7</td>
<td>92, 8</td>
<td>96, 4</td>
<td>93.7%, 6.3%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>41</td>
<td>Byte Hero</td>
<td>92, 8</td>
<td>97, 13</td>
<td>83, 17</td>
<td>87.3%, 12.7%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>42</td>
<td>Intellect Antivirus</td>
<td>96, 4</td>
<td>99, 1</td>
<td>99, 1</td>
<td>98%, 2%</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
7. CONCLUSION

The need to develop antivirus software that can intelligently detect malicious programs and at the same time can automatically identify the type of malicious program has attracted a great deal of concern from the antivirus community. However, research efforts towards automatically indentifying malicious programs and categorizing them into their types based on their behaviour has not been successful. Through thorough review of this discipline, some weaknesses were seen which drove this study to develop a proposed antivirus product that would have a better performance with the absence of a malicious signature database and an internet updating capabilities.

This research work has exposed the secrets of how best to develop an effective antivirus product by examining the argument of API functions used by an executable program and then checking it for malicious attributes. Significantly, this research is a contribution to the existing knowledge on computer antivirus development, we have been able to contribute the following to:

i) Derive two new algorithms that use Naïve Bayes and Chi Square Techniques to aid virus detection.
ii) Show that these the two new algorithms aid in automatic identification of viruses, worms and Trojan horses from available malicious attributes.
iii) Re-design and re-implement Microsoft dumpbin software to have SoftIce features.
iv) Implement Model checking analysis in this research, which before now was only a prototype.
v) Develop an antivirus software which neither uses a malicious signature database nor needs an internet updating process.
vi) Develop a new antivirus software that can coexist with another antivirus already installed and running in the system.

The existing Windows operating system provides system resources for the portable executable programs by allowing them to have access to the DLL functions directly. The purpose of using API functions imported from these DLLs not checked by Windows operating system. Instead, they subject the operating system users to install antivirus products to help alleviate the numbers of infections caused by malicious samples in the computer system. When the proposed intelligent computer virus detection system is implemented as part of the functional components of Windows operating system, it alters the operations of the operating system as follows:

a) The portable executable wishing to use the system resources in the form of API system calls should pass through the proposed intelligent computer virus detection system.
b) If the virus detector finds viruses, worms, Trojans or other malicious codes in the portable executable program, it would abort the executable program from running in the Windows

c) operating system environment.

Fig 3.: Intelligent Computer Virus Detection System
(d) If the virus detector could not find any traces of viruses, worms, Trojans and other malicious codes in the portable executable program, it would accept the executable and allow it to access the DLLs functions of Windows operating system.

(e) Incompatibility of antivirus software with the operating system component would no longer be a problem because the virus detector is now a part of the operating system components and not an external software that does alter the smooth running of Windows operating system.

REFERENCES


Authors’ Brief

Osaghae Edgar obtained B.Sc and M.Sc Degrees in Computer Science from University of Benin, Benin city, Nigeria. He is also a Doctoral student in Computer Science of the same University. He is presently a lecturer in the Department of Computer Science, University of Port Harcourt, Rivers State, Nigeria. His main research interest is Computer security, formal verification methods, and Computer Algorithms.

Prof. (Mrs.) Stella Chinye CHIMEKE is a Professor of Computer Science and currently the Director of UNIBEN ICT Centre, University of Benin, Benin City, Nigeria. Her teaching and research interests span from software engineering to industrial application of ICT. She is a member of the International Association of Engineers (IAENG), Computer Professional of Nigeria (CPN), Nigeria Computer Society (NCS), International Network for Woman Engineers and Scientists (INWES) Canada etc.
ABSTRACT
We seek to understand cyber victimization by determining what users do online that makes them vulnerable to different forms of cyber attacks. We set up an online trap platform that presents users with legal and illegal contents and see whether people who visited the platform for the purposes of gaining access to legal material would also attempt to access illegal and/or pornographic material. We then empirically observed the behaviour of users with emphasis on those who attempted to indulge in cyber criminal activities. The online statistical tool AWStats is used in addition to a specially developed platform called “resourcefulminds.com”. Premised on a similar research by Silke and Demetriou (2003), findings from our study and analysis of the study population showed that 76% of users accessing both legal and illegal material and 10% restricting their access to just legal and 6% accessed just illegal material. 8% of users did not access any material beyond the homepage. Two significant phenomena were the observation that half the total number of registered users registered via crime related links and over 77% of users who visited the website were only on the site for less than 30 seconds. Our findings offer insights into why users are victimized online.

Keywords: Online deviant behaviour, cybercrime, deindividuation

1. INTRODUCTION
Cyber crimes are criminal activities that are perpetrated using communication networks such as the Internet, telephone, wireless, satellite, and mobile networks are known as cyber crimes [1. Cyber crime may consequently be defined to cover all sorts of crimes committed with computers—from viruses, trojan horses, from hacking into private email to undermining defense and intelligence systems, from electronic thefts of bank accounts to disrupting web sites. Scholars have categorized cyber crime in its various forms as follows:

- Cyber-Trespass: This involves crossing boundaries into other people's property and/or causing damage, eg- hacking, defacement and viruses
- Cyber-Deceptions and Theft: This type of cyber crime involves stealing (money,property), eg-credit card fraud,intellectual property violation, piracy
- Cyber-Pornography: These are activities that breach laws on obscenity and decency
- Cyber Violence: This involves causing psychological harm to, or inciting physical harm against others, thereby breaching laws pertaining to the protection of the person. eg- hate speech [2][3]

Our efforts in this paper is directed at developing a scheme to understand cyber victimization by determining what users do online that makes them vulnerable to different forms of cyber attacks. Our approach is to set up a platform that presents users with legal and illegal contents and see whether people who visited the platform for the purposes of gaining access to legal material would also attempt to access illegal and/or
pornographic material. These methodology is then used to also determine the background or profile of users who typically commit cyber crimes as compared to those who are law abiding online.

The remaining parts of this paper is organized as follows. In section 2, we explore related works in the domain of cyber crime. Section 3 presents the methodology adopted for the research. This is followed by section 4 where results are presented and analysed. We ended the paper in section 5 with concluding remarks.

2. RELATED WORKS

In a much broader sense, cyber crime is a term that covers all sorts of crimes committed with computers. In [5], it was defined as just crimes over the Internet. The Brenner publications of 2004 unveiled some unique characteristics of cyber crime that is usually present when cyber crimes are committed. These distinguishing characteristics are explained below.

- **Transnational Nature and Jurisdictional Issues:** Cybercrime spills over national borders particularly in the matter of deciding which jurisdiction such crime should fall under. The law is not always prepared for meeting the demands of globalization as its cross-border character creates a need for improved cross-border law enforcement. Attacks can also be designed such that they appear to be originating from sources.

- **Proximity and Physical Constraints:** The constraints that govern action in the real world, physical world do not restrict perpetrators of cyber crime. Cyber crimes can be committed instantaneously and therefore require a rapid response: law enforcement, however is accustomed to dealing with real-world “crimes,” the investigation of which proceeds at a more deliberate space [7]. Unlike real world crime, cyber crimes do not require any degree of physical proximity between the victim and victimizer.

- **Scale, Velocity and Multiple Victimization:** Cyber crime is different because it is automated crime. Whereas a real or terrestrial world fraudster would need to manually defraud different people individually at different times, a cyber fraudster can automate the process defrauding many victims simultaneously and with essentially the same effort via technology. The automation gives the perpetrators the ability to commit many cyber crimes very quickly[8].

- **Perfect Anonymity:** Cyberspace also provides room for perpetrators to conceal or disguise their identities in a way that is not possible in the real world. [9] [10]. In the real world, an offender can wear a mask and perhaps take other efforts to conceal his identity, but certain characteristics such as height, weight, accent, and age - will still be apparent. In cyberspace one can achieve much perfect anonymity; a man can be a woman, a woman can be a man, a child can be an adult, a foreigner can pass for a native, all of which makes the apprehension of cyber criminals difficult.

One essential theory that has linked behaviour with cyber crime is the Space transition theory [11], the theory argues that, people behave differently when they move from one space to another. The postulates of the theory are:

1. Persons, with repressed criminal behavior (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they could not commit in physical space, due to their status and position.

2. Identity Flexibility, Dissociative Anonymity and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cyber crime.

3. Criminal behavior of offenders in cyberspace is likely to be imported to Physical space which, in physical space may be exported to cyberspace as well.

4. Intermittent ventures of offenders in to the cyberspace and the dynamic spatio-temporal nature of cyberspace provide the chance to escape.

5. (a) Strangers are likely to unite together in cyberspace to commit crime in the physical space.

   (b) Associates of physical space are likely to unite to commit crime in cyberspace.

6. Persons from closed society are more likely to commit crimes in cyberspace than persons from open society.

7. The conflict of Norms and Values of Physical Space with the Norms and Values of cyberspace may lead to cyber crimes.

This theory was further developed and modeled to become the Space Transition Model with specifically derived variables that can be tested to determine if it forms a reliable basis for testing. The variables were status, anonymity, deterrence factor, open or closed society and physical or cyber world associates. [12], [13] remarked that online users who commit crime are usually concerned about their social status in the physical world but are not bothered about their status in the cyberspace because there is no one to watch and stigmatize them.
3. METHODOLOGY

The website was named Resourceful Minds with the address http://www.resourcefulminds.com and monitored over a six month period. It was an experimental case study developed with the use of HTML and PHP with embedded SQL scripts and hosted on a Linux server running Apache as the webserver and MySQL as the database.

The links provided on the website included the following:

**Home**: This link displayed and looped to the initial homepage which provided access to all links on the website.

**Stolen Passwords**: This link was not a genuine one and did not work, it rather asked one to register to gain access to more details and in the process only collected information about the user and displayed a message asking the user to try next time.

**News**: This link provided users access to a page that provided access to news websites such as www.bbc.co.uk and www.cnn.com

**Pornography (child)**: This link was not a genuine one and did not work, it rather asked one to register to gain access to more details and in the process only collected information about the user and displayed a message asking the user to try next time.

**Academics**: This provided users access to online libraries and resourceful academic material.

**Illegal Shareware**: This link was not a genuine one and did not work, it rather asked one to register to gain access to more details and in the process only collected information about the user and displayed a message asking the user to try next time.

**Disclaimer**: This link provided access to a disclaimer statement about access to the website.

**Usable Credit Cards**: This link was not a genuine one and did not work, it rather asked one to register to gain access to more details and in the process only collected information about the user and displayed a message asking the user to try next time.

**Software Cracks**: This link was not a genuine one and did not work, it rather asked one to register to gain access to more details and in the process only collected information about the user and displayed a message asking the user to try next time.

**Illegal Games Download**: This link was not a genuine one and did not work, it rather asked one to register to gain access to more details and in the process only collected information about the user and displayed a message asking the user to try next time.

**Registration**: The registration link was accessible from every page and it provided users access to the registration form. The system could however log the exact page from which a registration was done via the a memory variable which stored the name of the accessed link.

The database was modeled using the conceptual modeling method which was translated into a relational schema and the ultimately a physical database as explained in [14].

Participants were recruited via e-mail notification and advertisement on facebook.com, click patterns were tracked based on unique session identification numbers and activities on the website where as registration count was based on unique identification accounts. It needs to emphasized that this did guarantee that specific individuals could not register more than once using different identification.

Every user who accessed the website for the first time was assigned a unique session identification number, subsequently, every link that was clicked was stored in a memory variable was declared for the purpose of tracking every single accessed page by the users. The accessed links are stored hence all users could be tracked to determine all accessed pages on the website while the session lasted.

4. RESULTS AND ANALYSIS

Presented below are the data showing different types of activities that users engage in on the “RESOURCEFULMINDS” website. Explanation are offered for each table contents at the end of the set of tables.

<table>
<thead>
<tr>
<th>Countries</th>
<th>Pages</th>
<th>Hits</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ghana</td>
<td>1,634</td>
<td>6,349</td>
<td>51.18 MB</td>
</tr>
<tr>
<td>United States</td>
<td>606</td>
<td>1,130</td>
<td>7.69 MB</td>
</tr>
<tr>
<td>European country</td>
<td>56</td>
<td>58</td>
<td>281.76 KB</td>
</tr>
<tr>
<td>Germany</td>
<td>35</td>
<td>138</td>
<td>1.06 MB</td>
</tr>
<tr>
<td>Norway</td>
<td>23</td>
<td>83</td>
<td>862.27 KB</td>
</tr>
<tr>
<td>Great Britain</td>
<td>22</td>
<td>122</td>
<td>1.18 MB</td>
</tr>
<tr>
<td>Russian Federation</td>
<td>7</td>
<td>37</td>
<td>448.93 KB</td>
</tr>
<tr>
<td>Canada</td>
<td>4</td>
<td>18</td>
<td>219.76 KB</td>
</tr>
<tr>
<td>New Zealand</td>
<td>4</td>
<td>34</td>
<td>355.48 KB</td>
</tr>
<tr>
<td>Hungary</td>
<td>2</td>
<td>16</td>
<td>210.86 KB</td>
</tr>
<tr>
<td>South Africa</td>
<td>2</td>
<td>16</td>
<td>210.86 KB</td>
</tr>
<tr>
<td>France</td>
<td>2</td>
<td>2</td>
<td>8.91 KB</td>
</tr>
<tr>
<td>India</td>
<td>2</td>
<td>16</td>
<td>210.86 KB</td>
</tr>
<tr>
<td>Senegal</td>
<td>2</td>
<td>16</td>
<td>210.79 KB</td>
</tr>
<tr>
<td>Japan</td>
<td>1</td>
<td>1</td>
<td>4.45 KB</td>
</tr>
<tr>
<td>Nigeria</td>
<td>1</td>
<td>8</td>
<td>105.43 KB</td>
</tr>
<tr>
<td>Others</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Source: AWStats Analysis
Table 2: Monthly Statistics of Access

<table>
<thead>
<tr>
<th>Month</th>
<th>Unique visitors</th>
<th>Number of visits</th>
<th>Pages</th>
<th>Hits</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 2011</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Feb 2011</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Mar 2011</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Apr 2011</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>May 2011</td>
<td>18</td>
<td>24</td>
<td>68</td>
<td>349</td>
<td>2.56 MB</td>
</tr>
<tr>
<td>Jun 2011</td>
<td>89</td>
<td>214</td>
<td>641</td>
<td>2,848</td>
<td>23.35 MB</td>
</tr>
<tr>
<td>Jul 2011</td>
<td>44</td>
<td>157</td>
<td>684</td>
<td>1,930</td>
<td>14.44 MB</td>
</tr>
<tr>
<td>Aug 2011</td>
<td>30</td>
<td>128</td>
<td>237</td>
<td>668</td>
<td>5.47 MB</td>
</tr>
<tr>
<td>Sep 2011</td>
<td>59</td>
<td>187</td>
<td>593</td>
<td>1,748</td>
<td>14.41 MB</td>
</tr>
<tr>
<td>Oct 2011</td>
<td>29</td>
<td>106</td>
<td>178</td>
<td>490</td>
<td>3.82 MB</td>
</tr>
<tr>
<td>Nov 2011</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Dec 2011</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>269</td>
<td>816</td>
<td>2,401</td>
<td>8,033</td>
<td>64.17 MB</td>
</tr>
</tbody>
</table>

Source: AWStats Analysis

Table 3: Access Robots

<table>
<thead>
<tr>
<th>11 different robots</th>
<th>Hits</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Googlebot</td>
<td>496</td>
<td>2.31 MB</td>
</tr>
<tr>
<td>Yahoo Slurp</td>
<td>204</td>
<td>1.83 MB</td>
</tr>
<tr>
<td>Unknown robot (identified by 'bot*')</td>
<td>171</td>
<td>709.33 KB</td>
</tr>
<tr>
<td>Unknown robot (identified by 'spider')</td>
<td>158</td>
<td>711.30 KB</td>
</tr>
<tr>
<td>Unknown robot (identified by empty user agent string)</td>
<td>74</td>
<td>809.82 KB</td>
</tr>
<tr>
<td>Unknown robot (identified by '*bot')</td>
<td>44</td>
<td>166.21 KB</td>
</tr>
<tr>
<td>Unknown robot (identified by 'crawl')</td>
<td>6</td>
<td>26.72 KB</td>
</tr>
<tr>
<td>Neteract</td>
<td>5</td>
<td>22.27 KB</td>
</tr>
<tr>
<td>Alexa (IA Archiver)</td>
<td>3</td>
<td>13.36 KB</td>
</tr>
<tr>
<td>Unknown robot (identified by 'scanner')</td>
<td>2</td>
<td>8.91 KB</td>
</tr>
<tr>
<td>Unknown robot (identified by 'robot')</td>
<td>1</td>
<td>4.45 KB</td>
</tr>
</tbody>
</table>

Last visit: 08 Nov 2011 - 03:55

Source: AWStats Analysis

Table 4: Average Duration of Visits

<table>
<thead>
<tr>
<th>Number of visits: 818 - Average: 169 s</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
</tr>
<tr>
<td>---------</td>
</tr>
<tr>
<td>0s-30s</td>
</tr>
<tr>
<td>30s-2mn</td>
</tr>
<tr>
<td>2mn-5mn</td>
</tr>
<tr>
<td>5mn-15mn</td>
</tr>
<tr>
<td>15mn-30mn</td>
</tr>
<tr>
<td>30mn-1h</td>
</tr>
<tr>
<td>1h+</td>
</tr>
</tbody>
</table>

Source: AWStats Analysis

Table 5: Regularly Accessed Links (Files)

<table>
<thead>
<tr>
<th>17 different pages-url</th>
<th>Viewed</th>
<th>Average size</th>
<th>Entry</th>
<th>Exit</th>
</tr>
</thead>
<tbody>
<tr>
<td>/</td>
<td>852</td>
<td>2.09 KB</td>
<td>750</td>
<td>599</td>
</tr>
<tr>
<td>register.php</td>
<td>301</td>
<td>7.68 KB</td>
<td>1</td>
<td>24</td>
</tr>
<tr>
<td>index.php</td>
<td>196</td>
<td>4.45 KB</td>
<td>30</td>
<td>42</td>
</tr>
<tr>
<td>/loginz.php</td>
<td>178</td>
<td>2.99 KB</td>
<td>3</td>
<td>8</td>
</tr>
<tr>
<td>/academics.php</td>
<td>134</td>
<td>4.02 KB</td>
<td>1</td>
<td>35</td>
</tr>
<tr>
<td>/porn.php</td>
<td>120</td>
<td>4.12 KB</td>
<td>3</td>
<td>14</td>
</tr>
<tr>
<td>/news.php</td>
<td>92</td>
<td>5.68 KB</td>
<td>4</td>
<td>15</td>
</tr>
<tr>
<td>/cards.php</td>
<td>75</td>
<td>2.78 KB</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>/cracks.php</td>
<td>75</td>
<td>4.80 KB</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>/shareware.php</td>
<td>66</td>
<td>4.16 KB</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>/hackedapp.php</td>
<td>63</td>
<td>2.96 KB</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>/hackedgam.php</td>
<td>57</td>
<td>3.59 KB</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>/notes/</td>
<td>37</td>
<td>82 Bytes</td>
<td>3</td>
<td>16</td>
</tr>
<tr>
<td>/cgi-sys/suspendedpage.cgi</td>
<td>36</td>
<td>3.55 KB</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>/passwords.php</td>
<td>35</td>
<td>3.43 KB</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>/disclaimer.php</td>
<td>16</td>
<td>4.56 KB</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

Source: AWStats Analysis

Table 6: Users' Operating System Platforms

<table>
<thead>
<tr>
<th>Operating Systems</th>
<th>Hits</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>6,553</td>
<td>81.4 %</td>
</tr>
<tr>
<td>Unknown</td>
<td>680</td>
<td>8.4 %</td>
</tr>
<tr>
<td>Java Mobile</td>
<td>346</td>
<td>4.3 %</td>
</tr>
<tr>
<td>BlackBerry</td>
<td>193</td>
<td>2.3 %</td>
</tr>
<tr>
<td>Macintosh</td>
<td>156</td>
<td>1.9 %</td>
</tr>
<tr>
<td>Linux</td>
<td>104</td>
<td>1.2 %</td>
</tr>
<tr>
<td>Java</td>
<td>12</td>
<td>0.1 %</td>
</tr>
</tbody>
</table>

Source: AWStats Analysis
<table>
<thead>
<tr>
<th>Browsers</th>
<th>Grabber</th>
<th>Hits</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS Internet Explorer</td>
<td>No</td>
<td>3,182</td>
<td>39.5 %</td>
</tr>
<tr>
<td>Firefox</td>
<td>No</td>
<td>2,319</td>
<td>28.8 %</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>No</td>
<td>1,094</td>
<td>13.6 %</td>
</tr>
<tr>
<td>Unknown</td>
<td>?</td>
<td>554</td>
<td>6.8 %</td>
</tr>
<tr>
<td>Opera</td>
<td>No</td>
<td>512</td>
<td>6.3 %</td>
</tr>
<tr>
<td>BlackBerry (PDA/Phone browser)</td>
<td>No</td>
<td>185</td>
<td>2.2 %</td>
</tr>
<tr>
<td>Safari</td>
<td>No</td>
<td>130</td>
<td>1.6 %</td>
</tr>
<tr>
<td>Mozilla</td>
<td>No</td>
<td>26</td>
<td>0.3 %</td>
</tr>
<tr>
<td>Nokia Browser (PDA/Phone browser)</td>
<td>No</td>
<td>14</td>
<td>0.1 %</td>
</tr>
<tr>
<td>LG (PDA/Phone browser)</td>
<td>No</td>
<td>12</td>
<td>0.1 %</td>
</tr>
<tr>
<td>Others</td>
<td></td>
<td>16</td>
<td>0.1 %</td>
</tr>
</tbody>
</table>

Source: AWStats Analysis

<table>
<thead>
<tr>
<th>Origin</th>
<th>Pages</th>
<th>Percent</th>
<th>Hits</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct address / Bookmark / Link in email...</td>
<td>870</td>
<td>91.2 %</td>
<td>1,001</td>
<td>92.3 %</td>
</tr>
<tr>
<td>Links from an Internet Search Engine - Full list</td>
<td>41</td>
<td>4.3 %</td>
<td>41</td>
<td>3.7 %</td>
</tr>
<tr>
<td>- Google</td>
<td>32 / 32</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Yandex</td>
<td>7 / 7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Microsoft Bing</td>
<td>1 / 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Yahoo!</td>
<td>1 / 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Links from an external page (other web sites except search engines) - Full list</td>
<td>42</td>
<td>4.4 %</td>
<td>42</td>
<td>3.8 %</td>
</tr>
<tr>
<td>- <a href="http://www.facebook.com/l.php">http://www.facebook.com/l.php</a></td>
<td>9 9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- <a href="http://ait-open.net/elearning/mod/assignment/view.php">http://ait-open.net/elearning/mod/assignment/view.php</a></td>
<td>8 8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- <a href="http://m.facebook.com/l.php">http://m.facebook.com/l.php</a></td>
<td>3 3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- <a href="http://3cp9lcq32dpm.yom.mail.yahoo.com/om/api/1.0/openmail.app">http://3cp9lcq32dpm.yom.mail.yahoo.com/om/api/1.0/openmail.app</a>...</td>
<td>2 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- <a href="http://us.ms1.mail.yahoo.com/dc/blank.html">http://us.ms1.mail.yahoo.com/dc/blank.html</a></td>
<td>2 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- <a href="http://us.ms1202.mail.yahoo.com/mc/showMessage">http://us.ms1202.mail.yahoo.com/mc/showMessage</a></td>
<td>2 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- <a href="http://www.asianefficiency.com/wp-admin/admin.php">http://www.asianefficiency.com/wp-admin/admin.php</a></td>
<td>1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- <a href="http://us.ms3.mail.yahoo.com/dc/launch">http://us.ms3.mail.yahoo.com/dc/launch</a></td>
<td>1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- <a href="http://uk.ms295.mail.yahoo.com/mc/welcome">http://uk.ms295.mail.yahoo.com/mc/welcome</a></td>
<td>1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- <a href="http://us.ms1.mail.yahoo.com/neo/launch">http://us.ms1.mail.yahoo.com/neo/launch</a></td>
<td>1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- <a href="http://www.text-link-ads.com">http://www.text-link-ads.com</a></td>
<td>1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- <a href="http://us.ms5.mail.yahoo.com/neo/launch">http://us.ms5.mail.yahoo.com/neo/launch</a></td>
<td>1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- <a href="http://uk.ms6.mail.yahoo.com/dc/launch">http://uk.ms6.mail.yahoo.com/dc/launch</a></td>
<td>1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- <a href="http://us.ms5.mail.yahoo.com/dc/launch">http://us.ms5.mail.yahoo.com/dc/launch</a></td>
<td>1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- <a href="http://whm.joykacatering.com/scripts2/suspendacct">http://whm.joykacatering.com/scripts2/suspendacct</a></td>
<td>1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- <a href="http://uk.ms40.mail.yahoo.com/dc/blank.html">http://uk.ms40.mail.yahoo.com/dc/blank.html</a></td>
<td>1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- <a href="http://us.ms4.mail.yahoo.com/dc/launch">http://us.ms4.mail.yahoo.com/dc/launch</a></td>
<td>1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- <a href="http://www.if-20.com">http://www.if-20.com</a></td>
<td>1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- <a href="http://36ohk6dgmcd1n.yom.mail.yahoo.net/om/api/1.0/openmail.app">http://36ohk6dgmcd1n.yom.mail.yahoo.net/om/api/1.0/openmail.app</a>...</td>
<td>1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- <a href="http://heritageemp.com">http://heritageemp.com</a></td>
<td>1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- <a href="http://us.ms4.mail.yahoo.com/dc/blank.html">http://us.ms4.mail.yahoo.com/dc/blank.html</a></td>
<td>1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- <a href="http://www.orangeask.com">http://www.orangeask.com</a></td>
<td>1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Unknown Origin

Source: AWStats Analysis
Table 9: Search Key Phrases

<table>
<thead>
<tr>
<th>17 different keywords</th>
<th>Search</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>resourcefulminds.com</td>
<td>13</td>
<td>27.6 %</td>
</tr>
<tr>
<td><a href="http://www.resourcefulminds.com">www.resourcefulminds.com</a></td>
<td>10</td>
<td>21.2 %</td>
</tr>
<tr>
<td>resourcefulminds.com</td>
<td>3</td>
<td>6.3 %</td>
</tr>
<tr>
<td>Time</td>
<td>2</td>
<td>4.2 %</td>
</tr>
<tr>
<td>Resourceful</td>
<td>2</td>
<td>4.2 %</td>
</tr>
<tr>
<td>Wast</td>
<td>2</td>
<td>4.2 %</td>
</tr>
<tr>
<td>http</td>
<td>2</td>
<td>4.2 %</td>
</tr>
<tr>
<td>Contained</td>
<td>2</td>
<td>4.2 %</td>
</tr>
<tr>
<td>Information</td>
<td>2</td>
<td>4.2 %</td>
</tr>
<tr>
<td>minds.com</td>
<td>2</td>
<td>4.2 %</td>
</tr>
<tr>
<td>In</td>
<td>1</td>
<td>2.1 %</td>
</tr>
<tr>
<td>resourcefulminds.com</td>
<td>1</td>
<td>2.1 %</td>
</tr>
<tr>
<td><a href="http://www.resourcefulminds.com">www.resourcefulminds.com</a></td>
<td>1</td>
<td>2.1 %</td>
</tr>
<tr>
<td>Account</td>
<td>1</td>
<td>2.1 %</td>
</tr>
<tr>
<td>//resourcefulminds.com/</td>
<td>1</td>
<td>2.1 %</td>
</tr>
<tr>
<td>Suspended</td>
<td>1</td>
<td>2.1 %</td>
</tr>
<tr>
<td>//www.resourcefulminds.com/</td>
<td>1</td>
<td>2.1 %</td>
</tr>
</tbody>
</table>

Source: AWStats Analysis

Table 10: Distribution of Session Identification Access

<table>
<thead>
<tr>
<th>Access Patterns based on Session Identification</th>
<th>Total Number Accessed</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crime Related Access (Only)</td>
<td>20</td>
<td>6 %</td>
</tr>
<tr>
<td>Resourceful Non-Crime Related Access (Only)</td>
<td>26</td>
<td>10 %</td>
</tr>
<tr>
<td>Both Crime and Non-Crime Related Access</td>
<td>193</td>
<td>76 %</td>
</tr>
<tr>
<td>Home Page Only</td>
<td>22</td>
<td>8 %</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>259</strong></td>
<td><strong>100 %</strong></td>
</tr>
</tbody>
</table>

Source: Resourceful Minds Tracking Database

Table 11: Distribution of Registered Users

<table>
<thead>
<tr>
<th>LINKS</th>
<th>No. of Registrations</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sharewares</td>
<td>4</td>
<td>7 %</td>
</tr>
<tr>
<td>Usable Credit Cards</td>
<td>6</td>
<td>11 %</td>
</tr>
<tr>
<td>Child Pornography</td>
<td>9</td>
<td>16 %</td>
</tr>
<tr>
<td>Good Resourceful Material (Non-Crime Related)</td>
<td>28</td>
<td>50 %</td>
</tr>
<tr>
<td>Stolen Passwords</td>
<td>1</td>
<td>2 %</td>
</tr>
<tr>
<td>Illegal Games Download</td>
<td>5</td>
<td>9 %</td>
</tr>
<tr>
<td>Software Cracks</td>
<td>4</td>
<td>7 %</td>
</tr>
</tbody>
</table>

Source: Resourceful Minds Tracking Database

Tables 1 shows that about 70% of hits to the site was from Ghana with the rest spread across the world, table 2 on the other hand shows that the peak of access was in June of 2011. Googlebot turned out to provide the highest number of hits as depicted in table 3 with over 77% of hits on the site lasting less that 30 seconds as shown in table 4. Table 5 showed that the most regularly accessed link was the registration link with the least accessed being the disclaimer.

Majority of users turned to be Microsoft Windows users and the most commonly used browser was Internet Explorer as shown in tables 6 and 7 respectively. Majority of referrals were from google searches and yahoo mails as depicted in table 8 with keywords such as time and resourceful being the exact strings that lead to the page as shown in table 9.

Fig 1: Distribution of Hits on the Site
Source: Resourceful Minds Tracking Database
Table 10 shows that about 76% of users accessed links that were both crime and non-crime related. Just about 6% accessed solely for crime related purposes. Table 11 further shows that 50% of registered users did so via crime related links and the same was the case for non crime related links. The results indicate that over 70% of access to the website originated from Ghana and the United States most users accessing the sites directly with very limited access from referral sources and robots. The largest referral sources were facebook and googlebot. The most used search key phrase was resourceful minds, it is understandably so due to the method of recruiting participants. A striking trend which is worth noting is the fact that over 77% of users who visited the website were only on the site for less than 30 seconds. A significant number of users accessed from Microsoft Windows platform and also used the browsers Internet Explorer and Mozilla.

The result also indicates that the most regularly accessed links on the site were the “Homepage” and “register” links, nonetheless, a small percentage of users actually registered to gain access to more resources. Ironically, 50% of registered users accessed good resourceful material whereas 50% registered as a result of crime related material as shown in Table 11. Given the results in Table 10 which revealed that 76% of users accessed both good resourceful material and crime related material, this implies majority of users would indulge in crime related material if it is made available.

5. CONCLUDING REMARKS

This research has shown three categories of users on the website, these are those who accessed crime related sites only, users who accessed resourceful non-crime related material and lastly users indulged in both crime and non-crime related material. A significant phenomenon was the observation that half the total number of registered users registered via crime related links. This phenomenon confirms assertion that as more people become aware of, and exposed to, a range of opportunities to commit various illegal and socially questionable behaviours, the total number of cyber crimes is very much likely to increase in number.

REFERENCES


Authors’ Briefs

Paul Asante Danquah is a Lecturer with the Faculty of IT, Pentecost University College. His has a background of MSc Information Security from Anglia Ruskin University (UK), BSc HONs in Computing from the University of Greenwich (UK), Graduate Diploma in MIS and the professional certifications MCSE and CCNP. He is a PhD candidate under the supervision of Dr. Longe Olumide at the Accra Institute of Technology, Ghana. Name: He can be reached at padanquah@ait.edu.gh.

Dr. Longe Olumide is on Faculty at the Department of Computer Science, University of Ibadan, Nigeria. His research has focused on using social theories and computer security theories to explain causation and apprehension of cyber crimes. He is currently a Fulbright Fellow at the International Centre for Information Technology & Development, College of Business, Southern University’, Baton Rouge, LA, USA. He can be reached by phone on +18572078409 and through E-mail longeolumide@fulbrightmail.org

Mr. Fred Totimeh is an Lecturer at Pentecost University College Ghana, with over twenty years industry experience as an IT Manager and a Programmer with Ghana Prisons Service and Office of the Ghanaian President respectively, he is a Masters Degree student in Information Technology at Sikkim Manipal University. He holds a Bsc. HONS in Computer Science degree and Postgraduate Certificate in Business Administration. He can be reached at ftotimeh@yahoo.com.
The African Journal of Computing & ICTS.

Call for Papers

The African Journal of Computing and ICT (AJCICT) was established by the Nigeria Computer section of the Institute of Electrical and Electronics Engineers (IEEE) Inc, New York, USA. Afr. J of Comp and ICT publishes both online and print editions in April, August, December. The Journal solicits original research articles from interested authors for her upcoming editions. The goal of the journal is to contribute to rapid IT developments in Nigeria, Africa and the world through the publication of topical and relevant papers from theoretic/academic and practical / industrial points of view. Submitted papers should contain substantial ideas which have the potential of aiding an invention or a technological breakthrough for general and specialized use.

SCOPE OF ARTICLES

Papers are welcome from pure/applied computing and ICT, and allied areas including but not limited to software engineering, computer communication/networks, human computer interaction, data mining, discrete/data structures, design & analysis of algorithms, web security, systems architecture, ubiquitous computing, systems design, information systems, bioinformatics, information management, information science and e-systems (e-health, e-learning, e-government).

The journal considers original research papers, case reports and review papers. Authors must clearly justify the importance of their submission to the readership of the journal. Prospective authors need not be a member of the (Computer Chapter) IEEE Nigeria Section before his/her paper is published. All papers are peer refereed and authors of accepted paper(s) will be required to sign copyright forms before papers are published. The AJCICT Publication guideline is on the next page(s).

SUBSCRIPTION DETAILS

Pagination Fees and Information for Subscribers And Advertisers

Authors of accepted papers will be charged a pagination fee of $150 (N20000). The subscription fee for yearly volumes of the journal to institutions and organizations is US $200 (N30000 Naira) excluding postage. Copies of individual volumes can be obtained at a cost of $50 (N5000) Correspondence on paper publications, book review, subscription and advertisement should be directed to the Dr. Longe Olumide. Vice Chairman, IEEE Computer Section Nigeria and Managing Editor, African Journal of ICT. Request for information pertaining to the Computer Chapter of the IEEE Nigeria Section should be sent to the Chair of the Chapter, Prof. ‘Dele Oluwade (bamideleoluwade@computer.org).

General information on the aim and objective as well as membership of IEEE, IEEE Computer Society and the IEEE Nigeria Section can be found on the following websites respectively: http://www.ieee.org; http://computer.org; http://www.ieee.org/nigeria.
Publication Template

African Journal Of Computing and ICT  IEEE Nigeria – Computer Section Journal

Paper Title (font Size 24)
Space (14 points font size)
Author’s names (12 Points Font Size Bold)
Affiliations (10 Points Font Size)
E-mail Address and Phone Numbers (10 Points Font Size Italicize)

ALL SECTIONS ABOVE IN A SINGLE COLUMN FORMAT

Abstract
This electronic document is a “live” template. The various components of your paper [title, text, heads, etc.] are already defined on the style sheet, as illustrated by the portions given in this document.

Keywords- component; formatting; style; styling; insert

1. INTRODUCTION
All manuscripts must be A4 size paper, one inch top and bottom margin and 0.75 left and right margins. It should be written in English. These guidelines include complete descriptions of the fonts, spacing, and related information for producing your manuscripts for publication. Follow the style in this template for preparing your articles/papers/manuscripts for submission.

2. TYPE STYLE AND FONTS
Times New Roman 10 points is the acceptable font for typesetting the entire body of the manuscript. If this is available on your word processor, please use the font closest in appearance to Times. Pictures and graphics, preferably in Jpeg format or Bitmap format can be embedded as well as mathematical and scientific symbols. Equations should be numbered and acronyms/abbreviations should be explained/defined or written fully on first use.

3. CITATIONS IN THE BODY OF THE WORK
Referencing style in the body of the work should use square [7 ] braces. Works cited should be listed in the bibliography/referencing section at the end of the paper chronologically. Footnotes are not encouraged.

3.1 Main and Sub-Headings
Main Headings should be in UPPERCASE and proceeded by a point number. For Sub-Headings, use toggle case – or capitalize the first letter of each sentence/sub heading. Sub headings should be bold and italicised. Provide a space between each section and sub-sections.

3.3 Columns
Submission MUST follow the two column format depicted in this document. Equal width of 3.38cm and column spacing of 2.5cm. Lines are not allowed between columns. Where necessary or unavoidable, the two column format can be merged to a column to accommodate pictures, tables or graphics.

3.4 Paragraphing
The block structure is adopted for this journal.

4. TABLES AND FIGURES
Table headings/titles should be written above the tables. Figure headings should be written below the tables. These titles should proceed sequentially within the body of the text. Fig. 1 for the first figure, the next Fig 2 etc. Figures should not be numbered based on subsections of the manuscripts. Tables should also be labeled in the same sequence. Centralize Figures. Align Tables to the LEFT.

Table 1: How To Set Tables

<table>
<thead>
<tr>
<th>Table Head</th>
<th>Table Column Head</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy</td>
<td>More table copy</td>
</tr>
</tbody>
</table>

Source – [5]

Figure 1. Example of a figure Caption

4.1 Units
The SI Unit is the acceptable Unit for specifying scientific measurements in this journal.
4.2 Equations

Authors are encouraged to use the equation editor facilities provided in MS Word to prepare equations for the manuscript. In very extreme situations, you may use either the Times New Roman or the Symbol font (please no other font) to prepare equations for publications. To create multileveled equations, it may be necessary to treat the equation as a graphic and insert it into the text after your paper is styled. Equations should be numbered equations consecutively. Equation numbers, within parentheses, are to position flush right, as in (1), using a right tab stop. To make your equations more compact, you may use the solidus ( / ), the exp function, or appropriate exponents. Italicize Roman symbols for quantities and variables, but not Greek symbols. Use a long dash rather than a hyphen for a minus sign. Punctuate equations with commas or periods when they are part of a sentence. For example:

Align equations to the left.

Acknowledgement

A section on acknowledgement for sponsored research, collaborations, funds, grants/ other research material sources

REFERENCES

List and number all bibliographical references in 10 point Times, single-spaced, at the end of your paper. When referenced in the text, enclose the citation number in square brackets, for example [1] where appropriate, include the name(s) of editors of referenced books.

Unless there are more than 3 authors or more give all authors’ names; do not use “et al.”. Papers that have not been published, even if they have been submitted for publication, should not be cited [4]. Papers that have been accepted for publication should be cited as “in press” [5]. Capitalize only the first word in a paper title, except for proper nouns and element symbols. For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation [6].

[8] Electronic Publication: Digital Object Identifiers (DOIs):
Article in a journal:
Template Adapted from -
http://www.computer.org/portal/web/cscps/frmatting
The African Journal of Computing & ICT

All Rights Reserved
© 2012

Published for the Institute of Electrical & Electronics Engineers (IEEE)
Nigeria Section Computer Chapter

By
The Trans-Atlantic Management Consultants
2580 Fairham Drive
Baton Rouge LA, USA

For further enquiries please contact
Dr. Longe Olumide
Department of Computer Science
University of Ibadan
Ibadan, Nigeria
Email: submissions@ajocict.net or longeolumide@fulbrightmail.org
Tel: +2348024071175

USA – Contact Information
Dr. Longe Olumide
Fulbright SIR Fellow
Int. Centre for IT and Development
Southern University System
Baton Rouge, Louisiana, USA
Email: submissions@ajocict.net or longeolumide@fulbrightmail.org
Tel: +18572078409