ITB Journal

Issue Number 3, May 2001

Contents

Editorial 3

Market Orientation: The Implementation of The Marketing Concept 4
Maura O Connell. Institute of Technology, Blanchardstown.

The Role of Cryptography in Security for Electronic Commerce 21
Ann Murphy. Dublin Institute of Technology
David Murphy. Institute of Technology Blanchardstown

Passive Voice Constructions in Modern Irish. 51
Brian Nolan. Institute of Technology Blanchardstown, Dublin

An evaluation of CAN8 as a Computer Assisted Language Learning tool in the context of current research. 79
Ruth Harris. Institute of Technology Blanchardstown, Dublin

The academic journal of the Institute of Technology Blanchardstown

Papers for submission to the next ITB Journal should be sent to the editor at the address below. Alternatively, papers can be submitted in MS-Word format via email to brian.nolan@itb.ie

Brian Nolan

Editor

ITB Journal

Institute of Technology Blanchardstown

Blanchardstown Road North

Blanchardstown

Dublin 15

Editorial

It gives me great pleasure to introduce you to this, the third edition of the ITB Journal, the academic journal of the Institute of Technology Blanchardstown. It uniquely offers the opportunity for the members of ITB, visitors and guest contributors to publish an article on their research in a multidisciplinary journal. The hope is that by offering the chance to bring their work out of their specialised area into a wider forum, they will share their work with the broader community at ITB and other academic institutions.

In this issue we have again have papers treating a wide range of subject matter. Maura O Connell examines aspects of Market Orientation and the Implementation of the Marketing Concept. Ann Murphy of DIT and David Murphy of ITB explore, in a joint paper, the very topical and important subject of the Role of Cryptography in Security for Electronic Commerce. Brian Nolan undertakes a linguistic analysis of the passive constructions in modern Irish and finds that an event based perspective sensitive to prototypicality provides a means of delivering a unifying these constructions. An interesting paper by Ruth Harris offers an evaluation of CAN8 as a Computer Assisted Language Learning tool in the context of current research.

We hope that you enjoy the papers in this edition of the ITB Journal.

Brian Nolan
Editor
ITB Journal
Institute of Technology Blanchardstown
Blanchardstown Road North
Blanchardstown
Dublin 15

Market Orientation:

The Implementation of the Marketing Concept

Maura O Connell. Institute of Technology, Blanchardstown.

Introduction

The marketing literature has provided little guidance in relation to creating market driven organisations. It has traditionally provided pieces of the puzzle i.e. the product life cycle, segmentation etc, but it has fallen short of demonstrating how to put the pieces together to complete the picture i.e. creating a market oriented organisation. As a result marketing has largely been confined to 'overseeing and co-ordinating activities directly involved with the outside - such as sales, promotion and delivery' (Witcher B J, 1990). This has led to a situation where many organisations have reservations about the success achieved with the implementation of the marketing concept (Darden and Barksdale 1971).

Marketing needed to be brought out of the marketing department and into a position where it is the concern of all employees and is a top priority throughout the company. Until the late 1980's it was unclear exactly what a market orientation was. Since then, a number of empirical studies have investigated the concept and a sizeable body of work has been published (Day 1990; Kohli & Jaworski 1990/3; Narver & Slater 1990; Deshpande 1993; Webster 1992) There is general agreement on the components of market orientation but very little on how to successfully develop it. The following definition was proposed by Kohli and Jaworski 1990 :

'*Market orientation is the organisation wide generation of market intelligence pertaining to current and future customer needs, dissemination of the intelligence across departments and organisation wide responsiveness to it'*. Similarly Day (1994) says that market driven organisations have superior market sensing, customer linking

and channel bonding capabilities. Let us now look at the components of market orientation.

1. Market Sensing / Generation of Market Intelligence

In its narrowest sense market sensing involves obtaining information from customers on their needs. However to be truely market oriented a company needs to examine any factor that might affect customers needs in the present or in the future. This involves monitoring not just expressed customer needs but also the competitive, technological, political, legal and economic environments of the customer and company. The information should be conducted by all functional areas on both a formal and informal basis. This information should be held in company memory e.g. via a database and should be easily accessible for decision making throughout the organisation. In this way the organisation will be able to anticipate customer needs as well as satisfy current ones.

While companies proclaim an external focus, the reality is that most organisations are internally focused (Kordupleski, Rust and Zahorick 1993). Even those exceptional firms which have an external focus are inclined to concentrate on current issues - often technical in nature.

2. Dissemination of Intelligence

Unless market information is communicated throughout the organisation it is of little use in decision making. A market-oriented company makes information available at the point of contact with the customer. It can also be achieved via cross-functional teamworking, flatter hierarchies and employee empowerment. This type of organisational structure enables rapid dissemination of information throughout the firm. Empirical studies have shown that interdepartmental connectedness and decentralised decision making are positively related to market orientation (Kohli & Jaworski1993)

Responsiveness to Market Intelligence

Responsiveness requires application of the marketing tools to elicit favourable market response. These tools take the form of segmenting and selecting target markets, designing products, setting pricing strategies etc. Unfortunetly frontline employees generally do not have sufficient knowledge of marketing, the company markets or marketing strategy to be able to take on this responsibility with marketing decisions. It would require extensive training e.g. before an operative could decide to develop a new product as a response to a customer problem. Responsiveness requires an innovative corporate culture and a positive attitude toward risk (Kohli & Jaworski 1993). To create a market-oriented company a certain level of guidance is needed from the top. An integrated approach needs to be taken to decision making i.e. a combination of top down strategy development and bottom up employee empowerment. Frontline employees should be able to make everyday decisions pertaining to the customer via cross-functional teamworking but management should set the broad marketing strategies. To achieve this employees would need to be taught to recognise the significance of certain types of market intelligence and how to respond to it, in the same way that they have learned to recognise important information on quality and the appropriate responses to take.

The following study aims to gain further insights into the concept of market orientation by examining the pre-requisites to its development in Irish companies.

Research Design

The study was undertaken with firms in the Irish Print industry to examine some of the essential elements and consequences of a market orientation. The researcher used a judgement sampling procedure, based on extensive knowledge of the industry, to choose companies that varied in size and industry subsector. The sample size was 22. Data was gathered via a postal survey. The questionnaire was addressed to the managing director because it was felt s/he would have a less biased view than the marketing manager when it came to the companies degree of market orientation. Over

70% of the sample firms were found to be strongly market oriented i.e. they scored 3.55 or more on a scale of 1-5. The remainder were found to have a weak market orientation. For the remainder of this paper these firms will be referred to as strong and weak respectively. Data was analysed using the statistical package SPSS.

Measurement

Market Orientation

Market orientation was measured using scales devised by Kohli and Jaworski (1993). Twenty of the original thirty-six scales were used (see appendix A).

Business Performance

One measure of business performance was chosen i.e. Net operating profit margin. This measure was deemed appropriate because the industry was experiencing a period of severe recession coupled with market / technological transition. It was felt net operating profit margin would provide a true measure of business performance since it disregards extraordinary items such as acquisitions. This was an important consideration because there was a move towards consolidation in the industry at the time. While this is not a comprehensive measure it was sufficient to enable a tentative examination of the relationship between market orientation and business performance.

Hypotheses

The author set out to test the following Hypotheses:

H_1 Market orientation varies with the number of marketing personnel employed.

H_2 Interdepartmental conflict has a negative effect on market orientation.

H_3 Risk aversion has a negative effect on market orientation.

H_4 Strongly market oriented companies pursue more aggressive growth strategies than companies with a weak market orientation.

H5 Market orientation is positively related to superior business performance.

H6 Top management support is critical in fostering a market orientation.

Discussion

H1. Market orientation varies with the number of marketing personnel employed

One would expect that the more marketing personnel an organisation employed, the greater the liklihood that firm would be market oriented.

H2 Interdepartmental conflict has a negative effect on market orientation.

An empirical study found that the less conflict there was between departments, the greater was the market orientation of the firm (Kohli & Jaworski 1993). This finding supports the idea of integrated marketing deemed to be so important in many marketing texts (Kotler 1994, p 756). Many scholars have put forward the view that interdepartmental conflict may be detrimental to the implementation of the marketing concept as it inhibits communication between functional areas (Levitt, 1969; Lusch, Udell and Laczniak 1976; Felton 1959). Information dissemination is a vital component of market orientation and it is therefore important for firms to develop a degree of interdepartmental connectedness to facilitate the dissemination of and responsiveness to market intelligence.

H3 Risk aversion has a negative effect on market orientation .

A market orientation requires response to market intelligence, which often requires developing strategies for the introduction of new products or for the use of innovative marketing techniques. Therefore managers must be willing to take some risks in order to be successful. Where managers are very risk averse, the market orientation of the company is likely to be diminished. Rogers supports this proposition (1983, p 260),

reporting that in 43 of 57 studies a positive relationship was found between risk aversion and the degree of market orientation.

H_4. Market oriented companies pursue aggressive growth strategies.

If market oriented companies have a positive attitude toward risk, then it is likely that they will also pursue more aggressive marketing objectives.

H_5 Market orientation is positively related to superior business performance.

The marketing literature has long espoused the relationship between the application of the marketing concept and superior business performance. However since there was no real measure of market orientation until recent years it was impossible to empirically test this proposition. A 1990 study (Narver & Slater) found that firms with a strong market orientation had higher return on investment than companies with a weak market orientation. They also found that strong firms were better at retaining customers and that they were associated with the highest profitability. A similar study (Deshpande et al 1993) found that market orientation was a key determinant of business performance.

While these findings provide a first step in validating the posited relationship between market orientation and business performance, they are far from conclusive. In order to increase confidence in the results, the studies need to be replicated in diverse environments over time. Hence the inclusion of H_5 in this study.

H_6 The role of senior management is critical in fostering a market orientation.

Webster (1988 p37) asserts that customer oriented values and beliefs are "uniquely the responsibility of top management." Likewise Felton (1959, p55), asserts that the most important ingredient of a market orientation is an appropriate state of mind and that it is attainable only if the board of directors " appreciate the need to develop this marketing state of mind.'' Other authors concentrate on the need for top management

to communicate the message (Day, 1990 p 369; McNamara, 1972 p 55-6), by deeds and time invested in marketing activities. If the words are not consistent with actual behaviour the organisation soon learns the real priorities of top management and acts accordingly. Unfortunately many senior managers pay lip service to marketing and then wonder why their organisations are not market driven. This gap between word and action can be clearly seen in table 1, drawn from a study of 236 CEOs of Fortune 1000 companies:

Table 1 CEO Concerns and Priorities
(% of CEOs answering 'YES')

	'Is this function very important to corporate growth and profit	'Do you have considerable involvement with the following functions
Financial Planning	57%	46%
Customer relations	57	14
Production / Manufacturing	42	9
New Product Development	**41**	**8**
Research and Development	36	7
Labour Relations	28	5
Personnel Management	26	5
Market Analysis	**24**	**3**

Source: Richard T. Hise and Stephen W. McDaniel, "American Competitiveness and the CEO - Who's Minding the Shop," Sloan Management Review, 30 (Winter, 1988), 49-55.

It is not only important, therefore, for top management to be market oriented but they must also demonstrate it in action and deed.

Results of the Study

Market Orientation and Marketing Personnel

64% of sample firms did not employ any full-time marketing personnel. A cross tabulation of marketing personnel by degree of market orientation produced the following results:

Table 2 Marketing Personnel

No. of Marketing Personnel employed	None	One	Two	Three+
Strong Firms	60%	17%	23%	-----
Weak Firms	80%	20%	-----	-----

A chi - square test showed no significant difference between weak and strong firms in terms of numbers of marketing personnel employed.

These findings are very interesting because although the majority of respondent firms were found to be market driven, 60% did not employ any marketing professionals. Companies that did employ professionals were not found to be significantly different from companies that did not employ professionals, in terms of degree of market orientation. This supports much of the marketing literature which espouses the idea that marketing should not be the sole responsibility of the marketing department but rather the concern of all company departments (Kotler, 1994;.Felton,1959; McNamara, 1972).

Market Orientation and Interdepartmental Conflict / Connectedness

The average score for strong firms was 4.19. A t-test indicated, at the 95% confidence level, that strong firms enjoyed a greater degree of interdepartmental connectedness than weak firms. This is not a surprising finding since information dissemination, which is an integral component of market orientation, can only successfully occur if there are open lines of communication within an organisation.

Market Orientation and Risk Aversion

Only 27% of respondent firms received a strong score for positive attitude toward risk. A t-test confirmed with 95% confidence that strong firms were more inclined to have a positive attitude toward risk than companies with a weak market orientation. This supports kohli and Jaworski's (1993) finding that risk aversion has a negative effect on market orientation. It should be noted however that only 27% of respondents had a positive attitude toward risk and therefore it would not appear to be a prerequisite of market orientation. It may be the case that a positive attitude toward risk occurs in the later stages of market orientation development, while companies concentrate on 'safer' tasks like gathering information and opening lines of communication during the earlier stages.

Market Orientation and Company Objectives

A chi-square test indicated that strongly market oriented companies pursue more aggressive goals than companies with a weak market orientation. This was found to be significant at the 95% confidence level.

Table 2 Company Objectives

Objective	Weak	Strong
Generate good short term profits	***60%***	***----***
Defend position	***20%***	***6%***
Pursue steady growth	***20%***	***70%***
Pursue aggressive growth	***---***	***24%***
Dominate market	***---***	***---***

The author found that 94% of strongly market oriented companies pursued growth strategies, while only 20% of weak firms did. This provides tentative support for the hypothesis in relation to risk aversion i.e. that market oriented companies are inclined to be more aggressive.

Market Orientation and Business Performance

A t - test of net operating profit margin by degree of market orientation indicated that strong firms performed significantly better than weak firms on this variable. Strong firms averaged profit margins of between 21 - 25%, while weak companies only averaged between 6 - 15%. The author can say with 95% confidence that strongly market oriented print firms enjoy greater profitability than firms with a weak market orientation.

This supports findings by Narver and Slater (1990) and Deshpande, (1993), who also found a positive link between strong market orientation and profitability. This is an interesting finding as very few empirical studies have examined this, much spoken about, relationship.

Market Orientation and Top Management Support

The author found top management support of 'marketing' to be present in the majority (82%) of firms, regardless of their degree of market orientation. There was no significant difference found between weak and strong firms on this variable. The author feels this is because the measurement scales used in this study measure lip service rather than true management support. The scales used were as follows:

1. **Top managers repeatedly tell employees that this business and its survival depends on its adapting to market trends.**
2. Top managers often tell employees to be sensitive to the activities of our competitors.
3. **Top managers keep telling people around here that they must gear up now to meet customers future needs.**
4. According to top managers here, serving customers is the most important thing our business unit does.

An investigation of the relationship between top management support and market orientation would require that the scales measure actual top management support i.e. actions as well as words (Day, 1990).

Summary

Irish firms have shown similar results to those previously found i.e. interdepartmental connectedness and a positive attitude toward risk appear to be pre - requisites of a strong market orientation. Additionally this study has demonstrated that the number of marketing personnel employed is not related to the degree of market orientation and that market oriented firms are more inclined to pursue aggressive growth strategies. Finally these findings support the proposition that market orientation is positively related to superior profitability.

Research Agenda

This research highlights some research topics which need to be addressed including:

1. Investigation of organisations that have successfully managed the transition from marketing department to market orientation.

2. Identification of the key capabilities/ skills required to develop a market orientation.

3. Development of tools / formulae to enable employees to become empowered to make marketing decisions.

References

Barksdale, Hiram C. and Bill Darden(1971), "Marketers Attitude toward the Marketing Concept," Journal of Marketing, 35(October), 29-36.

Day, George S.(1990), Market Driven Strategy: Processes for Creating Value. New York: The Free Press, pp15-18, 369.

Day, George S.(1994), '' Managerial Representations of Competitive Positioning,'' Journal of Marketing, 58 (April), 31-44.

Deshpande, Rohit, John U. Farley, and Frederick E. Webster, Jr.(1993), "Corporate

Culture,Customer Orientation and Innovativeness in Japanese Firms : A Quadrad Analysis," Journal of Marketing, 57(January), 23-27.

Felton, Arthur P.(1959), " Making the Marketing Concept Work," Harvard Business Review 37 (July-August), 55-65.

Hise, Richard T.(1965), "Have Manufacturing Firms Adopted the Marketing Concept?". Journal of Marketing, 29(July), 9-12.

Hise, Richard T. and Stephen W. McDaniel, "American Competitiveness and the CEO – Who's Minding the Shop," Sloan Management Review, 30(Winter 1988),49-55.

Jaworski, Bernard J. & Ajay K. Kohli(1990), " Market Orientation; The Construct, Research Propositions and Management Implications," Journal of Marketing, 54(April), 1-18.

Jaworski, Bernard J. and Ajay K. Kohli (1993), "Market Orientation: Antecedents and Consequences," Journal of Marketing, 57(July), 53-70.

Kordupleski, Raymond E., Roland T. Rust, and Antony J. Zahorik (1993). '' Why Improving Quality Does'nt Improve Quality or Whatever Happened to Marketing?'' California Management Review (Spring), 82-95.

Kotler, Philip (1994), Marketing Management, Englewood Cliffs, NJ : Prentice Hall, Inc.

Levitt, Theodore(1969), The Marketing Mode. New York : McGraw Hill Book Company.

Lusch, Robert F., Jon G. Udell, and Gene R. Laczniak(1976), "The Practice of Business," Business Horizons, 19(December), 65-74.

McNamara, Carlton P.(1972), "The Present Status of the Marketing Concept," Journal of Marketing, 36 (January), 50-57.

Narver, John C. and Stanley F. Slater (1990), " The Effect of a Market Orientation on Business Profitability." Journal of Marketing, 54(October), 20-35.

Rogers, Everett M. (1983), Diffusion of Innovations, Third Edition. New York; The Free Press.

Peters, Thomas J. (1989), Thriving on Chaos, Handbook for a Management Revolution. Pan MacMillan London.

Webster, F.E., Jr.(1992), '' The Changing Role of Marketing in the Corporation,'' Journal of Marketing, 56 (October), 1-17.

Witcher Barry J. (1990), 'Total Marketing : Total Quality and the Marketing Concept,' The Quarterly Review of Marketing (Winter)

Appendices

Research Instrument

Section A Company Overview

1. Please indicate which of the following best describes your business
   (Please tick one only)

❒Security / Form printing
❒Magazines / Journals
❒Greeting / View cards
❒Instant / Demand printing
❒Pharmaceutical printing
❒Screen printing
❒Computer manuals
❒Book printing
❒General printing

2. Current employment _____

3. Current turnover

❒Less than £ 100,000
❒£100,000 - £250,000
❒£250,000 - £500,000
❒£500,000 -£2m
❒£2m - £5m
❒Over £5m

4. Which of the following best describes your company's current objective?
   (Please tick one only)

❒Generate good short-term profits
❒Defend position
❒Generate steady growth
❒Pursue aggressive growth
❒Dominate market

Section B-Gathering Intelligence

Please indicate how strongly each of the following statements reflect your business

(1= strongly agree 3= Neutral/Don't Know 5= Strongly disagree)

We meet with customers at least once a year to find out

-What products they will need in the future.	1	2	3	4	5
-We conduct a lot of in-house market research.	1	2	3	4	5
-We conduct on going customer satisfaction surveys	1	2	3	4	5
-Individuals from our manufacturing department interact directly with customers to learn how to servethem better.	1	2	3	4	5
-We collect industry information via informal means (e.g. lunch with industry friends).	1	2	3	4	5
-We have a formalised system for collection of data on competitors.	1	2	3	4	5
-We are slow to detect fundamental shifts in our industry.	1	2	3	4	5

Section C - Dissemination of intelligence

-A lot of casual talk concerns our competitor’s strategies.	1	2	3	4	5
-We have interdepartmental meetings at least once a quarter to discuss market trends and developments.	1	2	3	4	5
-Data on customer satisfaction are disseminated at all levels in the business on a regular basis.	1	2	3	4	5
-There is minimal communication between marketing and manufacturing departments concerning market development.	1	2	3	4	5

Section D-Responsiveness to Intelligence

-For one reason or another we tend not to respond to changes in customers needs *(e.g. lower prices, new products/services)*	1	2	3	4	5
- Departments get together to plan responses to changes taking place in the marketplace.	1	2	3	4	5
-Our business plans are driven more by production capability than by market research.	1	2	3	4	5
We annually produce a written marketing plan.	1	2	3	4	5
When we come up with a great marketing plan we have difficulty implementing it in a timely fashion.	1	2	3	4	5
Niche marketing drives new product development.	1	2	3	4	5
We review our new product development plans on an on-going basis	1	2	3	4	5
We are quick to respond to significant changes in our competitors pricing structures.	1	2	3	4	5
If a major competitor were to launch an intensive campaign targeted at our customers we would implement a response immediately.	1	2	3	4	5

Section E- Antecedents of Market Orientation

Top managers repeatedly tell employees that the business & its survival depends on its adapting to market trends.	1	2	3	4	5
Top management feel serving customers is the most important thing the business does.	1	2	3	4	5
Top managers encourage the development of innovative marketing plans knowing well that some will fail.	1	2	3	4	5
Top managers implement plans only if they are very certain they will work.	1	2	3	4	5
Top managers accept occasional new product failures as normal	1	2	3	4	5
Most departments get along well with each other	1	2	3	4	5
Protecting one's departmental turf is considered a way of life in this business.	1	2	3	4	5
The objectives pursued by the marketing department are often incompatible with those of the manufacturing department.	1	2	3	4	5
The marketing department has equal standing with the production department.	1	2	3	4	5
Managers discourage employees from discussing work related matters with those who are not their immediate superior /subordinate	1	2	3	4	5
Employees from different departments feel comfortable calling each other when the need arises.	1	2	3	4	5
Sales people s monetary compensation is based almost entirely on sales volume.	1	2	3	4	5
Customer satisfaction assessments influence senior managers pay in this business.	1	2	3	4	5

Section F

Do you feel you supply more or less the same products / services as your main competitors?

❒Yes ❒No

Can your new products be easily be imitated by competitors ?

❒Yes ❒No

Please indicate which of the following best-described company performance in 1994

Sales Growth	-20%	-10%	0%	+10%	+20%	20%+
Op.Profit Margin	0-5%	6-10%	11-15%	16-20	21-25%	26%+

How many (if any) full time marketing personnel do you employ (not including sales people)

❒None ❒One ❒Two ❒Three or more

THANK YOU FOR YOUR CO OPERATION

The Role of Cryptography in Security for Electronic Commerce

Ann Murphy. Dublin Institute of Technology
David Murphy. Institute of Technology Blanchardstown

Abstract

Many businesses and consumers are wary of conducting business over the Internet due to a perceived lack of security. Electronic business is subject to a variety of threats such as unauthorised access, misappropriation, alteration and destruction of both data and systems. This paper explores the major security concerns of businesses and users and describes the cryptographic techniques used to reduce such risks.

Keywords

Internet, Web Security, cryptography, hackers, public and private keys, PKI, CAs, Client Security, Server Security, DES, RSA, digital signature, SSL, SET

Introduction

Most organisations either utilise the Internet for business purposes already or intend doing so in the very near future (Ernst & Young, 1998). As the importance of information systems for society and the global economy intensifies, systems and data are increasingly exposed to a variety of threats, such as unauthorised access and use, misappropriation, alteration and destruction (OECD, 1999). The main concern cited by most decision- makers when it comes to e-commerce is the threat of computer security, or rather the lack thereof (Foresight, 1998; Hawkins *et al.*, 2000). The Internet has frequently been viewed as an unregulated, unsafe place to do business (Cross, 1999) and for all practical purposes comes with a 'use at your own risk' label (Labuchagne & Eloff, 2000). Things are not getting safer, now that more networks and PCs are linked via high-speed, always-on connections, hackers now enjoy a 24 hour window of opportunity to break into Internet-based systems, and it is difficult for companies to keep up with the latest security options (Dysart, 2000). Recent virus outbreaks such as Melissa and ILOVEYOU and web-site attacks against Yahoo,

Amazon and eBay indicate that security issues must become a primary concern for everyone doing business on the Internet (McGuire & Roser, 2000).

When networked information systems perform badly or don't work at all, lives, liberty and property can be put at risk. Interrupting service can threaten lives, while the disclosure or destruction of information or it's improper modification can disrupt the work of governments, corporations and individuals (Schneider, 1998).

Web security means different things to different users. For researchers it is the ability to browse the Web without interference. For businesses and consumers, it is the capability to conduct financial and commercial transactions safely, with confidence that neither the information, connections or sites have been interfered with. Many users need to operate with the conviction that the credentials of all parties can be verified and validated. In the Electronic Commerce Report (2000), Adams and Bond summarised the facilities required from an Internet based infrastructure as:

1. *Confidentiality* – the ability to keep things secret from prying eyes
2. *Integrity* – the ability to protect information from authorised changes or to be able to detect if such changes have occurred
3. *Authentication* – that the identities of all parties are assured
4. *Non-Repudiation* – that neither the sender nor receiver can deny communication
5. *Copy Protection* – from unauthorised copying of intellectual property
6. *Availability* – ensuring that access to information or services are available as and when required
7. *Legal Admissibility* – the capability of providing irrefutable evidence that a particular transaction has occurred.
8. *Standards Based* – maximum use of industry-accepted standards

The quality of security for information and communication systems and the data that is stored and transmitted on them depends not only on the technical measures, including the use of both hardware and software tools, but also on good managerial, organisational and operational procedures (OECD, 1997; 1999)

This paper examines the major security concerns of businesses and consumers engaging in electronic commerce and focuses principally on the role of cryptography in reducing the risk of conducting business on the Internet. The techniques and terminology used by cryptologists, including private and public key encryption and their use and advantages in securing both information and systems are described in detail. The issues involved in authentication using digital signatures and Certification Authorities are discussed, as are the issues involved in key management.

The Internet

Brief History

The web has emerged as the most dynamic force in the Information Technology (IT) industry during the past decade. This growth has been facilitated by the confluence of increasingly powerful and inexpensive technologies that permitted large-scale usage and the provision of scalable systems and applications, allied with the growing availability of telecommunications due to declining costs and increasing bandwidth thereby allowing the spread of digital information (Salnoske, 1998).

Benefits to Business

Greenstein and Feinman (2000) identify potential benefits to business which include :

1. Internet and web-based electronic commerce is more affordable and hence allows more business partners to be reached than with traditional electronic data interchange (EDI).
2. A geographically dispersed customer base is available
3. Procurement processing and purchasing costs can be lowered
4. Reduction in inventories with lower cycle times and
5. Better customer services with lower marketing and sales costs

Benefits to Consumers

Consumers benefit in a number of ways such as :

1. Increased choice of vendors and products
2. Convenience coupled with competitive prices and increased price comparison capabilities

3. Greater amounts of information that can be accessed on demand
4. Customisation in the delivery of services

   (US Department of Commerce, 1998).

Web Security

While technology can deliver innumerable benefits, it introduces new vulnerabilities that can be exploited by persons with the necessary technical skills. Hackers represent a well-known threat, but increasingly other criminal elements must be taken into consideration (Furnell, 1999). An international survey carried out in 1998 reported that 73% of all companies reported some security breach or corporate espionage during the previous 12 months. Companies carrying out their business electronically were significantly more likely to be victims of security loss that affected their revenues and corporate data than traditional businesses (Information Week, 1998). The joint annual study between the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI) has shown that verifiable losses in 1999 soared to $265.6 million, more than double the total reported for the three years 1996 to 1998 inclusive (Gold, 2000). Over 90% of respondents had detected some form of security attack on their computer systems during the year– denial of service (32%), sabotage of data or networks (19%), financial fraud (14%), insider abuse of Internet access privileges (97%), virus contamination (90%), (CSI Press Release, 1999).

While outside intruders are perceived by the world to be the largest threat to security, FBI studies have revealed that 80% of intrusions and attacks come from within organisations (Price, 1999). An insider is someone who has been (explicitly or implicitly) granted privileges that authorise them to use a particular system of facility. Insider misuse involves misuse of authorised privileges. Insiders may have better knowledge of system vulnerabilities and the whereabouts of sensitive information (Neuman, 2000).

Nonetheless, to understand the security threats involved in using the Internet for communications, it is essential to understand that there are threats evident at different parts of the infrastructure used for electronic commerce.

Web system infrastructures are composed of three parts :

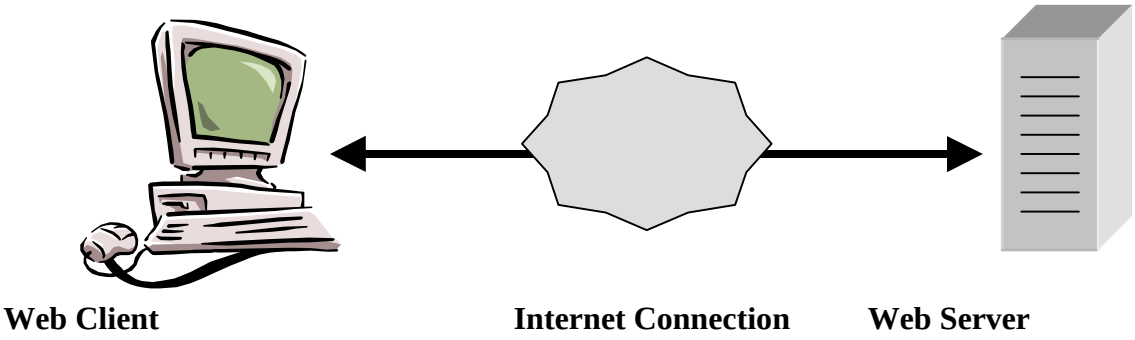


Figure 1: Web Infrastructure (Stein, 1998)

1. The Web Client[1]
2. The Web Server
3. The Connection between the two

Regarding security, the entire system is only as strong as the weakest link in the chain (Budge, 1998). Stein (1998) proposes that the integrity of the system relies on the following assumptions:

From the User's (Client's) Viewpoint

1. The Web Server is owned and operated by the organisation that claims to own it.
2. The documents returned in response to the user's request are free from viruses.
3. The remote server will not use any information either knowingly or unknowingly provided by the user for any purpose other than that required by the transaction. Examples of this type of information would include credit card details or browsing habits.

From the Web Servers Viewpoint

[1] In Business to Business Transactions, the Web Client also acts as a Server

1. The user will not attempt to alter the contents of the Web site.
2. The user will not attempt to break into the Servers Computer system.
3. The user will not try to gain access to unauthorised areas of the site.
4. The user will not try to crash the server thereby making it unavailable to other users
5. That the user is who they claim to be.

From Both Parties Viewpoint

1. That the connection is free from third parties listening in on the communications line.
2. That the information sent between browser and server is delivered intact and free from tampering.

Section 4 describes the role of cryptography in addressing some of these issues, in particular those of information integrity and user and server authentication.

Cryptography

The ability to conduct all kinds of transactions across open information and communication networks has led to increasing concern about the security of the information itself (DTI, 1997).

Background

The word cryptography comes from the Greek word *kruptós logos* meaning *hidden word* and has been used for "secret writing" for many years. Encryption is defined as the transformation of data (plaintext), via a cryptographic mathematical process, into a form (ciphertext) that is as close as possible to unreadable by anyone who does not possess the appropriate knowledge. Decryption is the reverse of encryption, the transformation of encrypted information back into its original form. Encryption and decryption require the use of some secret information – *key*. There are two main types of encryption systems, code and cipher systems. The distinction between a code and a cipher system is that using a cipher system, anything can be encrypted while using a code system the context of the type of information that will be encrypted is needed

before the codes can be devised (Beckett, 1988). The disadvantages of a code system are that usually only a few terms of the message will be encrypted, making it easier to decrypt the message especially if a number of samples of encrypted data are available (Held, 1993).

In ancient cryptography, messages were encrypted by hand with a method (algorithm) usually based on the alphabetic letters of the message. The two main types were ***substitution ciphers*** where every occurrence of a given letter is replaced by a different letter and ***transposition ciphers*** where the ordering of the letters is shifted (Deitel *et al.*, 2000). For example, if every other letter starting with 's' in the word security creates the first word of the ciphertext and the remaining letters create the second word, the word security would encrypt to *scrt euiy*. Combining substitution and transposition ciphers created more complicated ciphers.

Some famous examples of encryption include:

1. From ancient Greece where the Spartan Generals wrote messages on narrow ribbons of parchment that were wound around a cylindrical staff known as a scytale, when the ribbon was unwound, it could only be read by a person who had an exact matching cylinder (Garfinkel & Spafford, 1996).
2. A Caesar Cipher (named after Julius Caesar) is a simple encryption system that replaces individual letters by those three positions further down the alphabet (PGP, 2001).
3. The development of Morse Code in 1832 allowed the transfer of communications over wire and used a series of dots and dashes for letters in the alphabet (Morse, 1840).

Historically, cryptography has been associated with spies, governments and the military and has been used in warfare for thousands of years, the most famous case being the Enigma Cipher, used by the Germans in World War II to code the Third Reich's most secret messages (Treese & Stewart, 1998).

The problem with many historical ciphers is that their security relied on the sender and receiver to remember the encryption algorithm and keep it secret.

Cryptographic Systems

Today, cryptographic methods are more sophisticated and are used to support more than the confidentiality of the message, they also include integrity protection, authentication, non-repudiation and detection of unauthorised copying (Adams & Bond, 2000).

All cryptographic systems, no matter how complex have four basic parts :

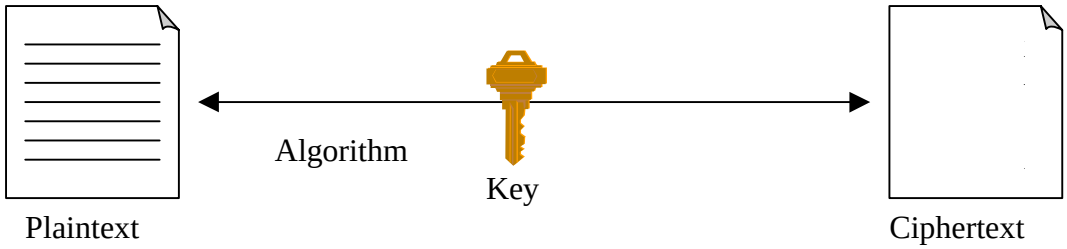


Figure 2 : Basic Cryptographic System

Plaintext	A message before anything has been done to it
Ciphertext	Unreadable Plaintext message after it has been modified in some way
Algorithm	Mathematical operation used to convert plaintext into ciphertext and vice versa
Key	Secret key used to encrypt and/or decrypt the message. A key is a word, phrase, numeric or alphanumeric string which when used in conjunction with the algorithm allows the plaintext to be encrypted and decrypted.

The advantage of cryptography is that the ciphertext can be transmitted across insecure, public communications channels. Even if the ciphertext is intercepted, it is useless to anyone who does not possess the decryption key (Stein, 1998). The key contains the binary code used to mathematically transform a message (Greenstein & Feinman, 2000). An important feature of cryptographic systems is that since the

security depends completely on the secrecy of the decryption key, it is not necessary to keep the workings of the algorithm secret. This allows the same algorithm to be reused by many people and avoids any need to protect cryptographic software (Stein, 1998). The principle is the same as that of a combination lock, where many people may use locks of the same design, but each one uses a different combination (Treese & Stewart, 1997). When creating a new algorithm, a cryptographer has no way of knowing for sure that it is airtight against thieves, the only way to achieve confidence is through trial and error as the number of people who try and fail to break it increases (Greenstein & Feinman, 2000).

Key Length

Modern cryptosystems are digital, their algorithms are based on individual bits of the message rather than letters of the alphabet. Encryption and decryption keys are binary strings with a given key length (Deitel *et al.*, 2001). Keys in a cipher system are described by the number of bits used to hold them, for a key with n bits, there are 2^n possible keys (Treese & Stewart, 1997). For example, 56 bit encryption systems have 72,057,594,037,927,936 possible key combinations. Longer keys have stronger encryption, so that it takes more time to 'break the code'. Current key length recommendations are using a 75 Bit Key for present day security and encrypting using a 90 Bit Key for information that must be kept secure for 20 years

Cryptanalysis

Even if keys are kept secret, it may be possible to compromise the security of a system. Trying to decrypt ciphertext without knowledge of the secret key is known as Cryptanalysis. Commercial encryption systems are constantly being researched by cryptologists to ensure that the systems are not vulnerable to attack. The most common form of attack is that in which the encryption algorithm is analysed to find relations between bits of the encryption key and bits of the ciphertext (Deitel *et al.*, 2001). The only perfect cryptosystem is called the *One Time Pad* in which the sheets of paper in a pad are filled with completely random characters. An exact copy of the pad is made and hand delivered to the correspondent, the ciphertext is created by writing the message by adding the letters pair wise where A=1st letter, B=2nd and Z wraps back to A. The process is reversed by the recipient revealing the plaintext. Once

a sheet of the pad is used, it is destroyed, if the pad contains truly random letters the code is absolutely secure (Treese & Stewart, 1997). An obvious disadvantage of this method of encryption would be the logistics of distributing the pads as each pair of correspondents would require a unique pad.

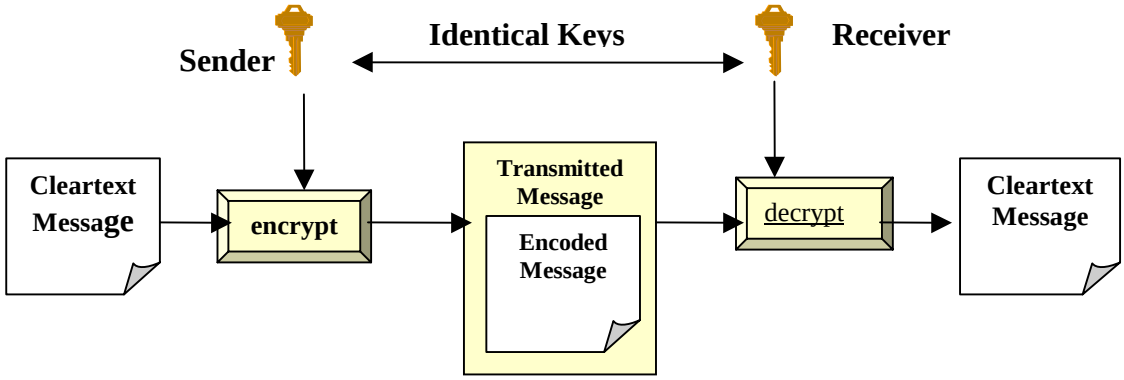
Public and Private Key Encryption

There are two basic types of cryptographic mechanisms to provide encryption capability, private or symmetric cryptography where entities share a common secret key, and public or asymmetric cryptography where each communicating entity has a unique key pair.

Private/Symmetric Key Encryption

Private key cryptography, the traditional form of cryptography, uses a single key to encrypt and decrypt a message. The main advantage of symmetric cryptography is its speed.

Figure 3 : Private Key Encryption (Greenstein & Feinman, 2000)



A **Block** cipher is a type of symmetric-key encryption that transforms a fixed-length of plaintext into a block of ciphertext data of the same length. Because each block of a cipher is independent, an eavesdropper may notice that certain blocks are repeated indicating that the plaintext blocks also repeat. A **Stream** cipher typically operates on smaller units of plain text and is designed to be exceptionally fast by using the key to produce a pseudorandom key stream which is then used to produce the ciphertext (Treese & Stewart, 1998).

Since both parties must know the same key, **authentication** is assured as when the message arrives, there is there is only one person that it could be from.

Message **integrity** can be verified by the use of a **Message Digest**, which generates a short fixed length value known as a hash. A **Hash** function is a transformation that reduces a large data message to one of a more comprehensible size – any message can be reduced to a fixed length, say 128 bits, using a hash function (Stein, 1998). There is no way to decrypt a hash, nor any known way to create two different messages that generate the same hash (Deitel *et al.*, 2001). The hash function ensures that if the information is changed in any way a different output value is produced.

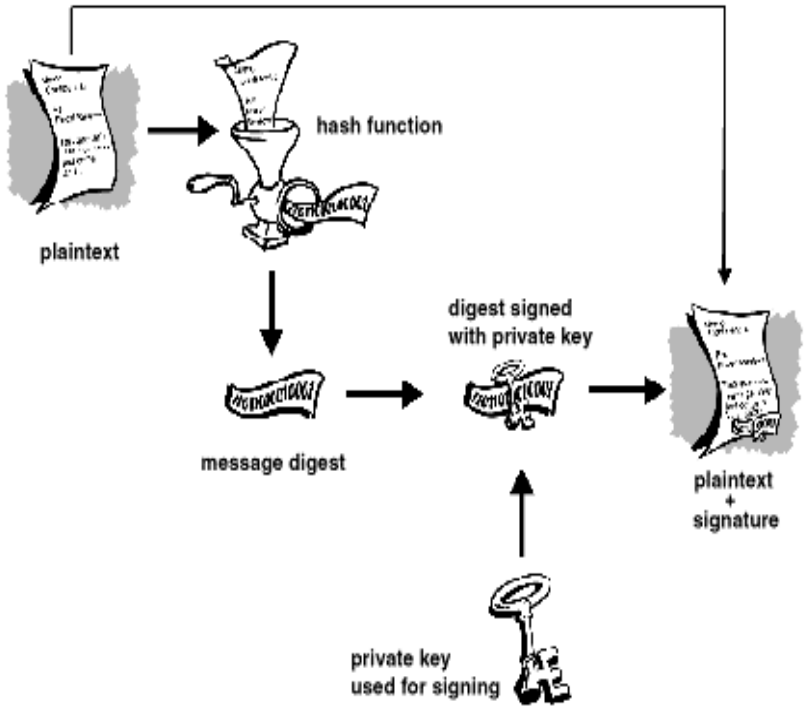


Figure 4 : Hash Function (PGP,2001)

One of the most commonly used symmetric encryption algorithms is the **Data Encryption Standard (DES)**, developed by IBM and US Government. DES is a block cipher, which uses a 56-bit key to encrypt a 64-bit plaintext block into a 64 bit ciphertext. DES became a recognised standard - Federal Information Processing Standards Publication in July 1977. DES consists of 16 blocks of operations that mix the data and the key together where the encryption of each block depends on the

contents of the previous one (Cipherblock Chaining). The message is first rewritten in binary format, then encrypted using the DES algorithm. (FIPS 46-2, 1993).
The main criticism of DES is that the key is not long enough and could be solved by a Brute Force Attack, which tries all possible key combinations in turn until the code is cracked. DES was broken in 1997 in five months by a group known as DESCHALL, which divided the list of possible keys into small segments and using the Internet, gave each segment to volunteers, along with a key-testing program (Stein, 1998). In July, 1998, the supercomputer DES Cracker, designed by Electronic Frontier Foundation, assisted by 100,000 distributed PCs on the Internet was able to crack DES in only 22 hours. This DES challenge can be seen at http://www.eff.org/descracker.html (RSA, 2000).

DES in Triple Encryption Mode (**Triple DES**) is a variant that decreases the risk of brute force attack, by using longer keys. The message is first encrypted using one secret key, decrypted with the second key (the decryption operation does not yield the plain text, since a different key is used) and then encrypted again using a third key as shown in Figure 5.

Other common symmetric encryption algorithms include the European International Data block cipher Encryption Algorithm (**IDEA**), developed by James Massey and Xeujia Lai in 1990. IDEA uses 128-bit key for encryption, which is considered significantly more secure than DES. RC2 and RC4 stream ciphers, designed by RSA are widely used for bulk encryption and use keys of varying length as high as 2048 bits. Crippled versions, (versions which have been deliberately disabled to operate at only a limited key length), that use 40 bit keys have been licensed for export beyond the USA (which prohibited the export of encryption techniques until mid 2000) and are frequently used by web browsers and servers (Stein, 1998).

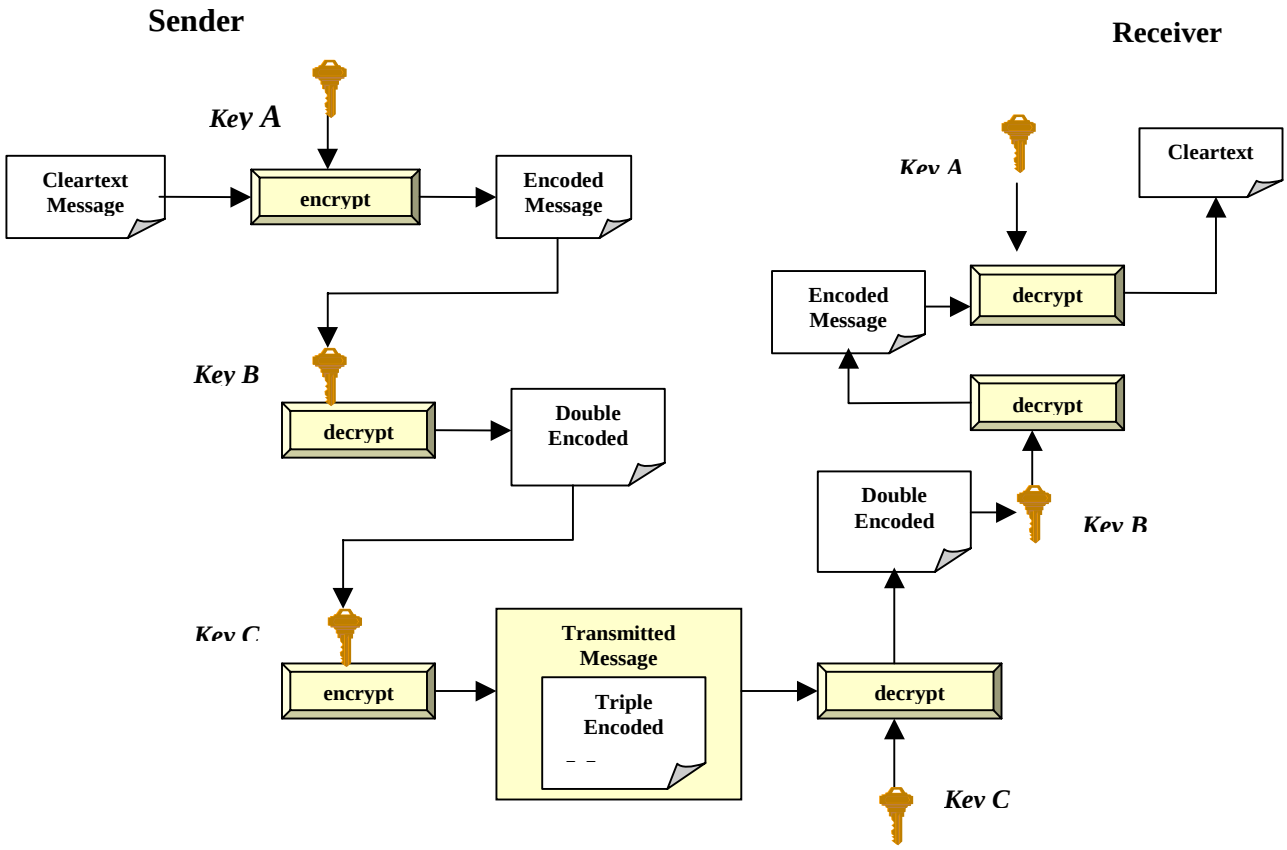


Figure 5 : Triple DES (Greenstein & Feinman, 2000)

Blowfish is a freely available, variable length block cipher designed by Bruce Schneier of Counterpane Systems, (http://www.counterpane.com/blowfish). It is nearly three times faster than DES and is being widely used in PC file encryption and secure tunnelling applications (Treese & Stewart, 1998).

The general consensus of the U.S. National Institute of Standards and Technology is that DES is no longer strong enough for today's encryption needs and is currently working on the Advanced Encryption Standard (**AES**) which is expected to remain a standard well into the 21st century (RSA, 2000).

Private Key Distribution

Distribution of private keys is a major issue in the security of symmetric cryptography. There are several methods for key sharing:

1. Meet in Person – simplest method but doesn't scale well
2. Courier – Can the courier be trusted, this can be overcome by splitting the key and using alternative routes to send key parts
3. Telephone, email or letter

The problem with key distribution, is that anyone who intercepts the key in transit can later modify and forge all information that is encrypted or authenticated with that key.

Public/Asymmetric Key Encryption

One of the main challenges for private key encryption is enabling the sender and receiver to agree on the secret key without anyone else finding out. Another important problem occurs on the Internet, where parties often need to communicate without having previously met. Even if it were possible to securely distribute the servers secret key to the thousands of users, it would be impossible to keep the key secret for long (Stein, 1998).

Public key cryptography, developed by Diffie & Hellman (1976), allows a sender and receiver to generate a shared secret key using an algorithm based on the senders and receivers public and private information.

Figure 6 illustrates the steps:

1. The sender determines a secret value a
2. A related value A, derived from a is made public
3. The receiver determines a secret value b
4. A related value B, derived from b is made public

5. The Diffie-Hellman algorithm is used to calculate a secret key corresponding to the key pairs (a,B) and (b,A),

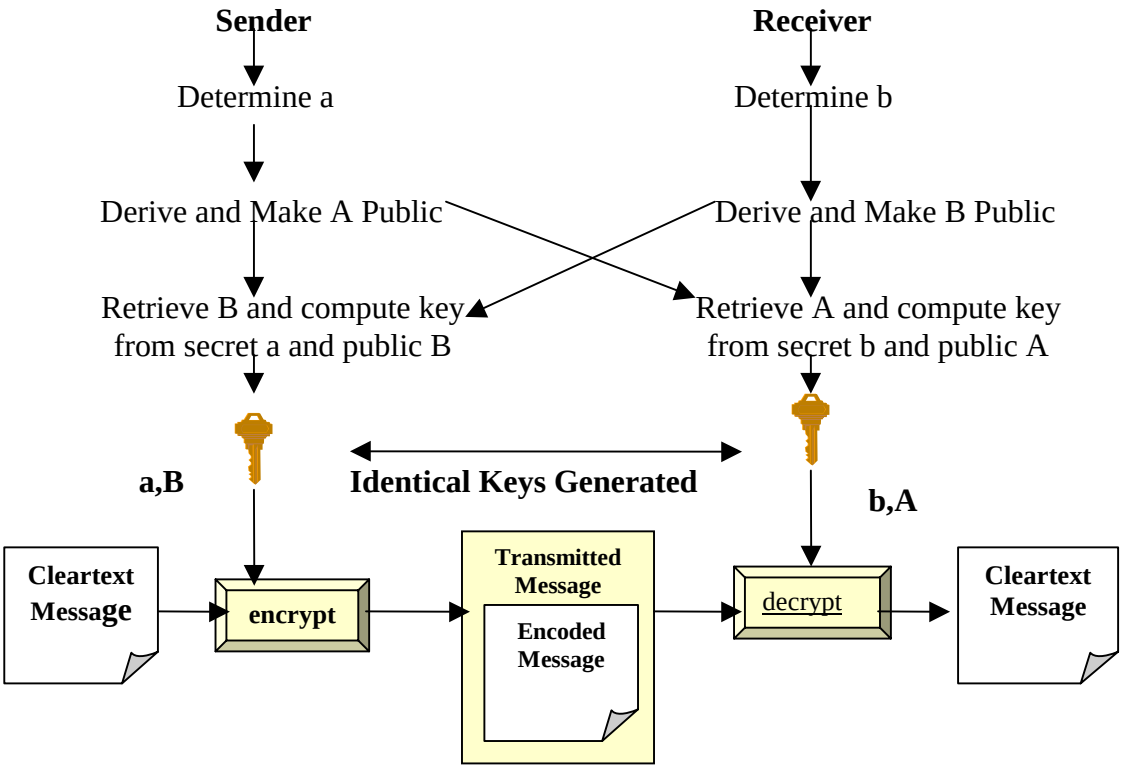


Figure 6 : Diffie-Hellman Public Key Cryptography(Greenstein & Feinman, 2000)

Two way public key communication using Diffie-Hellman cryptography is vulnerable to a man-in-the-middle attack where a hacker intercepts both the senders and receivers public keys and replaces them with his own value, then either renders the communication indecipherable or generates a matching key in order to alter the message. Neither sender nor receiver realise their message has been intercepted or altered (Greenstein & Feinmann, 2000).

RSA is an asymmetric encryption scheme, which was developed by **R**ivest, **S**hamir and **A**dleman in 1977. It uses a pair of keys for encryption, a **public** key which encrypts data, and a corresponding **private** key for decryption. The public key method allows a sender and receiver to generate a shared secret key over an insecure telecommunications line, where each participant creates his own key pair, the private key is kept secret and never revealed or shared, while the public key is distributed

freely (Treese & Stewart, 1998). The need for the sender and receiver to share secret information is eliminated, as all communications involve only public keys. Anyone can send a confidential message using the public key but the message can only be decrypted using the private key, which is in the sole possession of the intended recipient (RSA, 2000). An illustration of a public key system is a safe with a slot at the top, anyone can put items into the safe, but only the person who knows the combination can get the items out (Treese & Stewart, 1998).

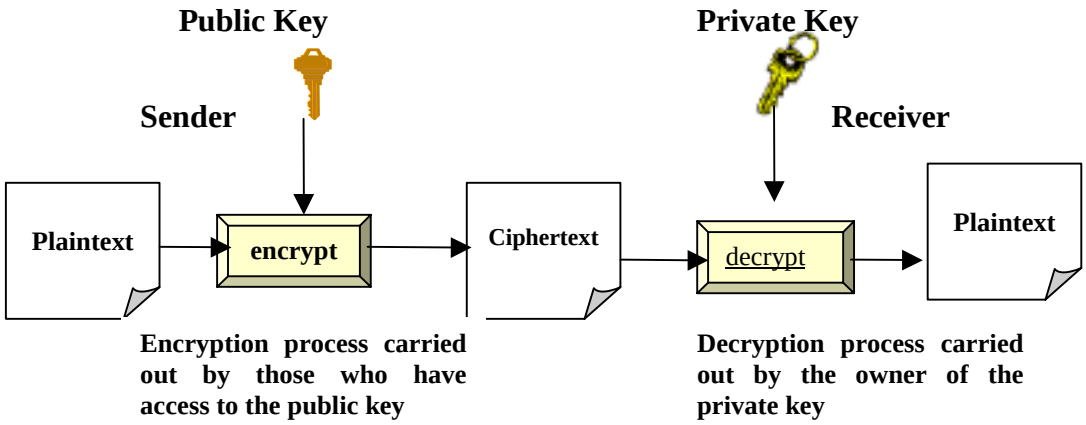


Figure 7 : Public Key/Asymmetric Encryption

The RSA encryption algorithm is based on prime numbers and uses variable key lengths ranging from 512 to greater than 1024 bits.

In some applications, a critical document may be divided into pieces and allocated to different locations over the Internet for security access concern, to access the document, the divided pieces must then be reconstructed from these locations (Lee *et al.*, 2000).

Digital Signatures

One problem with public key encryption is that anyone could have sent the message. Digital signatures are a reversal of the public key encryption /decryption scheme. Instead of encryption taking place using the receiver's public key, the message is encrypted (signed) using the sender's private key. This receiver of the message

decodes the signature using the sender's public key thereby verifying the message sender's identity.

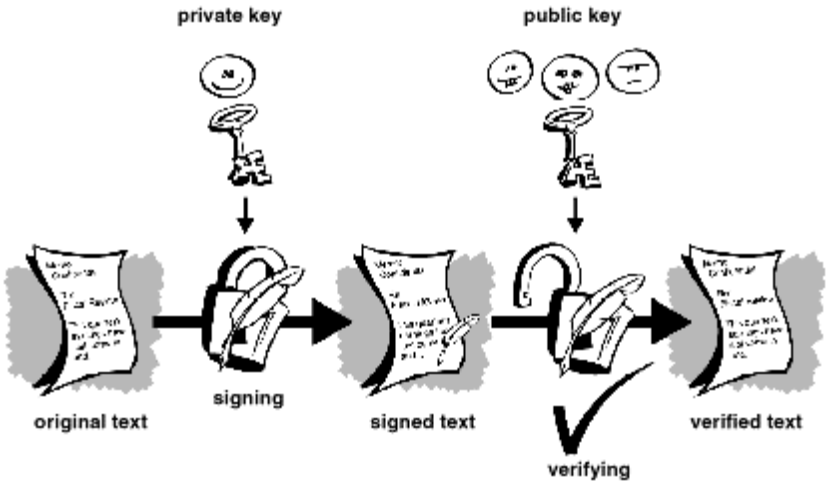


Figure 8 : Digital Signature (PGP, 2001)

Rather than creating a digital signature by encrypting the entire message using the sender's private key, a hash of the message can be encrypted instead. This creates a small fixed size signature, regardless of the length of the message. However, a digital signature does not prove that the authenticated sender actually sent the message, only that the computer did! If the computer were inappropriately infected, malicious code could use the key to sign documents without the user's knowledge or permission. The legal acceptance of digital signatures shifts the burden of proof to the negative, that the signature in dispute was not signed rather than was signed (Ellison & Schneier, 2000)

Digital Envelopes and Session Keys

One of the main disadvantages of public key encryption is speed since public key encryption is noticeably slower than private key encryption (Garfinkel, 1996 ; RSA, 2000). Since encryption using public key cryptography is much slower to carry out than symmetric key cryptography, the use of public key cryptography would reduce business exchanges to a crawling pace. Consequently, a symmetric key is used to encrypt bulk documents and then public key cryptography is used to deliver the key to the recipient. Under this regime, session symmetric keys are randomly generated for

each exchange (Adams & Bond, 2000). This combination of private and public is carried out as follows:

1. A secret (session) key is generated at random
2. The message is encrypted using the session key and the symmetric algorithm
3. The session key is then encrypted with the receiver's public key – this is known as the Digital Envelope
4. Both the encrypted message and the digital envelope are sent to the receiver
5. The receiver uses their private key to decrypt the digital envelope recovering the session key which is used to decrypt the message (Stein, 1998).

Notarisation and Time Stamping

Digital Certificates can be used to irrefutably sign a document. If an electronic notary receives the signatures of two or more parties, he can formally record an agreement between the parties. Using a reliable and verifiable independent clock to time stamp the receipt of the digital signatures, the exact time of a commercial event can be recorded (Cross, 1999).

Key Management

While secure communication over the Internet has become an essential requirement for any value-added Internet application, the use of cryptography for secure communication brings out the need for cryptographic key management (Zhou, 2000). The main challenge for symmetric cryptography is getting the sender and receiver to agree on the secret key without anyone else finding out and then storing the key safely. The generation, distribution and storage of keys is known as key management (RSA, 2000). In addition, encrypted messages must remain secret for the useful life of the information. There is usually a need to update keys, if, for example, a key can be broken in two years and the lifetime of the information is 6 months then the key should be changed every 18 months.

Key Storage

Proper short and long-term storage of cryptographic keys is essential for good security. When a key is used on a computer, it must be stored in memory, which makes it available to other software on the same system, an online key is only as

secure as access to the machine and the password protection mechanisms. Cryptographic keys are usually stored in disk files as they may be randomly generated and are too long to be used manually. At present private keys are generally stored on the owner's PC and protected by a password. If the PC is hacked or stolen, the private key could be fraudulently used, hence the keys themselves are usually stored in an encrypted format.

Smart Cards

A smart card contains a microprocessor and storage unit. Features such as card size, contact layout and electrical characteristics have been standardised (ISO 7816). Smart cards have physical tamper-resistant properties, plus secure storage and processing capabilities. The mechanism employed to ensure that the card is being used by its authorised user is achieved by off-line entry of a PIN ('something you know') known only to the card and its rightful holder ('something you have') (Trask & Meyerstein, 1999). This 'two-factor' authentication is currently being extended to incorporate biometric properties 'something you are'. An example of this is currently being piloted by the Bank of America using fingerprint recognition to give individuals access to their on-line services (Internet News, 1999). Biometrics are unique identifiers but they are not secrets. Anyone can steal a copy of your fingerprint or your iris patterns. If someone steals an element of your biometrics, it remains stolen for life, there's no getting back to a secure situation (Schneier, 1999).

The use of a smart card for private key storage both allows more security and enables the key to be used on any PC. The owner can store a number of digital certificates containing different private keys on the same smart card (Cross, 1999). For greater security, the smart card can by synchronised with the host computer to generate a new password at pre-specified intervals after which time the password is unusable (Greenstein & Feinman, 2000).

Secret Sharing

Truly valuable keys may be used only on isolated computer systems and stored safely when not in use, for example in a bank vault. If the safety of a single copy could be compromised, the key may be split, thereby allowing the trust of a secret to be

distributed among a designated set of people whose cumulative information suffices to determine the secret.

Key Recovery

This term refers to the useful technology that allows a key to be revealed if a user accidentally loses or deletes the key, or if a law enforcement agency wants to eavesdrop on a suspected criminal without the suspect's knowledge.

Key Destruction

Keys should be destroyed after use, as they remain valuable after they have been replaced. If the attacker retains the ciphertext and the key becomes available, then it can be easily decrypted.

Public Key Infrastructure (PKI)

A well-designed and implemented PKI is essential to establish maintain trust in digital certificates. Many studies have shown that the full potential of electronic commerce will not be realised until public key infrastructures emerge which generate sufficient trust for businesses and individuals to commit their information and transactions to the emerging public networks (OECD, 1997).

Trusted Third Parties

In order for public key systems to work in the public domain, not only must the public key be freely accessible, but also senders and receivers must have a reliable way of determining that public keys are truly the keys of those parties with whom they wish to interact (OECD, 1997).

In a world where more and more transactions are taking place on open electronic networks, there has been a growing demand for strong encryption services to help protect the integrity and confidentiality of information while safeguarding law enforcement which encryption can prevent (Taylor, 1997). A critical issue presented by cryptography is the possible conflict between privacy and law enforcement, since cryptography can also be put to improper use such as hiding the illegal activities of criminals and terrorists. Many governments consider it essential that the ability of security, intelligence and law enforcement agencies to conduct effective legal

interception of communications under the Interception of Communications Act 1985 is preserved (DTI Proposals, 1997; usdoj, 2001). The need to maintain a balance between commercial requirements, together with the need to protect users and the need to safeguard law enforcement and national security requirements has been met by the introduction of licensed Trusted Third Parties (TTPs) for the provision of encryption services.

Legal access can be achieved by making use of a key escrow/recovery system which allows authorised persons, under certain conditions to decrypt messages with the help of cryptographic key information, held in escrow, and supplied by one or more trusted parties (DTI Proposals, 1997).

Certification Authorities

A digital certificate is an electronic credit card that establishes the credentials for doing business or other transactions on the Web. A Certification Authority (CA) issues the certificate which contains the user's name, a serial number, expiration dates, a copy of the certificate holder's public key and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real (DeVeau, 1999).

A CA acts like the passport office, which checks the credentials of individuals and entities and issues them with electronic certificates that are trusted throughout the community. Trust models are emerging, within diverse online business partnerships, through the mutual recognition of their respective CAs (Wilson, 1997).

The two of the main components of PKI are:

1. Certification Authority (CA) run by a Trusted Third Party (TTP) which issues and revokes certificates according to a published Certification Practice Statement and,
2. A Registration Authority which authenticates the identities of individuals and authorities who apply for digital certificates (Cross, 1999)

Secure Sockets Layer (SSL)

SSL is a non-proprietary protocol, developed by Netscape, used to secure communication on the Internet. SSL uses public-key technology and digital certificates to authenticate the server in a transaction and protects private information as it passes from one party to another. SSL transactions do not require client authentication (Deitel *et al.*, 2001).

The steps in the process are shown in Figure 9.

1. Client opens a connection to the Server port and sends a 'Client Hello' Message, letting the server know the version of SSL used, the cipher suites and data compression it supports
2. Server responds with the chosen cipher suite and data compression methods, along with a session identifier. If there is no match between the cipher suites supported by the client and server, the server sends a 'handshake failure' message and hangs up.
3. Server sends its signed CA certificate, if the CA is not a root certifing authority, the server sends the chain of signed certs that lead to the primary CA.
4. The client generates a session key which the browser encrypts using the Servers Public key to create a digital envelope which is forwarded to the server, this session key is decrypted using the servers private key
5. Both client and server confirm that they are ready to start communicating using the agreed cipher and session key
6. Client and Server send *Finished* messages which confirm that their messages were received intact and not tampered with en-route.

At this point, both client and server switch to encrypted mode, using the session key to symmetricaly encrypt subsequent transmissions in both directions (Stein, 1998)

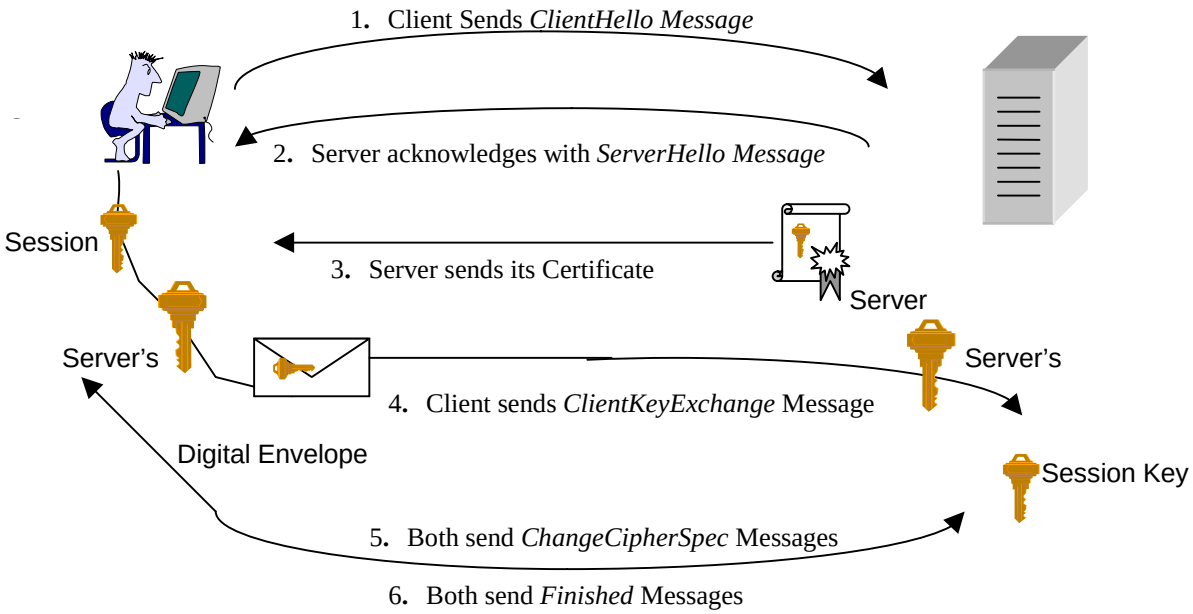


Figure 9 : SSL Handshake (Stein, 1998)

If Client authentication is required, in addition to the steps outlined above, the server can request a Client Certificate. If the client has no certificate, the server may choose to abort the transmission with a 'handshake failure' message or continue on. If client authentidation is in place, the client sends a digital signature to prove its identity.

While SSL is the dominant protocol for encrypting general communications between client and server, *it does not encrypt data at the server site* (Larsen, 1999). This means that if private information, for example, credit card numbers, are stored on the merchant's server they are vulnerable to both outside and insider attack (Deitel *et al.*, 2001).

Secure Electronic Transactions (SET)

SET is a specialised protocol, developed by Visa, Mastercard, Netscape and Microsoft, for safeguarding credit-card-based transactions between customers and merchants (Stein, 1998) and uses cryptography to:

1. Provide confidentiality of information through encryption
2. Ensure payment integrity through digital signatures and message digests
3. Authenticate both merchants and cardholders through the use of digital signatures and certificates
4. Interoperate with other protocols (Greenstein & Feinman, 2000).

The SET protocol involves the cardholder, the merchant, the card-issuing bank and the merchant's bank using public/private key pairs and signed certificates to establish each player's identity. Figure 10 shows how SET works.

1. **The Customer initiates a purchase**

   Customer browses Web Site, fills out order form and Presses Pay Button, Server sends customers computer a message initiating SET software
2. **The Client's Software sends the order and payment information**

   Clients SET software creates two messages, one containing order information, which is encrypted using a random session key and packaged into a digital envelope using the Merchant's public key. The other message contains payment information encrypted using the Merchant Banks public key. The software computes a hash of the order and payment information and signs it with the customer's private key.
3. **The Merchant passes payment information to the bank**

   SET software on the Merchants server generates an authorisation request, forwarding the customers encrypted information to the Bank, signing the message with its private key to prove its identity to the Bank. This request is encrypted with a new random session key and incorporated into a digital envelope using the Banks public key
4. **The Banks checks the validity of the card**

   The Bank decrypts and verifies the Merchant's message, then decrypts and verifies the customer's identity. It then generates an encrypted and digitally signed authorisation request to the Customer's bank
5. **The Customers Bank authorises payment**

The customer's bank confirms the merchant's bank identity, decrypts the information, checks the customer account and approves/rejects the request by digitally signing and encrypting it and returning it to the merchant's bank

6. **The Merchants Bank authorises the transaction**

   The Bank authorises, signs and returns the transaction to the Merchant

7. **The Merchant's Web Server completes the transaction**

   Merchant acknowledges the confirmation to the customer, via a confirmation page, and proceeds to transact the order

8. **The Merchant confirms the transaction to the Bank**

   The Merchant confirms the purchase to its bank, causing the customer's credit card to be debited and the merchant's account to be credited.

9. **The Customer's Bank sends credit card bill to customer**

   The charge appears on the customer's monthly statement

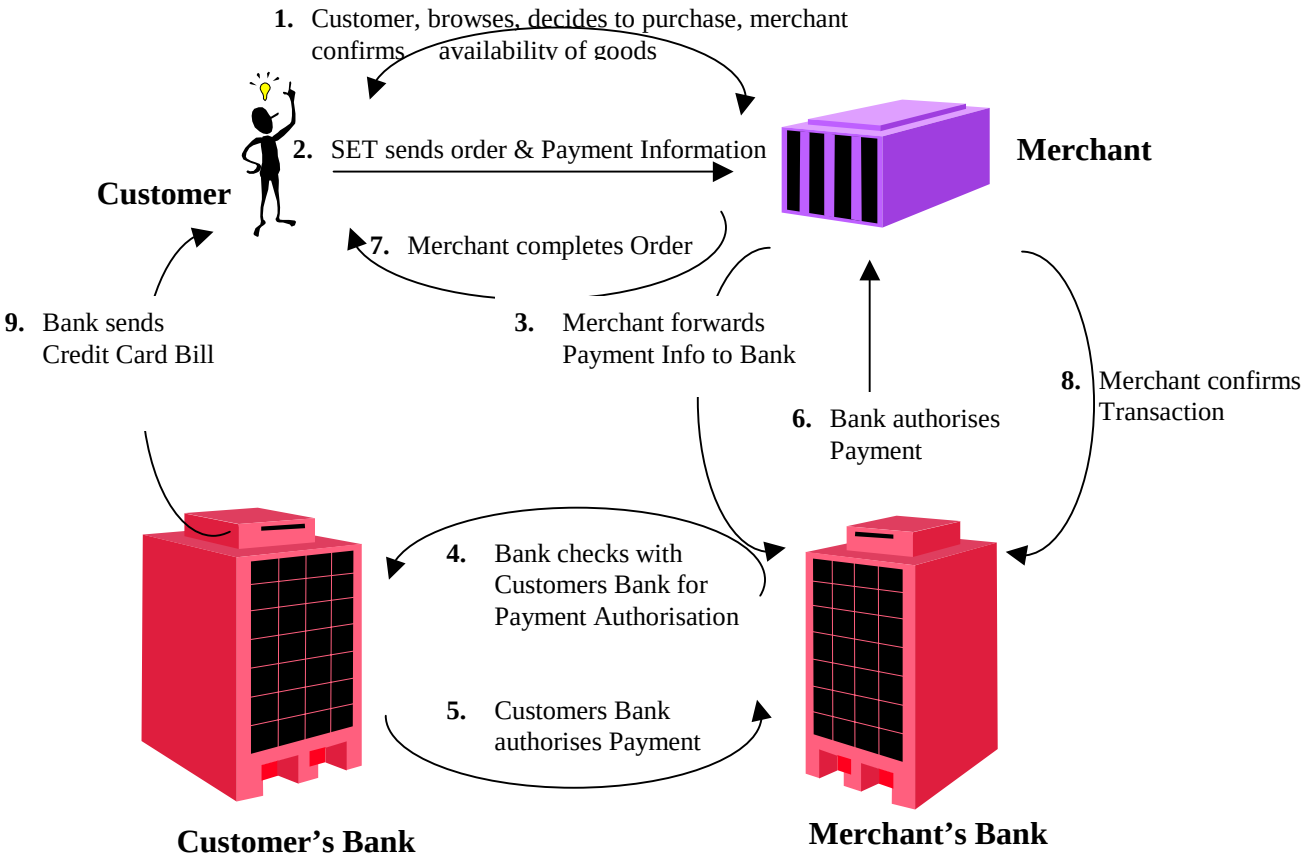


Figure 10 : SET Protocol (Stein, 1998)

In the SET protocol, the merchant never sees the client's proprietary information, considerably reducing the risk of fraud (Deitel *et al.*, 2001). SET focuses on confidentiality and authentication and ensures that not only can thieves not steal a credit card number but prevents merchants from seeing the number while still providing assurances that the card is valid (Hawkins *et al.*, 2000).

While SET provides a high level of security, business have been slow to embrace this technology because of the increased transaction time and the specialised software requirement on both the client and server sides which increases transaction costs (Deitel *et al.*, 2001).

Summary and Conclusions

Summary of techniques

The applications of cryptography that meet the facilities required from an Internet based infrastructure are summarised in Table 1.

Facilities Required	Method	Unique Features	Limitations
Confidentiality	• Encryption	• Scrambles the data before transmission	• Speed of transmission
Integrity	• Encryption /Decryption	• Electronic Key required to open encrypted data	• User may loose key • Key may fall into wrong hands
Authentication	• Digital Certificate confirmed by a CA	• Verifies the authenticity of sender • Alerts recipient if message has been altered	• Only useful if companies use a trusted third party Certificate Authority • Only verifies that the message was sent from the users computer or private key
Non-Repudiation	• Digital Certificate • Time Stamp from a CA	• Neither sender nor receiver can deny communication	
Copy Protection	• Encryption • Digital Time Stamp	• Prevents the data from being reproduced • Proves authorship	

Table 1 : Internet Security Components Addressed by Cryptography

Security, message integrity and authentication can be achieved by using SSL, which ensures secure communication between client and server by using public key technology to encrypt the data and authenticate the server. Although more complex and expensive to implement, SET enhances SSL by providing mechanisms to ensure Client Authentication and the security of financial transactions through the separation of merchant and payment information.

Conclusion

This paper has considered the history and techniques of cryptography used for securing communications over the Internet. The use of public and private key encryption infrastructures, digital signatures and time stamping, to ensure authentication and non-repudiation have been described. The significance of key management systems and the importance of establishing a Public Key Infrastructure using Trusted Third Parties and Certification Authorities to establish and maintain trust in digital certificates have been discussed. Methods of ensuring secure electronic communication using SSL and safeguarding financial transactions using SET have been described.

In order for companies to be confident that their electronic transactions can be carried out securely, Internet security will always be a never-ending challenge. As improvements in protocols, authentication, integrity, access control and confidentiality occur hacking techniques will also improve. The future of Internet Security will remain in human hands to continually monitor network infrastructures and to assess and implement hardware and software solutions.

Bibliography

Adams D. & Bond R. (2000) Secure E-Commerce – A Competitive Weapon, Electronic Commerce Report, UNICOM Seminars Ltd.

Beckett B. (1988) Introduction to Cryptography, Blackwell Scientific Publications, UK.

Budge P. (1998) How Safe is the Net ?. Business Week, June 22.

Cross B. (1999) BT Trustwise – Enabling eCommerce Through Trust. BT Technol J. Vol 17(3), 44-49.

CSI Press Release – March 5th 1999, Cyber Attacks Rise From Outside and Inside Corporations –

Dramatic Increase in Reports to Law Enforcementhttp://gocsi.com/prelea990301.htm accessed 15th March 2001

Deitel H., Deitel P. & Nieto T. (2001) e-Business & e-Commerce : How to Program. Prentice Hall NJ.

DeVeau P. (1999) VPN = Very Private News. America's Network, Vol. 103(21) May 21, p16.

Diffie W. & Hellman M. (1976) New Directions in Cryptography. IEEE Transaction on Information Theory, Nov. 644-654

DTI, (1997) Department of Trade and Industry Proposals for the Licensing of Trusted Third Parties for the Provision of Encryption Services, Public Consultation Paper on Detailed Proposals for Legislation.http://www.dti.gov.uk/pubs accessed March 15th 2001

Dysart J. (2000) Internet Security : Safeguard Your Network, Electrical World Vol. 214(3) 41-42.

Ellison C. & Schneier B. (2000) Risks of PKI, 116. Communications of the ACM, (42),12. Also available from the Collection of Inside Risks Columns on Peter Neumans Site at http://www.csl.sri.com/users/neumann/insiderisks.html. Accessed 14/03/01

Ernst & Young. (1998) Internet Shopping : An Ernst & Young Special Report, Section 2, January

Everett J. (1998) Internet Security. Employee Benefits Journal, Vol 23(3), 14-18.

FIPS 46-2, (1993) Data Encryption Standard. http://www.itl.nist.gov/fibpubs/fip46-2.htm Accessed 05/02/01

Foresight (1998) E-Commerce Sets New Rules. Systems Relationships Marketing, on behalf of Datatec Ltd. Vol. 1 No. 3, November

Furnell S. & Warren M. (1999) Computer Hacking and Cypher Terrorism : The Real Threats in the New Millennium. Computers & Security 18 (1) 28-34

Garfinkel S. & Spafford G. (1996) Practical UNIX and Internet Security, O'Reilly and Associates, NY.

Gold S. (2000), Costs of Online Breaches Soaring Says CSI/FBI Report, Newsbytes 22 March http://www.newsbytes.com/pubNews/00146090.html accessed March 15th 2001

Greenstein M. & Feinman T., (2000) Electronic Commerce : Security, Risk Management and Control, Irwin, McGrawHill, Boston.

Hawkins S., Yen D. & Chou D. (2000) Awareness And Challenges Of Internet Security. Information Management and Computer Security, 8(3), 131-143.

Held G. (1993) Top Secret Data Encrypting Techniques, SAMS Publishing, USA.

InformationWeek (1998), Global Information Security Survey Reflects IT Professionals Views Worldwide, Press Release, September 9.

Internet News (1999) Bank of America Offers Fingerprint Access to Online Banking http://www.internetnews.com/ec-news/article/0,,4_33221,00.html Accessed 18/04/01

ISO 7816 Identification Cards – Integrated Circuit(s) Cards With Contacts http://iso.ch/cate/d29257.html

Labuschagne L. & Eloff J. (2000) Electronic Commerce : The Information Security Challenge. Information Management and Computer Security, 8(3), 154-157

Larsen A. (1999) Global Security Survey : Virus Attack. Information Week, July, 42-46

Lee C., Yeh Y., Chen D. & Ku K. (2000) A Share Assignment Method to Maximise the Probability of Secret Sharing Reconstruction under the Internet. IEICE Transactions on Information Systems E83D (2) 190-199.

McGuire B. & Roser S. (2000) What Your Business Should Know About Internet Security. Strategic Finance, Vol. 82(5), 50-5

Morse S. (1840) US Patent for Morse Code, United States Patent and Trademark Office (USPTO), http://www.patentmuseum.com/listing.html Accessed 15/03/01

Neumann P. (2000) Risks of Insiders, 114. Communications of the ACM, (43),2. Also available from the Collection of Inside Risks Columns on Peter Neumans Site at http://www.csl.sri.com/users/neumann/insiderisks.html. Accessed 14/03/01

OECD (1997) Cryptography Policy : The Guidelines and the Issues
Available at http://www.oecd.org/dsti/sti/it/secur/prod/e-crypto.html
Accessed 02/04/01

OECD (1999) Joint OECD-Private Sector Workshop on Electronic Authentication. Available at http://www.oecd.org//dsti/sti/it/secur/act/wksp-auth.htm
Accessed 02/04/01

PGP (2001) How PGP Works http://www.pgpi.org/doc/pgintro/

Price K. (1999) Intrusion Detection Pages. http://www.cerial.purdue.edu/coast/intrusion-detection/welcome.html Accessed 18/04/01.

RSA (2000) Frequently Asked Questions About Today's Cryptography. RSA Laboratories

Salnoske K. (1998) Testimony before the Subcommittee on Telecommunications Trade and Consumer Protection Committee on Commerce. May 21 in Greenstein & Feinman (2000)

Schneider F. (1998) Towards Trustworthy Networked Information Systems, Inside Risks. 101. Communications of the ACM, (41),11. Also available from the Collection of Inside Risks Columns on Peter Neumans Site at http://www.csl.sri.com/users/neumann/insiderisks.html. Accessed 14/03/01

Schneier B. (1999) Biometrics : Uses and Abuses, Inside Risks. 110. Communications of the ACM, (42),8. Also available from the Collection of Inside Risks Columns on Peter Neumans Site at http://www.csl.sri.com/users/neumann/insiderisks.html. Accessed 14/03/01

Schneier B. (1999) Risks of Relying on Cryptography, Inside Risks. 112. Communications of the ACM, (42),10. Also available from the Collection of Inside Risks Columns on Peter Neumans Site at http://www.csl.sri.com/users/neumann/insiderisks.html. Accessed 14/03/01

Schneier B. (1999) The Trojan Horse Race, Inside Risks. 111. Communications of the ACM, (42),9. Also available from the Collection of Inside Risks Columns on Peter Neumans Site at http://www.csl.sri.com/users/neumann/insiderisks.html. Accessed 14/03/01

Stein L., (1998) Web Security : A Step-by-Step Reference Guide, Addison Wesley, MA.

Taylor I (1997) Forward to 'Licensing of Trusted Third Parties for the Provision of Encryption Services, Public Consultation Paper on Detailed Proposals for Legislation.'
http://www.fipr.org/polarch/ttp.html accessed March 15th 2001

The Computer Law & Security Report (1997) Binding Cryptography : A Fraud Detectable Alternative to

Key-Escrow Proposals. Available at http://cwis.kub.nl/~frw/people/koops/bind-art.htm Accessed 29/03/01

Trask N. & Meyerstein M. (1999) Smart Cards in Electronic Commerce. BT Technol J. Vol.17(3), 57-66

Treese G. & Stewart L. (1998) Designing Systems for Internet Commerce. Addison-Wesley, MA.

U.S. Department of Commerce (1998) The Digital Economy, April http://www.ecommerce.gov/danc1.html

usdoj (2001) United States Department of Justice. http://www.usdoj.gov/criminal/cybercrime/compcrime.html Accessed 10/04/01

Wilson S. (1997) Certificates and Trust in Electronic Commerce. Information Management and Computer Security, Vol.5(5) 175-181

Zhou J. (2000) Further analysis of the Internet Key Exchange Protocol. Computer Communications 23(17) 1606-1612

Passive Voice Constructions in Modern Irish[1]

Brian Nolan
Institute of Technology Blanchardstown, Dublin
Email: brian.nolan@itb.ie

Abstract

This paper is about the passive construction, of which modern Irish (a VSO language) has two primary forms, the personal passive and its variants, and the impersonal. An empirical question is posed as to whether a third passive form exists within the language, that of a functionally defined GET-passive. To deliver a unified analysis of the various passive constructions, a perspective that takes account of the complete event is necessary.

Irish supports three variants of the personal passive construction (i.e. perfective, progressive, prospective) each of which involves the substantive verb in a periphrastic form. The agent can optionally be represented obliquely. The active verb takes a non-finite form as a verbal adjective or verbal noun, depending on the personal passive variant. We note that a number of other voice constructions, specifically the reflexive and middle voice, appear to have some qualities in common with the personal passive.

The impersonal passive form occurs with all verbs of Irish, across all tenses, whether intransitive or transitive. The impersonal passive form is also to be found productively with the substantive verb across all tenses. It does not under any circumstances occur with the copula verb. Our view is that the impersonal passive construction has an indefinite actor at the level of the semantics and that the impersonal passive verb expresses this as a third person indefinite pronoun in the syntax via a synthetic post-verbal suffix rendered on the matrix verb. When considered in this way, the behaviour of the impersonal passive verb in the syntax is shown to be the same with respect to definite subject pronouns when they are expressed in a non-analytic manner, that is, in the synthetic form of the verb. The analysis here supports the view that there is strong link, reinforced by immediate proximity, between the verb and subject underpinning the VSO linear word order.

We investigate whether there is a third passive construction to be found in Irish, a GET passive. The GET passive is attested in many, but not all, of the world's languages (Siewierska (1984). We find evidence that a particular subset of constructions precisely exhibits the characteristics of the GET passive under strictly defined constraints. On the basis of this evidence, we claim that there is a functionally defined GET passive in modern Irish.

The commonality underpinning the passive constructions, including the functionally defined GET passive, can be explained in terms of the windowing of attention analysis in the sense of Talmy (1996), that is, a functional analysis with an event frame perspective sensitive to prototypicality. Irish follows a VSO word order with the subject more closely bound to the verb than the object. As well as looking at each of the passive constructions, we also briefly examine how the VSO word order is maintained through each.

1. Introduction

This paper is about the passive construction, of which Irish has two primary forms, the personal passive and its variants, and the impersonal. An empirical question is posed

[1] This paper was presented at the High Desert Linguistics Society Conference at the University of New Mexico, Albuquerque, New Mexico, USA in March 2001

as to whether a third passive form exists within the language, that of a functionally defined GET-passive.

The hypothesis in this paper is that the commonality underlying each of the passive constructions casts a different component of the event frame into the foreground, in the sense of a "windowing of attention" (Talmy 1996a).

Irish is a VSO language and therefore, in common with the other Celtic languages, the order of elements in the structure of transitive sentences is verb-subject-object.

The functional approach in this paper makes use of many of the insights of Role and Reference Grammar (RRG). In the Role and Reference framework (Van Valin 1993, Van Valin & LaPolla 1997), the semantic representation of sentences is based on the lexical representation of the verb. RRG employs a decompositional representation based on the theory of Aktionsart of Vendler (1967) and directly builds upon Dowty (1979, 1986, 1989, and 1991). The lexical representation of a verb or other predicate is its logical structure.

The semantic representation of an argument is a function of its position in the logical structure of the predicate and the RRG linking system refers to an element's logical structure position. RRG posits two generalised semantic roles, or in Van Valin's terminology, "semantic macroroles", which play a central role in the linking system. The macroroles are actor and undergoer, and they encapsulate the usually accepted clusters of thematic roles. They are the primary arguments of a transitive predication. In an intransitive predicate, the single argument can be either an actor or an undergoer, depending on the semantic properties of the predicate.

The relationship between the logical structure argument positions and macroroles is captured by the Actor-Undergoer Hierarchy (AUH). In this, the leftmost argument in terms of the hierarchy will be the actor and the rightmost argument will be the undergoer. Transitivity in RRG is therefore defined semantically in terms of the number of macroroles of a predicate.

The linking between semantics and syntax has two phases. The first phase consists of the determination of semantic macroroles based on the logical structure of the verb (or other predicate) in the clause. The second phase is concerned with the mapping of the macroroles and other arguments into the syntactic functions.

2. The Personal Passive

The language supports three variants of the personal passive construction, each of which involves the substantive verb in a periphrastic form. These relate to the nature of the aspect and are, accordingly: the progressive, the prospective and the perfective (Ó'Siadháil 1989:294, Stenson 1981:145*ff*, Russell 1995:100*ff*)).

They are passives (i.e. personal, not impersonal, passives) in the sense that a noun phrase, which does not represent the agent, appears as the subject of the substantive verb in the first argument slot following the substantive verb in the position reserved for the grammatical subject. The agent can optionally be represented obliquely by a prepositional phrase introduced by the preposition *ag* 'at' or *ó* 'from' and containing the nominal denoting the agent.

We can distinguish between three different, but related forms, of the personal passive by reference to the following schemata. The specific prepositions in each of the schema are a necessary part of the constructions.

Personal Passive[2]

(1) Perfective Passive [SUBV $NP_{\textbf{undergoer}}$ VA (+ $ag_{\textbf{PP}}$ $NP_{\textbf{actor}}$) …]

(2) a: Progressive Passive [SUBV $NP_{\textbf{undergoer}}$ (*dh*)$á_{\textbf{PP}}$ + $ADJ_{\textbf{possessive}}$ VN (+ $ag_{\textbf{PP}}$ $NP_{\textbf{actor}}$) …]

or

b: Progressive Passive [SUBV $NP_{\textbf{undergoer}}$ $i_{\textbf{PP}}$ $ADJ_{\textbf{possessive}}$ VN …]

(3) a: Prospective Passive [SUBV $NP_{\textbf{undergoer}}$ $le_{\textbf{PP}}$ VN (+ $ag_{\textbf{pp}}$ $NP_{\textbf{actor}}$) ….]

or

[2] Legend:

SUBV:	Substantive verb	VN:	Verbal Noun
VA:	Verbal Adjective	PP:	Preposition

b: Prospective Passive [SUBV $NP_{undergoer}$ do_{PP} +*a*:$PN_{possessive}$ VN (+ ag_{PP} NP_{actor}) …]

The personal passive construction reframes the event with a focus on the resulting state or the condition of the undergoer participant, depending on the particular variant of the personal passive. This state may be static if the action is completed, as in a perfective passive, or dynamic, as in a passive progressive construction. Each of these potential situations is reflected in the choice of the passive construction template employed. This process of reframing the event to focus on a resulting state or undergoer involves the use of a BE verb, that is, the substantive verb (but never the copula). It also involves the use of less finite verb form, i.e. a verbal adjective or verbal noun, the removal of the actor participant, or the demotion of the actor participant to an oblique position in the syntax. In the personal passive construction, the actor is subject to demotion or suppression while the undergoer carries the stative-resultative aspects of the event in focus. As we will see from our examples, the personal passive is usually not agent deleting but is agent demoting.

We now examine the variants of the personal passive constructions, starting with the perfective variant of the personal passive, and following this, with the progressive and prospective variant constructions respectively.

2.1 Perfective Variant of the Personal Passive

(4) *Tá an leabhar leite agam.*
Be:SUBV-PRES the:DET book:N read:VA at:PP+me:PN
LIT:'Be the book read at me'.
The book is read by me**.**
[**BE'**(**leigh'**(0, an leabhar), **ag'**(mé))]

The agentive phrase is optional and the construction may equally well be expressed without any mention of the agent (5).

(5) *Tá an leabhar leite.*
Be:SUBV-PRES the:DET book:N read:VA
LIT:'Be the book read'.
The book is read.
[**BE'**(**leigh'**(0, an leabhar))]

2.2 Progressive Variant of the Personal Passive

2.2.1 The (A) Template Form of the Progressive Passive Construction

(6) *Tá an doras dhá phéinteáil agam.*

Be:SUBV-PRES the:DET door:N to:PP+its:POSS-ADJ painting:VN by:PP+me:PN

LIT:'The door is to its painting by me'.

The door is being painted by me.

[**do'**(0, [**BE'**(**dhá'**(**péinteáil'**(0, an doras), ag'(mé)))])]

(7) *Bhí hataí agus miotógaí dhá scabadh fríd an aer.*[3]

The hats and belongings were being scattered through the air.

Bhí hataí agus miotógaí dhá scabadh

Be:SUBV-PRES hats:N and:CONJ belongings:N to:PP+for:PP scattering:VN

fríd an aer

through:ADV the:DET air:N

[**frid an aer**'([**do'**(0, [**BE'**(**dhá'**(**scabaigh'**(0, hataí agus miotógaí)))])])]

(8) *Bhí an gloine á bhriseadh.*

Be:SUBV-PAST the:DET glass:NP to:PP+for:PP breaking:VN

LIT:'The glass was to-its breaking'.

The glass was being broken.

[**do'**(0, [**BE'**(**á'**(**bris'**(0, an gloine)))])]

(9) *Bhí an liúdar á rúscadh agus na bádaí gann*.

Be:SUBV the:DET coal-fish:N for:PP stirring:VN and:CONJ the:DET boats:N scarce:N

LIT:'The coal-fish were for stirring and the boats were scarce'.

The coal-fish were being stirred but the boats were scarce.

[**do'**(0, [**BE'**(**á'**(**rúscaigh'**(0, an liúdar))) & (**gann'**(na bádaí)])]

2.2.2 The (B) Template Form of the Progressive Passive Construction

The constructions below follow the (**b**) schema and involve the possessive adjective. In these examples the undergoer of the action is affected and this participant appears

[3] As a convenience to the reader, where the gloss of the data example runs over a line we will state the sentence under discussion in standalone format at the beginning of the example.

in position next after the substantive verb with the activity denoted in a non-finite form as a verbal noun.

These examples are passive and progressive (Ó'Siadháil 1989:295), reflecting an ongoing dynamic state. The verbs, here expressed in the non-finite verbal noun form, are a special class of passive form of stative verbs which refocus the view on the state in a certain way. Crucially, in these examples, the actor is the initiator of the action and is the subject. The same participant, however, is also in the *state of undergoing the action* denoted by the verb in verbal noun form. There is no demotion or promotion.

(10) Schema Template for first person singular participant:
Tá mé$_1$ i mo$_1$ ***VN***.
LIT: 'I am in my VN-ing'.
I am VN-ing.
[**BE'**(mé, (**i**'(**mo'**(VN))))]

(11) *Tá mé i mo chodladh.*
Be:SUBV-PRES me:PN in:PP my:POSS-ADJ sleeping:VN
LIT: 'I am in my sleeping'.
I am sleeping.
[**BE'**(mé, (**i**'(**mo'**(chodladh))))]

(12) *Tá mé i mo chónaí.*
Be:SUBV-PRES me:PN in:PP my:POSS-ADJ living:VN
LIT: 'I am in my living'.
I am living.
[**BE'**(mé, (**i**'(**mo'**(chónaí))))]

Common to each of these examples is the utilisation of the substantive verb followed by the clause subject, followed in turn by the preposition *i* 'in' and a possessive adjective coindexed to the subject, followed immediately by the verbal noun. No oblique actor is specified, or can be specified, because of the nature of the construction.

2.3 Prospective Variant of the Personal Passive

Constructions in the prospective variant of the personal passive are classified as imperfective as they do not denote an action that has finished. Instead, the action has not yet taken place but is expected to occur at some future time.

2.3.1 Active Prospective Clause

(13) *Tá mé le leamh an leabhair.*
Be:SUBV me:PN with:PP reading:VN the:DET book:N
I am to read the book.
[**BE'**(**le'**(**léigh'** (mé, an leabhar))]

2.3.2 Passive Prospective Clause

(14) Tá an leabhair le leamh agam.
Be:SUBV the:DET book:N with:PP reading:VN at:PP+me:PN
LIT:'Be the book to read at me'.
The book is to be read by me.
[**BE'**(**le'**(**léigh'**(0, an leabhar)), (**ag'**(mé)))]

(15) *Tá anál an tsaoil seo le mothú ag éinne ar leacacha an bhaile*.
LIT:'The breadth of this life is to be felt by anyone on the pavingstones of the town'.
The breadth of life is to be felt by anyone on the town streets.
Tá anál an tsaoil seo le mothú ag éinne
Be:SUBV-PRES breadth:N the:DET life:N this:DET with:PP feeling:VN at:PP anyone:N
ar leacacha an bhaile
on:PP flagstones:N the:DET town:N
[**ar leacacha an bhaile'**([**BE'**(**le'**(**mothaigh'**(0, anál an tsaoil seo))), (**ag'**(éinne))])]

2.4 Personal Passive Summary

In the personal passive constructions of modern Irish, the actor is backgrounded by demotion down to an oblique position within a prepositional phrase introduced by *ag* 'at/by', or deleted. The next candidate participant in the logical structure to become the grammatical subject in the syntax is the undergoer. This gives the appearance that the object of the active verb is promoted up to become the subject of substantive verb in the personal passive construction irrespective of variant. This is, however, a side

effect of the defocusing (in the sense of Shibatani 1985) of the actor of the active clause in the passive voice construction.

A number of other voice constructions, specifically the reflexive, middle, and reciprocal (Nolan 2001) appear to have qualities in common with the personal passive. Described in terms of promotion and demotion, they all appear to "promote" or "upgrade" the grammatical object to subject status in some way and may even indicate a structural similarity between subject and object.

We now examine the impersonal passive construction.

3. The Impersonal Passive

3.1 The Impersonal Passive Construction

The impersonal passive verb form occurs with all verbs of Irish, across all tenses, whether intransitive or transitive, The impersonal passive form is also to be found productively with the substantive verb across all tenses. It does not under any circumstances occur with the copula verb. The impersonal passive form can be followed by a prepositional phrase, but only one that is introduced by *le* 'by/with' or *ó* 'from'.

In (16), the matrix verb is in the impersonal passive form. No subject is expressed in the clause. A grammatical object is expressed in the form of a third person pronoun, marked with accusative case. The marker *féin* is post adjacent to the grammatical object of the sentence giving an emphatic interpretation. Emphatic use of *féin* with a grammatical object is sanctioned, as simple proximity to the object entity is all that is required. This example illustrates the use of *féin* with an impersonal passive construction but deployed in an emphatic mode only, and not reflexively.

(16) *Tugadh é féin chun na modh-scoile i mBaile Átha Cliath ina dhiaidh sin.*
LIT: '(Someone) brought him (self) to the model school in Dublin after that'.
He himself came to the model school in Dublin after that.
Tugadh é féin chun na modh-scoile.
Came:V- IMPERS-PASS-PAST he:PN self:PART to:PP the:DET model-school:N

i mBaile Átha Cliath ina dhiaidh sin
in:PP Dublin:N in:PP after:ADV that:DET
[**cun'**(na modh-scoile$_3$, [**i'**(BAC$_4$, [**ina'**(diadh sin, [**do'**[x$_1$, [**tugadh'**(x$_1$, [**é$_2$**'(féin$_2$)])]])])])]
Where : **x$_1$** is an animate and human entity,
and BAC is used as an abbreviation for Baile Átha Cliath.

Example (17) has a construction that, at first glance, appears unusual in that it contains two conjoined clauses, both with the impersonal passive form of their respective verbs.

In addition, the first clause has apparently two arguments and the marker *féin* associated with the second of these in post adjacent position. The second clause has only one argument, the clausal object.

A contributor to the complexity of this sentence is these two arguments in the first clause, which look like subject and object. This cannot be, as the clause verb is in the impersonal passive form and cannot "promote" the object to subject position, in the sense of Givón (1984, 1990).

(17) *Tréigeadh an seanteampall é féin agus fágadh ina bhallóig é.*
LIT: '(Someone) deserted the old church itself and (someone) left it in ruins'.
The old church itself was deserted and left in ruins.
Tréigeadh ***an seanteampall é féin***
(Someone) deserted:V- IMPERS-PASS-PAST the:DET old:ADJ+church:N it:PN self:PART
agus fágadh ina bhallóig é.
and:CONJ (someone) left: V-IMP-PER-PAST in:PP ruin:N it:PN
[**do'**(x$_1$, [**tréig'**(x$_1$, [**an seanteampall$_2$'(é$_2$**'(féin$_2$))])])] &
[**do'**(x$_1$, **fág'**(x$_1$, [é$_2$, [**in'**[**a'$_2$**(ballóig)]]]))]
Where **x** is an animate and human entity, but unknown or irrelevant to the context.

The verb in the first clause has two participants. The first participant is indefinite and specific, but human and animate. The second participant is specific but non-human and inanimate. The problem lies with a potential ambiguity in the clause, which is only removed by the insertion of *é féin*. A speaker uttering *Tréigeadh an seanteampall*

féin … would be ambiguous between these two readings: 1) 'The old church itself was abandoned … ' and 2) 'Even the old church was abandoned … '.

To disambiguate the meaning to the intended first reading it is necessary to replace *féin* with ***é*** *féin* in the clause, hence the strangeness. The additional "argument" is a dummy and does not take an argument position or increase the valency in any way. The marker *féin* is used emphatically in this sentence and not reflexively. In the first clause, there is no visible human subject to act as reflexive antecedent, as the construction is an impersonal passive with no actor in the syntax.

All Irish verbs except the copula have an impersonal passive form. With the impersonal passive form of a verb, no specific definite actor is elaborated in logical structure. The actor is instead specific but indefinite. The actor remains specific because we are committed to their actual existance, but is indefinite to the degree that there is no subject available in argument structure. The *type* or *kind* of this specific indefinite actor is animate, usually human.

3.1.1 Impersonal Construction with an Actor Coded Obliquely

The examples here provide evidence that the actor may be deployed obliquely in impersonal passive constructions. This appears to be a recent phenomenon in the language.

The example in (18) of the impersonal passive does not have an actor expressed in subject position and the verb stem has the appropriate impersonal ending. The inanimate and non-human undergoer of the sentence appears as the grammatical object. This example is interesting for two reasons. The first is that it deploys the phrase *le chéile* 'together' that is normally used as a trigger for reciprocity (Nolan 2001). Use of the marker phrase *le chéile* 'together' is not reciprocal here as no actors are expressed in subject position. The second reason is that the clause, while impersonal, has an actor coded obliquely via a prepositional phrase introduced by *ag* 'at/by'. The actor that is obliquely expressed is not plural, having singular number. The phrase *le chéile* in this example simply denotes manner in relation to the verbal

action. Because English does not have an impersonal passive, the gloss does not quite capture the sense of the sentence. This is better expressed in the literal gloss.

(18) *Cuireadh an tuarascáil parlaiminte le chéile ag Astrid Thors MEP; ball de phobal na Suailainnise san Fhionlainn*.

LIT: '(Someone) put the parliamentary report together by Astrid Thors MEP; a member of the Swedish people in Finland'.

The parliamentary report was put together by Astrid Thors MEP; a member of the Swedish community in Finland.

Cuireadh *an* *tuarascáil parlaiminte le* *chéile* *ag*
Put:V-IMPERS-PASS-PAST the:DET report:N parliament:N with:PP together:PART by:PP
Astrid Thors *MEP;*
Astrid Thors:N MEP:N
ball *de* *phobal* *na* *Suailainnise san* *Fhionlainn*
member:N of:PP people:N the:DET Swedish:N in:PP+the:DET Finland:N

[**do'**(x_1, [**cuir'**(x_1, (**le chéile'**(an tuarascáil parlaiminte**,** (**ag'**(Astrid Thors MEP_1)))))])]

Where : $\mathbf{x_1}$ is an animate and human entity. In this instance, it is the entity expressed obliquely in the prepositional phrase phrase, Astrid Thors MEP.

In example (19), we demonstrate another example of an oblique actor recorded within an impersonal passive construction. The impersonal matrix verb and the verbal noun in this example re both instances of different forms of the same verb coexisting in the same sentence and delivering different functions. No subject is syntactically expressed in the sentence, as to be expected. The grammatical object is inanimate and non-human, being the quantity of money to be allocated. This object of the impersonal passive is the subject of the verbal noun appearing to the left of the verbal noun phrase. The verbal noun is immediately followed by the prepositional pronoun *acu* 'by them', marked for accusative third person plural. This is co-referential in the logical structure with the specific indefinite human animate actor denoted by $\mathbf{x_1}$. This specific indefinite human animate actor is not overtly expressed as grammatical subject in the syntax.

(19) *Caithfear 1.39 milliún Euro (£1.2 milliún) á caitheamh acu ar chúrsaí Bascaise do mhúinteoirí scoile*.

LIT:'(someone) will throw 1.39 million Euro (£1.2 million) for spending by them on Basque classes for school teachers'.

1.39 million Euro (£1.2 million) will be allocated for spending by them on Basque classes for school teachers.

Caithfear *1.39 milliún Euro (£1.2 milliún)*

Throw:V-IMPERS-PASS-FUT 1.39 million Euro (£1.2 million):NP

á *caitheamh* *acu* *ar* *chúrsaí* *Bascaise*

to:PP+for:PP spending:VN by:PP+them:PN on:PP classes:N Basque:N

do *mhúinteoirí scoile*.

to:PP teachers:N school:N

[**ar'**(chúrsaí Bascaise'**(do'**(mhúinteoirí scoile,

[**do'**(x_1, [**caith'**(x_1, (**á'(caith'**(1.39 milliún Euro**,** (**ag'**($siad_1$))))))])]))]

Where : $\mathbf{x_1}$ is an animate and human entity.

3.2 Discussion on the Impersonal Passive

What is common to the impersonal passive constructions in this section is that the actor is backgrounded to the extent that it becomes indefinite, and not, in any way, in focus. The *type* or *kind* of the actor is available as animate, usually human. Crucially, the actor must be specific while indefinite for quite particular reasons. Semantically, the impersonal construction is transitive with two participants recorded in the logical structure, an actor and undergoer. The actor is, however, an "impersonal agent". The clause is syntactically intransitive in that only one argument is expressed in the syntax, that of the undergoer which links to grammatical object. The actor is unexpressed and consequently there is no overt subject in the syntax. However, as the object stays in the same position and maintains object marking, the situation that holds at the level of the semantics must be visible to the syntax. Specifically, the object is not "promoted" to subject in this construction and the unexpressed actor is noted in the syntax by the device of marking by a suffix on the matrix verb. The behaviour of the clause object is very evident when the nominal is a pronoun.

Haspelmath (1997) has recently examined indefinite pronouns across a substantial number of the world's languages, over nine different functional domains. These domains are: specific known, specific unknown, irrealis non-specific, question, conditional, indirect negation, comparative, direct choice and free choice. He finds that in most languages several indefinite pronouns overlap in their distribution, that is, some functions may be expressed by several different indefinite pronouns.

For Irish, Haspelmath (1997:278) identifies an inventory of three series of indefinite pronouns, all of which are derived from generic nouns. The series consists of 1) the non-emphatic *éigin* 'some' series, 2) the negative-polarity series marked by *aon* 'any', and 3) the emphatic *ar bith* 'at all' series. An example of an active clause with specific known/unknown is:

(20) *Dúirt* *duine éigin* *liom* *é.*
Told:V-PAST person:N some:PN with:PP+me:PN it:PN
Somebody told it to me.
[**do'**(duine éigin, (**dúirt'**(duine éigin, (**le'**(mé, é)))))]

The impersonal passive equivalent of the above clause, with exactly the same meaning, is:

(21) *Dúradh* *liom* *é.*
Told:V -IMPERS-PASS- PAST with:PP+me:PN it:PN
Somebody told it to me.
[**do'**(x, (**dúirt'**(x, (**le'**(mé, é)))))]

This evidence suggests that the impersonal passive, with the conflated specific indefinite subject, is an extension of the cline within the functional domains. The agentive indefinite actor and syntactic subject of the active clause in (20) is made more indefinite in the impersonal passive (21) by the backgrounding to the extent that it is no longer explicitly expressed in the syntax of the impersonal passive. We still have a commitment to the actual and real existence of the actor that is now expressed at the semantic level only, in logical structure, and, because of this, it is specific but indefinite. The indefiniteness hierarchy may therefore be:

(22) *sé/sí/siad* 'he/she/them' ___ *duine* 'person' ___ *aon* 'any' ___ **Impersonal passive**
with conflated specific indefinite subject

Within these examples, the actor is backgrounded in the semantics of logical structure but still visible to the syntax as a conflated subject morphologicaly recorded on the verb. The evidence for this is that the object does not, and cannot, occupy the grammatical subject position in these constructions. The subject that is conflated is

specific and indefinite, animate and human. Because this participant is specific but indefinite, the behaviour is very similar to that of normal pronouns when expressed in synthetic forms of the verb, for instance, the third person pronoun with these human attributes.

We argue that the behaviour of the impersonal passive is in line with synthetic verb type behaviours, i.e. 1st person singular and 1st person plural, and others, across the tenses. Irish commonly exhibits this mix of synthethic and analytic usages, but to a greater or lesser degree depending on the region or locality (O Siadháil 1989, Stenson 1987). The impersonal passive behaviour is motivated by the use of the device of conflated subject as a means of backgrounding, but not fully deleting, the actor, and of highlighting the action of the verb itself.

We have however attested several examples above where an oblique agent is expressed at the end of the clause in the same position as the oblique agent of a personal passive passive. This appears to only occur in more recent usages of speech and may be indicative of a change in the underlying template on which the impersonal passive is constructed.

4. Impersonal passive of the Substantive Verb

4.1 The Substantive Verb

Irish has two forms of the verb 'to be', the copula *is* 'be' and the substantive verb *tá* 'to be'. The substantive verb can take a conjugation across all the tenses. For each of those tenses it also has an impersonal passive form. The substantive verb therefore fully supports the impersonal passive construction.

All substantive verb constructions therefore have a corresponding impersonal passive construction. This means that a speaker may choose to utilise the active form of a matrix verb, or may instead utilise a substantive verb construction for the personal passive with any of the three variants discussed earlier in the first section of this paper. It also means that personal passive forms using the substantive may also directly take the impersonal passive form of the substantive construction.

4.2 The Impersonal Passive Form of A Substantive Verb

An impersonal passive form of a substantive verb in a construction that is imperfective is illustrated in example (23). The state-of-affairs denoted by the clause is that of a progressing ongoing activity. The actor of the construction is backgrounded and does not appear anywhere in the syntax. The denoted action is represented by the verbal noun *obair* 'working', and this is fronted by the preposition *ag* 'at'. No verb undergoer is expressed and therefore no clause object is available to the syntax. The verb *obair* 'work' can also be deployed with the impersonal passive form of the verb *obair* itself, or in any of the variants of the personal passive.

(23) *Bítear* *ag* *obair.*
Be:SUBV-IMPER-PASS-HAB-PRES at:PP working:VN
LIT:'(Someone) was working'.
People were working.
[**do'**(x, [**BE'**(**ag'**(**obair'**(x)))])] where **x** is unspecified.

The example in (24) illustrates the impersonal passive form of the substantive verb, with a verbal noun form of a transitive verb denoting a progressing unbounded activity. No actor is expressed. The undergoer is expressed as the direct object of the verbal noun, that is, the direct object of the construction.

(24) *Bítear* *ag* *bhriseadh* *an* *gloine*
Be:SUBV-IMP-PASS-HAB-PRES at:PP breaking:VN the:DET glass:N
LIT:'(Someone) was breaking the glass'.
People were breaking the glass.
[**do'**(x, [**BE'**(**ag'**(**bris**(x, an gloine)))])] where **x** is unspecified.

The example in (25) contains three clauses of which the first utilises the impersonal passive form of the substantive verb. Like the previous example, there is no syntactic argument in subject position as, by definition, the verb is in the impersonal passive form. This particular clause also contains a verbal noun fronted by *á* 'to+for', usually deployed within the prospective passive variant of the personal passive. This clause is therefore an impersonal passive version of the progressive variant of the personal

passive. The second clause contains a substantive verb and denotes the state of *a mac ar dhuine den fhuirinn* 'her son is a member of the crew'. The action of the first clause is concerned with the state denoted in the second clause.

(25) *Bhítear á aidhbhsiughadh díthe go rabh a mac ar dhuine den fhuirinn agus go rabh sé báithte*.

LIT:'Someone was emphasising to her that her son was on person of the crew and that he was drowned'.

Someone was emphasising to her that her son was a member of the crew and that he was drowned.

Bhítear á aidhbhsiughadh díthe

Be:SUBV-IMPERS-PASS-HAB-PRES to:PP+for:PP emphasising:VN to:PP+her:PN

go rabh a mac ar dhuine den fhuirinn

to:PP be:SUBV-PRES her:POSS-ADJ son:N on:PP person:N of:PP+the:DET crew

agus go rabh sé báithte.

and:CONJ to:PP be:SUBV-PRES he:PN drowned:VA

[**do'**($í_1$, ([**BE'**(x_2, (**á'**(**aidhbhsiugh'**(x_2)))] &

[**BE'**(a_1'(mac_3), (ar'(duinne, (de'(an fhuirinn)))))] &

[**BE'**(**báigh'**($sé_3$))]

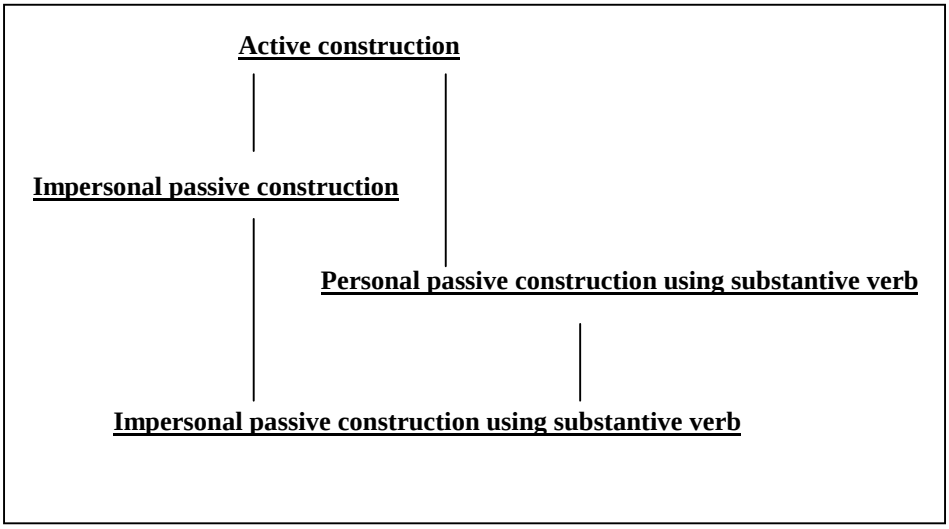
The third clause also contains a substantive verb and denotes the state of the son as *báithte* 'drowned'. The subject of this clause is *sé* 'he' and the state is recorded on the subject via a verbal adjective. This construction is therefore a typical example of a perfective variant of the personal passive. Its function is to describe the resultant state that holds after the action of the first two clauses in the construction.

We therefore have in the totality of this example an impersonal passive version of a progressive variant of the personal passive, followed by a substantive verb clause denoting a state-of-affairs of state and followed in turn by a substantive verb clause that employs the perfective variant of the personal passive.

4.3 Summary of the Impersonal Passive of the Substantive Verb

The availability of the impersonal passive of the substantive verb means that a speaker has a considerable number of strategies that can be deployed as the situation demands. We diagram this map of possibilities in (26).

(26)



5. The GET Passive

5.1 Background

This section investigates whether there is a third passive construction to be found in Irish, that is, a GET passive. The GET passive is attested in many, but not all, of the world's languages (Siewierska (1984).

From the literature, the defining characteristics of the GET passive include the following, which may be used as diagnostics to test for its discovery:

(27) **GET Passive Characteristics**[4]

a. GET passives are "*normally used in constructions without an agent*" (Leech & Svartvik, 1994: 330).
b. GET passives place "*the emphasis on the subject rather than the agent, and on what happens to the subject as a result of the event*" (Quirk et al., 1985:161).
c. GET passives emphasise the subject referent's condition, which is "*usually an unfavourable condition*" (Quirk et al., 1985: 161).
d. GET passives "*describe events that are perceived to have either fortunate or unfortunate consequences for the subject*" (Siewierska 1984:135).
e. The GET passive is likely to have a human subject that is non-agentive, affected and involved, (Givón 1993:119*ff*).

[4] Note: The underline in the quotations are mine in order to bring out certain points for discussion.

f. The GET passive is more likely to be inchoative and punctual, that is, INGR rather then BECOME (Arce-Arenales, Axelrod and Fox.(1993:11*ff*).

g. A GET passive may have an agentive phrase in an oblique position, similar to a BE passive (Arce-Arenales, Axelrod and Fox. 1993:11*ff*).

5.2 The Verb Faigh

Irish has a verb *faigh* 'get' that is a candidate for this construction in some of it usages. To determine whether it meets the required diagnostic characteristics, we need to look at its deployment over a number of GET constructions. The verb *faigh* has a different morphological shape over the tenses and for simplicity, we will use *faigh* to refer to these in a general way. The verb *faigh* has an impersonal passive form for each tense, a non-finite verbal noun and verbal adjective form. As well as having an impersonal passive form, the verb *faigh* can undergo each variant of the personal passive.

The verb *faigh* is transitive, taking two participants, an actor and undergoer. There is a quality about this verb in transitive usages under certain conditions that is particularly interesting. This is when the first participant is not an actor, but an undergoer, and the second participant is a nominal that represents a state. The action of the verb records, then, the fact of the first participant undergoing the state change identified by the nominal in the second participant position.

Even thought *faigh* constructions are transitive, there is a qualitative difference between the construction *fuair*$_{\mathbf{GET}}$ [X NP$_{\mathbf{entity}}$] and the construction *fuair* $_{\mathbf{GET}}$ [X NP$_{\mathbf{state}}$]. The second construction codes a state as a nominal, rather than as a verbal adjective as found in the perfective personal passive. The substantive verb is not employed.

The argument linked to subject position is that of the undergoer and not actor. The fact that the undergoer is coded in subject position reinforces the non-volitional and non-control attributes of the participant. No actor is coded. Indeed no actor coding in subject position is possible with this second construction in transitive form.

The construction is transitive with the undergoer coded as subject, and the state that affects the undergoer is strongly marked as a full nominal in clause object position. The relative coding of these arguments in the construction follows the animacy hierarchy with the human and animate participant coded first as subject and the non-human and inanimate entity coded next as object. The focus of the event is on the resultant state that the undergoer will be in after the event.

Syntactically, the construction is transitive as can be seen from (29) and (30). Schematically the construction differs regarding the role of the participant that takes subject position in the syntax. In example (28) below, the **x** participant is expected to be the undergoer that receives the state change denoted by the second participant, the theme. The undergoer must be human and animate. The situation type is that of an achievement.

(28) *Fuair* ***x*** *bás.*
Got:V-PAST x:N death:N
LIT: '**x** got death'.
x got killed.
[(¬ (**bás'**(x)) & [**do'**(0, (**fuair'**(0, **bás'**(x)))) & **INGR** [**BE'**(x, bás)]]]

The above example may be compared to (29) where the **y** participant merely receives simple possession of the entity denoted by the second participant, the theme. No state change takes place in relation to the first participant. The first participant need not be human or animate in this version of the construction. The clause typically codes for an accomplishment situation type.

(29) *Fuair* ***y*** *an* *úl.*
Got:V-PAST y:N the:DET apple:N
y got the apple.
[**do'**(0, **fuair'**(0, an úl) & **BE'**(**at'**(y), an úl)

The situation types underlying the transitive clause are those of accomplishment (BECOME) or achievement (INGR), depending on whether the state change was instantaneous or gradual. This is reflected by either BECOME or INGR in the logical

structure representations, along with possession of resulting state and the major state change on the undergoer actually affected by action of the verb, such that undergoer undergoes the state changes denoted in the second NP from the verb. Therefore, the first participant NP is not an actor but an undergoer, and the second participant NP is neither actor or undergoer but that of OTHER. Irish codes possession by use of the preposition *ag* 'at/by', as against ownership with *le* 'with' and we will see this reflected in the logical structure representations of these constructions.

In first example above in (28), **x** must prototypically be human and animate but, non-protypically, must be animate at the minimum. The NP *bás* 'death' is an nominal, from the verb *básigh* 'die', denoting the most prototypical state change that a human can undergo, that is, from animate to inanimate.

5.3 Get Constructions That Demonstrate the State Change

5.3.1 State Is Beneficial for Undergoer

Example (30) illustrates this phenomenon and encodes the beneficial state change. The clause is transitive with two participants. The first participant is human and animate and the undergoer of the action, not the actor. The second participant codes the state change that the first participant will undergo. After the event has taken place, the first participant will be transformed in a major way and will have, as a characteristic, the state denoted by the second participant. The state change will not be simple possession. What is important is the affectedness of the undergoer as a consequence of the event. The affectedness is beneficial to the undergoer in this particular example.

(30) *Fuair sé léigheas ar sin.*
Got:V-PAST he:PN healing/medicine:N on:PP that:DET
He got healed of that.
[[NOT [**BE'**(sé, léigheas)]] &
[**ar'**(sin, [**do'**(0, [**fuair'**(sé, léigheas)])])] & CAUSE BECOME [**BE'**(sé, léigheas)]]

The example in (31) is transitive with an undergoer participant as the clause subject. The object of the clause is complex with two conjoined nominals. A determiner with

universal logical scope, *uile* ‘every’, ranges over the plural subjects, such that each member of the set of undergoers is affected by both of the states denoted in the complex sentence object. The affectedness represented by both states is beneficial to all of the undergoers.

(31) *Fuair an uile dhuine a chroí agus a aigneadh ar an tsliabh*.
Every person found their heart and their character on the mountain.
Fuair an uile dhuine a chroí
Got:V-PAST the:DET every:DET person:N their:POSS-ADJ heart:N
agus a aigneadh ar an tsliabh.
and:CONJ their:POSS-ADJ disposition:N on:PP the:DET mountain:N
[[NOT [**BE’**(an uile dhuine, a chroí agus a aigneadh)]] &
[**ar an tsliabh’**[**do’**(0, [**fuair’**(an uile dhuine, a chroí agus a aigneadh)])]] &
CAUSE BECOME [**BE’**(an uile dhuine, a chroí agus a aigneadh)]]

5.3.2 State Has Negative Consequences For Undergoer

The affectedness in example (32) is <u>detrimental</u> to the welfare of the undergoer. The example in (32) is complex and contains two clauses. The <u>first clause</u> has a negative form on the verb *faigh* and shows that this phemomena is visible in this circumstance. An adverbial of time, with scope over the clause, gives the extent in time of the event. The <u>second clause</u> contains a substantive verb and a verbal noun fronted by the preposition *ag* ‘at’, diagnostic of an unbounded progressing activity. The first participant in the first clause is animate and human and the undergoer. No actor is coded. The second participant is inanimate and not human and denotes the state that affected the first participant, but expressed in the negative within the clause. The state of the undergoer acts as the depictive state for the second clause. The state-of-affairs of the second clause is an unterminated unbounded activity and this is a direct consequence of the resulting state of the first clause in the event action chain.

(32) *Ní fhuair sé a sháith am ar bith, agus bhí an t-ocras ag síor-phiocadh an ghoile aige*.
LIT:’He did not get his sufficiency (of food) anytime at all, and the hunger was continually picking at his stomach’.
He never got enough to eat and the hunger was hurting his stomach.
Ní fhuair sé a sháith am ar bith,
Not:NEG got:PAST he:PN his:POSS-ADJ fullness:N time:N on:PP any:ADV
agus bhí an t-ocras ag síor-phiocadh.

and:CONJ be:SUBV-PAST the:DET hunger:N at:PP continual:ADJ+picking:VN
an ghoile aige
the:DET stomach:N at:PP+him:PN
[NOT [**BE'**(sé$_1$, (**a$_1$**'(sáith)))] &
[**ar bith'**(NOT [**do'**(0, [**fuair'**(sé$_1$, (**a$_1$**'(sáith))))])]] &
CAUSE BECOME [NOT [**BE'**(sé$_1$, (**a$_1$**'(sáith)))]]
& [**BE'**(an t-ocras, [**ag'**(**sior-piochadh'**(an ghoile, (**ag'**(sé))))])]

The example in (33) is transitive with a human animate undergoer as the first participant and a second nominal representing the state that will affect the first participant. An adverbial of time informs us as to when the event happened with respect to a certain point in tine known to the dialogue participants, that is, *ceithre bliana roimhe sin* 'four years before that'. The second nominal encodes the most major state change that a living human can undergo, that is, death. This is precicely what this example encodes. As a consequence of this event the animate human will be dead, that is, human but inanimate. The affectedness is not beneficial to the undergoer.

(33) *Fuair m'athair bás ceithre bliana roimhe sin.*
Got:V-PAST my:POSS-ADJ+father death:N four:NUM years:N before:ADV that:DET
LIT:'My father got death four years before that'.
My father died four years before that.
[[NOT [**BE'**(sé, bás)]] &
[**ceithre bliana roimhe sin'**[**do'**(0, [**fuair'**(sé, bás)])]]
& CAUSE BECOME [**BE'**(sé, bás)]]

Example (34) and (35) demonstrate similar characteristics. The states described have two or more major negative consequences for the undergoer.

(34) *Fuair Brighid Ní Mhaoldoraidh íosbairt agus an-bhás ins an réagún a raibh sí.*
Brighid Ní Mhaoldoraidh got hardship and a violent death in the region that she was in.
Fuair Brighid Ní Mhaoldoraidh íosbairt agus an-bhás
Got:V-PAST Brighid Ní Mhaoldoraidh:N hardship:N and:CONJ violent-death:N
ins an réagún a raibh sí
in:PP the:DET region that:REL be:SUBV she:PN
[[NOT [**BE'**(Brighid Ní Mhaoldoraidh$_1$, íosbairt agus bhás)]] &
[**ins an réagún'**[**BE'**(sí$_1$, [**do'**(0, [**fuair'**(sí$_1$, íosbairt agus an-bhás)])])]]

& CAUSE BECOME [**BE'**(Brighid Ní Mhaoldoraidh$_1$, íosbairt)]
& CAUSE BECOME [**BE'**(Brighid Ní Mhaoldoraidh$_1$, an-bhás)]]]

(35) *Fuair sé cupla scannradh*.
Got:V-PAST he:PN several:DET frights:N
He got several frights.
[[NOT [**BE'**(sé, scannradh)]] &
[**cupla'** [**do'**(0, [**fuair'**(sé, scannradh)])]]
& CAUSE BECOME [**BE'**(sé, scannradh)]]

5.4 Discussion of the GET Passive Construction

Not all GET constructions are functional GET passives, only those where the undergoer is the subject and the direct object encodes a state in which the undergoer will be transformed, in some non-trivial way. The GET passive is therefore not de-transitivising. It orders the participants such that the actor is not coded (or coded obliquely), and the undergoer is the clause subject.

A GET passive is not a syntactic passive in the same way that we understand a personal passive construction to be, rather it is a functionally defined passive that exhibits the characteristics mentioned earlier. In the type of GET construction that we have examined, we have found evidence that a particular subset of constructions precisely exhibits these characteristics under strictly defined constraints.

On the basis of this evidence, we claim that this is a functionally defined GET passive. We will place the functionally defined GET passive in relation to the other passive constructions analysed shortly. Before we can approach this we need to examine the word order in the passive constructions.

6. Word Order in the Passive Constructions

We have already mentioned that Irish follows a **VSO** word order and that the subject is more closely bound to the verb than the object. Having looked at the form of each of the passive constructions, we can now briefly examine how word order is maintained through each. The word order in each construction including the active is

reflected in (36). Clearly, we can see that the VSO order is maintained across each of the constructions.

(36)		
	Active:	VSOX
	BE Passive:	SUBV Undergoer/$NP_{\mathbf{SUBJECT}}$ VA/VN {PP $NP_{\mathbf{IO}}$} {*ag* Actor/**NP**}
	GET Passive:	V Undergoer/$NP_{\mathbf{SUBJECT}}$ NP**state**$_{\mathbf{OBJECT}}$
	Impersonal Passive	$V_{\mathbf{IMPER\text{-}PASS}}$+ *Indefinite_Human_Actor* ***SUBJECT*** Undergoer/$NP_{\mathbf{OBJECT}}$
	BE Impersonal Passive:	$SUBV_{\mathbf{IMPER\text{-}PASS}}$+*Indefinite_Human_Actor* ***SUBJECT*** PP VN{Undergoer/$NP_{\mathbf{OBJECT}}$**}**

The need to preserve VSO order across all constructions can be understood to motivate the various construction schemata, and therefore, some of the behaviours of passives. For example, if the subject is deleted from the active clause with [V**S**O] then we are left with [VO], but this is confusing with intransitive and middle voice i.e. [**V NP].** If the subject is not deleted but simply demoted from [V**S**O] then we arrive at a structure of [VO**S]**, but this causes confusion with the interpretation of transitives using [V NP NP]. In the case of the impersonal passive where we have [V $NP_{\mathbf{DO}}$], the verb is marked morphologically to signify this fact, as we seen in our analysis.

The different construction templates are therefore necessary for the avoidance of structural confusion and the functional communication of the intended meaning by the speaker to the hearer. Through out, the VSOX order is maintained. Indeed, from the evidence presented we can see that VSO order is maintained across each of the passive constructions discussed so far, and that it is necessary to do so.

7. A Unified Analysis of the Passive Voice Constructions

In this paper we have examined the personal passive (and each of its variants), the impersonal passive and the impersonal passive form of the substantive verb. Comrie (1977) has claimed that any explanation of the "*impersonal passive should be within the passive domain*". This means that ideally, the impersonal passive should be explainable in a unified way that includes the other passive voice constructions. We have demonstrated this in our analysis.

We posed a question as to whether a third passive forms exists, that of a functionally defined GET passive. To inform our analysis, we determined the characteristics of the

GET passive from the literature in relation to its occurance in the world's languages and these we used these as a set of diagnostics for testing our hypothesis. We demonstrated that sufficient evidence exists to suggest that our hypothesis is true, that Irish does have a functionally defined third passive construction, the GET passive.

7.1 Window of Attention

The commonality underpinning the passive constructions can be explained in terms of the windowing of attention analysis in the sense of Talmy (1996a), which concerns itself with operations on the event frame, i.e. backgrounding, foregrounding, or gapping of event participant elements. The strategies for different types of passive constructions are primarily motivated by the need to background the actor to some degree, or fully. This is informed by the need of a speaker to create a certain focus of some component of the event, that is, by focus considerations. This commonality between each of these passive forms is clearly demonstrated in (37). This indicates where the particular window of attention lies with each construction type.

(37) **Active**

The logical structure (LS) represents the event frame with the window of attention on the actor.

BE passive

LS represents event frame with the window of attention on the resulting state on the undergoer.

GET passive

LS represents event frame with the window of attention on the undergoer that transforms to the resulting state.

Impersonal passive

LS represents event frame with the window of attention on the verbal action.

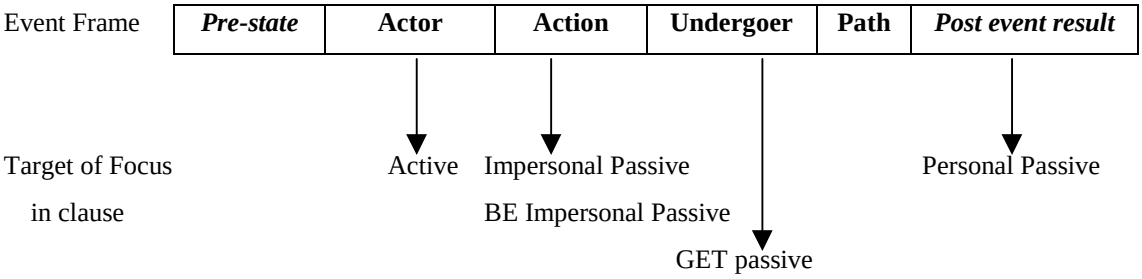
BE Impersonal passive

LS represents event frame with the window of attention on the verbal action.

7.2 Event Frame

This posits an event frame that can highlight the following event structure in an adequate manner. Such a structure is indicated in (38).

(38) **Relationship between perspective on the event frame and clause type**



7.3 Divergences from the Clause Prototype

In terms of divergences from a clause prototype, that is, the active transitive, we have found the following:

(39)

	Prospective passive:	SUB**V** **S**$_{undergoer}$ *le* VN (*ag* NP$_{actor}$)
	Progressive passive:	SUB**V** **S**$_{undergoer}$ (*dh*)*á* VN (*ag* NP$_{actor}$)
	Perfective passive:	SUB**V** **S**$_{undergoer}$ VA (*ag* NP$_{actor}$)
Prototype:	Active Transitive:	**V S O**
	Active Intransitive:	**V S** or SUB**V** **S** *ag* VN
	GET passive:	**V S**$_{undergoer}$ **O**
	Impersonal passive:	**V**$_{impersonal}$ + *Indefinite_Human_Actor* ***SUBJECT*** **O**$_{undergoer}$
	BE Impersonal passive:	SUB**V**$_{impersonal}$ + *Indefinite_Human_Actor* ***SUBJECT*** PP VN **O**$_{undergoer}$

We have analysed the passive constructions of modern Irish and demonstrated that they have an underlying commonality that is best explained in a functional analysis with an event frame perspective sensitive to prototypicality. This analysis takes the active transive clause as the base prototype, from which the other constructions diverge. Included in this commonality is the functionally defined GET passive.

8. References

Arce-Arenales, Manuel, Melissa Axelrod and Barbara A. Fox. (1993). Active Voice and Middle

Diathesis. In Fox, B and P.J Hopper (1993).*Voice, Form and Function*. John Benjamins Publishing Company.

Comrie, B. (1977) . In Defense of Spontaneous Demotion: The Impersonal Passive, in: *Grammatical Relations. Syntax and semantics Volume 8*. Academic Press. London.

Dowty, David R. (1979). *Word Meaning and Montague Grammar*. Reidel. Dordrecht.

Dowty, David R. (1986). Thematic Roles and Semantics. *Berkeley Linguistics Society* 12: 340-54.

Dowty, David R. (1989). On the semantic content of the notion "thematic role". In B. Partee, G. Chierchia, and R. Turner (eds) *Properties, Types and Meanings*, volume 2, 69-130. Knuth. Dordrecht.

Dowty, David R. (1991). Thematic proto-roles and argument structure selection. *Language* 67: 574 - 619.

Givón, T. (1981). Typology and functional domains, in: *Studies in Language* 5.2.

Givón, Talmy (1983). *Topic Continuity in Discourse: A Quantitative Cross-Language Study*. John Benjamin. Amsterdam and Philadelphia.

Givón, Talmy (1984). *Syntax: A Functional-Typological Introduction*. Vol. 1. John Benjamin. Amsterdam and Philadelphia.

Givón, Talmy (1990). *Syntax: A Functional-Typological Introduction*. Vol. 2. John Benjamin. Amsterdam and Philadelphia.

Haspelmath, Martin (1997). *Indefinite Pronouns.* Oxford Studies in Typology and Linguistic Theory. Oxford University Press. Oxford.

Langacker Ronald and Pamela Munro (1975). Passive and their Meaning, in *Language 51.4*.

Nolan, Brian (2001). *Reflexive and Reciprocal Constructions in Modern Irish*. ALT conference on Reflexives, Middles and Reciprocals at the University of Tunis, Tunisia.

Ó Siadháil, Michéal. (1989). *Modern Irish*. Cambridge University Press. Cambridge MA.

Russell, Paul. (1995). *An introduction to the Celtic Languages*. Longman London.

Shibatani, M. (1985). Passive and Related Constructions: A Prototype Analysis, in. *Language* 61.4.

Shibatani, Masayoshi. (1988). *Passive and Voice*. Typological Studies in Language. John Benjamin Publishing Company. Amsterdam, Philadelphia.

Shibatani & Thompson. (eds.) (1996). *Grammatical Constructions, their form and meaning*. Clarendon Press, Oxford.

Siewierska, Anna. (ed.). (1984). *The Passive: A Comparative Linguistic Analysis.* Croom Helm London.

Siewierska, Anna. (ed.). (1998). *Constituent Order in the Languages of Europe.* Empirical Approaches to Language Typology. Eurotype 21-1. Mouton de Gruyter. Berlin & New York.

Stenson, Nancy (1981) *Studies in Irish Syntax*. Narr, Tubingen.

Tallerman, Maggie. (1998). In (ed) Siewierska, Anna: *Constituent word order in the Languages of Europe*. Empirical Approaches to Language Typology. Eurotype 21-1. Mouton de Gruyter. Berlin & New York..

Talmy, Leonard. (1978). Figure and Ground in Complex Sentences, in J. H. Greenberg (Ed). *Universals of Human Language iv: Syntax.* Stanford University Press. Stanford, California.

Talmy, Leonard. (1985). Lexicalisation patterns: Semantic Structure in Lexical Forms in T. Shopen (Ed), *Language Typology & Syntactic Description* iii: Grammatical Categories and the Lexicon. Cambridge University Press. Cambridge MA.

Talmy, Leonard. (1988). Force Dynamics, in language and cognition, *Cognitive Science* 12:49-100.

Talmy, Leonard. (1996a). Windowing of attention in language in *Grammatical Constructions, their form and meaning* by Shibatani & Thompson. Clarendon Press, Oxford.

Talmy, Leonard. (1996b). Fictive motion in Language and "Ception": The Emanation Type, in P. Bloom et al (Eds.), *Language and Space*. MIT Press. Cambridge MA.

Van Valin, Robert D. (1993). *A Synopsis of Role and Reference Grammar. In Advances in Role and Reference Grammar,* ed. R. D. Van Valin, Jr. 1-164. John Benjamins. Amsterdam.

Van Valin, Robert D, Jr (1998) *Cross Linguistic Patterns of Linking*. MS. State University of New York ant Buffalo.

Van Valin, Robert D. and LaPolla, Randy J. (1997) *Syntax : structure, meaning, and function* Cambridge textbooks in linguistics. Cambridge University Press. Cambridge MA.

Vendler, Zeno. (1967). *Linguistics in Philosophy*. Cornell University Press. Ithaca. NY.

An evaluation of CAN8 as a Computer Assisted Language Learning tool in the context of current research.

Ruth Harris. Institute of Technology Blanchardstown

The CAN8 virtual language laboratory combines features of traditional language laboratory systems with typical CALL software and features of CBT to create a language learning environment which embraces many different theories of learning and more specifically of language learning.

Features of traditional language laboratories include:

- Listening and viewing of audio and video materials
- Student participation through listening, repeating and reviewing
- Teacher intervention to provide feedback

CALL type exercises (with feedback and scoring)

- Multiple choice questions
- Gap-filling
- Text-writing based on oral or written stimuli

CBT features

- Presentation screens for introducing materials
- Verbal instruction to guide students through a lesson
- Menu-driven to give students navigation control
- Tracking and scoring to allow the teacher monitoring control

Given the features outlined above, the question one must ask is if the technology of the CAN8 system is in fact effective in supporting language learning and if it has acquisition enhancing features which can lead to successful L2 learning. Several areas of research need to be looked at in this context, namely the broad principles of Second

Language Acquisition research, theoretical underpinnings of multimedia and aspects of the psychology of learning. A suggested best practice for designing lessons on CAN8 allows for integration of the theoretical background and evaluation of shortcomings outstanding in the light of recent research on technology in learning.

1. Second Language Acquisition theory

A brief overview of the requirements for second language acquisition to take place allows us to see how classroom teaching and by extension technology and in particular CAN8 can provide optimal learning environments. For this purpose, a basic model for language acquisition based on communicative methodologies will be used, summarised by Pica (1994) but drawing on work by Krashen (1980, 1985), Long, (1983, 1985), Swain (1985), Schmidt (1990), Lightbrown & Spada (1990)

Pica sees three ***learner related requirements***:

1. Comprehensible input must be provided which learners access for meaning
2. Learners produce modified output based on this new input
3. Learners need to attend to form, preferably at both the input and output stages

Process-related requirements are seen to be:

1. Positive input: input that is grammatically systematic must be available to serve the learning process
2. Enhanced L2 input which makes subtle use of more salient features can assist the learning process.
3. Feedback and negative input is needed to provide learners with meta-linguistic information on the clarity, accuracy and / or comprehensibility of their interlanguage.

The ***negotiation of meaning*** is seen to be one of the main ways in which input and output are manipulated in tandem to produce meaning but also to achieve levels of modification on the part of the learner's production. Pica defines negotiation of meaning thus:

> This term has been used to characterise the modification and restructuring of interaction, that occurs when learners and their interlocutors anticipate, perceive, or experience difficulties in message comprehensibility. As they negotiate, they work linguistically to achieve the necessary comprehensibility, whether repeating a message verbatim, adjusting its syntax, changing its words or modifying its form and meaning in a host of other ways.

While in recent times, the frequency of modified output arising from negotiation of meaning as a major feature of classroom interaction has been questioned, it still serves as a metaphor for the type of dialogue which occurs in classrooms between active learners and teachers. While it is a normal part of classroom discourse, it can be more difficult to incorporate into technology driven coursework. However, research by Ellis (1995) has shown that by pre-modifying input as one would expect to happen spontaneously in a classroom situation, an approximation of negotiation was arrived at and students seemed to benefit equally from this. In the context of CAN8, several modified forms of meaning can be presented through interactive processes, and with the presence of the teacher as interlocutor as well as the software, the negotiation of meaning can be extended beyond the technology to the human dimension.

2. The development of technology for language teaching

2.1 From language laboratory to multimedia laboratory

Traditionally the language laboratory was seen to be a learning environment which supported behaviourist theories of learning in the form of drill and practice, mostly listen and repeat. While behaviourist theories in the context of language learning have been largely dismissed since communicative methods have replaced audio-visual methods, there remains some place for some aspects of behaviourism. This is true particularly with regard to physiological aspects of language learning such as the training of the speech organs to produce sounds correctly through imitation and practice. In keeping with more modern thought on learner reflection, there are also deeper processes at work at the same time which can be built in at a more cognitive level such as attention to form and phonetic components. Wild (1996) notes:

> In much of the current and recurring debate about the role of educational and learning theory in instructional technologies (especially multimedia), there seems to be a readiness to polarise one theory of learning (behaviourism) with a meta-theory (constructivism), and further, to present the former as grossly deficient and the latter as the only credible explanation of student learning… there are various dimensions in different theories of learning, and not all fit along an imaginary continuum connecting two extremes.

The main difference between the language laboratory features of the traditional lab and of this virtual lab is probably in the pacing of the exercises. While the traditional lab led the student through a series of exercises at a pre-determined pace, this has given way to a more learner controlled environment where the learner has time to engage in the learning process, taking time to notice linguistic features and make evaluations of his own performance on the basis of feedback.

2.2 From floppy disk to multimedia

Many of the early CALL packages resembled language laboratory-type drills in written format, focussing on grammatical structures, at a time when behaviourist theories were already being discarded in favour of more communicative type approaches to language teaching. Watts (1997) in his evaluation of CALL software notes Cook's remark that

> there is a mismatch between the views of language teachers that students learn by making realistic use of language and CALL assumptions that students learn by drilling and mastering rules.

Watts notes that the advent of interactive multimedia did not necessarily mean a re-thinking on content, but rather adding on features and notes Conomos (1995) description of this sort of software as "shovelware".

Watts puts forward a learner-based approach to multimedia design in keeping with current thinking on language learning. The first reaction one would have on reading it is that it would be impossible for any one piece of software to fulfil the expectations put forward by Watts. On further reflection, it becomes apparent that perhaps only an authorable multimedia system such as CAN8 can be flexible enough to deliver on many of the suggested features.

Watts' main recommendations are to empower the learner as much as possible by giving him choice and control over his environment and sees this essentially in four areas. In the area of learner needs, he notes:

- The need for ***learner autonomy***, not just in process but also in content. CAN8 allows for discussion with learners in advance of design of their needs. It also allows for open-ended tasks to allow for learner expression.
- ***Mindful engagement*** is facilitated by the provision of menus and a range of exercise types clearly leading to an overall outcome.
- ***Learner strategy development*** is ongoing with student access to a visual representation of sound bars, for example and suggestions on how to approach a lesson.
- ***Different learner styles*** are facilitated through different exercises and by providing the student the choice of working with sound or with text + sound, or image + sound or text + image.

Other recommendations in the area of learner situations include the need to provide at times a totally autonomous individual environment possibly in distance learning mode and at other times a co-operative learning environment. In fact CAN8 provides a platform for each of these learning situations and allows for a combination of each.

2.3 Re-humanising the computer interface.

An important point with CAN8, is that unlike ready-made software, the teacher still has an important role to play in providing feedback and interaction. Barnett (1998) in

his article "Teacher off: computer technology, guidance and self-access", considers the role of the teacher in the context of new technologies, and in the overwhelming move towards self-access which technologies seem to imply. While he goes to great lengths to look at how the technology can replace the teacher as magister (information feeder) pedagogue (information source) as put forward by Higgins (1984) or as guide (trainer in strategies) as he suggests himself, and notes Meskill's study where provision of on-line messages re-humanised the face of her software, keeping the teacher within the loop does not appear to be an option. Many CD-ROM based language learning packages go to incredible lengths to anticipate all possible questions, or to provide feedback for a whole range of acceptable, semi-acceptable and unacceptable learner responses. Keeping the teacher as a flexible source of feedback may be more effective in terms of satisfactory learner interaction and also more cost-effective in terms of avoiding unnecessary programme preparation for hypothetical needs.

3. Psychological aspects of language learning and task design: Acquisition-promoting language tasks

Much research has been carried out in the area of learning psychology in general and in language learning in particular on the types of activities which enhance language acquisition.

3.1 Depth of processing

Craik & Lockhart (1972) put forward their Depth of Processing model which posits that processing of verbal information normally takes place at an automatic level and is processed superficially. By creating tasks at different levels of depth, the learner can be forced to engage in deeper levels of processing. The higher the level of cognitive engagement in the task, the greater the level of retention.

Based on these theories, Paribakht & Wesche (1997) carried out research to evaluate the types of possible tasks which learners and teachers find useful for promoting language acquisition and in this case in particular, vocabulary acquisition. They suggest 5 levels of task from low levels of engagement at the noticing level to high levels of engagement at the production level.

1. Selective attention: target words bold-faced or in italics, or glossary provided
2. Recognition: Matching words with definitions, synonyms, pictures etc.
3. Interpretation: Selecting correct and incorrect words, choosing from an MCQ
4. Manipulation: manipulating grammatical or morphological features
5. Production: cloze exercises, answer questions etc.

They found that students tended to prefer type 1 and 3 exercises, and it is important to note that these are still low in the area of engagement, and are fairly typical of many textbook type exercises. It is interesting to note that in that study, learners and teachers estimated that their learning gains were at around 60%, when in fact they were only at 36%. This would suggest that learners often content themselves with relatively superficial levels of engagement and over-estimate the level of acquisition they have reached with regard to new features of language, whether formal or lexical.

3.2 Generative models of learning

Joe (1998) carried out a similar study on the value of task-based learning, but she focused on the higher levels of engagement and in particular on generative type exercises. Her research found that generative processing enhanced learning, with greater levels of generative processing leading to greater levels of vocabulary gains. She used Wittrock's (1975) generative model as a basis for her design.

> The underlying assumption behind the generative model is that generative processing, generation or elaboration leads to improved retention by learners actively generating their own creative versions of language in response to target items read in a text for example, reformulating in their own words the meaning of a word and enriching and embellishing aspects of the target item

> which relate to existing knowledge. This process connects new information with existing information and enriches new items with what is already known.

Recall of recently learned language seems to have a double effect, and she notes Baddeley (1990)

> The act of successfully recalling an item increases the chance that the item will be remembered. This is not simply because it acts as another learning trial, since recalling the items leads to better retention than presenting it again: it appears that the retrieval route to that item is in some way strengthened by being successfully used.

While Craik & Lockhart's depth of processing model proposed an alternative to short term and long-term memory, there is a strong case for looking at generative learning as operating on information which is temporarily stored in working memory and which through recall and retrieval is committed to long term memory.

Implications for CALL:

It is clear that repetition and recognition type exercises alone will not be sufficient to create a depth of processing of language which will lead to satisfactory levels of acquisition. The challenge therefore is to harness the multimedia systems available to create greater depth of processing and higher levels of interaction to promote an enhanced acquisition-promoting environment.

3.3 An evaluation of the multimedia environment for language learning.

Research on multimedia in general tends to focus on the advantages of the multimedia environment over the paper environment, software over books, and the addition of sound to a previously silent means of presentation of material. The aim was therefore to create teaching materials which were different to books and imitated the lecture or lab and provided the learner with interactive opportunities to learn. In the context of language learning, the focus has been slightly different. While language learning also

drew on paper based resources, we also had a generation of technology-based learning environments which were based on audio, in the case of tape recorders and language laboratories and video in the case of TV / video based classes. Multimedia therefore in real terms meant the addition of textual and graphic support to a previously audio–dominated environment. Language learners staring into space as they mechanically repeated sentences in a language laboratory gave way to learners interacting with textual support and graphic and video displays.

3.4 Dual-coding theory

Paivio's dual coding theory supports the importance of imagery and visualisation in cognitive operations, and while it is important in all areas of educational psychology, it has particular applications in the area of language learning. Paivio states (1986)

> Human cognition is unique in that it has become specialised for dealing simultaneously with language and with non-verbal objects and events. Moreover, the language system is peculiar in that it deals directly with linguistic input and output (in the form of speech or writing) while at the same time serving a symbolic function with respect to non-verbal objects, events, and behaviours. Any representational theory must accommodate this dual functionality.

He identifies three types of processing involving dual-coding:

1. Representational: verbal or non-verbal information is directly activated
2. Referential: verbal information is activated by non-verbal information or non-verbal information is activated by verbal information
3. Associative processing: representations within the same systems are activated.

3.5 Towards a psycho-linguistic model of lexical development.

In the context of second language learning, the use of visual image with the L2 graphemic or phonetic representation has the further value of strengthening the connection between the "signifié" or signified object and that of the "signifiant" or signifier, while by-passing the L1 translation which often impedes progress in acquisition of a new word in its semantic entirety. In Jiang's (2000) analysis of lexical representation in L2 acquisition, he notes that there are three stages of lexical development and in many cases poor learners may never get past the early stages, and in fossilisation, learners fail to reach the final stage.

Stage 1

While L1 words are learned as both semantic and formal entities, L2 words are learned mainly as formal entities, the meaning being provided through association with the L1 word. This means that the L2 items have no lemmas (semantic and syntactic information). This is the formal stage of lexical development. Grammatical information is stored in a separate area of the L2 learner's knowledge and cannot be accessed automatically. He summarises the problem thus:

> In receptive use of the language, the recognition of an L2 word activates its L1 translation equivalent, whose semantic, syntactic, and morphological information then becomes available and assists comprehension. In productive L2 use, the pre-verbal message first activates the L1 words whose semantic specifications match the message fragments. The L1 words activate the corresponding L2 words through the lexical links between L1 and L2 words.

Stage 2 The L1 lemma mediation stage

At the second stage, the L2 lexical item has the lemma from the L1 equivalent and this is activated automatically.

> Information in L1 lemmas may be copied or attached to L2 lexical forms to form lexical entries that have L2 lexical forms but semantic and syntactic information of their L1 translation equivalents.

He notes that no morphological information is carried by the entry at either the first or second stage. Another important point is the fact that the L2 item has a very weak conceptual representation, and furthermore the L1 lemma is weak, part of it being lost in translation.

Stage 3 The L2 integration phase.

At the third stage the lemma for the L2 entry becomes filled out semantic, syntactic and morphological, as well as formal specifications about an L2 word are established within the lexical entry.

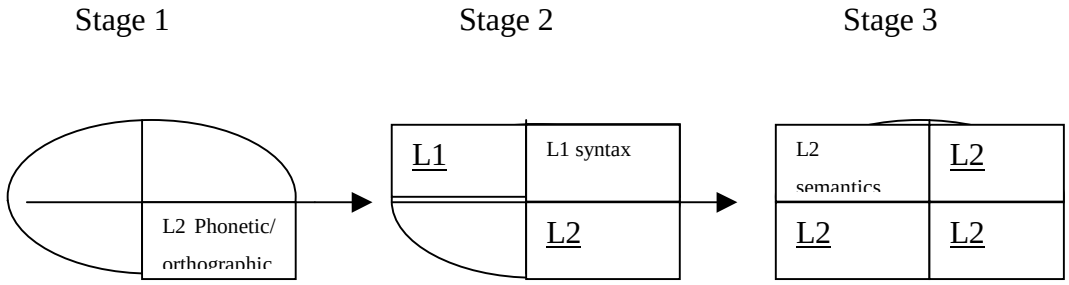


Figure 1. Jiang's model for the development of lexical competence.

An obvious aid to enriching the lexical entry for individual words would be to provide more visual material, and if this is evocative enough of the new cultural context, it might serve to move the L1 concept out of the L2 lemma space. Thus, learning the word "boulangerie" meaning bakery would be re-enforced if new information on the word included a visual representation of the concept, to displace the image of a bkery in an English-speaking context, which might very well be the sliced bread corner of the local supermarket.

3.6 Which visual aids?

While the value of visual materials is accepted, the choice of materials also needs to be considered. It is important that they aid comprehension rather than obstruct it. Poor use of visual aids can be distracting and may overload the learner's working

memory, leading him into irrelevant conceptualisations of supplementary materials rather than on focusing on the materials which are directly presented to him.

For this reason, Chun & Plass (1997) would argue that in using multimedia, a single still image should be used for a single lexical item. This provides an immediate representation of an unfamiliar object without overloading the cognitive facilities of the student. A video clip, which will provide a lot of incidental information not directly relevant to the understanding of a word may not leave the learner with a clear message, and later recall may in fact link the lexical item with some other element of the video clip. Other researchers such as Al–Seghayer (2001) have found that a video clip which clearly demonstrates an action, such as a yawn breaking out on somebody's face may however be more effective than a single image, as the element of curiosity at the blank face subsequently breaking into a somewhat humorous image may cause deeper levels of processing.

On the other hand, the value of video as an advance organiser, either to trigger background information or to provide new background information has been shown to be considerable. This would be in keeping with learning strategies in general and in particular in an autonomous or semi-autonomous learning environment where learners may not have enough linguistic competence to interpret the context of the information provided solely from its phonetic or graphemic format. This is especially true for culture specific information, and also for areas of LSP where the visual context can clarify a very specific area of language use which in real terms would rarely be divorced from its practical application.

4. The application of theory to design of a CAN8 lesson

Authoring on CAN8 is seen by many language teachers as being extremely time-consuming. However, this perception needs to be re-evaluated in the context of other authoring systems. Because the system is an authoring shell rather than a tool, the amount of time taken to create exercises is considerably less than for Authorware for example. Because it allows for integration of many different types of exercises, the

lesson designed will probably be considerably more effective than an equivalent exercise using a traditional language laboratory or paper-based materials, and levels of acquisition far greater.

By creating graded types of exercises, the student moves from lower levels of engagement such as recognition to higher levels of engagement with production. The process from recognition through to production has strong acquisition-promoting features, and as long as the student has the possibility of reflecting on this process as it is on-going through automatic feedback, scoring or teacher intervention, long-term memorisation of features should occur.

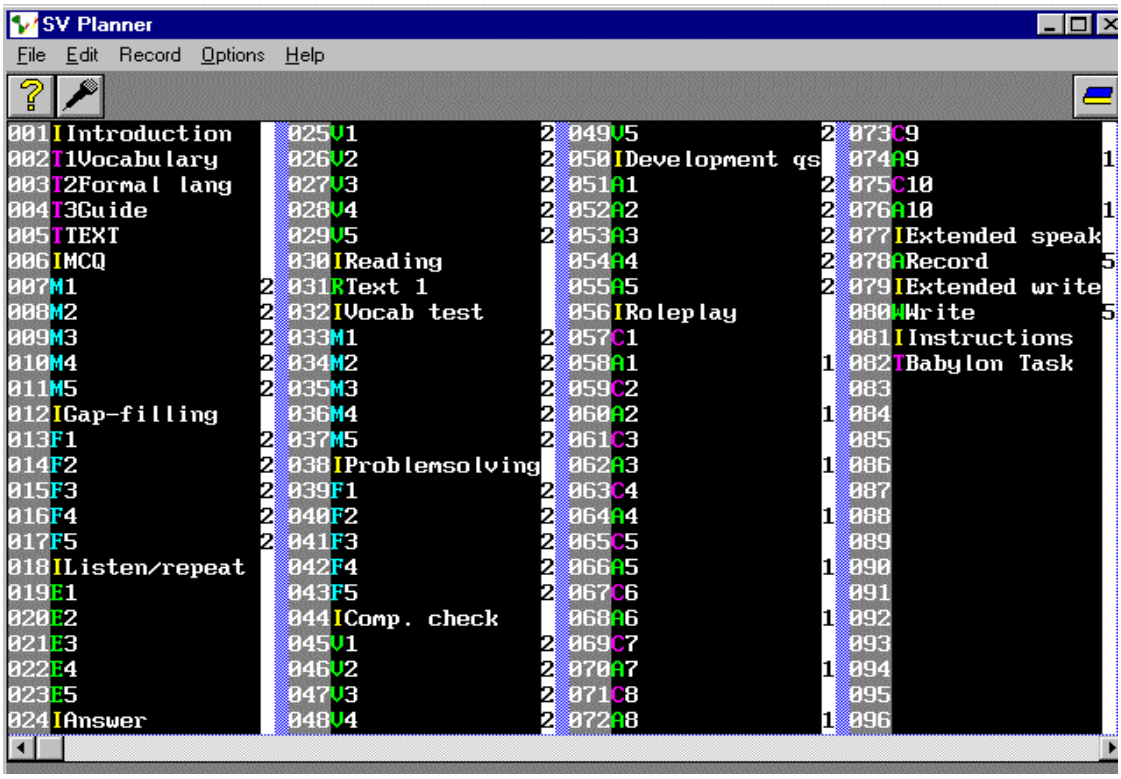


Fig 2. The planning screen for a CAN 8 lesson. The letter indicates the code for the particular type of exercise which may not immediately be evident from the context. Marks attributed to each exercise in the right-hand column add up to 100% and may be kept over a term for continuous assessment purposes.

Presentation stage

Teacher screen 1: Presentation of key vocabulary occurring in lesson (or several screens with graphics for each image), with or without sound

Teacher Screen 2: Presentation of grammatical feature(s) in lesson (with or without sound)

Teacher Screen 3: Presentation of suggested path and learner strategies which might be used during this lesson

Teacher Screen 4: Authentic sound or video recording of learning material.

Recognition stage: Familiarisation with lexical and grammatical features in context. (the sound recording can remain available to the student as a reference. Graphics can be added to aid referential processing)

(M) Multiple choice questions: a series of questions to test recognition of key vocabulary or other content

(F) Gap-filling: a series of gapped sentences based on key vocabulary or formal language

Oral Practice stage: From repetition to production

(E) Repetition screens: Each sentence can be repeated. A graphic display allows for comparison with an audio model to help the student analyse his own production.

(V) Speak and check: The student pronounces a sentence, then checks the model for the correct answer. The input can be either a sentence to be read, a sentence to be translated or a question to be answered.

(R) Reading For longer practice at the end of a lesson, the student can be required to read the entire text. The teacher must listen, mark and provide feedback.

Production without support: Evaluating and problem-solving (the sound file may be removed at this point, leaving only the graphic support or video)

(M) Multiple choice questions: Students choose correct forms of vocabulary, meaning, spelling or morphology

(F) Gap-filling: Comprehension type exercises where students use comprehension strategies and problem-solving skills to find correct answers

(V) Speak and check: Simple comprehension questions can be asked. The student provides the correct answer orally and records his answer. He then checks the model answer.

(A) Answer a question: As above, but no model answer is provided. The teacher listens in and checks.

Extended production exercises:

(C+A) Roleplay: The student can play the role of a character in a dialogue or interact with the teacher in a pre-recorded set of questions pertaining to the area studied. Text support can be provided in the form of hints, L1 or L2 vocabulary can be provided on screen to help the student to construct answers.

(A) Extended speaking Open speaking exercise: the student is asked to speak at some length using the language which has been learned in the lesson and record their answer. Again support can be provided in the form of an image, vocabulary, outline of what is expected etc. The teacher needs to listen and mark.

(W) Extended writing Similar to the speaking exercise, the student writes a paragraph. The teacher reads and marks or can print out and correct.

Babylon: this feature allows for pairwork, students are given a production task / paper –based gap information task and

have the opportunity to work together in oral interaction.

5. A re-appraisal of multimedia learning environments

While technology has led the way for creating learning environments which previously could not have been dreamed of, it is important that advances in technology do not dictate pedagogical issues. While this has already been highlighted in the design of multimedia materials, it is also important to consider the appropriateness of using multimedia materials at all. There has been some criticism of multimedia learning environments in recent times and an overview of these criticisms is revealing.

The first criticism is with regard to the depth of learning where Hannafin & Richter (1989) argue that methods used in CAL programmes typically such as

- Small learning units
- Controllable sequences
- Discrete discernible steps
- Behaviourally defined objectives and criteria

do not encourage deep mental processes.

Research by McAlpine (1996) shows that in certain conditions, learners learn better from multimedia materials than in others. He compared two groups in two different contexts and compared their reactions. The features which the high response group reported were:

- The programme was easy to use
- It fitted in well with the overall course
- It required them to think deeply about the topic
- It helped them gain an in-depth understanding of the topic.

The low response group reported opposite effects: little apparent relevance to overall coursework, did not contribute to deeper understanding etc.

He notes that this relates back to Jonassen's (1988) 4 levels of information processing strategies:

- Recall
- Integration
- Organisation of existing and new schema
- Elaboration: using and making judgements on the materials

As CAN8 materials can be authored on a week by week basis as the students require them, levels of integration far beyond those provided by ready-made CD-ROM materials can be achieved. They can tie in very precisely with the materials studied on other parts of the course.

There is also some debate on whether theories of instructional design such as those put forward by Merrill (1996) are ultimately incontestable and scientific. Wild (1996) does question them in the light of current research on the value of socially-mediated learning and collaborative learning tasks. He sees the individual working alone through a computer programme as being far from the optimal learning situation. He attempts to re-connect the concept of an artificial learning environment with real learning events, thus extending the relevance of CAL based learning materials. This belief has been re-iterated by other researchers such as Kearsley (1998) who believe that meaningful engagement in tasks can only be based on collaborative learning situations and real learning goals which go beyond the virtual environment.

Conclusion

While technology has been shown to be effective in promoting and facilitating learning, and CAN8 appears to correspond to the requirements for effective language learning in so far as it matches the requirements outlined in theoretical underpinnings, there remains an overall context which has not been resolved. If collaboration in learning is seen to be so important, then this should be even more so in the context of language learning. There remains a possibility of compromise in the context of Vygotskian learning patterns: if learning is seen to take place first of all between

human beings on an inter-psychological level and subsequently internally on an intra-psychological level, multimedia learning materials may well be effective at the second stage. The challenge to make multimedia work at the inter-psychological level, attempting to simulate negotiation of meaning and understandings and a human interface, may not be worth the effort. Let multimedia do what it does well, then switch the teacher back on again and allow our learners to talk to each other, and through collaboration and discussion deepen their understanding of their chosen field.

Bibliography:

Al-Seghayer, K (2001) "The effect of multimedia annotation modes on L2 vocabualry acquisition: a comparative study", in *Language Learning & Technology*, Vol 5 No 1 pp 202 – 232.

Baddeley, AD (1990) *Human memory: Theory and practice*, Hove: Lawrence Erlbaum Associates

Barnett, L (1993) "Teacher off: computer technology, guidance and self-access" in *System*, Vol 21, No 3, pp 295-304.

Chun D & Plass J (1997) "Research on text comprehension in multimedia environments" in Language Learning & Technology, Vol 1, No 1

Cook, VJ (1988) "designing CALL programmes for communicative teaching " in *ELT Journal*, 42, pp262 – 281.

Craik FIM & Lockhart RS (1972) "Levels of processing: a framework for memory research" in Journal of verbal learning and verbal behaviour 11: 671-84

Hegelheimer V & Chapelle C (2000) "Methodological issues in research on learner-computer interactions in CALL, in Language Learning & Technology, vol 4, No 1 pp 41-59

Higgins J, (1984) *Computers in language learning*, London: Collins

Jiang, N (2000) "Lexical Representation and Development in a Second Language" in *Applied Linguistics*. 21/1:47 – 77.

Jonassen, DH (1988) *Instructional design for Microcomputer Courseware*, Hillsdale NJ: Lawrence Erlbaum Associates

Joe, A (1998) "What Effects Do Text-based Tasks Promoting Generation Have On Incidental Vocabualry Acquisition?" In *Applied Linguistics*, 19/3: 357-377

Kearsley G & Schneiderman B, "Engagement theory: a framework for technology-based teaching and learning" http://home.sprynet.com~Kearsley/engage.htm

Krashen, S (1985) *The input hypothesis: issues and implications*, London: Longman

Laufer, B & Hulstijn J (2001) "Incidental Vocabulary Acquistion in a Second Language : the construct of task-induced involvement" in *Applied Linguistics*, 22/1: 1 – 26

Lightbrown P & Spada N (1990) "Focus-on-form and corrective feedback in

communicative language teaching: Effects on second language learning", in *Studies in Second Language Acquisition*, 12, 429 – 448.

Long, MH, (1985) "Input & Second Language acquisition theory", in Gass, SM & Madden CG (eds) *Input in Second Language acquisition*, Rowley MA: Newbury House.

McAlpine, I (1996) "A qualitative study of learning from CAL programs in two tertiary education courses" in Hedberg G et al. (eds) *Learning Technologies: prospects and pathways*, selected papers from EdTech 1996. Canberra: AJET

Merrill, D et al., (1996) "Reclaiming the discipline of instructional design". Available LISTSERV@UGA.CC.UGA. IT-FORUM, 19 February 1996

Paribakht & Wesche (1997) "Vocabulary enhancement activities and reading for meaning in second language acquisition" in Coady J & Huckin T, (eds) *Second Language Vocabulary Acquisition*, Cambridge, CUP

Pica, T (1994) "Research on Negotiation: What Does It Reveal About Second Language Learning, Conditions and Outcomes?" in *Language Learning* 44:3, pp 493-527

Plass, J (1998) "Design and evaluation of the user interface of foreign language mulitmedia software: a cognitive approach" in Language Learning & Technology, Vol 2, No 1, pp35 – 45

Schmidt, R., (1990) "The role of consciousness in second language acquisition" in *Applied Linguistics* 11, 129 – 158.

Swain, MK, (1985) "Communicative competence: some roles of comprehensible input and comprehensible output in its development", in Gass, SM & Madden CG (eds) *Input in Second Language acquisition*, Rowley MA: Newbury House.

Watts, N (1998) "A learner-based design model for interactive multimedia language learning packages", in *System*, Vol 25, No 1, pp1 – 8.

Wild (1996) "Perspectives on the place of educational theory in multi-media" in Hedberg G et al. (eds) *Learning Technologies: prospects and pathways*, selected papers from EdTech 1996. Canberra: AJET

Wittrock, MC (1974) "Learning as a generative process" in *Educational Psychologist*, 11/1: 87-95